

HP ProCurve Switches and Hubs

HP ProCurve

HP ProCurve Switches
1600M, 2424M, 4000M, and 8000M
Management and Configuration Guide



Less Work, More Network
<http://www.hp.com/go/procurve>

HP ProCurve Switches

1600M, 2424M, 4000M, and 8000M

Management and Configuration Guide

**© Copyright 1999 Hewlett-Packard Company
All Rights Reserved.**

This document contains information which is protected by copyright. Reproduction, adaptation, or translation without prior permission is prohibited, except as allowed under the copyright laws.

Publication Number

5969-2320
September 1999

Applicable Product

HP ProCurve Switch 2424M (J4093A)
HP ProCurve Switch 8000M (J4110A)
HP ProCurve Switch 1600M (J4120A)
HP ProCurve Switch 4000M (J4121A)

Trademark Credits

Microsoft, Windows, Windows 95, and Microsoft Windows NT are registered trademarks of Microsoft Corporation. Internet Explorer is a trademark of Microsoft Corporation. Ethernet is a registered trademark of Xerox Corporation. Netscape is a registered trademark of Netscape Corporation.

Disclaimer

The information contained in this document is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the Customer Support/Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Preface

Use of This Guide and Other ProCurve Switch Documentation

This guide describes how to use the browser interface and console interface for the HP ProCurve Switches 1600M, 2424M, 4000M, and 8000M - hereafter referred to individually as the “Switch 1600M, Switch 2424M, Switch 4000M, and Switch 8000M” and collectively as the “Switches 1600M/ 2424M/4000M/ 8000M”).

- If you need information on specific parameters in the switch console interface, refer to the online help provided in the interface.
- If you need information on specific features in the HP Web Browser Interface (hereafter referred to as the “web browser interface”), use the online help available with the web browser interface. For more information on Help options, refer to “Online Help for the HP Web Browser Interface” on page 3-10.
- If you need further information on Hewlett-Packard switch technology, refer to HP’s ProCurve Networking website at:

<http://www.hp.com/go/procurve>

Contents

Preface	iii
Use of This Guide and Other ProCurve Switch Documentation	iii
1 Selecting a Management Interface	
Understanding Management Interfaces	1-1
Advantages of Using the HP Web Browser Interface	1-2
Advantages of Using the Switch Console	1-3
Advantages of Using HP TopTools for Hubs & Switches	1-4
Network Devices	1-4
Network Traffic	1-5
Network Growth	1-5
2 Configuring an IP Address on the Switch	
Methods for Configuring an IP Address and Subnet Mask	2-2
Manually Configuring an IP Address	2-2
Where To Go From Here	2-4
3 Using the HP Web Browser Interface	
Overview	3-1
Web Browser Interface Requirements	3-2
Starting an HP Web Browser Interface Session with the Switch ..	3-3
Using a Standalone Web Browser in a PC or UNIX Workstation ...	3-3
Using HP TopTools for Hubs & Switches	3-4
Tasks for Your First HP Web Browser Interface Session	3-6
Viewing the “First Time Install” Window	3-6
Creating Usernames and Passwords in the Browser Interface	3-8
Using the Passwords	3-9
Using the User Names	3-9
If You Lose a Password	3-9
Online Help for the HP Web Browser Interface	3-10

Support URLs Feature	3-12
Support URL	3-12
Management Server URL	3-13
The Web Browser Interface Screen Layout	3-14
The Overview Window	3-14
The Port Utilization and Status Displays	3-16
Port Utilization	3-16
Port Status	3-18
The Alert Log	3-18
Sorting the Alert Log Entries	3-19
Alert Types	3-20
Viewing Detail Views of Alert Log Entries	3-21
The Alert Control Bar	3-22
The Tab Bar	3-23
Identity Tab	3-23
Status Tab	3-23
Configuration Tab	3-24
Security Tab	3-25
Diagnostics Tab	3-25
Support Tab	3-26
The Status Bar	3-26
Setting Fault Detection Policy	3-27
Working With Fault Detection	3-27

4 Using the Switch Console Interface

Overview	4-1
Starting and Ending a Console Session	4-2
How To Start a Console Session:	4-2
How To End a Console Session:	4-3
Main Menu Features	4-4
Screen Structure and Navigation	4-6
Using Password Security	4-9
To set Manager and Operator passwords:	4-10
Rebooting the Switch	4-12
The Command Prompt	4-14
How To Use the Command Prompt:	4-14

Commands Available	4-15
Set and Show Commands	4-17
Set Commands	4-17
Show Commands	4-18
5 Using HP TopTools or Other SNMP Tools To Monitor and Manage the Switch	
SNMP Management Features	5-1
SNMP Configuration Process	5-3
Advanced Management: RMON and HP Extended RMON Support	5-4
RMON	5-4
Extended RMON	5-4
6 Configuring the Switch	
Overview	6-1
Configuration Features	6-2
IP Configuration	6-4
Configuring IP Addressing from the Web Browser Interface	6-5
Configuring IP Addressing from the Switch Console	6-6
How IP Addressing Affects Switch Operation	6-8
DHCP/Bootp Operation	6-9
Overview	6-9
The DHCP/Bootp Process	6-9
Configuring DHCP/Bootp	6-12
Globally Assigned IP Network Addresses	6-13
SNMP Communities	6-14
Configuring SNMP Communities from the Switch Console	6-14
To View, Edit, or Add SNMP Communities:	6-15
Trap Receivers	6-17
Console/Serial Link	6-19
Configuring the Console/Serial Link from the Switch Console	6-20
Enhancing Security By Configuring Authorized IP Managers ...	6-21
Access Levels	6-21
Defining Authorized Management Stations	6-22
Overview of IP Mask Operation	6-22

Configuring IP Authorized Managers in the Web Browser Interface	6-23
Configuring IP Authorized Managers in the Console Interface	6-23
Building IP Masks	6-24
Configuring One Station Per Authorized Manager IP Entry	6-25
Configuring Multiple Stations Per Authorized Manager IP Entry	6-25
Additional Examples for Authorizing Multiple Stations	6-27
Operating and Troubleshooting Notes	6-27
System Information	6-28
Configuring System Parameters from the Web Browser Interface .	6-28
Configuring System Information from the Console	6-29
Port Settings	6-30
Configuring Port Parameters from the Web Browser Interface	6-32
Configuring Port Parameters from the Switch Console	6-33
Network Monitoring Port Features	6-34
Configuring Port Monitoring from the Web Browser Interface	6-34
Configuring Port Monitoring from the Switch Console	6-36
Spanning Tree Protocol (STP)	6-39
Enabling STP from the Web Browser Interface	6-40
Configuring STP from the Switch Console	6-41
How STP Operates	6-42
STP Fast Mode	6-43
STP Operation with 802.1Q VLANs	6-44
STP Operation with Switch Meshing	6-45
Further Information	6-45
Traffic/Security Filter Features	6-46
Configuring Traffic/Security Filters from the Switch Console	6-46
Filter Types and Operation	6-49
Multicast Filters	6-49
Protocol Filters	6-50
Source Port Filters	6-50
Port-Based Virtual LANs (VLANs)	6-51
Overview of Using VLANs	6-54
VLAN Support and the Default VLAN	6-54
Some Notes on Using VLANs	6-54
Further Information	6-55

Configuring VLAN Parameters from the Switch Console	6-56
To Activate VLANs	6-56
Adding or Editing VLAN Names	6-58
Adding or Changing a VLAN Port Assignment	6-60
VLAN Tagging Information	6-62
Effect of VLANs on Other Switch Features	6-66
Spanning Tree Protocol Operation with VLANs	6-66
IPX and IP Interfaces	6-66
VLAN MAC Addresses	6-67
Port Trunks	6-67
Port Monitoring	6-67
VLANs and Switch Meshing	6-67
VLAN Restrictions	6-68
Symptoms of Duplicate MAC Addresses in VLAN Environments	6-69
Load Balancing: Port Trunking	6-70
Interoperability	6-72
Trunk Configuration Options	6-73
Configuring Port Trunks from the Switch Console	6-73
Operating Information	6-77
Trunk Operation Using the “Trunk” Option	6-77
Trunk Operation Using the “SA-Trunk” Option	6-78
Trunk Operation Using the “FEC” Option	6-79
Load Balancing: Switch Meshing	6-80
Switch Meshing Fundamentals	6-82
Using the Console To Configure Switch Meshing	6-84
Operating Notes for Switch Meshing	6-87
Flooded Traffic	6-87
Unicast Packets with Unknown Destinations	6-88
Spanning Tree Operation with Switch Meshing	6-89
Filtering/Security in Meshed Switches	6-91
IP Multicast (IGMP) in Meshed Switches	6-91
802.1Q VLANs in Meshed Switches	6-91
Using Automatic Broadcast Control In Meshed Switches	6-92
Requirements and Restrictions	6-92
IP Multicast (IGMP) Features—Multimedia Traffic Control	6-95
Configuring IGMP from the Web Browser Interface	6-96
Configuring IGMP from the Switch Console	6-98

How IGMP Operates	6-100
Role of the Switch	6-101
Number of IP Multicast Addresses Allowed	6-104
Interaction with Multicast Traffic/Security Filters.	6-104
Changing the Querier Configuration Setting	6-105
Automatic Broadcast Control (ABC) Features	6-106
Configuring ABC from the Web Browser Interface	6-107
Configuring ABC from the Switch Console	6-108
How ABC Operates	6-113
Reducing ARP Broadcast Traffic	6-113
Reducing RIP and SAP Broadcast Traffic	6-115
Automatic Gateway Configuration for Networks Using DHCP To	
Manage IP Addresses.	6-115
Restrictions	6-116
Configuring and Monitoring Port Security	6-118
Basic Operation	6-118
Configuring Port Security	6-119
Planning	6-119
Using the Web Browser Interface to Configure Port Security .	6-121
Using the Switch Console To Configure Port Security	6-123
Reading and Resetting Intrusion Alarms	6-125
Notice of Security Violations	6-125
How the Intrusion Log Operates	6-128
Operating Notes for Port Security	6-129
Class of Service (CoS): Managing Bandwidth More Effectively	6-130
Definitions	6-131
Basic Operation	6-132
Criteria for Prioritizing Outbound Packets	6-133
How To Configure CoS	6-135
Configuring Class of Service from the Web Browser Interface . . .	6-137
Configuring Class of Service from the Console	6-139
The CoS Device Priority Screen	6-140
The CoS Type of Service (ToS) Priority Screen	6-140
The CoS Protocol Priority Screen	6-141
The CoS VLAN Priority Screen	6-142
Using Type of Service (ToS) Criteria to Prioritize IP Traffic	6-143
IP Multicast (IGMP) Interaction with CoS	6-146
Summary of CoS Operation	6-146

Supporting CoS with an 802.1Q Tagged VLAN Environment	6-151
Using the Default VLAN to Create a Single Tagged VLAN	6-151
Operating and Troubleshooting Notes	6-152

7 Monitoring and Analyzing Switch Operation

Overview	7-1
Status and Counters Screens	7-2
Switch Console Status and Counters Menu	7-3
Web Browser Interface Status Information	7-4
General System Information	7-5
Switch Management Address Information	7-6
Module Information	7-7
Port Status	7-8
Displaying Port Status from the Web Browser Interface	7-8
Displaying Port Status from the Console Interface	7-9
Port Counters	7-10
Displaying Port Counters from the Web Browser Interface	7-11
Displaying Port Counters from the Console Interface	7-12
Address Table	7-14
Port Address Table	7-15
Spanning Tree (STP) Information	7-17
IP Multicast (IGMP) Status	7-19
Automatic Broadcast Control (ABC) Information	7-21
Switch Mesh Information	7-22
VLAN Information	7-23

8 Troubleshooting

Troubleshooting Approaches	8-2
Browser or Console Access Problems	8-3

Unusual Network Activity	8-5
General Problems	8-5
Automatic Broadcast Control Problems	8-6
IGMP-Related Problems	8-7
Switch Mesh Problems	8-7
STP-Related Problems	8-9
VLAN-Related Problems	8-10
Using the Event Log To Identify Problem Sources	8-12
To Change the Severity Level of Event Log Messages	8-15
Diagnostics	8-17
Ping and Link Tests	8-17
Executing Ping or Link Tests from the Web Browser Interface	8-18
Executing Ping or Link Tests from the Switch Console	8-19
The Configuration File	8-21
Browsing the Configuration File from the Web Browser Interface	8-21
.....	8-21
Browsing the Configuration File from the Switch Console	8-22
Using the Command Prompt	8-23
Restoring the Factory Default Configuration	8-24

A File Transfers

Overview	A-1
Downloading an Operating System (OS)	A-1
Using TFTP To Download the OS File	A-2
Using the SNMP-Based HP Download Manager	A-4
Switch-to-Switch Download	A-4
Using Xmodem to Download the OS File	A-5
To Perform the OS Download:	A-5
Troubleshooting TFTP Downloads	A-6
Transferring Switch Configurations	A-8
Using Get and Put To Transfer a Configuration Between the Switch	A-8
and a Networked PC or Unix Workstation	A-8
Using XGet and XPut To Transfer a Configuration Between the	A-8
Switch and a PC or Unix Workstation	A-9

B MAC Address Management

Overview	B-1
Determining the MAC Addresses	B-1
The Base and VLAN MAC Addresses	B-2
Switch Port MAC Addresses	B-3

Index

Selecting a Management Interface

This chapter describes the following:

- Management interfaces for the Switches 1600M/2424M/4000M/8000M
 - Advantages of using each interface
-

Understanding Management Interfaces

Management interfaces enable you to reconfigure the switch and to monitor switch status and performance.

The HP Switches 1600M/2424M/4000M/8000M offer the following interfaces:

- the web browser interface—an interface that is built into the switch and can be accessed using a standard web browser (such as Netscape Navigator or Microsoft Internet Explorer). For specific requirements, see “Web Browser Interface Requirements” on page 3-2.
- the switch console—a VT-100/ANSI console interface built into the switch
- HP TopTools for Hubs & Switches—an easy-to-use, browser-based network management tool that works with HP proactive networking features built into managed HP hubs and switches (included on a CD with the switch at no extra cost)

Each interface consists of a series of management features, accessed either through a menu-driven screen system or a split Window with tab navigation. Each approach has its advantages that are described in the next sections.

This manual describes how to use the web browser interface (chapter 3) and the switch console (chapter 4), and how to configure the switch using either interface (chapter 6).

To use HP TopTools for Hubs & Switches, refer to the *HP TopTools User's Guide* and the TopTools online help, both of which are available on the CD-ROM shipped with your HP switch. For information on the methods for accessing browser interface Help, refer to “Online Help for the Web Browser Interface” on page 3-10.

Advantages of Using the HP Web Browser Interface

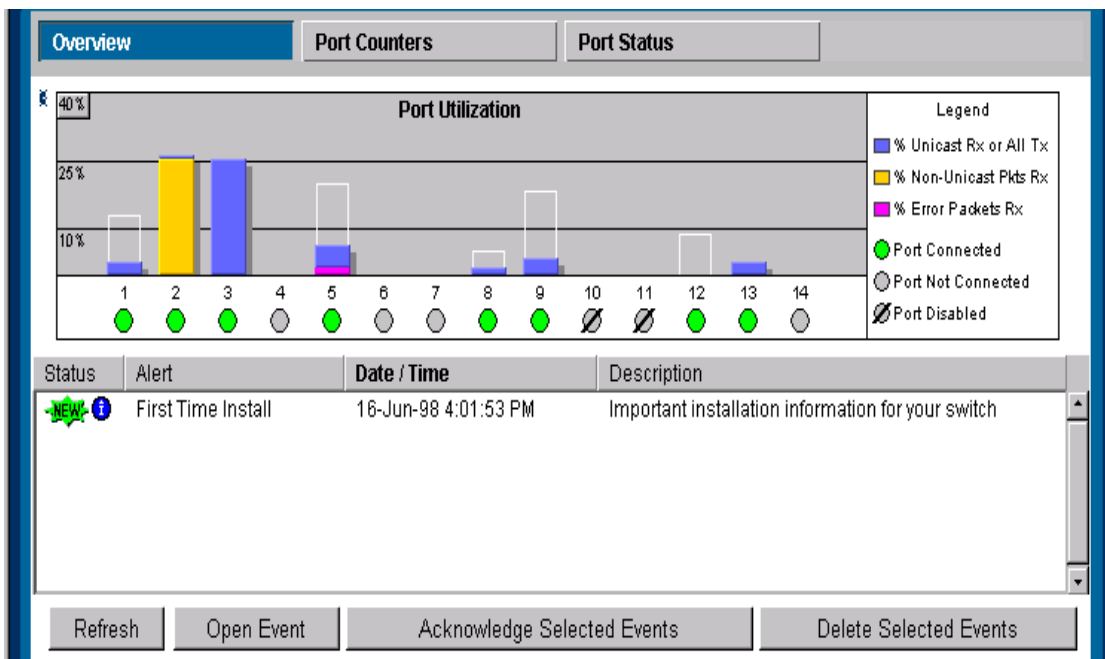


Figure 1-1. Example of the HP Web Browser Interface Display

- **Easy access** to the switch from anywhere on the network
- **Familiar browser interface**—locations of window objects consistent with commonly used browsers, uses mouse clicking for navigation, no terminal setup
- **Many features have all their fields in one screen** so you can view all values at once
- **More visual cues**, using colors, status bars, device icons, and other graphical objects to represent values rather than numeric values
- **Display of acceptable ranges of values available** in configuration list boxes

Advantages of Using the Switch Console

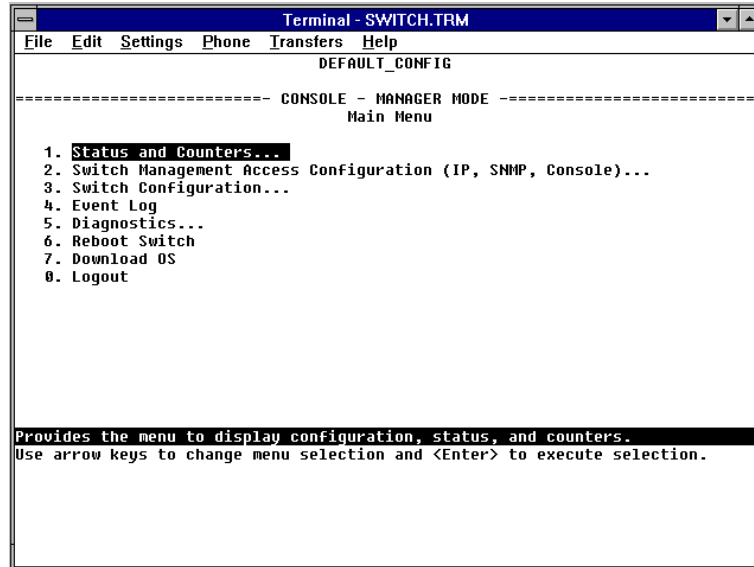


Figure 1-2. Example of the Console Interface Display

- **Contains a complete set of features and parameters**
- **Out-of-band access** (through RS-232 connection) to switch, so network bottlenecks, crashes, lack of configured or correct IP address, and network downtime do not slow or prevent access
- **Ability to configure management access**, for example, creating an IP address, and setting Community Names and Authorized Managers
- **Telnet access** to the full console functionality
- **Faster navigation**, avoiding delays that occur with slower display of graphical objects over a web browser interface
- **More secure**; configuration information and passwords are not seen on the network

Advantages of Using HP TopTools for Hubs & Switches

You can operate HP TopTools from a PC on the network to monitor traffic, manage your hubs and switches, and proactively recommend network changes to increase network uptime and optimize performance. Easy to install and use, HP TopTools for Hubs & Switches is the answer to your management challenges.

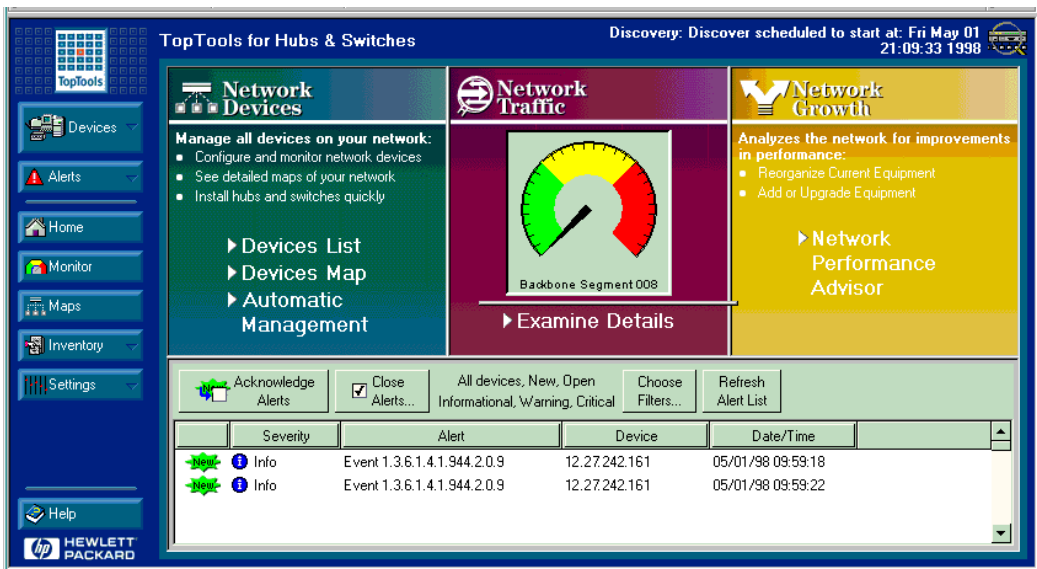


Figure 1-3. Example of HP TopTools Main Screen

HP TopTools for Hubs& Switches has three main sections: Network Devices, Network Traffic, and Network Growth:

Network Devices

- Enables fast installation of hubs and switches.
- Quickly finds and notifies you of the location of problems, saving valuable time.
- Notifies you when HP hubs use “self-healing” features to fix or limit common network problems.

- Identifies users by port and lets you assign easy-to-remember names to any network device.
- Enables you to configure and monitor network devices from your PC.

Network Traffic

- Watches the network for problems.
- Shows traffic and “top talker” nodes on screen.
- Uses traffic monitor diagrams to make bottlenecks easy to see.
- Improves network reliability through real-time fault isolation.
- See your entire network without having to put RMON probes on every segment (up to 1500 segments).

Network Growth

- Monitors, stores, and analyzes network traffic to determine where upgrades are needed.
- Uses Network Performance Advisor to give clear, easy-to-follow plans detailing the most cost-effective way to upgrade your network.

Configuring an IP Address on the Switch

This chapter helps you to quickly assign an IP (Internet Protocol) address and subnet mask to the switch. In the factory default configuration, the switch does not have an IP address and subnet mask, so it can be managed only by using a direct connection to the switch console.

Configuring an IP (Internet Protocol) address and subnet mask enables the switch to operate as a managed device in your network, giving you in-band (networked) access to these interfaces:

- HP web browser interface built into the switch
- HP TopTools for Hubs & Switches—SNMP-based network management software shipped with the switch
- the switch console through a telnet connection

For a listing of switch features available with and without an IP address, refer to “How IP Addressing Affects Switch Operation” on page 6-8.

For more information on this topic, refer to “IP Configuration” on page 6-4.

Note

The IP address and subnet mask assigned for the switch should be compatible with the IP addressing used in your network. If your network is a standalone network, your IP addressing and subnet mask scheme can be set up in any way that meets your local needs. However, if you will be connecting your network to other networks that use globally assigned IP addresses, refer to “Globally Assigned IP Network Addresses” on page 6-13.

Methods for Configuring an IP Address and Subnet Mask

If the switch has not already been configured with an IP address and subnet mask compatible with your network, use either of the following two methods to do so:

- **Manually through the switch console:** This is the easiest method if you have direct-connect or modem access to a terminal emulator on a PC (such as HyperTerminal in Windows 95 or Windows NT), or a direct connection to a VT-100 terminal. Refer to “Manually Configuring an IP Address” below.
- **Configure your DHCP/Bootp server to support the switch:** By default, the switch is configured to acquire an IP address configuration from a DHCP or Bootp server. To use DHCP/Bootp, refer to “DHCP/Bootp Operation” on page 6-9.

Manually Configuring an IP Address

This section describes how to use the switch console to configure an IP address. The following assumes that no VLANs have been configured on the switch.

Note

In its factory default configuration, all ports on the switch belong to one, default virtual LAN (VLAN), and only one IP address is needed. If you configure the switch with more than one VLAN, each VLAN may have its own IP address. For more on VLANs, refer to “Port-Based Virtual LANs (VLANs)” on page 6-51.

1. Use the instructions in your switch installation manual to connect a PC running a terminal emulator, or a terminal, to the Console port on the switch, and display the Main Menu.
2. From the Main Menu, select

2. Switch Management Access Configuration

1. IP Configuration

You will see a screen similar to the one shown in figure 2-1.

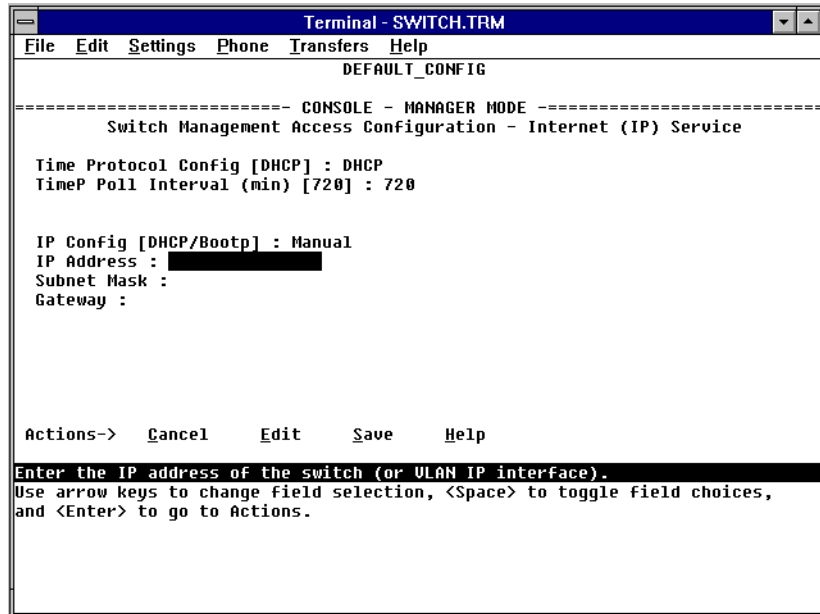


Figure 2-1. The Internet (IP) Service Screen

3. Press **E** to select **Edit**, then use the down arrow key (**↓**) to select **IP Config [DHCP/BOOTP]**.
4. Use the Space bar to display **Manual** for this field.
5. Press the down arrow key (**↓**) to display the three IP configuration parameters and select the **IP Address** field.
6. Enter the IP address you want to assign to the switch.
7. Select the **Subnet Mask** field and enter the subnet mask for your network.
8. If you want to reach off-subnet destinations, select the **Gateway** field and enter the address of the gateway router for your subnet.
9. Press **Enter**, then **S** (for **Save**), then proceed with any other console tasks.

Where To Go From Here

The above procedure configures your switch with an IP address and subnet mask. With the proper network connections, you can now manage the switch from a network management station or from a PC equipped with a web browser.

- To access the switch using a web browser, refer to chapter 3, “Using the HP Web Browser Interface”.
- To continue to use the console interface, refer to chapter 4, “Using the Switch Console Interface”.
- To access the switch using a network management tool, refer to chapter 5, “Using HP TopTools or Other SNMP Tools to Monitor and Manage the Switch”.
- Inbound telnet access to the switch is enabled in the factory default.
 - To change the current telnet access parameter, turn to “Configuring the Console/Serial Link from the Switch Console” on page 6-20.
 - To use telnet to access the switch console, refer to “Starting and Ending a Console Session” on page 4-2.

You can also start a telnet session to the switch console from the web browser interface. Click on the **Configuration** tab in the web browser interface, then click on **telnet session to the switch console**. If you need information on how to access the switch via the web browser interface, refer to chapter 3, “Using the HP Web Browser Interface”.

- For problems or error indications, refer to chapter 8, “Troubleshooting”.

Using the HP Web Browser Interface

Overview

The HP web browser interface built into the switch lets you easily access the switch from a browser-based PC on your network. This lets you do the following:

- optimize your network uptime by using the Alert Log and other diagnostic tools
- make configuration changes to the switch
- maintain security by configuring usernames and passwords

Using the web browser interface to configure the switch is covered in chapter 6, “Configuring the Switch”. This chapter covers the following:

- system requirements for using the web browser interface (page 3-2)
- starting a web browser interface session (page 3-3)
- tasks for your first web browser interface session (page 3-6):
 - creating usernames and passwords in the web browser interface (page 3-8)
 - selecting the fault detection configuration for the Alert Log operation (page 3-27)
 - getting access to online help for the web browser interface (page 3-10)
- description of the web browser interface:
 - the Overview window and tabs (page 3-14)
 - the Port Utilization and Status displays (page 3-16)
 - the Alert Log and Alert types (page 3-18)
 - setting the Fault Detection Policy (page 3-27)

Note

If you want security beyond that achieved with user names and passwords, you can disable access to the web browser interface. This is done by changing the **Web Agent Enabled** parameter setting in the Serial Link configuration screen in the switch console. See “Console/Serial Link” on page 6-19.

Web Browser Interface Requirements

You can use equipment meeting the following requirements to access the web browser interface on your intranet.

Table 3-1. System Requirements for Accessing the HP Web Browser Interface

Platform Entity and OS Version	Minimum	Recommended
PC Platform	90 MHz Pentium	120 MHz Pentium
HP-UX Platform (9.x or 10.x)	100 MHz	120 MHz
RAM	16 Mbytes	32 Mbytes
Screen Resolution	800 X 600	1,024 x 768
Color Count	256	65,536
Internet Browser* (English-language browser only)	PCs: <ul style="list-style-type: none"> • Netscape® Communicator 4.x • Microsoft®Internet Explorer 4.x UNIX: Netscape Navigator 3.1 or later	PCs: <ul style="list-style-type: none"> • Netscape Communicator 4.03 or later • Microsoft®Internet Explorer 4.01, SP1 or later UNIX: Netscape Navigator 4.03 or later
PC Operating System	Microsoft Windows®95 and Windows NT	
UNIX®Operating System	Standard UNIX®OS	
HP TopTools for Hubs & Switches (Optional)	use product HP J2569M or later	
*For notes on using Netscape and Microsoft web browsers, go to HP's ProCurve Networking web site, http://www.hp.com/go/procurve .		

Starting an HP Web Browser Interface Session with the Switch

You can start a web browser session in the following ways:

- Using a standalone web browser on a network connection from a PC or UNIX workstation:
 - directly connected to your network.
 - connected through remote access to your network.
- Using a management station running HP TopTools for Hubs & Switches on your network.

Note

HP TopTools is designed for installation on a network management workstation. For this reason, the HP TopTools system requirements are different from the system requirements for accessing the switch's web browser interface from a non-management PC or workstation. For HP TopTools requirements, refer to the information printed on the sleeve in which the HP TopTools CD is shipped, or to the system requirements information in the user's guide included on the HP TopTools CD.

Using a Standalone Web Browser in a PC or UNIX Workstation

This procedure assumes that you have a supported web browser (page 3-2) installed on your PC or workstation, and that an IP address has been configured on the switch. (For more on assigning an IP address, refer to chapter 2, "Configuring an IP Address on the Switch".)

1. Make sure the Java™ applets are enabled for your browser. If they are not, do one of the following:
 - In Netscape 4.03, click on **Edit, Preferences..., Advanced**, then select **Enable Java** and **Enable JavaScript** options.
 - In Microsoft Internet Explorer 4.x, click on **View, Internet Options, Security, Custom, Settings** and scroll to the **Java Permissions**. Then refer to the online Help for specific information on enabling the Java applets.

2. Type the IP address (or DNS name) of the switch in the browser **Location or Address** field and press . (It is not necessary to include `http://`.)

switch4000 (example of a DNS-type name)

10.11.12.195 (example of an IP address)

If you are using a Domain Name Server (DNS), your device may have a name associated with it (for example, **switch4000**) that you can type in the **Location or Address** field instead of the IP address. Using DNS names typically improves browser performance. See your network administrator for any name associated with the switch.

The web browser interface automatically starts with the Status Overview window displayed for the selected device as shown in figure 3-1 on page 3-5.

Using HP TopTools for Hubs & Switches

For information on HP TopTools web browser and system requirements, refer to the information printed on the sleeve in which the HP TopTools CD is shipped, or to the system requirements information in the user's guide included on the HP TopTools CD.

This procedure assumes that:

- You have installed the web browser recommended for HP TopTools on a PC or workstation that serves as your network management station.
- The networked device you want to access has been assigned an IP address and (optionally) a DNS name and has been discovered by HP TopTools. (For more on assigning an IP address, refer to chapter 2, "Configuring an IP Address on the Switch".)

To establish a web browser session with HP TopTools running, do the following on the network management station:

1. Make sure the Java™ applets are enabled for your web browser. If they are not, refer to the web browser online Help for specific information on enabling the Java applets.
2. Do *one* of the following tasks:
 - On the HP TopTools Maps view, double-click on the symbol for the networking device that you want to access.
 - In HP TopTools, in the Topology Information dialog box, in the device list, double-click on the entry for the device you want to access (IP address or DNS name).

- The web browser interface automatically starts with the Status Overview window displayed for the selected device, as shown in figure 3-1.

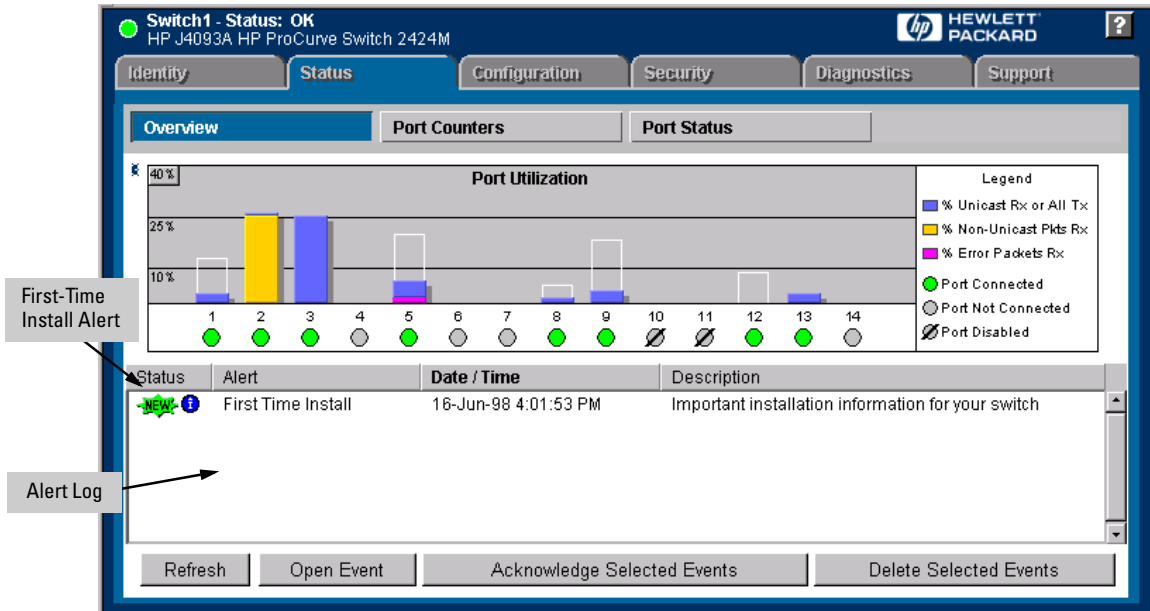


Figure 3-1. Status Overview Screen

Tasks for Your First HP Web Browser Interface Session

The first time you access the web browser interface, there are three tasks that you should perform:

- Review the “First Time Install” window
- Set Manager and Operator passwords
- Set access to the web browser interface online help

Viewing the “First Time Install” Window

When you access the switch’s web browser interface for the first time, the Alert log contains a “First Time Install” alert, as shown in figure 3-1. This gives you information about first time installations, and provides an immediate opportunity to set passwords for security and to specify a Fault Detection policy, which determines the types of messages that will be displayed in the Alert Log.

Double click on **First Time Install** in the Alert log (see above). The web browser interface then displays the “First Time Install” window, as shown in figure 3-2.

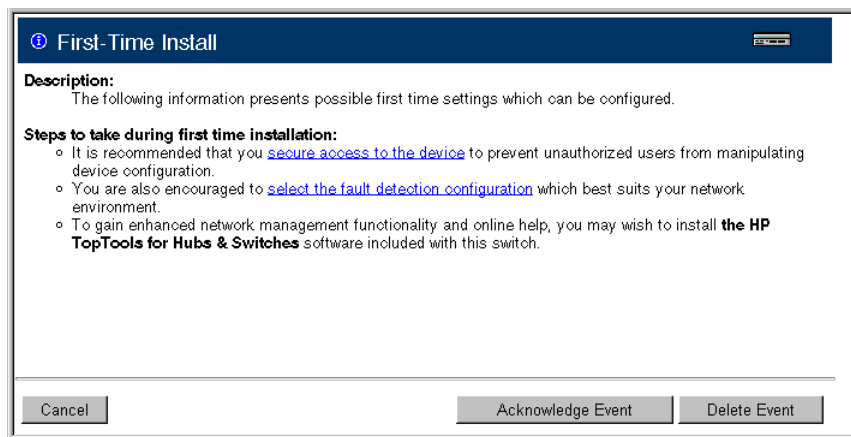


Figure 3-2. First-Time Install Window

This window is the launching point for the basic configuration you need to perform to set web browser interface passwords to maintain security and Fault Detection policy, which determines the types of messages that will be displayed in the Alert Log.

To set web browser interface passwords, click on the jump string **secure access to the device** to display the Device Passwords screen, and then go to the next page. You can also access the password screen by clicking on the Security tab.

To set Fault Detection policy, click on the jump string **select the fault detection configuration** in the second bullet in the window and go to the section, “Setting Fault Detection Policy” on page 3-27.

Creating Usernames and Passwords in the Browser Interface

You may want to create both a username and password to create access security for your switch. There are two levels of access to the interface that can be controlled by setting user names and passwords:

- **Operator.** An Operator-level user name and password allows read-only access to most of the web browser interface, but prevents access to the Security window.
- **Manager.** A Manager-level user name and password allows full read/write access to the web browser interface.

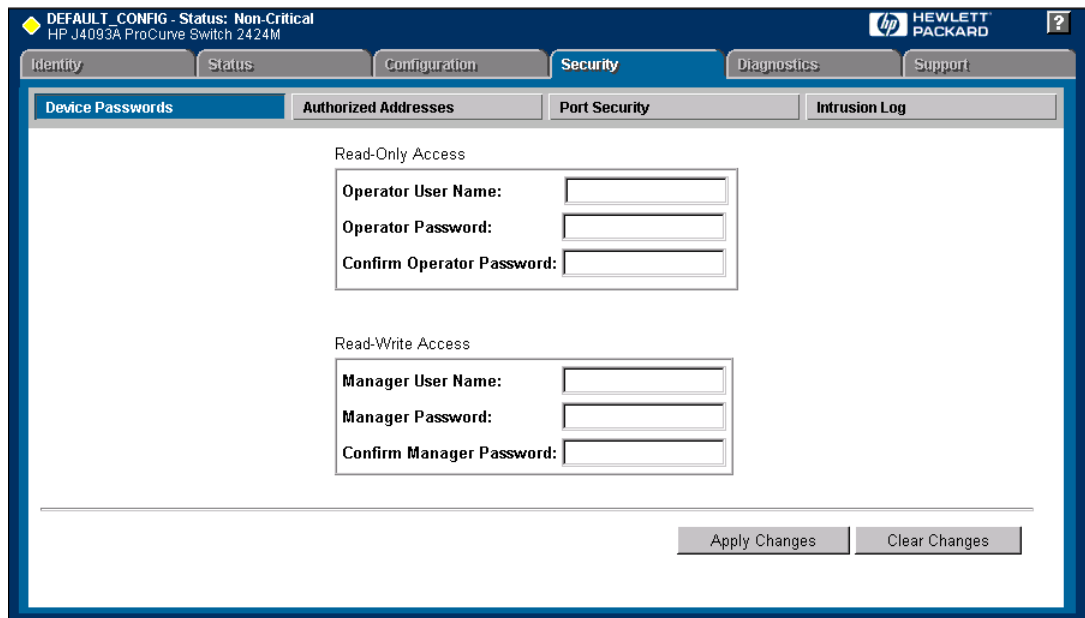


Figure 3-3. The Device Passwords Window

To set the passwords:

1. Access the Device Passwords screen by one of the following methods:
 - If the Alert Log includes a “First Time Install” event entry, double click on this event, then, in the resulting display, click on the **secure access to the device** link.
 - Select the Security tab.

2. Click in the appropriate box in the Device Passwords window and enter user names and passwords. You will be required to repeat the password strings in the confirmation boxes.

Both the user names and passwords can be up to 16 printable ASCII characters.

3. Click on to activate the user names and passwords.

Note

Strings you assign in the web browser interface will overwrite previous access strings assigned in either the web browser interface or the switch console.

Using the Passwords

The manager and operator passwords are used to control access to both the web browser interface and the switch console. Once set, you will be challenged to supply the password every time you try to access either the web browser interface or switch console. The password you enter determines the capability you have during that session:

- Entering the manager password gives you full read/write capabilities
- Entering the operator password gives you read and limited write capabilities.

Using the User Names

If you also set user names in the web browser interface screen, you must supply the correct user name for web browser interface access, but switch console access requires only the password. If a user name has not been set, you must leave the User Name field in the web browser interface access popup blank.

The switch console uses only the passwords and does not prompt you for the User Names.

If You Lose a Password

If you lose the passwords, you can clear them by pressing the Clear button on the front of the switch. This action deletes all password and user name protection for both the web browser interface and the switch console.

The Clear button is provided for your convenience, but its presence means that if you are concerned with the security of the switch configuration and operation, you should make sure the switch is installed in a secure location, such as a locked wiring closet.

Online Help for the HP Web Browser Interface

Online Help is available for the web browser interface. You can use it by clicking on the question mark in the upper right corner of any of the web browser interface screens. Context-sensitive help is provided for the screen you are on.

Providing Online Help. *The Help files are automatically available if you install HP TopTools for Hubs & Switches on your network or if you already have Internet access to the World Wide Web. (The Help files are included with HP TopTools for Hubs & Switches, and are also automatically available from HP via the World Wide Web.)*

Retrieval of the Help files as described above is controlled by automatic entries to the **Management Server URL** field on the **Configuration / Support URLs** screen, shown in figure 3-4. The switch is shipped with the URL set to retrieve online Help from the HP World Wide Web site. However, if HP TopTools for Hubs & Switches is installed on a management station on your network and discovers the switch, the Management Server URL is automatically changed to retrieve the Help from your TopTools management station.

If Online Help Fails To Operate. Do one of the following:

- If HP TopTools for Hubs & Switches is installed and running on your network, enter the IP address or DNS name of the network management station in the Management Server URL field shown in figure 3-4 on page 3-11.
- If you have World Wide Web access from your PC or workstation, and do not have HP TopTools installed on your network, enter the following URL in the Management Server URL field shown in figure 3-4 on page 3-11:

http://www.hp.com/rnd/device_help

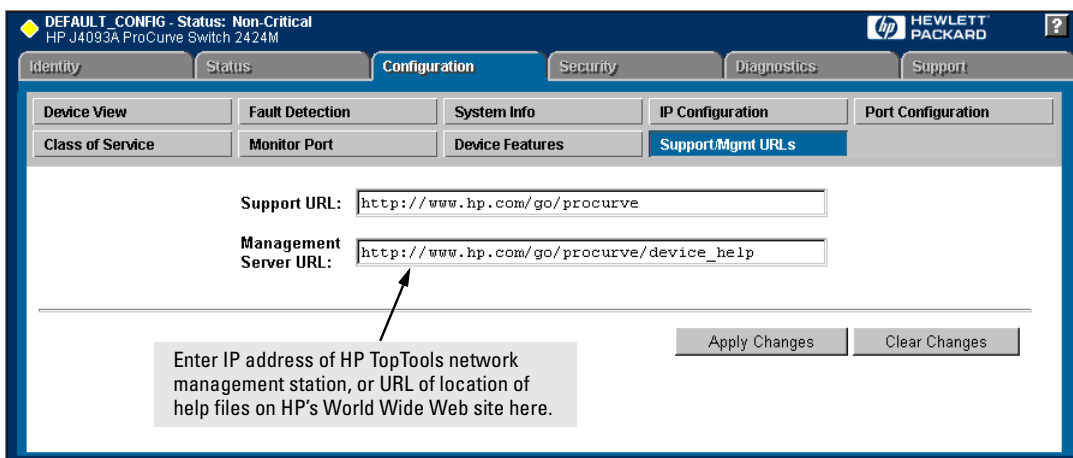


Figure 3-4. How To Access Web Browser Interface Online Help

If you do not have HP TopTools for Hubs and Switches installed on your network and do not have an active connection to the World Wide Web, then Online help for the web browser interface will not be available.

See also “Support URLs Feature” on the next page.

Support URLs Feature

The Support/Mgmt URLs window enables you to change the World Wide Web Universal Resource Locator (URL) for two functions:

- **Support URL** – a support information site for your switch
- **Management Server URL** – the site for online help for the web browser interface, and, if set up, the URL of a network management station running HP TopTools for Hubs & Switches.

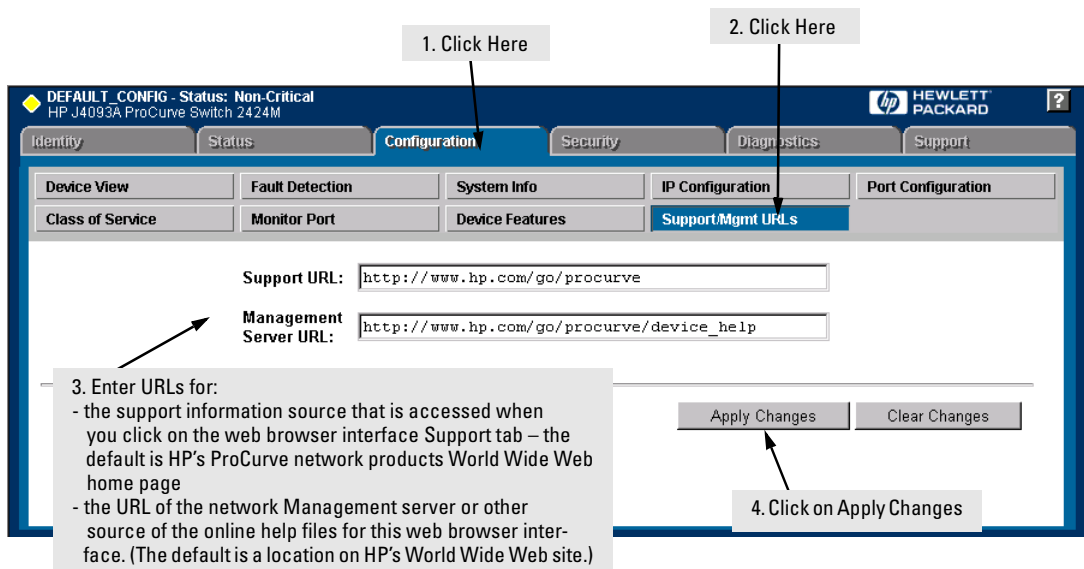


Figure 3-5. The Default Support/Mgmt URLs Window

Support URL

This is the site that will be accessed when you click on the **Support** tab on the web browser interface. The default URL is:

<http://www.hp.com/go/procurve>

which is the World Wide Web site for Hewlett-Packard's networking products.

Click on the button on that page and you can get to support information regarding your switch, including white papers, operating system (OS) updates, and more.

You could instead enter the URL for a local site that you use for entering reports about network performance, or whatever other function you would like to be able to easily access by clicking on the tab.

Management Server URL

This field specifies which of the following two locations the switch will use to find online Help for the web browser interface:

- The URL of online Help provided by HP on the world wide web
- The URL of a network management station running HP TopTools for Hubs & Switches

The default URL is:

http://www.hp.com/rnd/device_help

which is the location on HP's World Wide Web site of the help files for the web browser interface. To use this site, you must have a modem link or other access to the World Wide Web operating when you run the web browser interface. Then, when you click on the button on any of the web browser interface screens, the context sensitive help for that screen will be retrieved from HP.

Alternatively, if you install HP TopTools for Hubs & Switches on your network and TopTools discovers your switch, it automatically overwrites the Management Server URL field with the address or name of the TopTools management station. In this case, online help will automatically be provided from the network management station. Refer to "Online Help for the HP Web Browser Interface" on page 3-10.

Additionally, HP Top Tools for Hubs & Switches has the capability to perform network-wide policy management and configuration of your switch. This field identifies the management station that is performing that function. For more information, refer to the documentation provided on the HP TopTools CD shipped with the switch.

The Web Browser Interface Screen Layout

This section describes the elements of the web browser interface screen layout starting with the first screen you see, the Status, Overview window.

The Overview Window

The Overview Window is the home screen for any entry into the web browser interface. The following figure identifies the various parts of the screen.

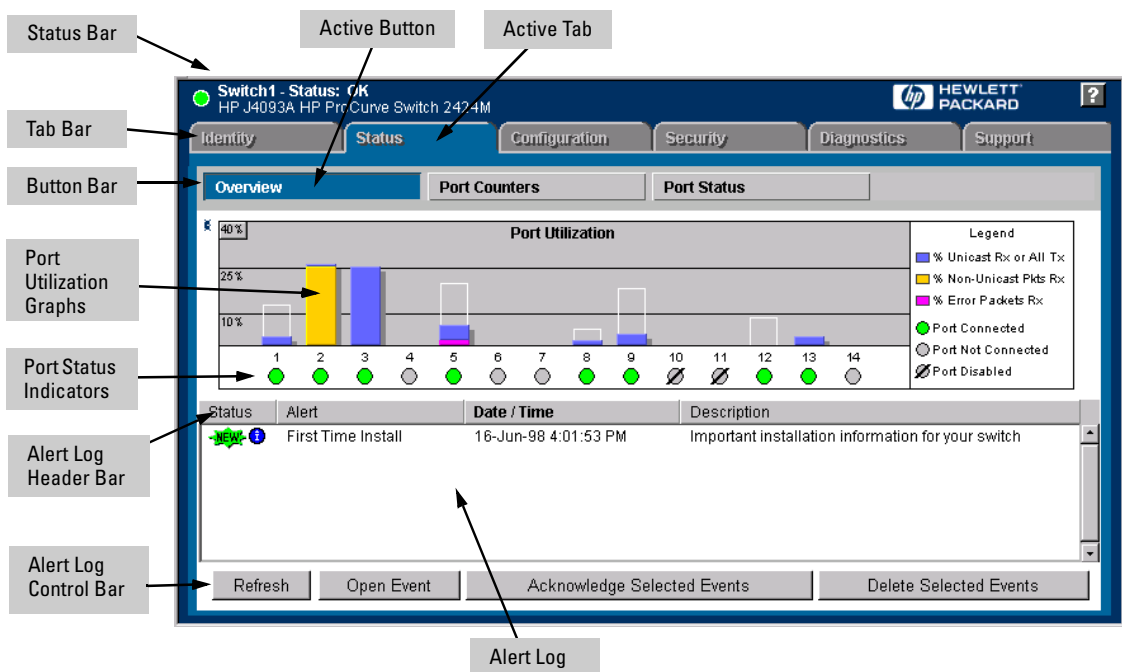


Figure 3-6. The Overview Window

The areas and fields in the web browser interface Overview Window are described on the next page.

- **Tab Bar.** The row of tabs displaying all the top level menus for the web browser interface.
- **Active Tab.** The current tab selected. The tab is darkened and all the buttons under the tab are displayed.
- **Status Bar.** The region above the Tab Bar that displays status and device name information.
- **Port Utilization and Status Displays.** The region containing graphs that indicate network traffic on each switch port and symbols indicating the status of each port.
- **Button Bar.** The row of buttons that are contained within the Active Tab.
- **Active Button.** The current button selected. The button is darkened and the window associated with the button is displayed.
- **Alert Log.** A list of all events, or alerts, that can be retrieved from the switch's firmware at the current time. Information associated with the alerts is displayed, including Status, Alert Name, the date and time the Alert was reported by the switch, and a short description of the alert. You can double click on any of the entries in the log and get a detailed description. See "The Alert Log" on page 3-18.
- **Alert Log Header Bar.** The row of column heads running across the top of the Alert Log.
- **Alert Log Control Bar.** The region at the bottom of the Alert Log containing buttons that enable you to refresh the Alert Log to display all alerts that have been reported since you first displayed the log. Also available in the bar are a button to acknowledge new alerts and a button to delete alerts.

The Port Utilization and Status Displays

The Port Utilization and Status displays show an overview of the status of the switch and the amount of network activity on each port. The following figure shows a sample reading of the Port Utilization and Port Status.

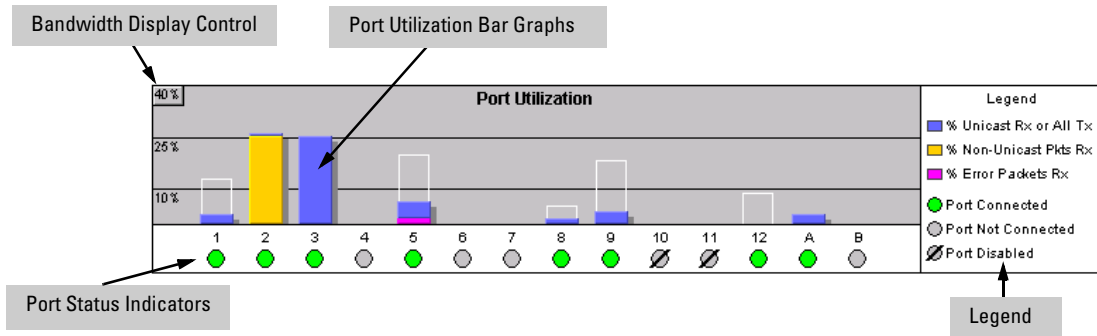


Figure 3-7. The Graphs Area

Port Utilization

The Port Utilization bar graphs show the network traffic on the port with a breakdown of the packet types that have been detected (unicast packets, non-unicast packets, and error packets). The Legend identifies traffic types and their associated colors on the bar graph:

- **% Unicast Rx & All Tx:** This is all unicast traffic received and all transmitted traffic of any type. This indicator (a blue color on many systems) can signify either transmitted or received traffic.
- **% Non-Unicast Pkts Rx:** All multicast and broadcast traffic received by the port. This indicator (a gold color on many systems) enables you to know “at-a-glance” the source of any non-unicast traffic that is causing high utilization of the switch. For example, if one port is receiving heavy broadcast or multicast traffic, all ports will become highly utilized. By color-coding the received broadcast and multicast utilization, the bar graph quickly and easily identifies the offending port. This makes it faster and easier to discover the exact source of the heavy traffic because you don’t have to examine port counter data from several ports.
- **% Error Pkts Rx:** All error packets received by the port. (This indicator is a reddish color on many systems.) Although errors received on a port are not propagated to the rest of the network, a consistently high number of errors on a specific port may indicate a problem on the device or network segment connected to the indicated port.

A network utilization of 40% is considered the maximum that a typical Ethernet-type network can experience before encountering performance difficulties. If you observe utilization that is consistently higher than 40% on any port, click on the Port Counters button to get a detailed set of counters for the port.

- **Maximum Activity Indicator:** As the bars in the graph area change height to reflect the level of network activity on the corresponding port, they leave an outline to identify the maximum activity level that has been observed on the port.

To change the amount of bandwidth the Port Utilization bar graph shows. Click on the bandwidth display control button in the upper left corner of the graph. (The button shows the current scale setting, such as 40%.) In the resulting menu, select the bandwidth scale you want the graph to show (3%, 10%, 25%, 40%, 75%, or 100%), as shown in figure 3-7.

Note that when viewing activity on a gigabit port, you may want to select a lower value (such as 3% or 10%). This is because the bandwidth utilization of current network applications on gigabit links is typically minimal, and may not appear on the graph if the scale is set to show high bandwidth utilization.

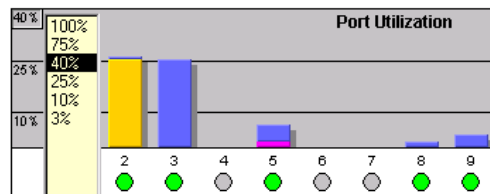


Figure 3-8. Changing the Graph Area Scale

To display values for each graph bar. Hold the mouse cursor over any of the bars in the graph, and a pop-up display is activated showing the port identification and numerical values for each of the sections of the bar, as shown in figure 3-9.

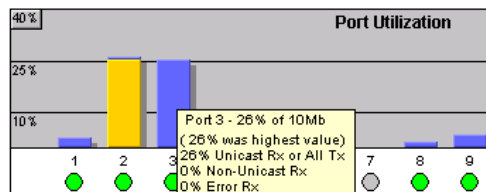


Figure 3-9. Display of Numerical Values for the Bar

Port Status

The Port Status indicators show a symbol for each port that indicates the general status of the port. There are four possible statuses:

- **Port Connected** – the port is enabled and is properly connected to an active network device.
- **Port Not Connected** – the port is enabled but is not connected to an active network device. A cable may not be connected to the port, or the device at the other end may be powered off or inoperable, or the cable or connected device could be faulty.
- **Port Disabled** – the port has been configured as disabled through the web browser interface, the switch console, or SNMP network management.
- **Port Fault-Disabled** – a fault condition has occurred on the port that has caused it to be auto-disabled. Note that the Port Fault-Disabled symbol will be displayed in the legend only if one or more of the ports is in that status. See chapter 7, “Monitoring and Analyzing Switch Operation” for more information.

The Alert Log

The web browser interface Alert Log, shown in the lower half of the screen, shows a list of network occurrences, or *alerts*, that were detected by the switch. Typical alerts are, **Broadcast Storm**, indicating an excessive number of broadcasts received on a port, and **Problem Cable**, indicating a faulty cable. A full list of alerts is shown in the table on page 3-20.

Status	Alert	Date / Time	Description
	Excessive CRC/alignment errors	16-Sep-99 7:58:44 AM	Excessive CRC/Alignment errors on port: 8.
	First time installation	13-Sep-99 3:36:29 PM	Important installation information for your switch

Refresh Open Event Acknowledge Selected Events Delete Selected Events

Figure 3-10. The Alert Log

Each alert has the following fields of information:

- **Status** – The level of severity of the event generated. Severity levels can be Information, Normal, Warning, and Critical. If the alert is new (has not yet been acknowledged), the New symbol is also in the Status column.
- **Alert** – The specific event identification.
- **Date/Time** – The date and time the event was received by the web browser interface. This value is shown in the format: **DD-Mon-YY HH:MM:SS AM/PM**, for example, **16-Sep-99 7:58:44 AM**.
- **Description** – A short narrative statement that describes the event. For example, **Excessive CRC/Alignment errors on port: 8**.

Sorting the Alert Log Entries

The alerts are sorted, by default, by the Date/Time field with the most recent alert listed at the top of the list. The second most recent alert is displayed below the top alert and so on. If alerts occurred at the same time, the simultaneous alerts are sorted by order in which they appear in the MIB.

The alert field that is being used to sort the alert log is indicated by which column heading is in bold. You can sort by any of the other columns by clicking on the column heading. The Alert and Description columns are sorted alphabetically, while the Status column is sorted by severity type, with more critical severity indicators appearing above less critical indicators.

Alert Types

The following table lists the types of alerts that can be generated.

Table 3-2. Alert Strings and Descriptions

Alert String	Alert Description
First Time Install	Important installation information for your switch.
Too many undersized/giant packets	A device connected to this port is transmitting packets shorter than 64 bytes or longer than 1518 bytes (longer than 1522 bytes if tagged), with valid CRCs (unlike runts, which have invalid CRCs).
Excessive jabbering	A device connected to this port is incessantly transmitting packets (“jabbering”), detected as oversized packets with CRC errors.
Excessive CRC/alignment errors	A high percentage of data errors has been detected on this port. Possible causes include: <ul style="list-style-type: none">• Faulty cabling or invalid topology.• Duplex mismatch (full-duplex configured on one end of the link, half-duplex configured on the other)• A malfunctioning NIC, NIC driver, or transceiver
Excessive late collisions	Late collisions (collisions detected after transmitting 64 bytes) have been detected on this port. Possible causes include: <ul style="list-style-type: none">• An overextended LAN topology• Duplex mismatch (full-duplex configured on one end of the link, half-duplex configured on the other)• A misconfigured or faulty device connected to the port
High collision or drop rate	A large number of collisions or packet drops have occurred on the port. Possible causes include: <ul style="list-style-type: none">• A extremely high level of traffic on the port• Duplex mismatch• A misconfigured or malfunctioning NIC or transceiver on a device connected to this port• A topology loop in the network
Excessive broadcasts	An extremely high percentage of broadcasts was received on this port. This degrades the performance of all devices connected to the port. Possible causes include: <ul style="list-style-type: none">• A network topology loop—this is the usual cause• A malfunctioning device, NIC, NIC driver, or software package
Network Loop	Network loop has been detected by the switch.
Loss of Link	Lost connection to one or multiple devices on the port.

Note

When troubleshooting the sources of alerts, it may be helpful to check the switch's Port Status and Port Counter windows (page 7-8 and page 7-10) and the Event Log in the console interface (page 8-12).

Viewing Detail Views of Alert Log Entries

By double clicking on Alert Entries, the web browser interface displays a Detail View or separate window detailing information about the events. The Detail View contains a description of the problem and a possible solution. It also provides four management buttons:

- **Acknowledge Event** – removes the New symbol from the log entry
- **Delete Event** – removes the alert from the Alert Log
- **Retest Button** – polls the switch again to determine whether or not the alert can be regenerated.
- **Cancel Button** – closes the detail view with no change to the status of the alert and returns you to the Overview screen.

A sample Detail View describing an Excessive CRC/Alignment Error alert is shown here.

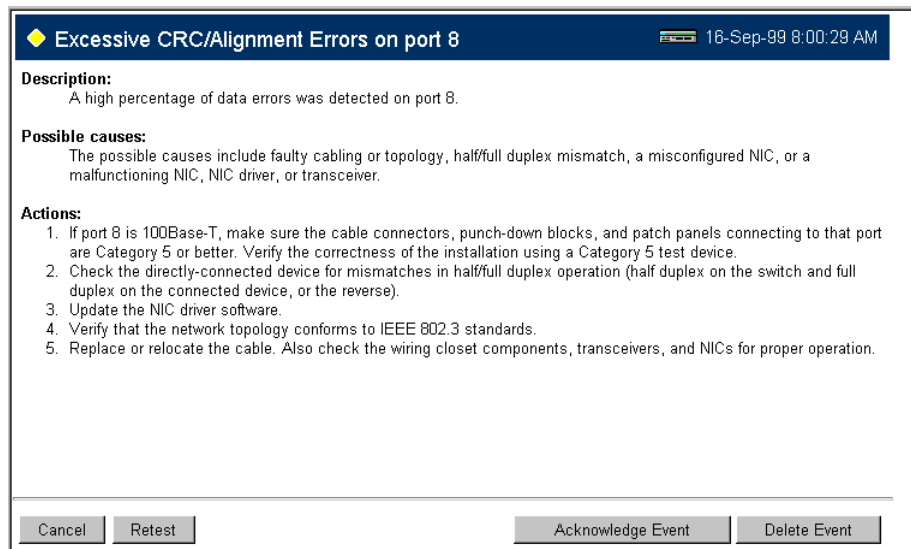


Figure 3-11. Alert Log Detail View

The Alert Control Bar

The Alert Control Bar appears at the bottom of the Alert Log and contains buttons that enable you to manage the Overview Window.



The buttons in the control bar are:

- **Refresh** – redraws the Alert Log screen and displays new alerts that have occurred since you opened or last refreshed this window.
- **Open Event** – displays the detailed view of the highlighted alert; the same as double-clicking on the alert.
- **Acknowledge Selected Events** – removes the New symbol from the entry. This feature is useful if you have more than one system administrator working on a problem. It shows that someone has looked at it.

If an alert has not been acknowledged, the **New** label continues to appear in the Status column to the left of the Status Indicator. Once the alert has been acknowledged from either the Alert Log screen or the Detailed View screen, the New label is removed.

- **Delete Selected Events** – removes an alert from the Alert Log.

The Tab Bar

The Tab bar in the web browser interface contains six tabs, four of which launch button bars which launch specific functional windows. One tab, Identity, launches a dedicated functional window with no buttons. Another tab, Support, launches a separate web page with support information.

To navigate through the different features of the web browser interface, click on the appropriate tab in the Tab Bar. The tabs are as follows:

Identity Tab



This tab displays the Identity Window which is a source of quick information about the switch.

- **Editable Information (System Name, Location, and Contact)** – is maintained in the Administration dialog box.
- **Read-Only Information** – The **System Up Time** shows the elapsed time since the switch was last rebooted. **Product** is the switch product name. **Version** is the software (operating system) version currently running in the switch. **IP Address** is the IP address assigned to the switch. **Management Server** is the currently assigned Management Server URL (page 3-12).

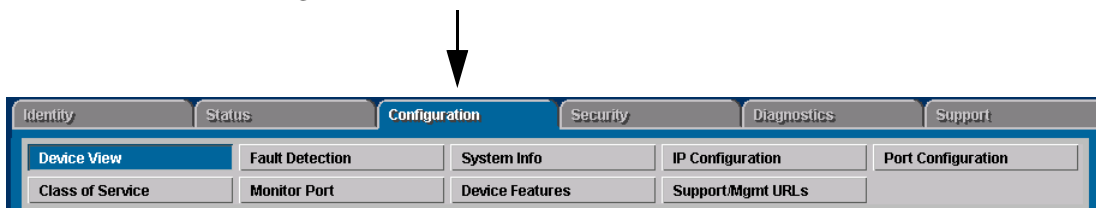
Status Tab



This tab displays the Status Button bar which contains buttons that display switch settings and statistics that represent recent switch behavior. The buttons are:

- **Overview** – the home position for the web browser interface. Displays the screen shown in figure 3-6.
- **Port Counters** – displays a summary of the network activity statistics for all the switch ports, with access to detailed port-level statistics
- **Port Status** – displays a summary table of the operational status of all the switch ports

Configuration Tab



This tab displays the Configuration Button bar which contains buttons that launch screens for setting or changing some of the switch configuration. The buttons are:

- **Device View.** Displays a graphical representation of the front panel of the device, allowing you enable and disable ports on the device by clicking on port graphics and an enable or disable port button. This view also lets you Telnet to the switch console. See the online Help for this view.
- **Fault Detection.** Controls the alert log sensitivity, and port disabling.
- **System Information.** Enables you to view and set system information for a selected device.
- **IP Configuration.** Lets you view or change the existing value for an IP address, subnet mask, and the gateway address for the switch. (Note that changing the IP address from the web browser interface will cause you to lose the current connection to the switch.)
- **Port Configuration.** Lets you enable and disable ports in addition to viewing the security and source address information.
- **Class of Service.** Lets you configure the switch Class of Service features to set the priority for traffic from specific devices, protocols, VLANs, or based on the contents of the IEEE 802.3 Type of Service packet field.
- **Monitor Port.** Lets you designate a port for monitoring traffic on one or more other ports or on a VLAN configured on the switch.
- **Device Features.** Lets you enable or disable Spanning Tree Protocol (STP), Automatic Broadcast Control (ABC), and IP Multicast (IGMP).
- **Support/Mgmt URLs.** Specifies the URL of the web site that will be automatically accessed when you open the Support tab, and the URL for the source of online Help for the web browser interface (page 3-12). The Support URL is configured to automatically access HP's ProCurve networking products website on the World Wide Web. However, if you have an internal support structure, you may wish to change the Support URL to access that structure.

Security Tab



This tab displays the Security Button bar which contains buttons that enable you to view and set switch security features. The buttons displayed are:

- **Device Passwords.** Enables you to set operator and manager-level user names and passwords for the switch.
- **Authorized Addresses.** Enables you to authorize which stations (PCs or workstations) are allowed to access the switch's web browser interface, telnet into the switch's console interface, and perform TFTP transfers of configurations and software updates into the switch.
- **Port Security.** Enables you to configure each switch port with a list of the MAC addresses of devices that are authorized to access the network through that port.
- **Intrusion Log.** Displays the list of any devices that have attempted to access the network through the switch but are not authorized to do so. Authorization is set through the Port Security tab.

Diagnostics Tab



This tab displays the Diagnostics Button bar which contains buttons that enable you to perform troubleshooting tasks for your switch. The buttons are:

- **Ping/Link Test.** Enables you to send test packets to devices connected to a port, using both the IP address (Ping) and the MAC address (Link) as criteria for a valid connection.
- **Device Reset.** Causes the switch to reset its state as though it were powered on and off.
- **Configuration Report.** Displays a master list of various settings for the switch, including information about port status, authorized managers, community names, backup links, IP addresses, security configuration, and general system information.

Support Tab



This tab displays the web page for support information. The URL for this page is set in the **Configuration | Support/Mgmt URLs** option. By default, it is set to Hewlett-Packard's ProCurve web site, but you can change it to the URL for another location, such as an internal support resource. See also page 3-10 and "Support URLs Feature" on page 3-12.

The Status Bar

The Status Bar is displayed in the upper left corner of the web browser interface screen. Figure 3-12 shows an expanded view of the status bar.

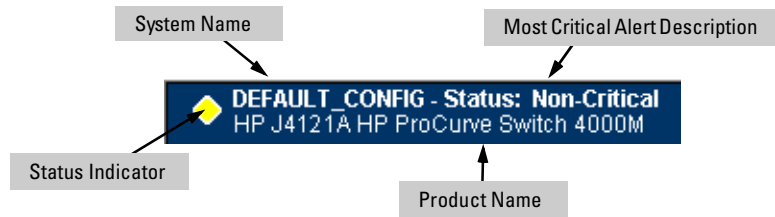





Figure 3-12. Example of the Status Bar

The Status bar consists of four objects:

- **Status Indicator.** Indicates, by icon, the severity of the most critical alert in the current display of the Alert Log. This indicator can be one of three shapes and colors as shown in the following table.

Table 3-3. Status Indicator Key

Color	Switch Status	Status Indicator Shape
Green	Normal Activity	
Yellow	Warning	
Red	Critical	

- **System Name.** The name you have configured for the switch in the Identity screen or through the switch console **System Information** screen.
- **Most Critical Alert Description.** A short narrative description of the earliest, unacknowledged alert with the current highest severity in the Alert Log, appearing in the right portion of the Status Bar. In instances where multiple critical alerts have the same severity level, only the earliest unacknowledged alert is deployed in the Status bar.
- **Product Name.** The product name of the switch to which you are connected in the current web browser interface session.

Setting Fault Detection Policy

One of the powerful features in the web browser interface is the Fault Detection facility. For your switch, this feature controls the types of alerts reported to the Alert Log based on their level of severity.

Set this policy in the Fault Detection window (figure 3-13).

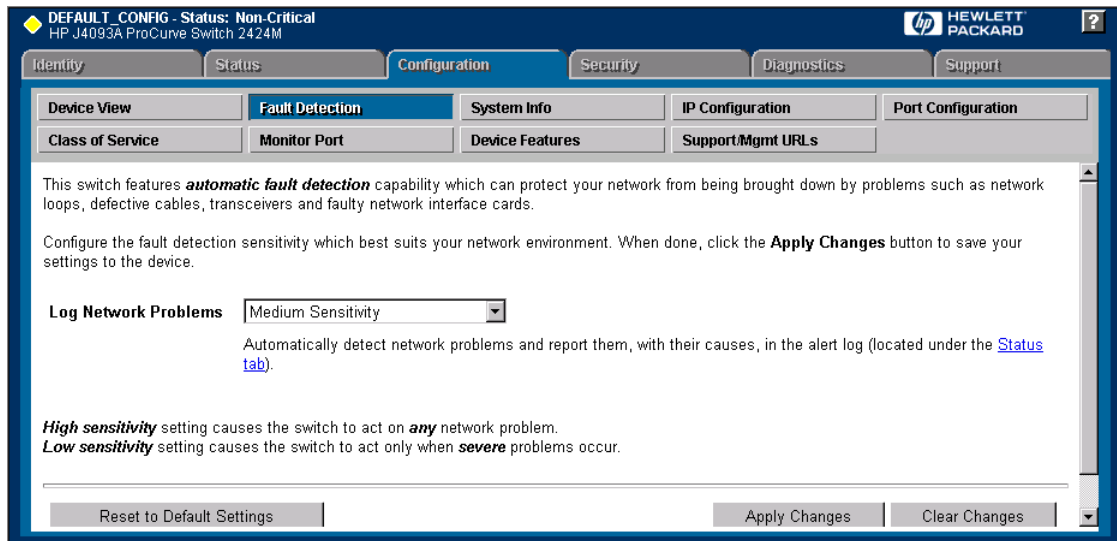


Figure 3-13. The Fault Detection Window

Working With Fault Detection

The Fault Detection screen contains a list box for setting fault detection and response policy. You set the sensitivity level at which a network problem should generate an alert and send it to the Alert Log.

To provide the most information on network problems in the Alert Log, the recommended sensitivity level for **Log Network Problems** is **High Sensitivity**. The Fault Detection settings are:

- **High Sensitivity.** This policy directs the switch to send all alerts to the Alert Log. This setting is most effective on networks that have none or few problems.
- **Medium Sensitivity.** This policy directs the switch to send alerts related to network problems to the Alert Log. If you want to be notified of problems which cause a noticeable slowdown on the network, use this setting.
- **Low Sensitivity.** This policy directs the switch to send only the most severe alerts to the Alert Log. This policy is most effective on a network that normally has a lot of problems and you want to be informed of only the most severe ones.
- **Never.** Disables the Alert Log and transmission of alerts (traps) to the management server (in cases where a network management tool such as HP TopTools for Hubs & Switches is in use). Use this option when you don't want to use the Alert Log.

The Fault Detection Window also contains three Change Control Buttons:

- **Apply Changes.** This button stores the settings you have selected for all future sessions with the web browser interface until you decide to change them.
- **Clear Changes.** This button removes your settings and returns the settings for the list box to the level it was at in the last saved detection-setting session.
- **Reset to Default Settings.** This button reverts the policy setting to Medium Sensitivity for Log Network Problems.

Using the Switch Console Interface

This chapter describes the following features:

- overview of the switch console (page 4-1)
 - starting and ending a console session (page 4-2)
 - the Main Menu (page 4-4)
 - screen structure and navigation (page 4-6)
 - using password security (page 4-9)
 - rebooting the switch (page 4-12)
 - using the command prompt (page 4-14)
-

Overview

About the Switch Console. The switch console enables you to do the following:

- Modify the switch's configuration (see chapter 6).
- Configure the switch with an IP address that allows you to manage the switch from an SNMP-based network management station (chapter 2), through the switch's web browser interface (chapter 3), or through Telnet access to the console. (See "How To Start a Console Session" on page 4-2.)
- Monitor the switch and its port status (chapter 7).
- Monitor the network activity through the switch (page 6-34).
- Control console security by configuring passwords. (See "Using Password Security" on page 4-9.)
- Download new software to the switch (appendix A).

Switch Console Interaction with the Web Browser Interface. Configuration changes made through the console will overwrite previous changes made through the web browser interface. Similarly, configuration changes made through the web browser interface will overwrite any prior changes made through the console. The console gives you access to all switch configuration parameters (except for control of the Alert Log in the web browser interface). The web browser interface gives you access to a subset of switch configuration parameters, plus easy-to-use status and alert information. Refer to chapter 3, "Using the HP Web Browser Interface" and chapter 6, "Configuring the Switch".

Starting and Ending a Console Session

You can access the switch console interface using either:

- a direct serial connection to the switch's console port, as described in the installation guide you received with the switch
- through a Telnet from a networked PC running a Telnet application or running the web browser interface. (Telnet access to the switch is available from the web browser interface.) Telnet requires that an IP address and subnet mask have already been configured on the switch—see chapter 2.

Note

This section assumes that either a terminal device is already configured and connected to your switch (as described in chapter 1, “Installation” of the *Installation Guide* that came with your switch) or that you have already configured an IP address on the switch so you can start a Telnet session with the switch.

How To Start a Console Session:

1. Start your PC terminal emulator or terminal, or Telnet to the switch from a remote terminal device or from the web browser interface. (For web browser access, see “Starting an HP Web Browser Interface Session with the Switch” on page 3-3.)
2. Do one of the following:
 - If you are using Telnet, go to step 3.
 - If you are using a PC terminal emulator or a terminal, press twice.
3. The screen briefly displays a message indicating the baud rate at which the serial interface is operating, followed by the copyright screen. Do one of the following:
 - If a password has been set, the Password prompt appears. Type the password and press to display the Main Menu (figure 4-1). Figure 4-1 shows the Main Menu for manager-level access. If you enter the operator password to start the console session, the Main Menu has a subset of these items.

- If no password has been set, you will see this prompt:

Press any key to continue.

Press any key to display the Main Menu (figure 4-1).

If there is any system-down information to report, the switch displays it in this step and in the Event Log.

For a description of Main Menu features, refer to “Main Menu Features” on page 4-4.

How To End a Console Session:

The process of ending the console session depends on whether, during the console session, you have made any changes to the switch configuration that requires a reboot of the switch to activate. Configuration changes requiring a reboot of the switch are indicated by an asterisk (*) next to the configured item in the Configuration menu and also next to the Switch Configuration item in the Main Menu.

1. If you have *not* made configuration changes in the current session that require a switch reboot to activate, return to the Main Menu, and press **0** to log out. Then just exit from the terminal program, turn off the terminal, or quit from the Telnet session.
2. If you *have* made configuration changes that require a switch reboot:
 - a. Return to the Main Menu.
 - b. Press **6** to select **Reboot Switch** and follow the instructions on the reboot screen.

Rebooting the switch terminates the console session, and, if you are using Telnet, disconnects the Telnet session.

(See “Rebooting To Activate Configuration Changes” on page 4-13.)

3. Exit from the terminal program, turn off the terminal, or close the Telnet application program.

Main Menu Features

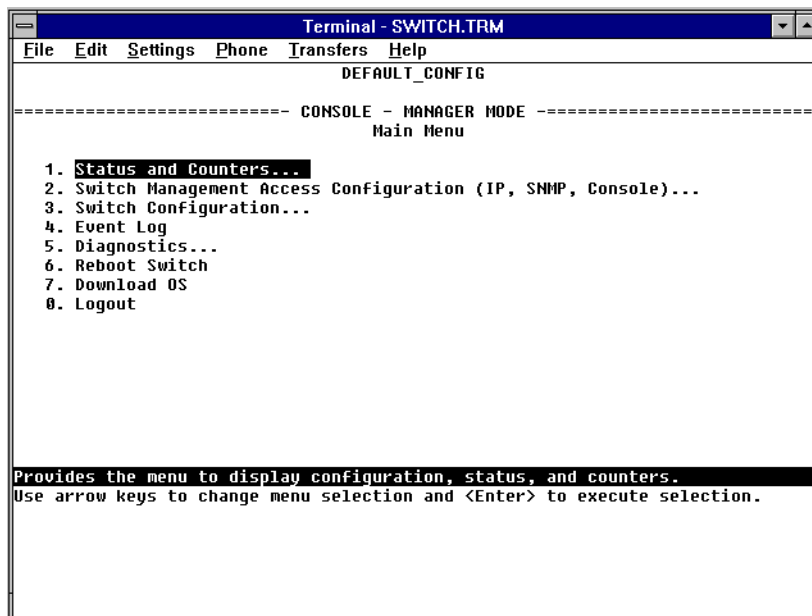


Figure 4-1. The Main Menu

The Main Menu gives you access to these console interface features:

- **Status and Counters:** Provides access to display screens providing information on switch and port status, network activity, the address tables, and spanning tree operation. (Refer to chapter 7, “Monitoring and Analyzing Switch Operation”.)
- **Switch Management Access Configuration:** Provides access to configuration screens that control interaction between the switch and network management, including IP address, SNMP community names and trap receivers, console/serial link parameters, and console passwords.
- **Switch Configuration:** Provides access to configuration screens that enable you to display the current configuration settings and to customize the configuration of the switch features. (Refer to chapter 6, “Configuring the Switch”.)

- **Event Log:** Enables you to read progress and error messages that are useful for checking and troubleshooting switch operation. (Refer to “Using the Event Log To Identify Problem Sources” in chapter 8, “Troubleshooting”.)
- **Diagnostics:** Provides access to screens for doing Link and Ping connectivity testing, listing the current switch configuration, and to a command prompt for executing system management, monitoring, and troubleshooting commands. (Refer to “Diagnostics” in chapter 8, “Troubleshooting”.)
- **Reboot Switch:** Performs a software reboot of the switch, which clears most temporary error conditions, resets the network activity counters to zero, and resets the system up time to zero. A reboot is required (in one case) to activate a configuration change that has been made. (Refer to “Rebooting To Activate Configuration Changes” on page 4-13.)
- **Download OS:** Enables you to download a new software version to the switch. (Refer to appendix A, “Transferring an Operating System or Configuration”.)
- **Logout:** Terminates the console session and disconnects Telnet access to the switch. (Refer to “How to End a Console Session” on page 4-3.)

Screen Structure and Navigation

Console screens include these three elements:

- Parameter fields and/or read-only information such as statistics
- Navigation and configuration actions, such as Save, Edit, and Cancel
- Help line to describe navigation options, individual parameters, and read-only data

For example, in the System Information screen on the next page:

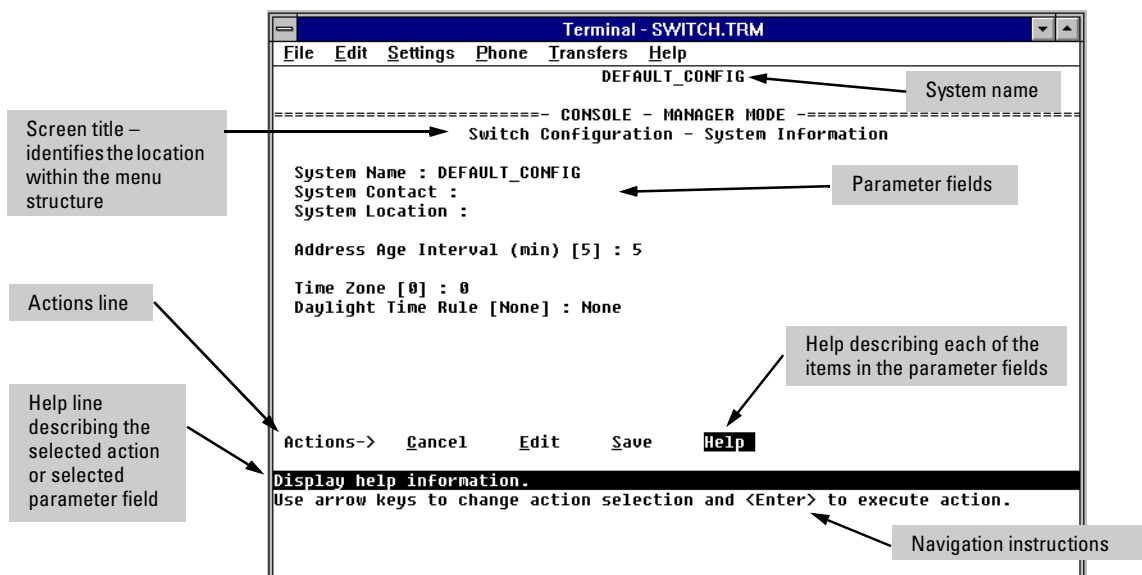


Figure 4-2. Elements of the Screen Structure

“Forms” Design. The configuration screens, in particular, operate similarly to a number of PC applications that use forms for data entry. When you first enter these screens, you see the current configuration for the item you have selected. To change the configuration, the basic operation is to:

1. Press **[E]** to select the **E**dit action.
2. Navigate through the screen making ALL the necessary configuration changes. (See Table 4-1 on the next page.)
3. Press **[Enter]** to return to the **A**ctions line. From there you can save the configuration changes or cancel the changes. Cancel returns the configuration to the values you saw when you first entered the screen.

Table 4-1. How To Navigate in the Console

Task:	Actions:
Execute an action from the "Actions →" list at the bottom of the screen:	<p>Use either of the following methods:</p> <ul style="list-style-type: none"> • Use the arrow keys (← , or →) to highlight the action you want to execute, then press Enter. • Press the key corresponding to the capital letter in the action name. For example, in a configuration menu, press E to select Edit and begin editing parameter values.
Reconfigure (edit) a parameter setting or a field:	<ol style="list-style-type: none"> 1. Select a configuration item, such as System Name. (See figure 4-2.) 2. Press E (for Edit on the Actions line). 3. Use Tab or the arrow keys (← , → , ↑ , or ↓) to highlight the item or field. 4. Do one of the following: <ul style="list-style-type: none"> – If the parameter has preconfigured values, either use the Space bar to select a new option or type the first part of your selection and the rest of the selection appears automatically. (The help line instructs you to "Select" a value.) – If there are no preconfigured values, type in a value (the Help line instructs you to "Enter" a value). 5. If you want to change another parameter value, return to step 3. 6. If you are finished editing parameters in the displayed screen, press Enter to return to the Actions line and do one of the following: <ul style="list-style-type: none"> – To save any configuration changes you have made, press S (for the Save action). – To exit from the screen without saving any changes that you have made (or if you have not made changes), press C (for the Cancel action). <p>Note: Most parameter changes are activated when you execute Save, and it is therefore not necessary to reboot the switch after making these changes. But if an asterisk appears next to any menu item you reconfigure, it is necessary to reboot the switch to implement the change. In this case, rebooting should be done after you have made all desired changes and then returned to the Main Menu.</p> 7. When you are finished editing parameters, return to the Main Menu. 8. If necessary, reboot the switch by highlighting Reboot Switch in the Main Menu and pressing Enter. (Refer to the Note, above.)
Exit from a read-only screen.	Press B (for the Back action).

To get Help on individual parameter descriptions. In all screens except the Command Prompt screen there is a **Help** option in the **Actions** line. Whenever any of the items in the **Actions** line is highlighted, press [H], and a separate help screen is displayed. For example:

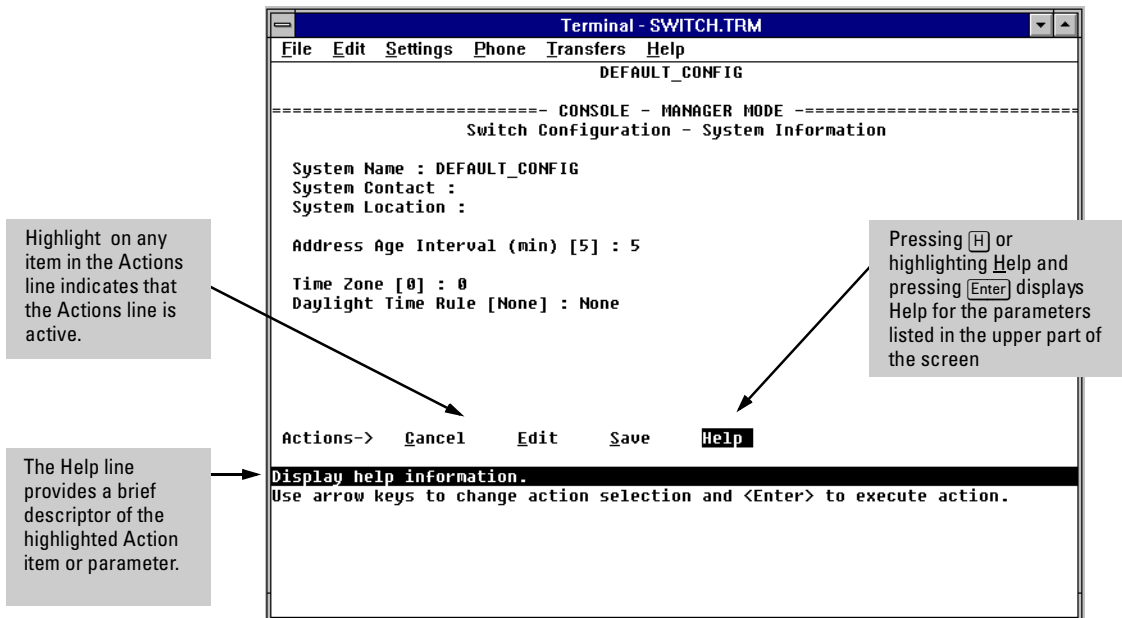


Figure 4-3. Example Showing How To Display Help

To get Help on the actions or data fields in each screen: Use the arrow keys (←, →, ↑, or ↓) to select an action or data field. The help line under the **Actions** items describes the currently selected action or data field.

For guidance on how to navigate in a screen: See the instructions provided at the bottom of the screen, or refer to “Screen Structure and Navigation” on page 4-6.)

Using Password Security

There are two levels of console access: Manager and Operator. For security, you can set a password on each of these levels.

Level	Actions Permitted
Manager:	Access to all console interface areas. <i>This is the default level.</i> That is, if a Manager password has <i>not</i> been set prior to starting the current console session, then anyone having access to the console can access any area of the console interface.
Operator:	Access to the Status and Counters menu, the Event Log, and the Diagnostics menu, but no Configuration capabilities. On the Operator level, the configuration menus, Download OS, and Reboot Switch options in the Main Menu, and the Command Prompt option in the Diagnostics menu are not available.

To use password security:

1. Set a Manager password (and an Operator password, if applicable for your system) as described on page 4-10.
2. Exit from the current console session. A Manager password will now be needed for full access to the console.

If you do steps 1 and 2, above, then the next time a console session is started, the console interface will prompt for a password. Assuming that both a Manager password and an Operator password have been set, the level of access to the console interface will be determined by which password is entered in response to the prompt.

If you set a Manager password, you may also want to configure the **Connection Inactivity Time** parameter in the Console/Serial Link configuration screen that is under the **Switch Management Access Configuration** menu (see page 6-20). This causes the console session to end after the specified period of inactivity, thus giving you added security against unauthorized console access.

Note

The manager and operator passwords control access to both the web browser interface and the switch console interface.

Note

If there is only a Manager password set (with no Operator password), and the Manager password is not entered correctly when the console session begins, the switch operates on the Operator level.

If there are both a Manager password and an Operator password, but neither is entered correctly, access to the console will be denied.

*If a Manager password is not set, anyone having access to the console interface can operate the console with full manager privileges, regardless of whether an Operator password is set, by simply pressing **Enter** at the password prompt.*

Passwords are case-sensitive.

The rest of this section covers how to:

- Set Passwords
- Delete Passwords
- Recover from a Lost Password

To set Manager and Operator passwords:

1. From the Main Menu select:
 - 2. Switch Management Access Configuration**
 - 5. Console Passwords**

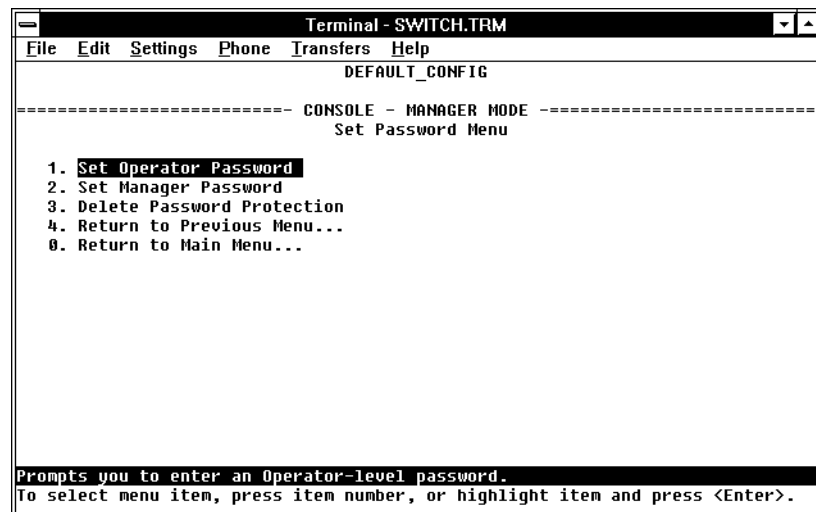


Figure 4-4. The Set Password Screen

2. To set a new password:
 - a. Select **Set Manager Password** or **Set Operator Password**. You will then be prompted with **Enter new password**.
 - b. Type a password of up to 16 ASCII characters with no spaces and press **[Enter]**. (Remember that passwords are case-sensitive.)
 - c. When prompted with **Enter new password again**, retype the new password and press **[Enter]**.
3. When you have finished all password configuration, select **Return to Main Menu** to return to the Main menu, or **Return to the Previous Menu** to return to the Switch Management Access Configuration menu.

After a password is set, if you subsequently start a new console session, you will be prompted to enter the password.

To Delete Password Protection (Including Recovery from a Lost Password): This procedure deletes *both* passwords (Manager and Operator). If you have physical access to the switch, press the Clear button on the front of the switch to clear all password protection, then enter new passwords as described earlier in this chapter. If you do not have physical access to the switch, you will need the Manager password:

1. Enter the console at the Manager level.
2. Go to the **Console Passwords** screen as described above.
3. Select **Delete Password Protection**. You will then see the following prompt:

Continue Deletion of password protection?
4. Press the Space bar to select **Yes**, then press **[Enter]**.
5. Press **[Enter]** to clear the Password Protection message.
6. Select **Return to Main Menu** to return to the Main menu, or **Return to the Previous Menu** to return to the **Switch Management Access Configuration** menu.

To Recover from a Lost Manager Password: If you cannot start a console session at the manager level because of a lost Manager password, you can clear the password by getting physical access to the switch and pressing the Clear button. This action deletes all passwords and user names (Manager and Operator) used by both the console and the web browser interface.

Rebooting the Switch

Rebooting the switch terminates the current console session and performs a reset of the operating system. Rebooting the switch also activates certain configuration changes that require a reboot and resets statistical counters to zero. (Note that statistical counters can be reset to zero without rebooting the switch. See “Displaying Port Counters from the Console Interface” on page 7-12.)

To Reboot the switch, use the **Reboot Switch** option in the Main Menu. (Note that the Reboot Switch option is not available if you log on in Operator mode; that is, if you enter an Operator password instead of a manager password at the password prompt.)

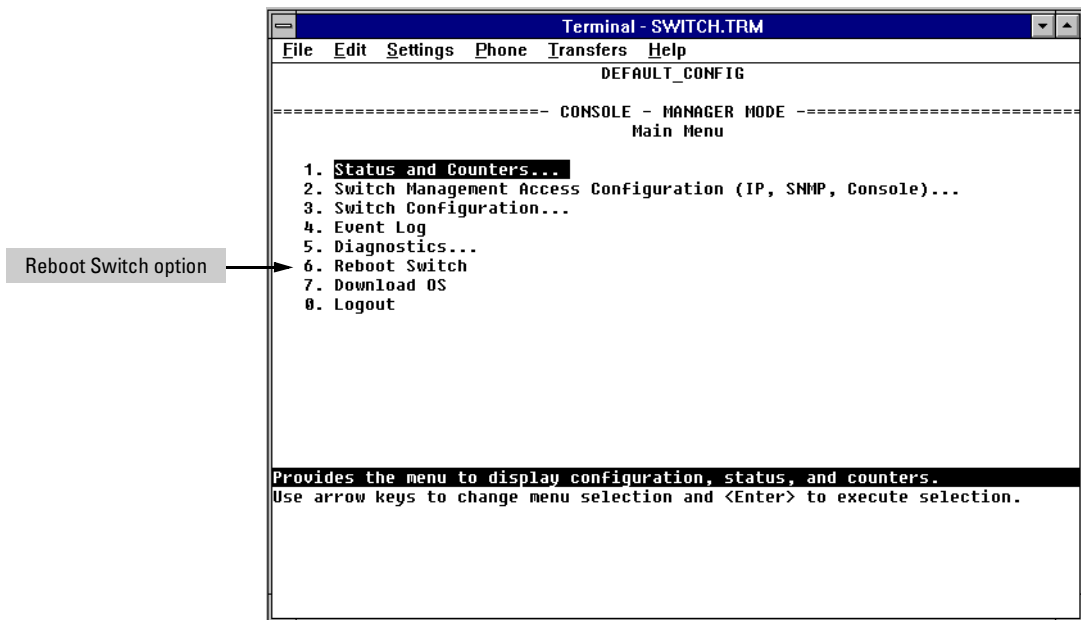


Figure 4-5. The Reboot Switch Option in the Main Menu

Rebooting To Activate Configuration Changes. Configuration changes for some parameters become effective as soon as you save them. However, you must reboot the switch in order to implement any changes to any parameters in the following areas:

- Console/Serial Link (under **2. Switch Management Access Configuration** menu)
- VLAN Names (under **3. Switch Configuration | 5. Advanced Feature | 4. VLAN Menu**)

If configuration changes requiring a reboot have been made, the switch displays an asterisk (*) next to the menu item in which the change has been made. For example, if you change and save parameter values for the switch's Console/Serial Link configuration, the need for rebooting the switch would be indicated by an asterisk appearing next to the item **Console/Serial Link** in the **Switch Management Access Configuration** menu, and in the Main Menu as shown in figure 4-6:

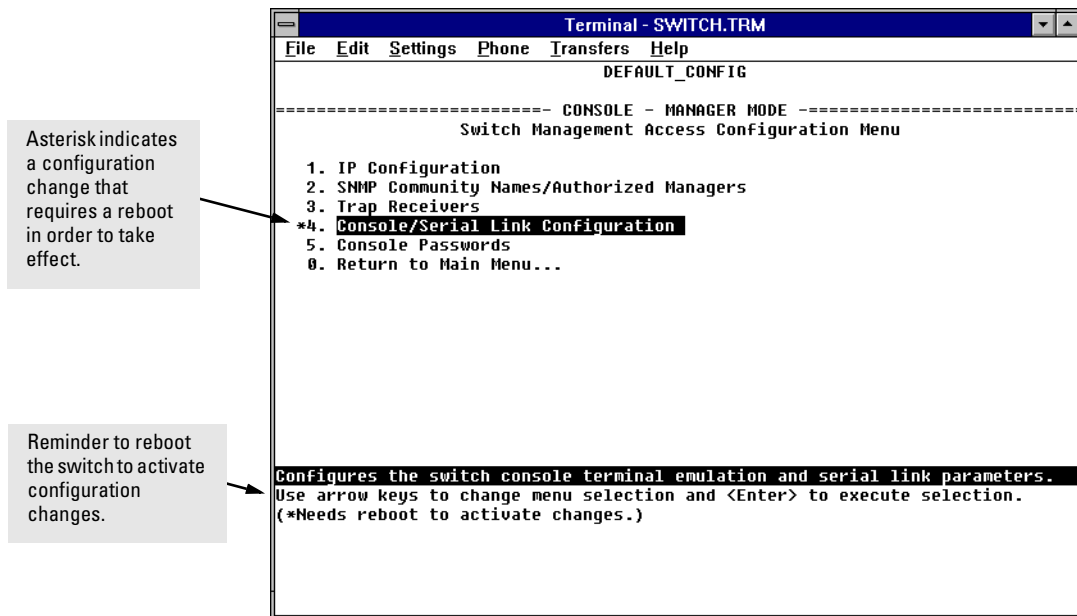


Figure 4-6. Example of a Configuration Change Requiring a Reboot

The Command Prompt

In addition to the menu-based part of the console interface, under the Diagnostics Menu, a command-line based interface is available. The commands are primarily for the expert user and for diagnostics purposes, although there are commands for setting some basic items on the switch such as the date and time. Additionally, the **Set** command can be used to configure a number of switch parameters and the **Show** command can be used to display switch status and network counters information.

How To Use the Command Prompt:

1. From the Main Menu, select **5. Diagnostics ...** , then from the Diagnostics Menu, select **4. Command Prompt**
2. One of the following appears:

- If VLANs are configured, you will see a prompt similar to the following:

Select VLAN : DEFAULT_VLAN

Use the Space bar to select the VLAN in which you want to execute a command, then press to display the command prompt. The text in the prompt will match the name of the VLAN you select.

- If no VLANs are configured, the command prompt appears near the bottom of the screen. For example:

DEFAULT_CONFIG:

The text in the prompt matches the System Name parameter. In the above example, the factory default configuration name appears because no system name is configured.

3. Type in the command you want to execute and press . For example, to set the time to 9:55 a.m. you would execute the following command:

DEFAULT_CONFIG: time 9:55

How To Exit from the command prompt:

Type **exit** and press to return to the Diagnostics Menu.

Commands Available

The following commands are available from the command prompt (this information can also be displayed by entering **help** or **he** at the command prompt. When you see **-- MORE --** at the bottom of the screen:

- To advance the display one line at a time, use `[Enter]`.
- To advance the display one screen at a time, use the Space bar.
- To stop the help listing, press `[Q]`:

Table 4-1. List of Commands Available at the Command Prompt

Command	Description
Help	Help [All]; Shows help information about commands.
Exit	Returns to the Diagnostics Menu.
Browse	Displays the switch configuration in readable form.
Config	Displays the switch configuration file stored in flash.
Date	Displays or sets the date and time; to set: date mm/dd/yy.
Time	Displays or sets the date and time; to set: time hh:mm:ss
Set	Configures some switch parameters. Use 'set help' for more information.
Show	Displays some switch settings. Use 'show help' for more information.
Delete	delete CONFIG; Deletes the configuration file stored in flash.
History	Displays the switch shutdown history.
Kill	Kills all other active telnet/console sessions.
Get	get <ip-addr> CONFIG <remote-file>; Copies the configuration file <remote-file> from the host identified by <ip-addr>
Put	put <ip-addr> <file> <remote-file> [UNIX PC]; Copies the item specified by <file> to the host identified by <ip-addr>. <file> is CONFIG or any command; <remote-file> is the destination file name on the host; UNIX formats a text file with line feeds (default).
LinkTest	linktest <MAC-addr>; Sends an 802.2 Test packet to the device identified by <MAC-addr>.
Log	log [-a keyword -a keyword]; Displays the current switch log; -a displays the entire internal event log; keyword displays only the events that contain the keyword.
Page	Toggles paging mode on and off for display commands.

Command	Description
Ping	ping <ip-addr> [count] [wait]; Sends IP 'Echo Request' packets to the device identified by <ip-addr>. count sets the number of packets, wait sets the time to wait for a response in seconds.
Print	print <cmd>; Sends the output from the command <cmd> to a printer or file.
Redo	redo [? <number> <string>]; Displays command history or executes a command from the history: redo -- re-executes the most recent command. redo ? -- displays the command history. redo <number> -- re-executes a previous command indexed by <number> redo <string> -- re-executes a previous command that begins with the text <string>.
GetMIB	getmib <obj-id>; Shows the value of the managed object <obj-id>.
SetMIB	setmib <obj-id> <type> <value>; Sets the value of the managed object <obj-id> of the type <type> with the value <value>.
Xget	xget CONFIG; Retrieves the configuration file using XModem.
Xput	xput <file> [PC UNIX]; Sends the item identified by <file> using XModem. <file> is CONFIG, CRASHREC, LOGFILE, or any command. PC formats the file with carriage returns and line feeds; UNIX formats the file with line feeds only.
romversion	Displays the switch ROM version.
Version	Displays the switch OS version.
Vlan	vlan <vlan-name>; Changes the VLAN in which the commands are executed.
WalkMIB	walkmib <obj-id>; Displays a group of managed object values.

Set and Show Commands

Most of the commands at the command prompt are useful for diagnostics purposes, but the **set** commands can be used to configure some of the switch's basic features, and the **show** commands can be used to display switch and port status and activity information. These commands can be run from UNIX scripts so they can be executed on an automatic, timed basis.

To get help on the **set** and **show** commands, type **help** at the end of the command line; for example **show help** to display help for the show command, or **set spantree hello help** to display help on how to configure the Spanning Tree Hello Time parameter.

Set Commands

Table 4-2. Set Commands Available at the Command Prompt

Command	Description
set abc	set abc <enable disable>; Enables or disables the Automatic Broadcast Control (ABC) feature. This feature is disabled by default. For more information on ABC, see page 6-106.
set igmp	set igmp <enable disable>; Enables or disables the IP Group Management Protocol (IGMP) feature for IP multicast traffic control. This feature is disabled by default. For more information on IGMP, see page 6-95.
set port	set port <enable disable> <port-number>; Enables or disables the switch port specified by <port-number>. All the switch ports are enabled by default.
set spantree	<p>set spantree <parameter>; Configures the Spanning Tree Protocol (STP) parameters, where <parameter> can be:</p> <ul style="list-style-type: none"> • enable -- enables STP operation on the switch, using the default values for the STP parameters (STP is disabled by default). • disable -- disables STP operation. • fwwdelay <delay> -- sets the STP forward delay value (default = 15, range = 4 - 30 seconds). • hello <interval> -- sets the STP hello time interval (default = 2, range = 1 - 10). • maxage <agingtime> -- sets the STP max aging interval (default = 20, range = 6 - 40). • portcost <port-number> <cost> -- sets the STP port cost for the specified switch port (default = <i>dependent on port speed</i>, range = 1 - 65535). • portpri <port-number> <priority> -- sets the STP port priority for the specified port (default = 128, range = 0 - 255). <p>For more information on Spanning Tree, see page 6-39.</p>

Command	Description
set system	set system <parameter>; Configures the switch identification parameters, where <parameter> can be: <ul style="list-style-type: none">• contact <contact-name> -- sets a user-defined name for someone to contact for switch administration.• location <location> -- sets a user-defined switch location description.• name <switch-name> -- sets a user-defined identification name for the switch.

Show Commands

Table 4-3. Show Commands Available at the Command Prompt

Command	Description
show bridge	show bridge [port-number]; Displays the switch address table, or optionally for the specified port.
show filters	show filters; Displays the traffic/security filters that have been configured on the switch.
show ip	show ip; Displays the switch IP address configuration. If multiple VLANs are configured, the IP address configuration for all VLANs is displayed.
show module	show module; Displays status information for any modules installed in the switch.
show port	show port <parameter>; Displays status information for the switch ports, where <parameter> can be: <ul style="list-style-type: none">• counters [port-number] -- displays network traffic counters for all the switch ports, or optionally, for the specified port.• status [port-number] -- displays the status of all the switch ports, or optionally, for the specified port.• spantree -- displays a summary of the spanning tree configuration and status of all the switch ports.
show snmp	show snmp; Displays the switch SNMP communities configuration.
show spantree	show spantree; Displays a summary of the switch-level Spanning Tree configuration and status.
show system	show system; Displays a summary of the switch system configuration and switch memory and buffer usage.

Using HP TopTools or Other SNMP Tools To Monitor and Manage the Switch

You can manage the switch via SNMP from a network management station. Included with your switch is a CD-ROM containing a copy of HP TopTools for Hubs & Switches, an easy-to-install and use network management application that runs on your Windows NT- or Windows 95-based PC.

HP TopTools for Hubs & Switches provides control of your switch through its graphical interface. In addition, it makes use of the RMON agent and statistical sampling software that is included in the switch to provide powerful, but easy-to-use traffic monitoring and network activity analysis tools.

This chapter provides:

- An overview of SNMP management for the switch
- An overview of the configuration process for supporting SNMP management of the switch. (For the configuration procedures for specific features, refer to chapter 6, “Configuring the Switch”.)
- Information on advanced management through RMON and HP Extended RMON Support

To implement SNMP management, you must either configure the switch with the appropriate IP address or, if you are using DHCP/Bootp to configure the switch, ensure that the DHCP or Bootp process provides the IP address. (The IPX address is automatically learned.) If multiple VLANs are configured, each VLAN interface should have its own IP or IPX network address.

SNMP Management Features

SNMP management features on the switch include:

- Security via configuration of SNMP communities
- Event reporting via SNMP traps and RMON
- Managing the switch with a network management tool such as HP TopTools for Hubs & Switches

- Monitoring data normally associated with the SNMP agent (“Get” operations). Supported *Standard* MIBs include:
 - Bridge MIB (RFC 1493)
dot1dBase, dot1dTp, dot1dStp
 - Ethernet MAU MIB (RFC 1515)
dot3IfMauBasicGroup
 - Interfaces Evolution MIB (RFC 1573)
ifGeneralGroup, ifRcvAddressGroup, ifStackGroup
 - RMON MIB (RFC 1757)
etherstats, events, alarms, and history
 - SNMP MIB-II (RFC 1213)
system, interfaces, at, ip, icmp, tcp, udp, snmp
 - Entity MIB (RFC 2037)

HP Proprietary MIBs include:

- Statistics for message and packet buffers, tcp, telnet, and timep (netswtst.mib)
- Port counters, forwarding table, and CPU statistics (stat.mib)
- tftp download (downld.mib)
- Integrated Communications Facility Authentication Manager and SNMP communities (icf.mib)
- HP ProCurve Switch configuration (config.mib)
- HP VLAN configuration information (vlan.mib) supporting hpVlanGeneralGroup
- HP Extended RMON MIB version 4 to allow statistical sampling
- HP Entity MIB (entity.mib)

The switch SNMP agent also uses certain variables that are included in a Hewlett-Packard proprietary MIB file you can add to the SNMP database in your network management tool. You can copy the MIB file from the HP TopTools for Hubs & Switches CD shipped with the switch, or from following World Wide Web site:

<http://www.hp.com/go/procurve>

For more information, refer to Customer Support/Warranty booklet included with your switch.

SNMP Configuration Process

This requires that you configure the switch with the appropriate IP address. (Refer to chapter 2, “Configure an IP Address on the Switch”. If you are using DHCP/Bootp to configure the switch, ensure that the DHCP/Bootp process provides the IP address. (Refer to “DHCP/Bootp Operation” on page 6-9.)

The general steps to configuring for SNMP access to the preceding features are:

1. From the Main menu, select
 - 2. Switch Management Access Configuration**
 - 1. IP Configuration**
2. Use either of the following methods to configure a network address for the switch, including any necessary gateway:
 - Use DHCP/Boot, which is enabled by default, to acquire an IP address. Make sure the DHCP/Bootp server is configured to support the switch. (Refer to “DHCP/Bootp Operation” on page 6-9.)
 - Manually configure an IP address. (Refer to chapter 2, “Configuring an IP Address on the Switch”.)
3. Configure the appropriate SNMP communities. (The “public” community exists by default and is used by HP’s network management applications.) (For more on configuring SNMP communities, refer to “SNMP Communities” on page 6-14.)
4. Configure the appropriate trap receivers. (For more on configuring trap receivers, refer to “Trap Receivers” on page 6-17.)

In many networks, manager addresses are not used. In this case, all management stations using the correct community name may access this device with the View and Access levels that have been set for that community. If you want to restrict access to one or more specific nodes, you can enter up to ten IP addresses of such nodes into the Manager Address field. *Configuring one or more IP addresses in the Manager Address field means that only the network management stations at those addresses are authorized to use the community name to access the switch.*

Caution

Deleting the community named “public” disables many network management functions (such as auto-discovery, traffic monitoring, and threshold setting). If security for network management is a concern, it is recommended that you change the write access for the “public” community to “Restricted”.

Note

SNMP community and trap receiver configurations are activated when saved. Rebooting the switch is not necessary unless you have also configured other parameters that require rebooting in order to be activated. (For more on when it is necessary to reboot, refer to “Rebooting the Switch” on page 4-12.)

Advanced Management: RMON and HP Extended RMON Support

The switch supports RMON (Remote Monitoring) and HP Extended RMON on all connected network segments. This allows for troubleshooting and optimizing your network.

RMON

The following RMON groups are supported:

- Ethernet Statistics (except the numbers of packets of different frame sizes)
- Alarm
- History (of the supported Ethernet statistics)
- Event

You can access the Ethernet statistics, Alarm, and Event groups from the HP TopTools for Hubs & Switches network management software included with your switch.

Extended RMON

Extended RMON provides network monitoring and troubleshooting information that analyzes traffic from a network-wide perspective. Extended RMON notifies you about network problems and identifies the end node at fault. That information can be used to set up RMON to study the problem more closely, if desired. Because it is based on detailed statistical sampling, Extended RMON lessens the load on devices and network bandwidth.

Configuring the Switch

Overview

This chapter describes the switch configuration features available in both the switch console and the HP web browser interface. If you need information on how to operate either the web browser interface or the console, refer to:

- Chapter 3, “Using the HP Web Browser Interface”
- Chapter 4, “Using the Switch Console Interface”

Why Reconfigure? In its factory default configuration, the switch operates as a multiport learning bridge with network connectivity provided by the ports on the switch and/or on the particular modules you have installed. However, to enable specific management features and to “fine-tune” your switch for the specific performance and security needs in your network, you may want to reconfigure individual switch parameters.

How To Find Configuration Information. Each section in this chapter is organized as follows:

- **Introductory feature information:** Provides an overview of the feature.
- **“How-To” Configuration steps:** Describes the step-by-step process used to actually configure the feature. It also includes examples of the web browser interface and console interface screens.
- **Detailed feature information:** Provides a more in-depth description of the feature, along with notes on interoperation with other features.

To find a specific feature, see the table in the next section.

Configuration Features

Table 6-1. Configurable Feature Comparison

Feature	Switch Console	Web Browser	Page
Authentication Traps/ Trap Receivers	Yes	—	6-17
Authorized IP Managers	Yes	Yes	6-21
Automatic Broadcast Control (ABC)	Yes	Yes	6-106
Class of Service (CoS)	Yes	Yes	6-130
Console/Serial Link			6-19
• Enable Inbound Telnet to Console	Yes	—	6-20
• Enable Web Browser Interface Access	Yes	—	6-20
• Terminal Settings	Yes	—	6-20
Fault Detection	Yes	Yes	3-27
IP Configuration	Yes	Yes	6-4
IP Multicast (IGMP) Enable/Disable	Yes	Yes	6-95
IGMP Priority and Port Settings	Yes	—	
Load Balancing: Port Trunking	Yes	—	6-70
Load Balancing: Switch Meshing	Yes	—	6-80
Network Monitoring Port	Yes	Yes	6-34
Operator and Manager Usernames	—	Yes	3-8
Operator and Manager Passwords	Yes	Yes	3-8, 4-9
Port Settings	Yes	Yes	6-30
Port Security	Yes	Yes	6-118
Port-Based Virtual LANs (VLANs)	Yes	—	6-51
SNMP Communities	Yes	—	6-14
Spanning Tree Enable/Disable	Yes	Yes	6-39
Spanning Tree Parameters	Yes	—	
System Information	Yes	Yes	6-28
Address Age Interval	Yes	—	
System Time	Yes	—	
Time Protocol	Yes	—	6-7
Traffic/Security Filters	Yes	—	6-46

Note

In the factory default configuration, the Spanning Tree Protocol (STP—which automatically blocks redundant links) is disabled. Generally, you should enable STP to prevent broadcast storms if there are redundant links in your network that are not part of a switch mesh. However, due to the requirements of the 802.1Q VLAN standard, STP blocks unmeshed redundant physical links even if they are in separate VLANs. This could result in blocking links unnecessarily. Switch meshing can allow use of STP without the problem of blocking links that could remain open. For more information, refer to “Load Balancing: Switch Meshing” on page 6-80, and “Spanning Tree Protocol” on page 6-39.

IP Configuration

Configuring the switch with an IP address expands your ability to manage the switch, and also enhances the switch features that can be used.

The **switch console screen** enables you to configure the initial values for:

- IP address, subnet mask, and (optionally) the gateway address for the switch so that it can be managed in an IP network
- The time server information (used if you want the switch to get its time information from another device operating as a Timep server)

The **web browser interface** screen enables you to modify the initial IP configuration if needed.

Note

If you change the IP address through the web browser interface, the browser will lose connection to the switch. You can reconnect by entering the new IP address as the URL.

By default, the switch is configured to receive IP addressing from a DHCP/Bootp server that you have configured correctly with information for your switch. (Refer “DHCP/Bootp Operation” on page 6-9 for information on setting up automatic configuration from a server.) Through the web browser interface or switch console, you can manually enter a different address, or you can disable the IP operation.

Notes

- If VLANs are not configured, then configure one IP address for the entire switch. If VLANs are configured, then configure an IP address for each VLAN. This is because each VLAN is a separate network and requires a unique IP address, and subnet mask. A gateway (IP) address is optional. For more on VLANs, refer to “Virtual LANs (VLANs)” on page 6-51.
 - The IP addressing used in the switch should be compatible with your network: the IP address must be unique, and the subnet mask must be the same for all devices on the same IP network.
 - If you plan to connect to other networks that use globally administered IP addressing, refer to “Globally Assigned IP Network Addresses” on page 6-13.
-

For information on how IP addressing affects switch performance, refer to “How IP Addressing Affects Switch Operation” on page 6-8.

Configuring IP Addressing from the Web Browser Interface

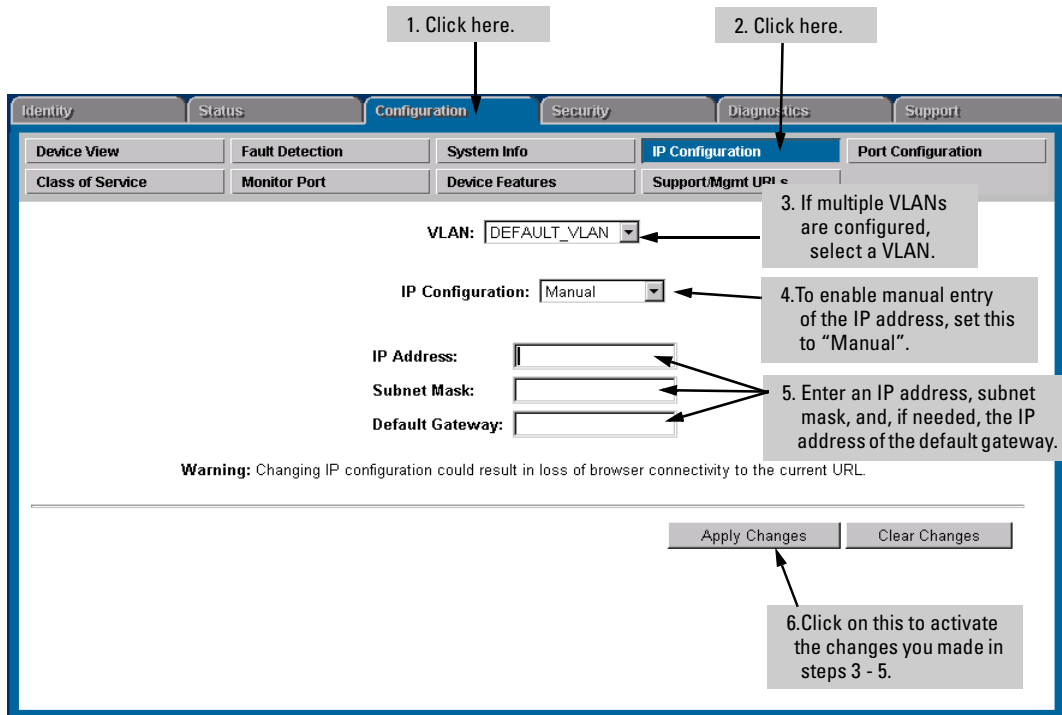


Figure 6-7. Configuring IP Addressing on the Web Browser Interface

Parameter	Description
VLAN	If you have configured multiple VLANs, then use this parameter to select the VLAN to which you want to assign an IP address. Otherwise, leave it set to the default.
IP Configuration	The method the switch uses to acquire its IP configuration. <ul style="list-style-type: none"> DHCP/Bootp (default): The switch attempts to get its IP configuration or its complete configuration from a DHCP or Bootp server. Manual: Enables you to manually enter the IP configuration into the next three fields. Disabled: Network management access to the switch over IP is disabled.

Parameter	Description
IP Address	IP address for the switch (or VLAN) IP interface. If DHCP/Bootp is selected for IP Configuration, this is a read-only field displaying the value received from a DHCP or Bootp server.
Subnet Mask	The same subnet mask that is used by all devices in the IP subnet being configured. If DHCP/Bootp is selected for IP Configuration, this is a read-only field displaying the value received from a DHCP or Bootp server.
Default Gateway	The IP address of the next-hop gateway node for reaching off-subnet destinations. Used as the default gateway if the requested destination address is not on the local subnet. If DHCP/Bootp is selected for IP Configuration, this is a read-only field displaying the value received from a DHCP or Bootp server.

Configuring IP Addressing from the Switch Console

You can use the console to manually configure an IP address, subnet mask, and a Gateway IP address (if needed). Or, you can use DHCP/Bootp to configure IP from a DHCP or Bootp server. (To use the DHCP/Bootp option, you must also configure the DHCP or Bootp server accordingly.)

Do one of the following:

- To use the console, set the **IP Config** parameter to **Manual** and then manually enter the IP address, subnet mask, and default gateway you want for the switch.
- If you plan to use DHCP or Bootp, use the console to ensure that the **IP Config** parameter is set to **DHCP/Bootp**, then refer to “DHCP/Bootp Operation” on page 6-9.

To Access IP Addressing:

1. From the Console Main Menu, Select...
 2. **Switch Management Access Configuration (IP, SNMP, Console)...**
 1. **IP Configuration**

Note

If multiple VLANs are configured, a screen showing all VLANs appears instead of the following screen. You would first select the VLAN you want to configure, then the following screen would appear to configure IP for that VLAN.

The default setting for Time Protocol Config is DHCP. Setting it to **Manual**, then pressing **↓** or **Tab** causes the Timep Server Address parameter to appear.

The default setting for IP Config is DHCP/Bootp. Using the Space bar to set it to **Manual**, then pressing **↓** or **Tab** causes the IP Address, Subnet Mask, and Gateway parameters to appear.

For descriptions of these parameters, refer to the online Help for this screen.

Before using the DHCP/Bootp option, refer to DHCP/Bootp Operation on page 6-9.

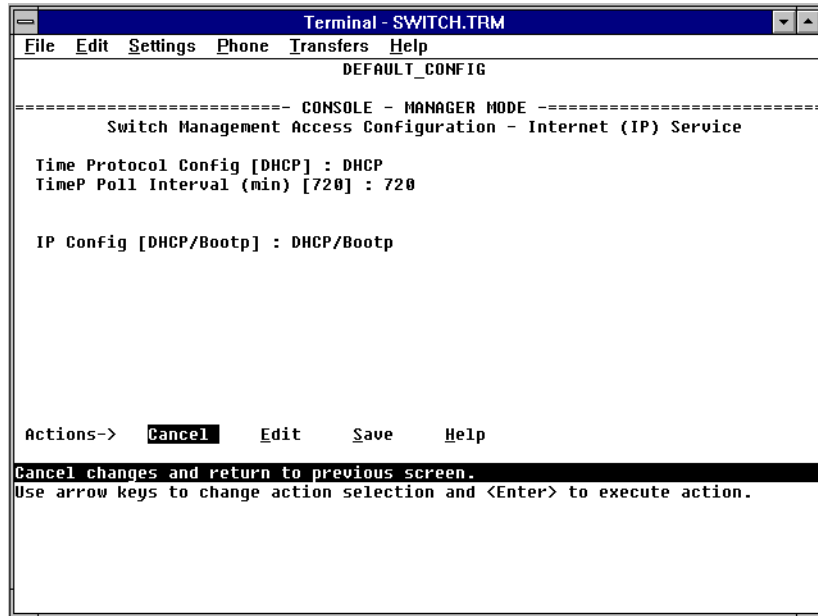


Figure 6-8. Example of the IP Service Configuration Screen

2. Press **E** (for **Edit**).
3. At the **Time Protocol Config** field, if you want the switch to obtain its system time from a Timep server, and the server is configured correctly, keep the value as **DHCP**, or use the Space bar to select **Manual**. If you don't have a Timep server set up, use the Space bar to change to value to **Disable**.
4. If you select **Manual**, press the Tab or Down Arrow key, and additional fields will be displayed for entering the IP address and subnet mask for the Timep server.
5. Select the **Time Poll Interval** field if you want to change to value for how often the switch will poll the Timep server for time information.
6. If you want to have the switch retrieve its IP configuration from a DHCP or Bootp server, at the **IP Config** field, keep the value as **DHCP/Bootp** and go to step 10. If you want to manually configure the IP information, use the Space bar to select **Manual** and press the Tab or Down Arrow key to reveal the other IP configuration fields.
7. Select the **IP Address** field and enter the IP address for the switch.
8. Select the **Subnet Mask** field and enter the subnet mask for the IP address.

9. If you want to reach off-subnet destinations, select the **Gateway** field and enter the IP address of the gateway router.
10. Press **[Enter]**, then **[S]** (for **Save**).
11. Return to the Main Menu.

How IP Addressing Affects Switch Operation

Without an IP address and subnet mask compatible with your network, the switch operates as a multiport transparent bridge and can be managed only through a direct terminal device connection to the Console RS-232 port. In this state, the switch simply learns which nodes are on which ports and forwards or blocks traffic accordingly. You can use direct-connect console access to take advantage of features that do not depend on IP addressing. However, to realize the full performance capabilities HP proactive networking offers through the switch, configure the switch with an IP address and subnet mask compatible with your network. The following table lists the general features available with and without a network-compatible IP address configured.

Features Available Without an IP Address	Additional HP Proactive Networking Features Available with an IP Address and Subnet Mask
<ul style="list-style-type: none">• Direct-connect console access• DHCP or Bootp support for automatic IP address configuration, and DHCP support for automatic time server IP address configuration• Spanning Tree Protocol• Port trunking• Traffic filtering• Console-based status and counters information for monitoring switch operation and diagnosing problems.• VLANs• Serial downloads of operating system (OS) updates and configuration files (Xmodem)	<ul style="list-style-type: none">• HP web browser interface access, with configuration, security, and diagnostic tools, plus the Alert Log for discovering problems detected in the switch along with suggested solutions• SNMP network management access such as HP TopTools network configuration, monitoring, problem-finding and reporting, analysis, and recommendations for changes to increase control and uptime• Telnet console access• Automatic Broadcast Control (ABC)• IGMP• Time server configuration• TFTP download of configurations and OS updates• Ping test

DHCP/Bootp Operation

Overview

DHCP/Bootp is used to download configuration data from a DHCP or Bootp server respectively to the switch or to a VLAN configured on the switch. With DHCP you can have the switch automatically retrieve the IP address with no configuration required on either the switch or the DHCP server. A Bootp server requires some configuration, but you can additionally identify a file to be downloaded to the switch containing a full switch configuration.

Note

The Switches 1600M/2424M/4000M/8000M are compatible with both DHCP and Bootp servers.

To use DHCP/Bootp for IP configuration of a VLAN, the DHCP/Bootp server must be in that VLAN in order for the switch to access it.

The DHCP/Bootp Process

Whenever the **IP Config** parameter in the switch or in an individual VLAN in the switch is configured to **DHCP/Bootp** (the default), or when the switch is rebooted with this configuration:

1. DHCP/Bootp requests are automatically broadcast on the local network. (The switch sends one type of request which either a DHCP or Bootp server can process.)
2. When a DHCP or Bootp server receives the request, it replies with an automatically generated IP address and subnet mask for the switch. The switch also receives an IP Gateway address if the server has been configured to provide one. In the case of Bootp, the server must first be configured with an entry that has the MAC address of the switch. (The switch properly handles replies from either type of server. If multiple replies are returned, the switch tries to use the first DHCP reply.)

If the switch is initially configured for DHCP/Bootp operation (the default), or if it is rebooted with this configuration, it immediately begins sending request packets on the network. If the switch does not receive a reply to its DHCP/Bootp requests, it continues to periodically send request packets, but with decreasing frequency. Thus, if a DHCP or Bootp server is not available or accessible to the switch when DHCP/Bootp is first configured, the switch may not immediately receive the desired configuration. After verifying that the server has become accessible to the switch, reboot the switch to re-start the process.

DHCP Operation. A significant difference between a DHCP configuration and a Bootp configuration is that an IP address assignment from a DHCP server is automatic, requiring no configuration of the DHCP server. Using that automatic feature, though, the address is temporarily leased. Periodically the switch may be required to renew its lease of the IP configuration. Thus, the IP addressing provided by the server may be different each time the switch reboots or renews its configuration from the server. However, you can fix the address assignment for the switch by doing either of the following:

- Configure the server to issue an “infinite” lease.
- Using the switch’s MAC address as an identifier, configure the server with a “Reservation” so that it will always assign the same IP address to the switch. (For MAC address information, refer to appendix B, “MAC Address Management”.)

For more information on either of these procedures, refer to the documentation provided with the DHCP server.

Bootp Operation. When a Bootp server receives a request it searches its Bootp database for a record entry that matches the MAC address in the Bootp request from the switch. If a match is found, the configuration data in the associated database record is returned to the switch. For most Unix systems, the Bootp database is contained in the `/etc/bootptab` file. In contrast to DHCP operation, Bootp configurations are always the same for each receiving device. That is, the Bootp server replies to a request with a configuration previously stored in the server and designated for the requesting device.

Bootp Database Record Entries. A minimal entry in the Bootp table file `/etc/bootptab` to update an IP address and subnet mask to the switch or a VLAN configured in the switch would be similar to this entry:

```
j4121switch:\  
  ht=ether:\  
  ha=040009123456:\  
  ip=55.66.77.88:\  
  sm=255.255.248.0\  
  gw=55.66.77.1\  
  lg=11.22.33.44\  
  hn\  
  vm=rfc1048
```

An entry in the Bootp table file `/etc/bootptab` to tell the switch or VLAN where to obtain a configuration file download would be similar to this entry:

```
j4121switch:\
  ht=ether:\
  ha=040009123456:\
  ip=55.66.77.88:\
  sm=255.255.248.0:\
  gw=55.66.77.1:\
  lg=11.22.33.44:\
  T144="switch.cfg":\
  vm=rfc1048
```

where:

j4121switch	is a user-defined symbolic name to help you find the correct section of the bootptab file. If you have multiple switches that will be using Bootp to get their IP configuration, you should use a unique symbolic name for each switch.
ht	is the "hardware type". For the Switches 1600M/2424M/4000M/8000M, set this to ether (for Ethernet). <i>This tag must precede the ha tag.</i>
ha	is the "hardware address". Use the switch's (or VLAN's) 12-digit MAC address.
ip	is the IP address to be assigned to the switch (or VLAN).
sm	is the subnet mask of the subnet in which the switch (or VLAN) is installed.
gw	is the IP address of the default gateway.
lg	TFTP server address (source of final configuration file)
T144	is the vendor-specific "tag" identifying the configuration file to download.
vm	is a required entry that specifies the Bootp report format. For the Switches 1600M/2424M/4000M/8000M, set this parameter to rfc1048 .

Note

The above Bootp table entry is a sample that will work for the Switches 1600M/2424M/4000M/8000M when the appropriate addresses and file names are used. There are other features and parameters that can be implemented with Bootp. See the documentation for your Bootp server for more information.

Configuring DHCP/Bootp

In its default configuration, the switch is configured for DHCP/Bootp operation. However, if an IP address has previously been configured or if the **IP Config** parameter has been set to **Disabled**, then you will need to use this procedure to reconfigure the parameter to enable DHCP/Bootp operation.

This procedure assumes that, for Bootp operation:

- A Bootp database record has already been entered into an appropriate Bootp server.
- The necessary network connections are in place
- The Bootp server is accessible from the switch

and, for DHCP operation:

- The necessary network connections are in place
- A DHCP server is accessible from the switch

To configure the switch or a VLAN for DHCP/Bootp:

1. From the Main Menu, select
 - 2. Switch Management Access Configuration (IP, SNMP, Console)**
 - 1. IP Configuration**
2. Press **[E]** (for Edit mode), then use **[↓]** to move the cursor to the **IP Config** parameter field.
3. Use the Space bar to select the **DHCP/Bootp** option for the **IP Config** parameter. (This disables access to the IP Address, Subnet Mask, and Gateway parameters.)
4. Press **[Enter]** to exit from edit mode, then press **[S]** to save the configuration change.

When you press **[S]** to save the configuration change or reboot the switch with DHCP/Bootp enabled in a network providing DHCP/Bootp service, it will do the following:

- Receive an IP address and subnet mask and, if configured in the server, a gateway IP address and the address of a Timep server.
- For Bootp operation, if the reply provides information for downloading a configuration file, the switch then uses TFTP to download the file from the designated source, then reboots itself. (This assumes that the switch or VLAN has connectivity to the TFTP file server specified in the Bootp database configuration record, that the Bootp database record is correctly configured, and that the configuration file exists in the TFTP directory.)

Globally Assigned IP Network Addresses

If you intend to connect your network to other networks that use globally administered IP addresses, Hewlett-Packard strongly recommends that you use IP addresses that have a network address assigned to you. There is a formal process for assigning unique IP addresses to networks worldwide. Contact one of the following companies:

Country	Phone Number/E-Mail/URL	Company Name/Address
United States/ Countries not in Europe or Asia/Pacific	1-703-742-4777 questions@internic.net http://rs.internic.net	Network Solutions, Inc. Attn: InterNIC Registration Service 505 Huntmar Park Drive Herndon, VA 22070
Europe	+31 20 592 5065 ncc@ripe.net http://www.ripe.net	RIPE NCC Kruislaan 409NL-1098 SJ Amsterdam, The Netherlands
Asia/Pacific	domreg@apnic.net http://www.apnic.net	Attention: IN-ADDR.ARPA Registration Asia Pacific Network Information Center c/o Internet Initiative Japan, Inc. Sanbancho Annex Bldg. 1-4 Sanban-cho Chiyoda-ku Tokyo 102, Japan

For more information, refer to *Internetworking with TCP/IP: Principles, Protocols and Architecture* by Douglas E. Comer (Prentice-Hall, Inc., publisher).

SNMP Communities

From the **switch console only** you can add, edit, or delete SNMP communities. Use this feature to restrict access to the switch by SNMP management stations. You can configure up to five SNMP communities, each with either an operator-level or a manager-level view, and either restricted or unrestricted write access.

In the default configuration, no Manager addresses are configured, and all management stations using the correct community name may access the switch with the corresponding View and Access levels specified for those communities. For any community name, if you want to restrict access to one or more specific nodes, you can enter up to ten IP addresses of such nodes into the Manager Address field. Entering one or more IP addresses in the Manager Address field restricts access with that community to only those addresses.

For more on this topic, refer to chapter 5, “Using HP TopTools or Other SNMP Tools To Monitor and Manage Your Network”, and to the online Help.

Configuring SNMP Communities from the Switch Console

Before you begin, ensure that the switch has been configured for IP.

Caution

Deleting or changing the community named “public” prevents network management applications (such as auto-discovery, traffic monitoring, and threshold setting) from operating in the switch. (Changing or deleting the “public” name also generates an Event Log message.) If security for network management is a concern, it is recommended that you change the write access for the “public” community to “Restricted”.

To View, Edit, or Add SNMP Communities:

1. From the Console Main Menu, Select:
 2. **Switch Management Access Configuration (IP, SNMP, Console)...**
 2. **SNMP Community Names/Authorized Managers**

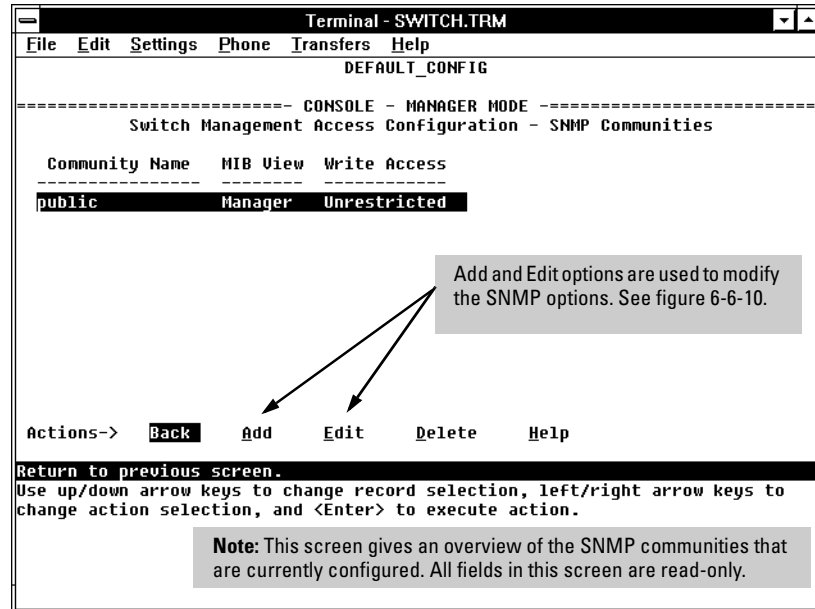


Figure 6-9. The SNMP Communities Screen (Default Values)

2. From the Configuration screen, select SNMP Communities to display a screen similar to the one above.
3. Press **[A]** (for **Add**) to display the following screen:

If you are adding a community, the fields in this screen are blank.

If you are editing an existing community, the values for the currently selected Community appear in the fields.

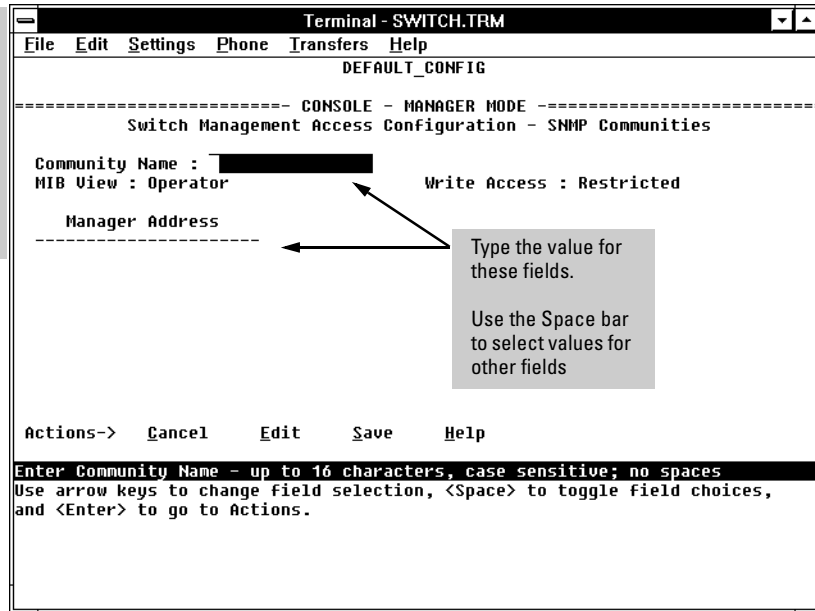


Figure 6-10. The SNMP Add or Edit Screen

Note

In the default configuration, no manager addresses are configured. In this case, all management stations using the correct community name may access the switch with the corresponding View and Access levels. If you want to restrict access to one or more specific nodes, you can enter up to ten IP addresses of such nodes into the Manager Address field. Entering one or more IP addresses in the Manager Address field limits access to only those addresses.

4. Enter the appropriate value in each of the above fields (use the **Tab** key to move from one field to the next).
5. Press **Enter**, then **S** (for **Save**).

Trap Receivers

From the **switch console only** you to configure up to ten IP management stations (*trap receivers*) to receive SNMP trap packets sent from the switch. Trap packets describe specific event types. (These events are the same as the log messages displayed in the event log.) The Address and Community define which management stations receive the traps.

If the **Send Authentication Traps** field is set to Yes, an authentication trap is sent to the addresses on the screen if any management station attempts an unauthorized access of the switch. Check the event log in the console interface to help determine why the authentication trap was sent. (Refer to “Using the Event Log To Identify Problem Sources” on page 8-12.)

To configure Trap Receivers from the switch console:

1. From the Console Main Menu, select
 2. **Switch Management Access Configuration (IP, SNMP, Console)...**
 3. **Trap Receivers**

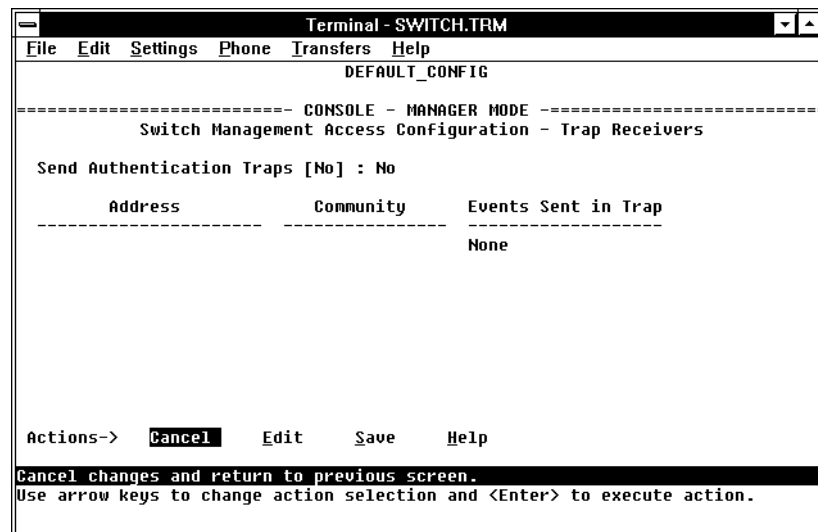


Figure 6-11. The Trap Receivers Configuration Screen (Default Values)

2. Press **[E]** (for **E**dit). The cursor moves to the **Send Authentication Traps** field.
3. Press the Space bar to enable (Yes) or disable (No) sending authentication traps, then press **[Tab]** to move the cursor to the Address field.
4. Type in the IP address of a network management station to which you want the switch to send SNMP trap packets, then press **[Tab]** to move the cursor to the Community field.
5. Type in the name of the SNMP community to which the network management station belongs, then press **[Tab]** to move the cursor to the Events field.
6. Use the Space bar to select the level of internal switch events that cause trap packets to be sent:

Event Level	Description
None (default)	Send no log messages.
All	Send all log messages.
Not INFO	Send the log messages that are not information-only.
Critical	Send critical-level log messages.
Debug	Reserved for HP-internal use.

7. Press **[Enter]**, then press **[S]** (for **S**ave) and return to the Main Menu.

Console/Serial Link

From the **switch console only** you can configure the following console terminal emulation and communication characteristics:

- Enable or disable inbound Telnet access (default: enabled)
- Enable or disable HP web browser interface access (default: enabled)
- Specify:
 - Terminal type (default: VT-100)
 - Console screen refresh interval for statistics screens (the frequency with which statistics are updated on the screen—default: 3 seconds)
 - The types of events displayed in the console event log (default: all)
- Customize the Console configuration for the PC or terminal you are using for console access.
 - Baud Rate (default: Speed Sense)
 - Flow Control (default: XON/XOFF)
 - Connection Inactivity Time (default: 10 minutes)

In most cases, the default configuration is acceptable for standard operation. If you need to change any of the above parameters, use the switch console.

Note

If you change the Baud Rate or Flow Control settings for the switch, you should make the corresponding changes in your console access device. Otherwise, you may lose connectivity between the switch and your terminal emulator due to differences between the terminal and switch settings for these two parameters.

Configuring the Console/Serial Link from the Switch Console

This screen allows you to:

- Enable or disable inbound Telnet and web browser interface access
- Determine which log events will be displayed
- Modify console and serial link parameters

To Access Console/Serial Link Features:

1. From the Console Main Menu, Select...
 2. **Switch Management Access Configuration (IP, SNMP, Console)...**
 4. **Console/Serial Link Configuration**

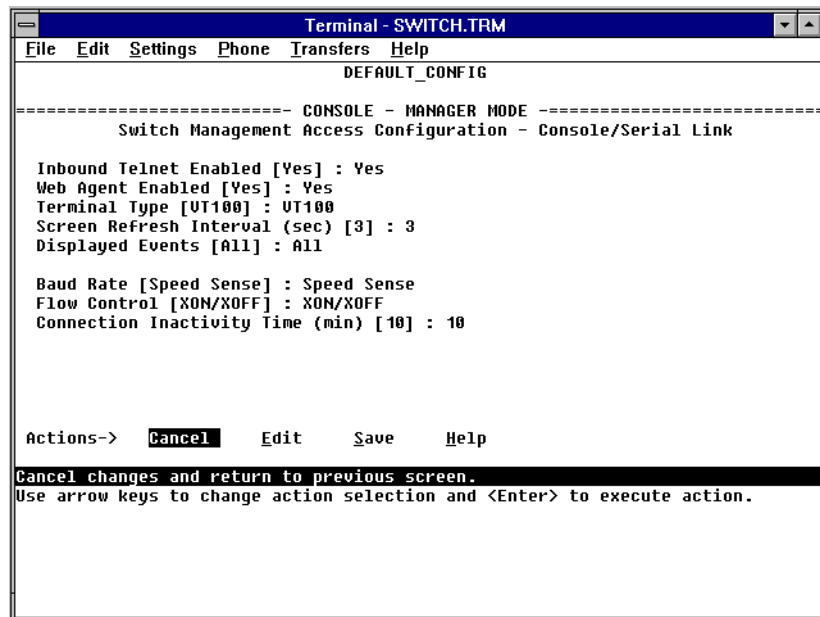


Figure 6-12. The Console/Serial Link Configuration Screen (Default Values)

2. Press **[E]** (for **Edit**). The cursor moves to the top field on the screen.
3. Refer to the online help provided with this screen for further information on configuration options for these features.
4. When you have finished making changes to the above parameters, press **[Enter]**, then press **[S]** (for **Save**) and return to the Main Menu

Enhancing Security By Configuring Authorized IP Managers

This feature enables you to enhance security on the switch by using IP addresses to authorize which stations (PCs or workstations) are allowed to:

- Access the switch's web browser interface
- Telnet into the switch's console interface
- Perform TFTP transfers of configurations and software updates into the switch

Note

This feature does not affect SNMP access to the switch by SNMP-authorized management stations. (SNMP access is protected by community names and an independent SNMP Authorized Managers list.)

You can configure:

- Up to 10 authorized manager addresses, where each address applies to either a single management station or a group of stations
- Either a Manager or Operator access level

Note

This feature does not protect access to the switch through a modem or direct Console (RS-232) port connection. Also, if the IP address assigned to an authorized management station is configured in another station, the other station can gain management access to the switch even though a duplicate IP address condition exists. For these reasons, you should enhance your network's security by keeping physical access to the switch restricted to authorized personnel, using the password features built into the switch, and preventing unauthorized access to data on your management stations.

Access Levels

For each authorized manager address, you can configure either one of these access levels:

- **Manager:** Enables full access to all web browser and console interface screens for viewing, configuration, and all other operations available in these interfaces.
- **Operator:** Allows view-only access from the web browser and console interfaces. (This is the same access that is allowed by the switch's operator-level password feature.)

Defining Authorized Management Stations

- **Authorizing Single Stations:** The table entry authorizes a single management station to have IP access to the switch. To use this method, just enter the IP address of an authorized management station in the Authorized Manager IP column, and leave the IP Mask set to **255.255.255.255**. This is the easiest way to use the Authorized Managers feature. (For more on this topic, see “Configuring One Station Per Authorized Manager IP Entry” on page 6-25.)
- **Authorizing Multiple Stations:** The table entry authorizes a defined group of stations to access the switch. This is useful if you want to easily authorize several stations to have access to the switch without having to type in an entry for every station. All stations in the group defined by the one Authorized Manager IP table entry and its associated IP mask will have the same access level—Manager or Operator. (For more on this topic, see “Configuring Multiple Stations Per Authorized Manager IP Entry” on page 6-25.)

To configure the switch for authorized manager access, enter the appropriate *Authorized Manager IP* value, specify an *IP Mask*, and select either **Manager** or **Operator** for the *Access Level*. The IP Mask determines how the Authorized Manager IP value is used to define authorized IP addresses for management station access.

Overview of IP Mask Operation

The default IP Mask is 255.255.255.255 and allows switch access only to a station having an IP address that is identical to the Authorized Manager IP parameter value. (“255” in an octet of the mask means that only the exact value in the corresponding octet of the Authorized Manager IP parameter is allowed in the IP address of an authorized management station.) However, you can alter the mask and the Authorized Manager IP parameter to specify ranges of authorized IP addresses. For example, a mask of **255.255.255.0** and any value for the Authorized Manager IP parameter allows a range of 0 through 255 in the 4th octet of the authorized IP address, which enables a block of up to 256 IP addresses for IP management access. A mask of **255.255.255.252** uses the 4th octet of a given Authorized Manager IP address to authorize four IP addresses for management station access. The details on how to use IP masks are provided under “Building IP Masks” on page 6-24.

Note

The IP Mask is a method for recognizing whether a given IP address is authorized for management access to the switch. This mask serves a different purpose than IP subnet masks and is applied in a different manner.

Configuring IP Authorized Managers in the Web Browser Interface

1. Click here.

2. Click here.

3. Enter an Authorized Manager IP address here.

4. Use the default mask to allow access by one management station, or edit the mask to allow access by a group of management stations (page 6-24).

5. Select Manager level or Operator level access (page 6-21.)

6. Click here to add your entry to the list.

Example of entry with default IP mask (allowing access by only one station).

Authorized Manager IP	IP Mask	Access Level
11.33.248.5	255.255.255.255	Manager
11.33.244.1	255.255.248.0	Manager
11.33.254.1	255.255.255.0	Operator

Authorized Manager IP:

IP Mask:

Access Level:

This allows you to specify which bits in the Manager IP address to compare against when validating an authorized manager.

Figure 6-13. Example of an Authorized IP Manager List with Manager and Operator Assignments

Configuring IP Authorized Managers in the Console Interface

From the console Main Menu, select:

2. Switch Management Access Configuration (IP, SNMP, Console) . . .
6. IP Authorized Managers

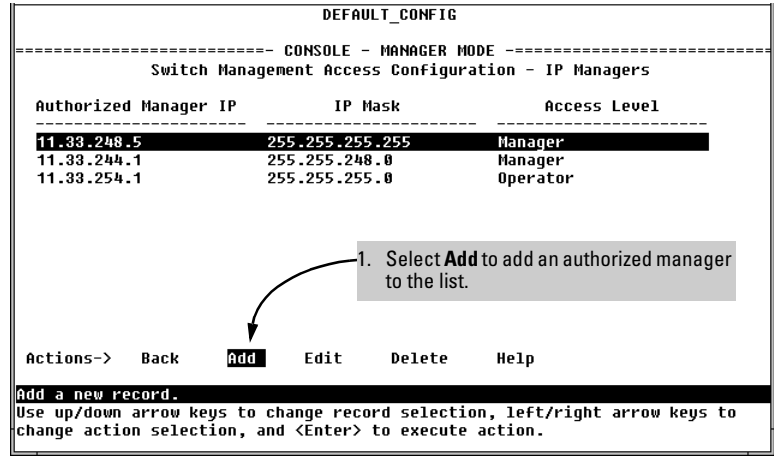


Figure 6-14. Example of How To Add an Authorized Manager Entry

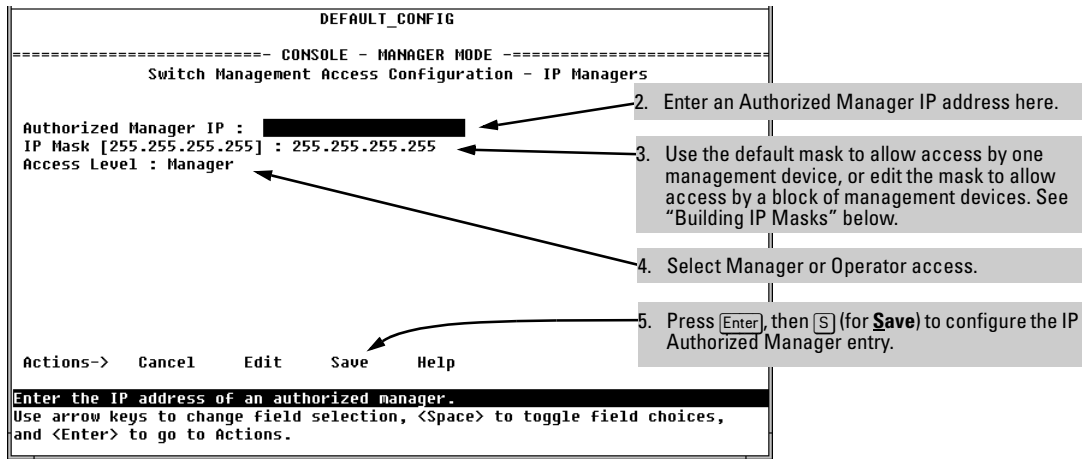


Figure 6-15. Example of How To Add an Authorized Manager Entry (Continued)

Editing or Deleting an Authorized Manager Entry. Go to the IP Managers List screen (figure 6-14), highlight the desired entry, and press [E] (for **E**dit) or [D] (for **D**elete).

Building IP Masks

The IP Mask parameter controls how the switch uses an Authorized Manager IP value to recognize the IP addresses of authorized manager stations on your network.

Configuring One Station Per Authorized Manager IP Entry

This is the easiest way to apply a mask. If you have ten or fewer management and/or operator stations, you can configure them quickly by simply adding the address of each to the Authorized Manager IP list with **255.255.255.255** for the corresponding mask. For example, as shown in figure 6-13 on page 6-23, if you configure an IP address of **11.33.248.5** with an IP mask of **255.255.255.255**, only a station having an IP address of **11.33.248.5** has management access to the switch.

Table 6-2. Analysis of IP Mask for Single-Station Entries

	1st Octet	2nd Octet	3rd Octet	4th Octet	Manager-Level or Operator-Level Device Access
IP Mask	255	255	255	255	The "255" in each octet of the mask specifies that only the exact value in that octet of the corresponding IP address is allowed. This mask allows management access only to a station having an IP address of 11.33.248.5.
Authorized Manager IP	11	33	248	5	

Configuring Multiple Stations Per Authorized Manager IP Entry

The mask determines whether the IP address of a station on the network meets the criteria you specify. That is, for a given Authorized Manager entry, the switch applies the IP mask to the IP address you specify to determine a range of authorized IP addresses for management access. As described above, that range can be as small as one IP address (if **255** is set for all octets in the mask), or can include multiple IP addresses (if one or more octets in the mask are set to less than **255**).

If a bit in an octet of the mask is "on" (set to 1), then the corresponding bit in the IP address of a potentially authorized station must match the same bit in the IP address you entered in the Authorized Manager IP list. Conversely, if a bit in an octet of the mask is "off" (set to 0), then the corresponding bit in the IP address of a potentially authorized station on the network does not have to match its counterpart in the IP address you entered in the Authorized Manager IP list. Thus, in the example shown above, a "255" in an IP Mask octet (*all* bits in the octet are "on") means only one value is allowed for that octet—the value you specify in the corresponding octet of the Authorized Manager IP list. A "0" (all bits in the octet are "off") means that any value from 0 to 255 is allowed in the corresponding octet in the IP address of an authorized station. You can also specify a series of values that are a subset of the 0-255 range by using a value that is greater than 0, but less than 255.

Table 6-3. Analysis of IP Mask for Multiple-Station Entries

	1st Octet	2nd Octet	3rd Octet	4th Octet	Manager-Level or Operator-Level Device Access
IP Mask	255	255	255	0	The "255" in the first three octets of the mask specify that only the exact value in the octet of the corresponding IP address is allowed. However, the zero (0) in the 4th octet of the mask allows any value between 0 and 255 in that octet of the corresponding IP address. This mask allows switch access to any device having an IP address of 11.33.248.xxx, where xxx is any value from 0 to 255.
Authorized Manager IP	11	33	248	5	
IP Mask	255	255	255	249	In this example (figure 6-16, below), the IP mask allows a group of up to 4 management stations to access the switch. This is useful if the only devices in the IP address group allowed by the mask are management stations. The "249" in the 4th octet means that bits 0 and 3 - 7 of the 4th octet are fixed. Conversely, bits 1 and 2 of the 4th octet are variable. Any value that matches the authorized IP address settings for the fixed bits is allowed for the purposes of IP management station access to the switch. Thus, any management station having an IP address of 11.33.248. <u>1</u> , <u>3</u> , <u>5</u> , or <u>7</u> can access the switch.
Authorized IP Address	11	33	248	5	

4th Octet of IP Mask:				249					
4th Octet of Authorized IP Address:				5					
Bit Numbers	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0	
Bit Values	128	64	32	16	8	4	2	1	
4th Octet of IP Mask (249)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Bits 1 and 2 in the mask are "off", and bits 0 and 3 - 7 are "on", creating a value of 249 in the 4th octet of the mask.
4th Octet of IP Authorized Address (5)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Where a mask bit is "on", the corresponding bit setting in the address of a potentially authorized station must match the IP Authorized Address setting for that same bit. Where a mask bit is "off" the corresponding bit setting in the address can be either "on" or "off". In this example, in order for a station to be authorized to access the switch:
									<ul style="list-style-type: none"> • The first three octets of the station's IP address must match the Authorized IP Address. • Bit 0 of the 4th octet in the station's address must be "on" (value = 1). • Bits 3 through 7 of the 4th octet in the station's address must be "off" (value = 0). • Bits 1 and 2 can be either "on" or "off". This means that stations with the IP address 11.33.248.X (where X is 1, 3, 5, or 7) are authorized.

Figure 6-16. Example of How the Bitmap in the IP Mask Defines Authorized Manager Addresses

Additional Examples for Authorizing Multiple Stations

	Entries for Authorized Manager List				Results
IP Mask	255	255	0	255	This combination specifies an authorized IP address of 10.33.xxx.1. It could be applied, for example, to a subnetted network where each subnet is defined by the third octet and includes a management station defined by the value of "1" in the fourth octet of the station's IP address.
Authorized Manager IP	10	33	248	1	
IP Mask	255	238	255	250	Allows 230, 231, 246, and 247 in the 2nd octet, and 194, 195, 198, 199 in the 4th octet.
Authorized Manager IP	10	247	100	195	

Operating and Troubleshooting Notes

- **Network Security Precautions:** You can enhance your network's security by keeping physical access to the switch restricted to authorized personnel, using the password features built into the switch, and preventing unauthorized access to data on your management stations.
- **Modem and Direct Console Access:** Configuring authorized IP managers does not protect against access to the switch through a modem or direct Console (RS-232) port connection.
- **Duplicate IP Addresses:** If the IP address configured in an authorized management station is also configured in another station, the other station can gain management access to the switch even though a duplicate IP address condition exists.
- **Web Proxy Servers:** If you use the web browser interface to access the switch from an authorized IP manager station, it is recommended that you avoid the use of a web proxy server in the path between the station and the switch. This is because switch access through a web proxy server requires that you first add the web proxy server to the Authorized Manager IP list. This reduces security by opening switch access to anyone who uses the web proxy server. The following two options outline how to eliminate a web proxy server from the path between a station and the switch:
 - Even if you need proxy server access enabled in order to use other applications, you can still eliminate proxy service for web access to the switch. To do so, add the IP address or DNS name of the switch to the non-proxy, or "Exceptions" list in the web browser interface you are using on the authorized station.
 - If you don't need proxy server access at all on the authorized station, then just disable the proxy server feature in the station's web browser interface.

System Information

From the **web browser interface and the switch console** you can configure basic switch management information, including system data, address aging, and time zone parameters.

Configuring System Parameters from the Web Browser Interface

In the web browser interface, you can enter the system information shown below. For access to the Address Age Interval and the Time parameters, use the console.

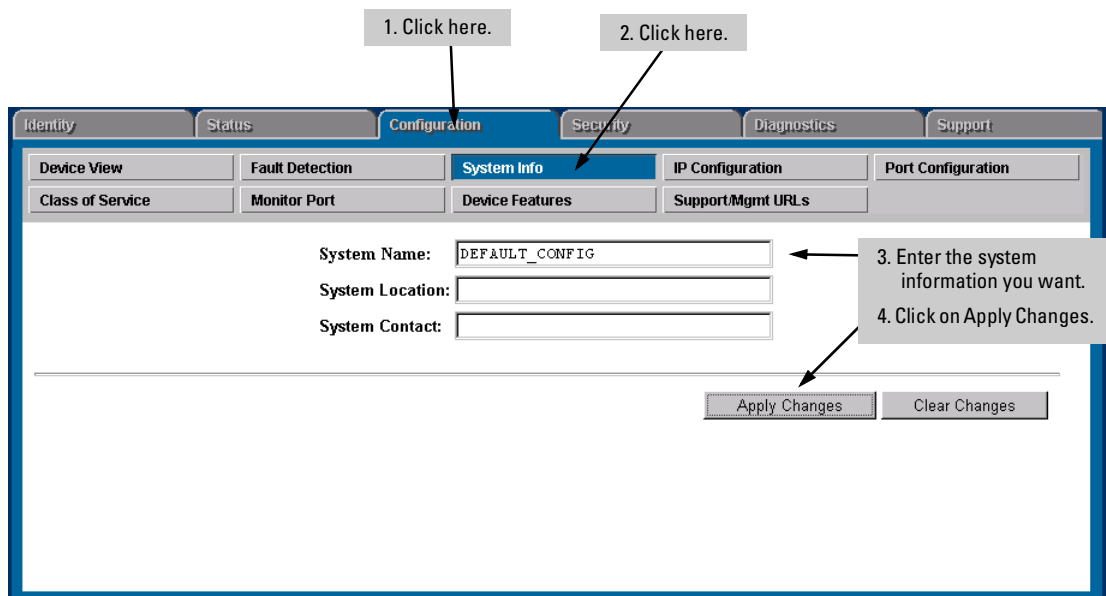


Figure 6-17. Example of System Info Screen on the Web Browser Interface

Configuring System Information from the Console

To Access System Information:

1. From the Console Main Menu, Select...

3. Switch Configuration...

1. System Information

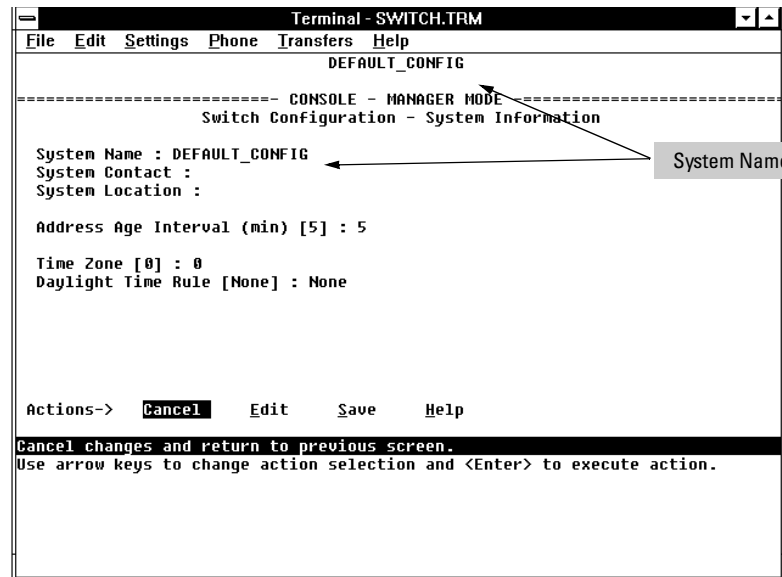


Figure 6-18. The System Configuration Screen (Default Values)

Note

To help simplify administration, it is recommended that you configure **System Name** to a character string that is meaningful within your system.

To set the time and date, set the Time Protocol parameters under “IP Configuration” (page 6-4) for your time server or use the time and date commands described in chapter 7, “Monitoring and Analyzing Switch Operation”.

2. Press **[E]** (for **E**dit). The cursor moves to the **System Name** field.
3. Refer to the online help provided with this screen for further information on configuration options for these features.
4. When you have finished making changes to the above parameters, press **[Enter]**, then press **[S]** (for **S**ave) and return to the Main Menu.

Port Settings

From the **web browser interface and switch console** you can configure the operating state for each port. Also optionally enables you to restrict the amount of broadcast traffic on the port. The read-only fields in this screen display the port numbers and port types. Port numbers in the configuration correspond to port numbers on the front of the switch.

The following table shows the settings available for each port type. The same parameter settings are available in both the web browser interface and the switch console.

Parameter	Description
Enabled	Yes (default): The port is ready to be connected in a network. No : The port will not operate, even if properly connected in a network. Use this setting if the port needs to be shut down for diagnostic purposes or while you are making topology changes, for example.
Mode or Config Mode	The operational mode of the port. For gigabit fiber-optic ports (Gigabit-SX and Gigabit-LX): 1000FDx (default): 1000 Mbps (1 Gbps), Full Duplex Auto : The port operates at 1000FDx and auto-negotiates flow control with the device connected to the port. For 100/1000Base-T ports: Auto (default): Auto-negotiates with the port at the other end of the link for speed (100 Mbps or 1000 Mbps - Gigabit), and port operation (MDI-X or MDI). Note : Ensure that the device attached to the port is configured for the same setting that you select here. Also, if "Auto" is used, the device to which the port is connected must operate in compliance with the IEEE 802.3ab "Auto Negotiation" standard for 1000Base-T networks. 100Fdx : 100 Mbps, Full-Duplex 100Hdx : 100 Mbps, Half-Duplex For 10/100TX ports: Auto (default): Auto-negotiates with the port at the other end of the link for speed (10 Mbps or 100 Mbps), flow control (enabled or disabled), and data transfer operation (half-duplex or full-duplex). Note : Ensure that the device attached to the port is configured for the same setting that you select here. Also, if "Auto" is used, the device to which the port is connected must operate in compliance with the IEEE 802.3u "Auto Negotiation" standard for 100Base-T networks. If the other device does not comply with the 802.3u standard, or is not set to Auto, then the port configuration on the switch must be manually set to match the port configuration on the other device. 10HDx : 10 Mbps, Half-Duplex 100HDx : 100 Mbps, Half-Duplex 10FDx : 10 Mbps, Full-Duplex 100FDx : 100 Mbps, Full-Duplex

Parameter	Description
	<p>For 100FX ports: 100HDx (default): 100 Mbps, Half-Duplex 100FDx: 100 Mbps, Full-Duplex</p> <p>For 10 FL ports: 10HDx:(default): 10 Mbps, Half-Duplex 10FDx: 10 Mbps, Full-Duplex</p>
Flow Control	<p>Maximizes circuit efficiency by enabling negotiation of packet parameters with the device to which the port is connected.</p> <p>Disabled (default): The port will not generate flow control packets and drops received flow control packets.</p> <p>Enabled: The port uses 802.3x Link Layer Flow Control, generates flow control packets and processes received flow control packets.</p>
Bcast Limit	<p>The theoretical maximum of network bandwidth percentage that can be used for broadcast and multicast traffic. Any broadcast or multicast traffic exceeding that limit will be dropped. Zero (0) means the feature is disabled.</p>

Note

Broadcast limit (the Bcast Limit parameter) can be set for all ports in the switch (or VLAN, if VLANs are configured) from the Automatic Broadcast Control (ABC) screen (page 6-106 and following) if ABC is enabled. Setting the broadcast limit in the web browser interface or the console Port Setting screen is on a per-port basis and *overrides* any settings done in Automatic Broadcast Control. Also, if broadcast limits are configured on a group of ports, and those ports are later configured as a trunk, then the broadcast limit for the trunk will be the highest limit that was previously configured on the individual ports in the trunk.

Configuring Port Parameters from the Web Browser Interface

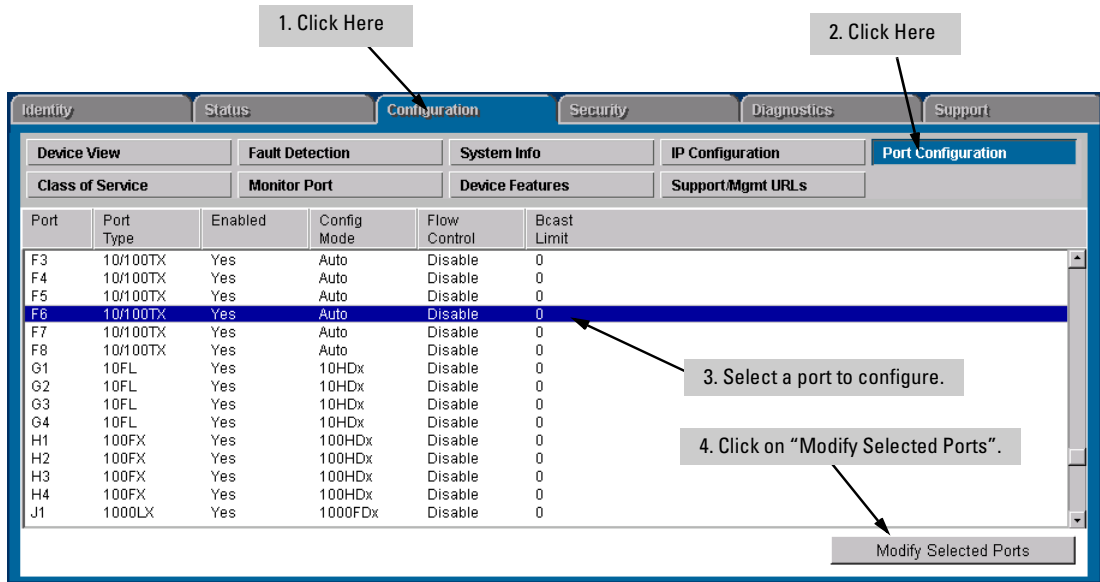


Figure 6-19. Example of Port Configuration Screen on the Web Browser Interface

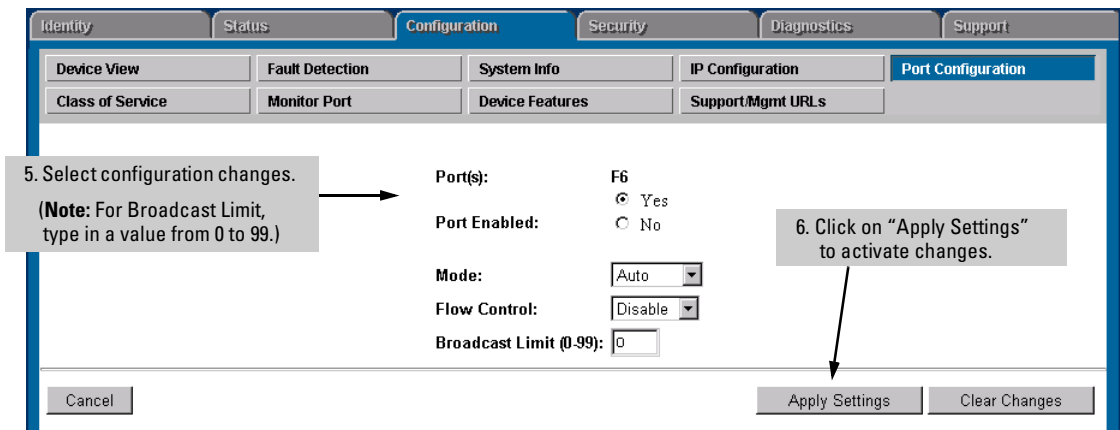


Figure 6-20. Example of Port Modification Screen on the Web Browser Interface

Configuring Port Parameters from the Switch Console

To Access Port Settings:

1. From the Console Main Menu, Select:
 - 3. Switch Configuration...**
 - 2. Port Settings**

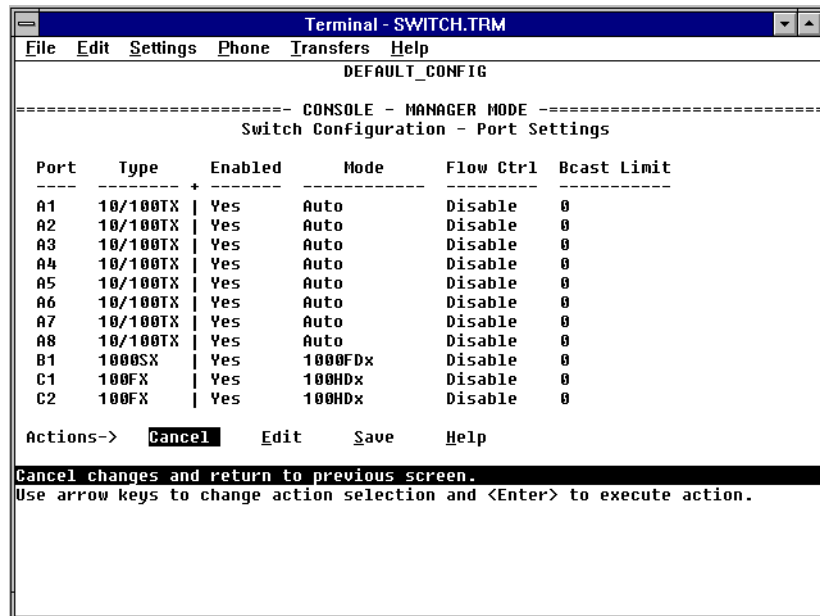


Figure 6-21. Example of the Port Settings Screen

2. Press **[E]** (for **E**dit). The cursor moves to the **Enabled** field for the first port.
3. Refer to the online help provided with this screen for further information on configuration options for these features.
4. When you have finished making changes to the above parameters, press **[Enter]**, then press **[S]** (for **S**ave) and return to the Main Menu.

Network Monitoring Port Features

From the **web browser interface and switch console** you can designate a port for monitoring traffic on one or more other ports or on a VLAN configured on the switch. The switch monitors the network activity by copying all traffic from the specified ports or VLAN to the designated monitoring port.

Note

It is possible, when monitoring multiple ports in networks with high traffic levels, to copy more traffic to a monitor port than the link can support. In this situation, some packets may not be copied to the monitor port.

Configuring Port Monitoring from the Web Browser Interface

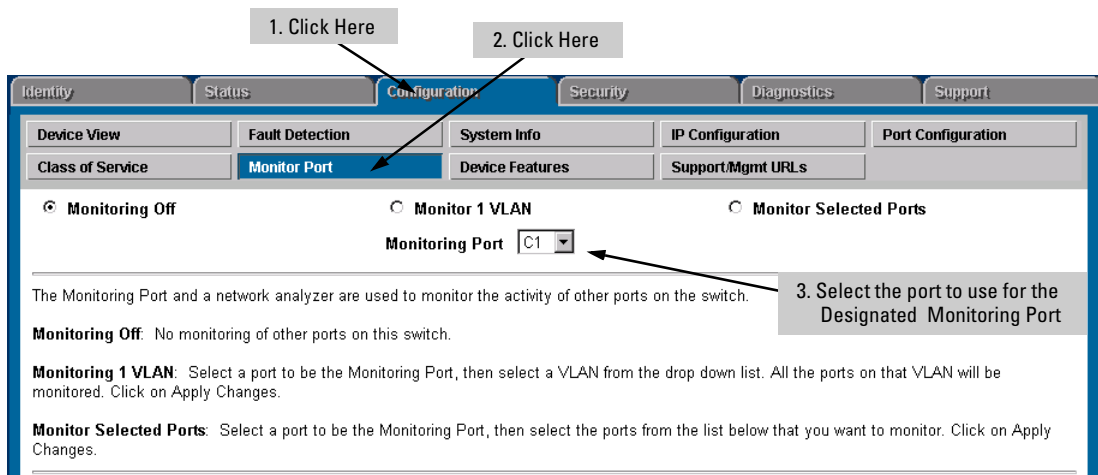


Figure 6-22. Setting Up Port Monitoring on the Web Browser Interface

Do one of the following:

- If you want to monitor one port or several ports, click on the **Monitor Selected Ports** button. (See figure 6-23, below.)
- If you want to monitor VLAN traffic, click on the **Monitor 1 VLAN** button. (See figure 6-24, below.)

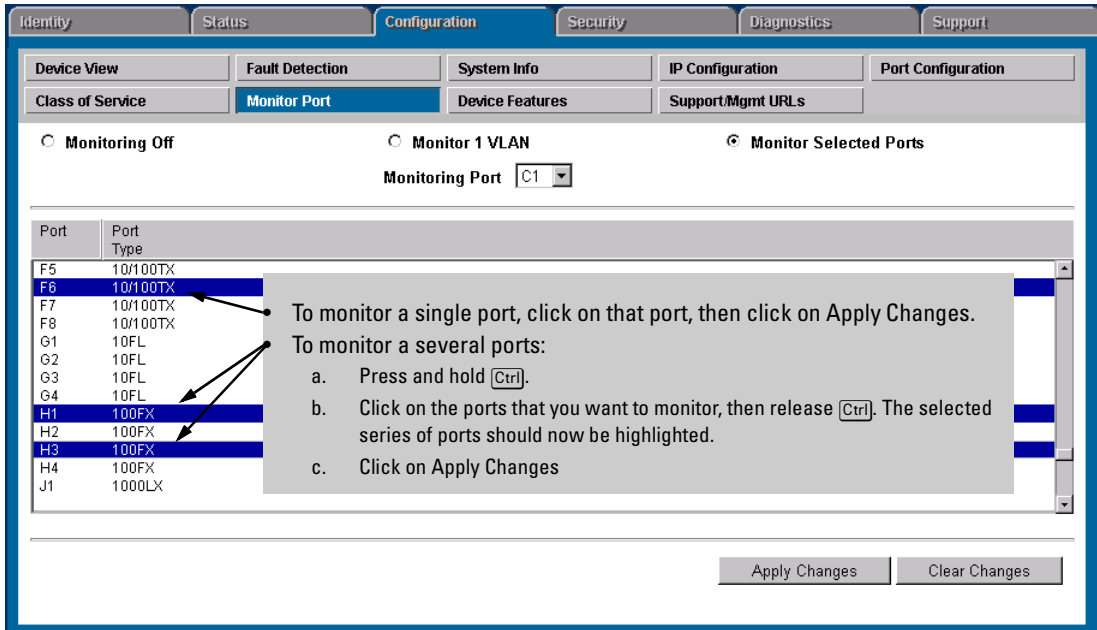


Figure 6-23. Selecting the Port(s) To Monitor

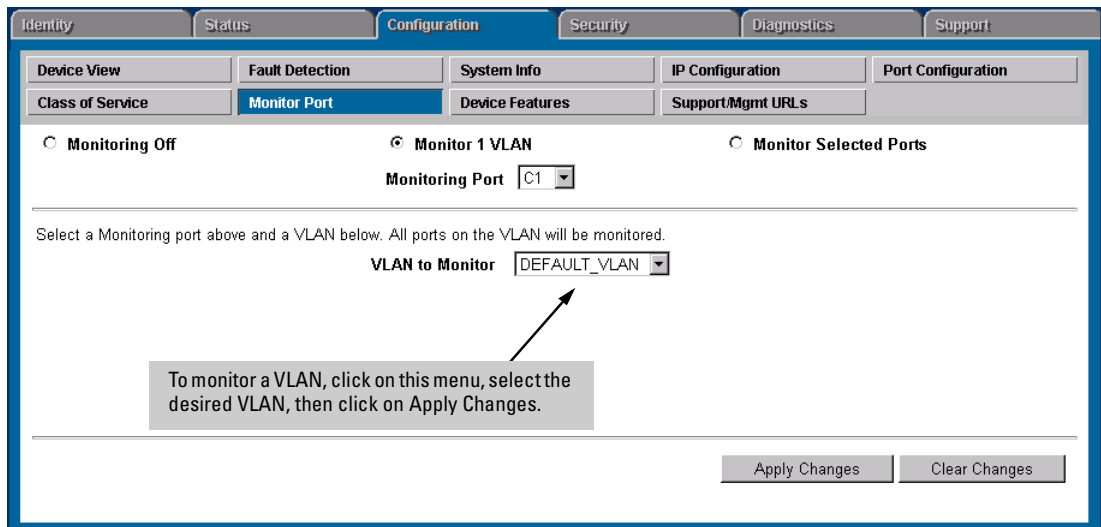


Figure 6-24. Selecting a VLAN To Monitor

Configuring Port Monitoring from the Switch Console

To Access Port Monitoring:

This procedure describes configuring the switch for monitoring when monitoring is disabled. (If monitoring has already been enabled, the screens will appear differently than shown in this procedure.)

1. From the Console Main Menu, Select:
3. Switch Configuration...
3. Network Monitoring Port

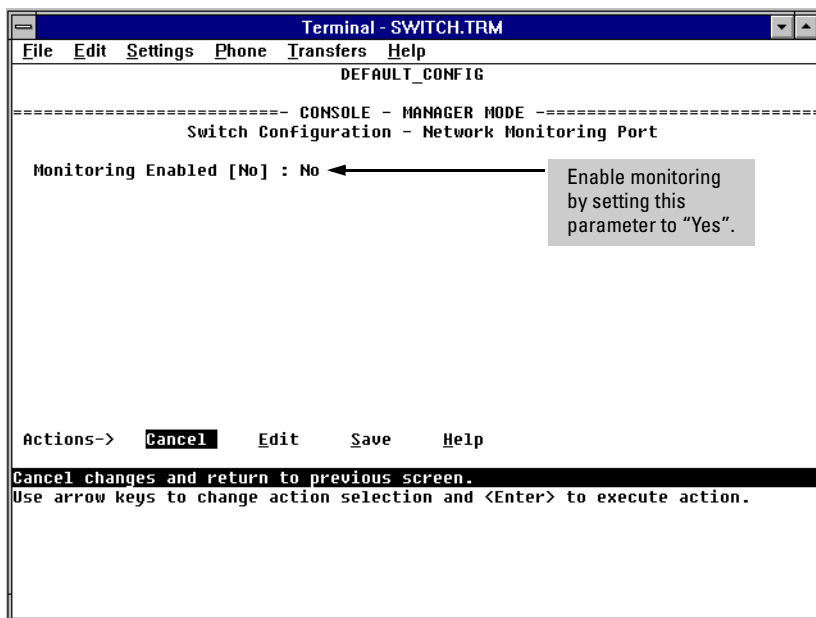


Figure 6-25. The Default Network Monitoring Configuration Screen

2. In the Actions menu, press **[E]** (for **Edit**).
3. If monitoring is currently disabled (the default) then enable it by pressing the Space bar (or **[Y]**) to select **Yes**.
4. Press **[↓]** to display a screen similar to the following and move the cursor to the **Monitoring Port** parameter.

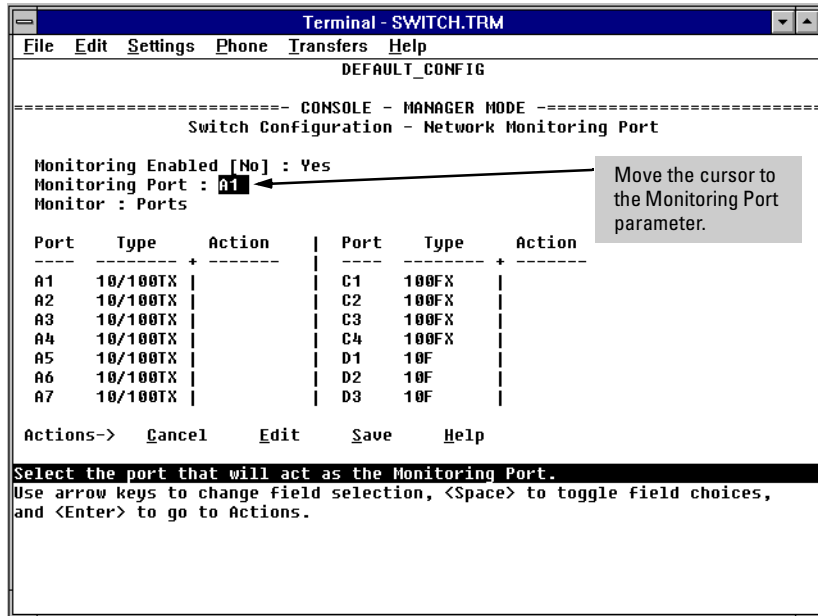


Figure 6-26. Example of Selecting a Monitoring Port

5. Use the Space bar to select which port to use for the monitoring port, then press to move to the **Monitor** parameter. (The default setting is **Ports**, which you will use if you want to monitor one or more individual ports on the switch.)
6. Do one of the following:
 - If you want to monitor individual ports, leave the **Monitor** parameter set to **Ports** and press to move the cursor to the **Action** column for the individual ports. Press the Space bar to select **Monitor** for each port that you want monitored. (Use to move from one port to the next in the **Action** column.) When you are finished, press , then press (for **Save**) to save your changes and exit from the screen.
 - If, instead of individual ports, you want to monitor all of the ports in a VLAN, press the Space bar to select **VLAN** in the **Monitor** parameter, then press to move to the **VLAN** parameter (figure 6-21 on page 6-38). Then press the Space bar again to select the VLAN that you want to monitor. When you are finished, press , then press (for **Save**) to save your changes and exit from the screen.

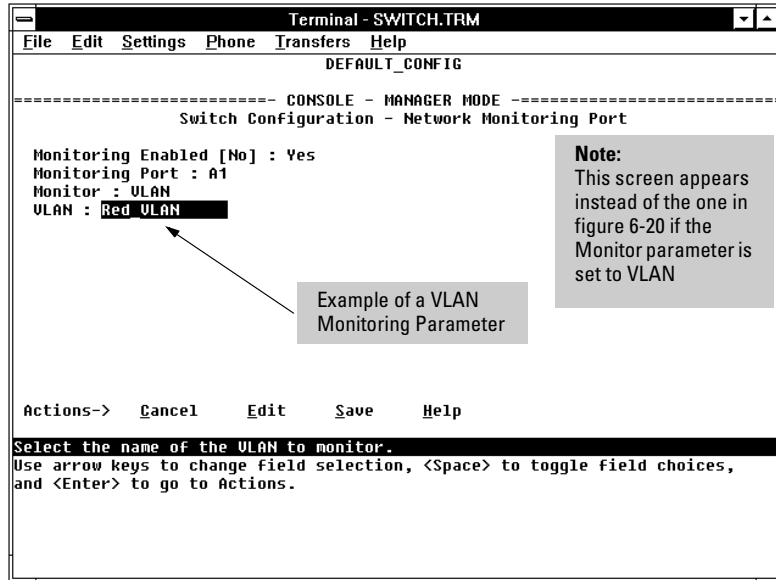


Figure 6-27. Example of Selecting a VLAN to Monitor

7. Return to the Main Menu.

Spanning Tree Protocol (STP)

The switch uses the IEEE 802.1D Spanning Tree Protocol (STP), when enabled, to ensure that only one path at a time is active between any two nodes on the network. (A switch mesh domain is seen as one path by STP.) In networks where there is more than one physical path between any two nodes, STP ensures a single active path between them by blocking all redundant paths. Enabling STP is necessary in such networks because having more than one path between a pair of nodes causes loops in the network, which can result in duplication of messages, leading to a “broadcast storm” that can bring down the network.

Note

You should enable STP in any switch that is part of a redundant physical link (loop topology). (It is recommended that you enable STP on all switches belonging to a loop topology.) This topic is covered in more detail under “How STP Operates” on page 6-42.

As recommended in the IEEE 802.1Q VLAN standard, the Switches 1600M/2424M/4000M/8000M use **single-instance STP**; a single spanning tree is created to make sure there are no network loops associated with any of the connections to the switch, regardless of whether VLANs are configured on the switch. Thus, these switches do not distinguish between VLANs when identifying redundant physical links. However, STP sees a switch mesh domain as a single link, which enables you to use both STP and meshing without blocking switch ports that you want to remain open. If VLANs are configured on the switch, see “STP Operation with 802.1Q VLANs” on page 6-44.

From the **web browser interface**, you can activate and deactivate the IEEE 802.1D Spanning Tree Protocol (STP); from the **switch console**, you can activate and deactivate STP and adjust the STP parameters. In the factory default configuration, STP is off. If a redundant link (loop) exists between nodes in your network, you should set the Spanning Tree Enabled parameter to **Yes**.

Caution

Because the switch automatically gives faster links a higher priority, the default STP parameter settings are usually adequate for spanning tree operation. Because incorrect STP settings can adversely affect network performance, you should avoid making changes without having a strong understanding of how STP operates. For more on STP, examine the IEEE 802.1D standard.

Enabling STP from the Web Browser Interface

This procedure enables or disables STP on the switch.

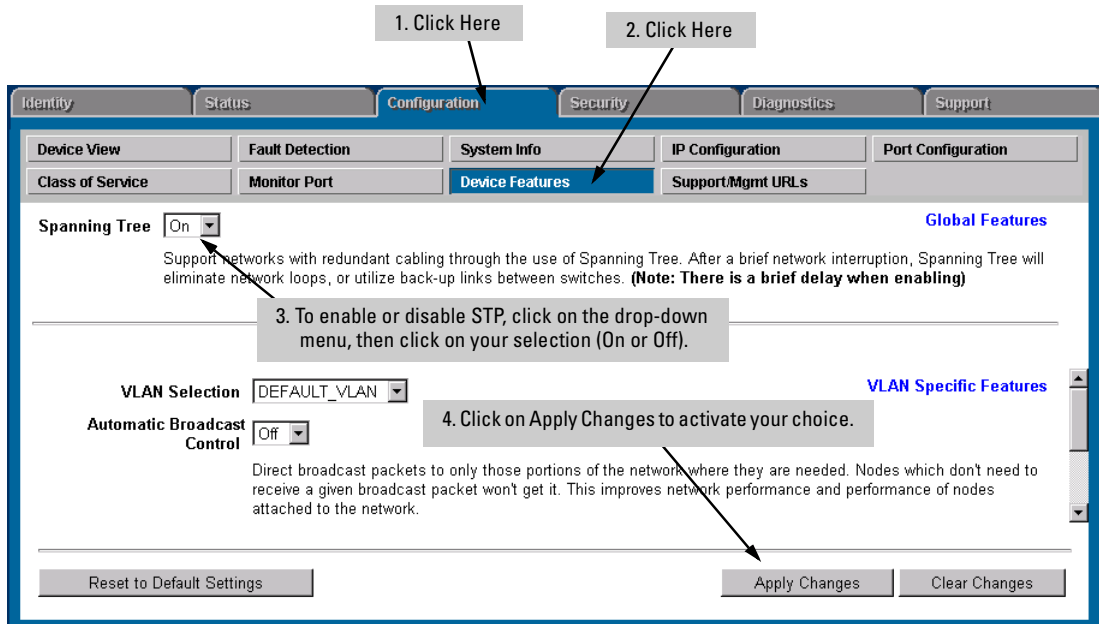


Figure 6-28. Configuring STP from the Web Browser Interface

Parameter	Description
Spanning Tree	Enables or disables Spanning Tree Protocol across all ports on the switch, including those in separate VLANs. Other STP parameters are available through the console interface. Enabling or disabling STP through the web browser interface does not affect the settings of these other parameters. For more information on STP operation, refer to “How STP Operates” on page 6-42.
Default: Off	

Configuring STP from the Switch Console

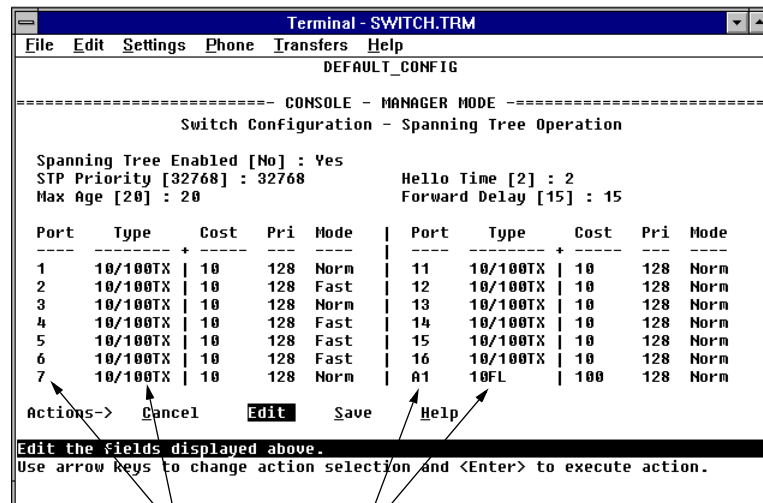
In most cases, the default STP parameter settings are adequate. In cases where they are not, use this procedure to make configuration changes.

Caution

If you enable STP, it is recommended that you leave the remainder of the STP parameter settings at their default values until you have had an opportunity to evaluate STP performance in your network. Because incorrect STP settings can adversely affect network performance, you should avoid making changes without having a strong understanding of how STP operates. To learn the details of STP operation, refer to the IEEE 802.1D standard.

To Access STP:

- From the Main Menu, select:
 - 3. Switch Configuration . . .**
 - 4. Spanning Tree Operation**
- Press **[E]** (for **Edit**) to highlight the **Spanning Tree Enabled** parameter.
- Press the Space bar to select **Yes**. (This enables STP.)



Read-Only Fields

Figure 6-29. Example of the STP Configuration Screen

- If the remaining STP parameter settings are adequate for your network, go to step 8.

5. Use **Tab** or the arrow keys to select the next parameter you want to change, then type in the new value or press the Space Bar to select a value. (If you need information on STP parameters, press **Enter** to select the **Actions** line, then press **H** to get help.)
6. Repeat step 5 for each additional parameter you want to change.
For information on the Mode parameter, see “STP Fast Mode” below.
7. When you are finished editing parameters, press **Enter** to return to the **Actions** line.
8. Press **S** to save the currently displayed STP parameter settings, then return to the Main Menu.

How STP Operates

The switch automatically senses port identity and type, and automatically defines port cost and priority for each type. The console interface allows you to adjust the Cost and Priority for each port, as well as the Mode for each port and the global STP parameter values for the switch.

While allowing only one active path through a network at any time, STP retains any redundant physical path to serve as a backup (blocked) path in case the existing active path fails. Thus, if an active path fails, STP automatically activates (unblocks) an available backup to serve as the new active path for as long as the original active path is down. For example:

- Active path from node A to node B: 1 → 3
- Backup (redundant) path from node A to node B: 4 → 2 → 3

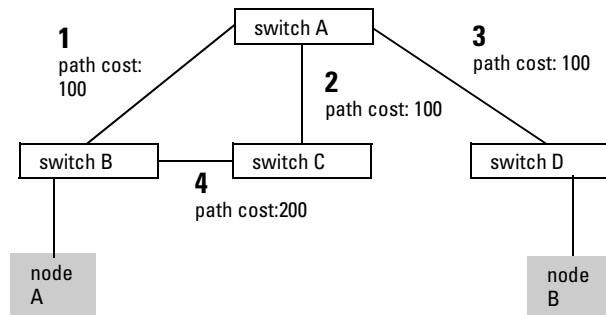


Figure 6-30. Example of Redundant Paths Between Two Nodes

STP Fast Mode

For standard STP operation, when a network connection is established on a device that is running STP, the port used for the connection goes through a sequence of states (Listening and Learning) before getting to its final state (Forwarding or Blocking, as determined by the STP negotiation). This sequence takes two times the forward delay value configured for the switch. The default is 15 seconds on HP switches, per the IEEE 802.1D standard recommendation, resulting in a total STP negotiation time of 30 seconds. Each switch port goes through this start-up sequence whenever the network connection is established on the port. This includes, for example, when the switch or connected device is powered up, or the network cable is connected.

A problem can arise from this long STP start-up sequence because some end nodes are configured to automatically try to access a network server whenever the end node detects a network connection. Typical server access includes to Novell servers, DHCP servers, and X terminal servers. If the server access is attempted during the time that the switch port is negotiating its STP state, the server access will fail. To provide support for this end node behavior, the Switches 1600M/2424M/4000M/8000M offer a configuration mode, called “Fast Mode”, that causes the switch port to skip the standard STP start-up sequence and put the port directly into the “Forwarding” state, thus allowing the server access request to be forwarded when the end node needs it.

If you encounter end nodes that repeatedly indicate server access failure when attempting to bring up their network connection, and you have enabled STP on the switch, try changing the configuration of the switch ports associated with those end nodes to STP Fast Mode.

Caution

The Fast Mode configuration should be used only on switch ports connected to end nodes. Changing the Mode to Fast on ports connected to hubs, switches, or routers may cause loops in your network that STP may not be able to immediately detect, in all cases. This will cause temporary loops in your network. After the fast start-up sequence, though, the switch ports operate according to the STP standard, and will adjust their state to eliminate continuing network loops.

To Configure Fast Mode for a Switch Port. From the switch console configuration screen for Spanning Tree Operation, shown on page 6-41:

1. Select the Edit action.
2. Scroll or Tab to the Mode column for the port you want to change.
3. Press the Space Bar to display **Fast**.

- Repeat steps 2 and 3 for all the switch ports you want to change that are connected to end nodes.
- When you have finished the configuration changes, press **[Enter]** to return to the Actions line and press **[S]** to save the new configuration.

STP Operation with 802.1Q VLANs

As recommended in the IEEE 802.1Q VLAN standard, when spanning tree is enabled on the switch, a single spanning tree is configured for all ports across the switch, including those in separate VLANs. This means that if redundant physical links exist in separate VLANs, spanning tree will block all but one of those links. However, if you need to use STP on the Switch 4000M or Switch 2424M in a VLAN environment with redundant physical links, you can prevent blocked redundant links by using a port trunk. The following example shows how you can use a port trunk with 802.1Q (tagged) VLANs and STP without unnecessarily blocking any links or losing any bandwidth.

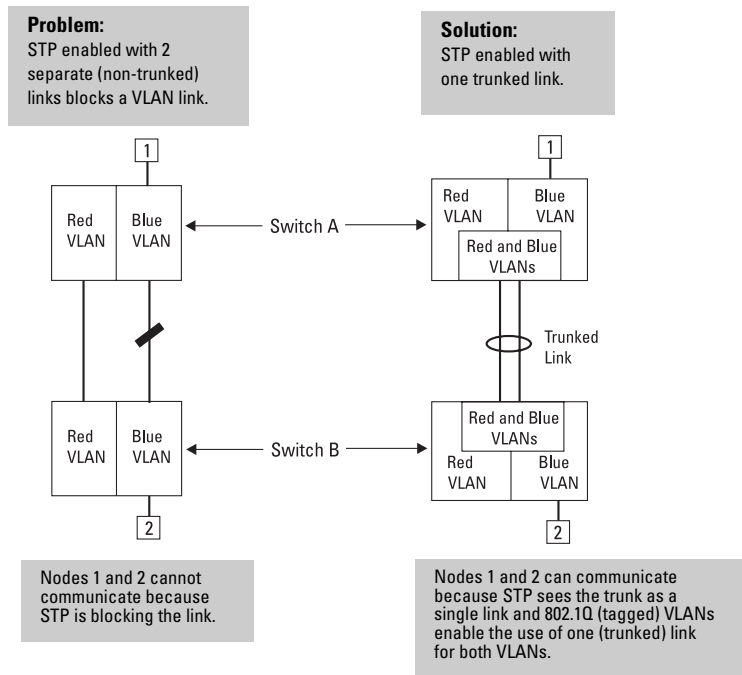


Figure 6-31. Example of Using a Trunked Link with STP and VLANs

For more information, refer to “Spanning Tree Protocol Operation with VLANs” on page 6-66.

STP Operation with Switch Meshing

As noted earlier in this section, STP sees a switch mesh domain as a single path. This makes switch meshing a useful tool for preventing STP from blocking redundant physical links in separate VLANs. (A switch mesh domain is a member of all VLANs configured on the switch.)

In some cases, switch meshing will automatically change STP Cost and Priority information. For more on this topic, refer to “Spanning Tree Operation with Switch Meshing” on page 6-89.

Further Information

For further explanation and examples of Spanning Tree Protocol operating with other switch features, see HP’s ProCurve Networking website at the following URL on the World Wide Web:

<http://www.hp.com/go/procurve>

Traffic/Security Filter Features

From the **switch console only**, you can enhance bandwidth usage and in-band security on the switch by configuring static per-port filters to forward desired traffic or drop unwanted traffic, as described below.

Table 6-4. Filter Types and Criteria

Static Filter Type	Selection Criteria
Multicast	Traffic having a specified multicast address will be forwarded or dropped on a per-port (destination) basis.
Protocol	Traffic having the selected frame (protocol) type will be forwarded or dropped on a per-port (destination) basis.
Source Port	Traffic from a designated source port will be forwarded or dropped on a per-port (destination) basis within the same VLAN.

Up to 50 static filters can be configured in the switch. For configuration information, turn to the next page. For more information on filter types and operation, refer to “Filter Types and Operation” on page 6-49.

Configuring Traffic/Security Filters from the Switch Console

Use this procedure to specify the type of filters to use on the switch and whether to forward or drop filtered packets for each filter you specify.

To Access Traffic/Security Filters

1. From the Console Main Menu, Select:
 - 3. Switch Configuration...**
 - 5. Advanced Features...**
 - 1. Traffic/Security Filters**

and the following screen appears:

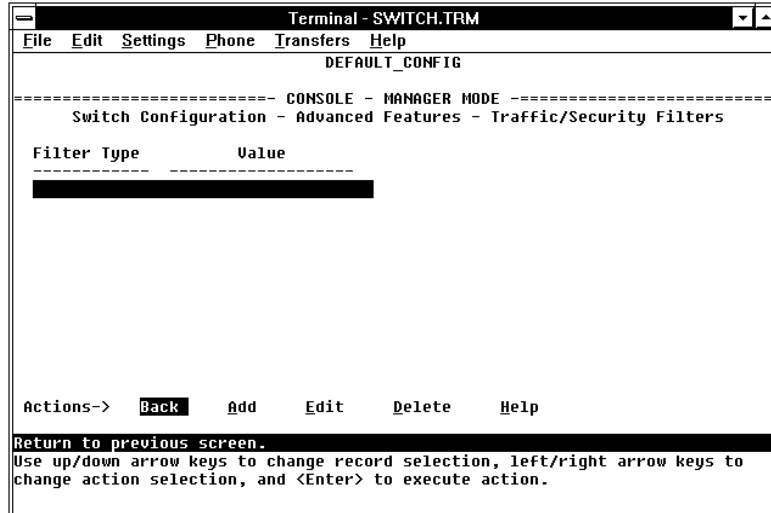


Figure 6-32. The Traffic/Security Filters List Screen (Default Values)

- In the Actions line, press **[A]** (for **Add**) to display the Traffic/Security Filters Configuration screen shown in figure 6-32.

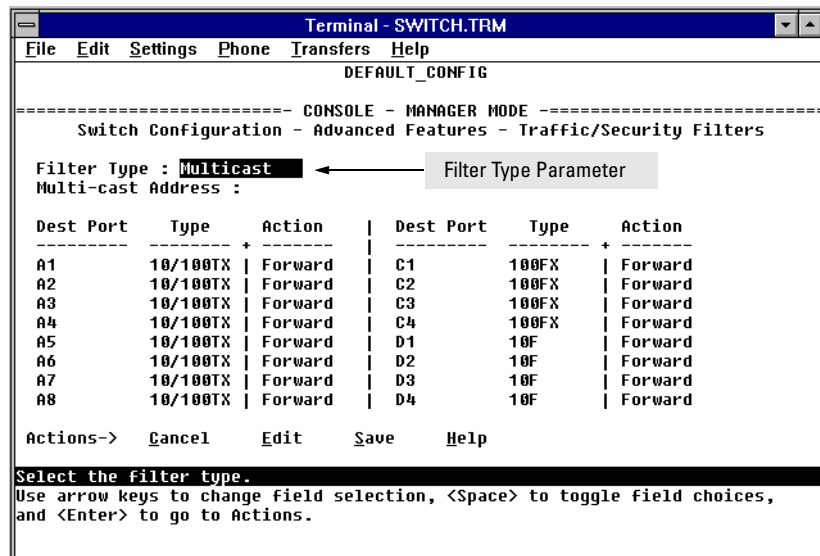


Figure 6-33. Example of the Traffic/Security Filters Configuration Screen

3. Press the Space bar to select the type of filter you want to configure. The options are:
 - Multicast (the default)
 - Protocol
 - Source Port
4. Press **↓** once to highlight the next line. Depending on the type of filter you selected in step 3, select one of the options listed in the following table:

Filter Type Option Selected in step 3	Next Line for Filter Type Option	Action for Selected Filter Option
Multicast	Multicast Address	Type in the multicast address.
Protocol	Frame Type	Use the Space bar to select the frame type.
Source Port	Source Port	Use the Space bar to select the source port.

5. Configure the filter action for each destination port. For example:

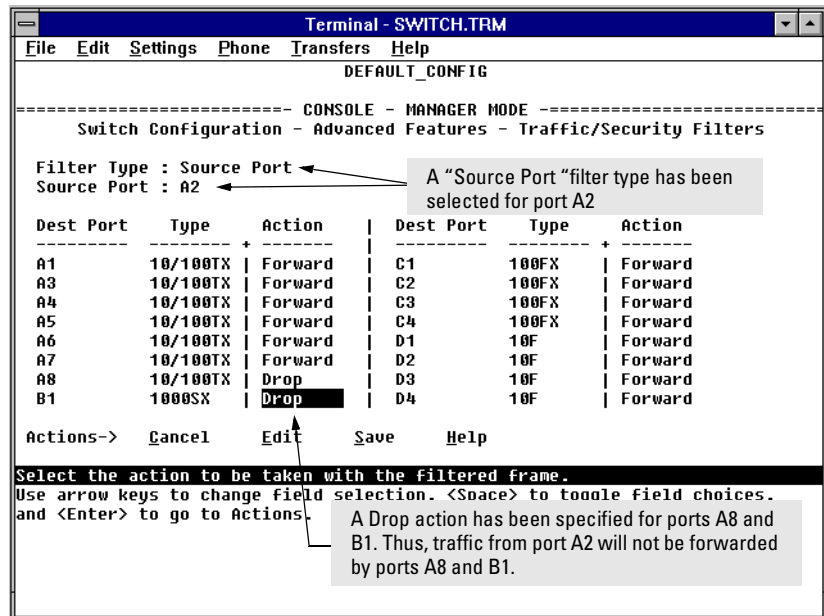


Figure 6-34. Example of Specifying Filter Actions for Individual Ports

- a. Press **↓** to highlight the **Action** option for a destination port (**Dest Port**).

- b. Press the Space bar to select the filter action for that port (**Forward** filtered packets—the default—or **Drop** filtered packets).
- c. Do one of the following:
 - To configure the filter action for another destination port, return to step a.
 - If you are finished configuring actions for the current filter, go to step 6.
6. Press **[Enter]** to return to the Actions line, then press **[S]** (for **Save**) to save the current filter configuration.
7. Do one of the following:
 - If you want to configure another filter, return to step 3.
 - If you are finished configuring filters, press **[B]** (for **Back**) to return to the Configuration menu.
8. When you are finished configuring the switch, return to the Main Menu.

Filter Types and Operation

Multicast Filters

This filter type enables the switch to send multicast traffic to a specified set of destination ports. This helps to preserve bandwidth by reducing multicast traffic on ports where it is unnecessary, and to isolate multicast traffic to enhance security.

IGMP-controlled filters will override multicast filters defined in the Traffic/Security Filters screen and having the same multicast address as specified by IGMP (page 6-95). Static multicast filters and IGMP filters (addresses) together can total up to 255 in the switch. If multiple VLANs are configured, then each filter is counted once per VLAN in which it is used.

Note:

IP Multicast Filters. Multicast filters are configured using the Ethernet format for the multicast address. IP multicast addresses occur in the range from 224.0.0.0 through 239.255.255.255 (which corresponds to the Ethernet multicast address range of 01005e-000000 through 01005e-7fffff). Any static Traffic/Security filters (page 6-46) configured with a “Multicast” filter type and a “Multicast Address” in this range will continue to be in effect unless IGMP learns of a multicast group destination in this range. In this case, IGMP takes over the filtering function for the multicast destination address(es) for as long as the IGMP group is active. If the IGMP group subsequently deactivates, the static filter resumes control over traffic to the multicast address.

Caution

If Spanning Tree is enabled, then the Spanning Tree multicast MAC address should not be filtered. (STP will not operate properly if the multicast MAC address is filtered.)

Protocol Filters

This filter type enables the switch to restrict traffic of a particular protocol type to a specific destination port or ports on the switch (or to be dropped for all ports on the switch). Filtered protocol types include:

- IP
- ARP
- DEC LAT
- AppleTalk
- SNA
- NetBEUI
- IPX

Only one filter for a particular protocol type can be configured at any one time. For example, a separate protocol filter can be configured for each of the protocol types listed above, but only one of those can be an IP filter. Also, the destination ports for a protocol filter can be on different VLANs.

Source Port Filters

This filter type enables the switch to restrict traffic from *all* end nodes on the indicated source port to specific destination ports (or to be dropped for all destination ports on the switch). If VLANs are configured, the destination port must be in the same VLAN as the source port. Only one source port filter can be configured for each of the ports in the switch.

Note

If more than one VLAN is configured, then the set of destination ports (Dest Port parameter) can consist of only the destination ports that are in the same VLAN as the source port.

Port-Based Virtual LANs (VLANs)

A VLAN is a group of ports designated by the switch as belonging to the same broadcast domain. (That is, all ports carrying traffic for a particular subnet address would normally belong to the same VLAN.) Using a VLAN, you can group users by logical function instead of physical location. This helps to control bandwidth usage by allowing you to group high-bandwidth users on low-traffic segments and to organize users from different LAN segments according to their need for common resources.

The Switches 1600M/2424M/4000M/8000M enable you to configure up to 30 port-based, 802.1Q-compatible VLANs. The 802.1Q compatibility enables you to assign each switch port to two or more VLANs, if needed, and the port-based nature of the configuration allows interoperation with older switches that require a separate port for each VLAN.

General Use and Operation. Port-based VLANs are typically used to enable broadcast traffic reduction and to increase security. A group of network users assigned to a VLAN form a separate traffic domain; packets are forwarded only between ports that are designated for the same VLAN. Thus, all ports carrying traffic for a particular subnet address should be configured to the same VLAN. Cross-domain broadcast traffic is eliminated and bandwidth is saved by not allowing packets to flood throughout the network. An external router is required to enable separate VLANs to communicate with each other.

For example, referring to figure 6-35, if ports 1 through 4 belong to VLAN_1 and ports 5 through 8 belong to VLAN_2, traffic from end-node stations on ports 2 through 4 is restricted to only VLAN_1, while traffic from ports 5 through 7 is restricted to only VLAN_2. For nodes on VLAN_1 to communicate with VLAN_2, their traffic must go through an external router via ports 1 and 8.

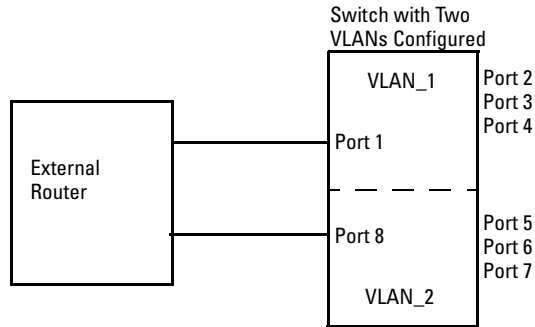


Figure 6-35. Example of Routing Between VLANs via an External Router

Overlapping (Tagged) VLANs. A port on the Switches 1600M/2424M/4000M/8000M can be a member of more than one VLAN if the device to which they are connected complies with the 802.1Q VLAN standard. For example, a port connected to a central server using a network interface card (NIC) that complies with the 802.1Q standard can be a member of multiple VLANs, allowing members of multiple VLANs to use the server. Although these VLANs cannot communicate with each other through the server, they can all access the server *over the same connection from the switch*. Where VLANs overlap in this way, VLAN “tags” are used to distinguish between traffic from different VLANs.

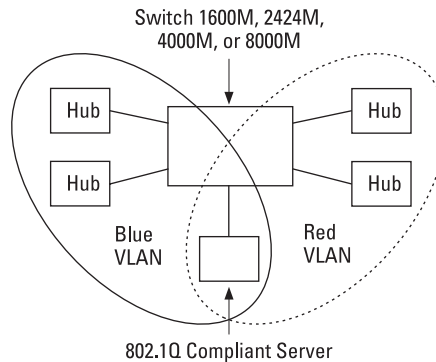


Figure 6-36. Example of Overlapping VLANs Using the Same Server

Similarly, using 802.1Q-compliant switches, you can connect multiple VLANs through a single switch-to-switch link.

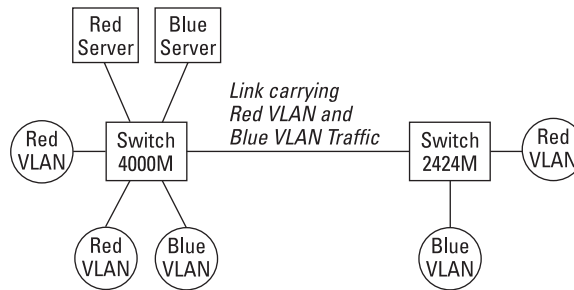


Figure 6-37. Example of Connecting Multiple VLANs Through the Same Link

Introducing Tagged VLAN Technology into Networks Running Legacy (Untagged) VLANs. You can introduce 802.1Q-compliant devices into networks that have built untagged VLANs based on earlier VLAN technology. The fundamental rule is that legacy/untagged VLANs require a separate link for each VLAN, while 802.1Q, or tagged VLANs can combine several VLANs in one link. This means that on the 802.1Q-compliant device, a separate port must be used to connect separate VLANs to non-802.1Q devices.

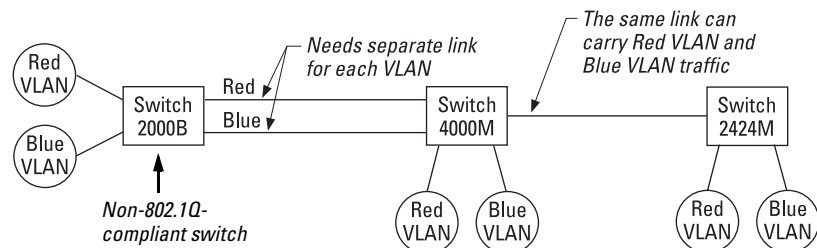


Figure 6-38. Example of Tagged and Untagged VLAN Technology in the Same Network

For more information on VLANs, refer to:

- “Overview of Using VLANs”, on the next page.
- “Configuring VLAN Parameters from the Switch Console” on page 6-56.
- “VLAN Tagging Information” on page 6-62.
- “Effect of VLANs on Other Switch Features” on page 6-66.
- “VLAN Restrictions” on page 6-68.

Overview of Using VLANs

VLAN Support and the Default VLAN

In the factory default configuration, VLAN support is de-activated and all the ports are only in the switch physical broadcast domain, which is given the name **DEFAULT_VLAN**. You can partition the switch into multiple virtual broadcast domains by adding one or more additional VLANs and moving ports from the default VLAN to the new VLANs. Because the default VLAN permanently exists in the switch, adding one new VLAN results in two VLANs existing in the switch. Adding another VLAN results in three VLANs existing in the switch, and so on. (The switch can have a maximum of 30 VLANs, including the default VLAN.)

To use VLANs, follow these general steps:

1. Plan your VLAN strategy and create a map of the logical topology that will result from configuring VLANs. Include consideration for the interaction between VLANs and other features such as Spanning Tree Protocol, load balancing, and IGMP. (Refer to “Effect of VLANs on Other Switch Features” on page 6-66.)
2. Enable VLAN support in the switch. (In the factory default configuration, VLAN support is disabled.)
3. Reboot the switch to activate the VLAN support.
4. Configure at least one VLAN in addition to the default VLAN.
5. Assign the desired switch ports to the new VLAN(s).
6. If you are managing VLANs with SNMP in an IP network, each VLAN must have an IP address. Refer to “IP Configuration” on page 6-4.

Some Notes on Using VLANs

- Automatic Broadcast Control (ABC), IGMP, and some other features operate on a “per VLAN” basis. This means you must configure such features separately for each VLAN in which you want them to operate.
- **DEFAULT_VLAN** *can be renamed, but not deleted.*
- Any ports *not* specifically assigned to another VLAN will remain assigned to **DEFAULT_VLAN**.
- Before you delete a VLAN, you must first re-assign its ports to another VLAN.

- If you enable VLAN support and configure VLANs, then subsequently disable VLAN support, all VLANs except the DEFAULT_VLAN will be cleared from the switch and all ports will be reassigned to the default VLAN. Depending on the network topology, this could result in redundant links causing broadcast storms unless the Spanning Tree Protocol is enabled.
- **Changes to the VLAN configuration are dynamic.** Once VLAN support has been enabled and activated (by rebooting the switch), all other changes to the VLAN configuration (except the maximum number of VLANs) can be performed without additional switch reboots.

Further Information

For further explanation and examples of VLANs operating with other switch features, see HP's ProCurve Networking web site at the following URL:

<http://www.hp.com/go/procurve>

Configuring VLAN Parameters from the Switch Console

In the factory default state, VLANs are disabled and all ports belong to the same broadcast/multicast domain. This domain is called **DEFAULT_VLAN** and appears in the “VLAN Names” screen after you activate VLAN support and reboot the switch. You can create up to 29 additional VLANs by adding new VLAN names, and then assigning one or more ports to each VLAN. (The switch accepts a maximum of 30 VLANs, including the default VLAN.) Note that each port can be assigned to multiple VLANs by using VLAN tagging (described later in this section).

To Activate VLANs

In the factory default configuration, VLANs are disabled. Before you can configure VLANs, you must first enable VLAN support and reboot the switch to activate the VLAN support.

1. From the Main Menu select:
 - 3. Switch Configuration**
 - 5. Advanced Features**
 - 6. VLAN Menu . . .**

You will then see the following screen:

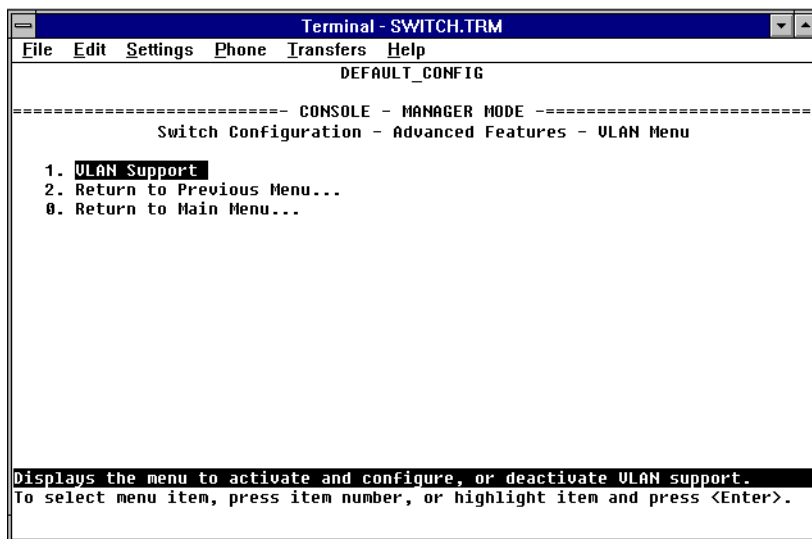


Figure 6-39. The VLAN Menu Screen

2. Press **[Enter]** or **[1]** to select **VLAN Support** and you will see a screen with the **Activate VLANs** field set to **No**.
3. Press **[E]** (for **Edit**), then press the Space bar to select **Yes**.
4. Press the **[Tab]** or Down Arrow **[↓]** key to reveal the **Total Number of VLANs** field.
5. Use the default number of VLANs (8), or enter the maximum number of VLANs you will be configuring (up to 30).

Note

For optimal switch memory utilization, set the number of VLANs at the number you will likely be using or a few more. If you need more VLANs later, you can increase this number, but a switch reboot will be required at that time.

6. Press **[Enter]** and then **[S]** to save the VLAN configuration.

You are then returned to the VLAN Menu screen which now has an asterisk next to the **VLAN Support** item, as shown in the next screen. The asterisk indicates that the switch must be rebooted to activate the configuration change.

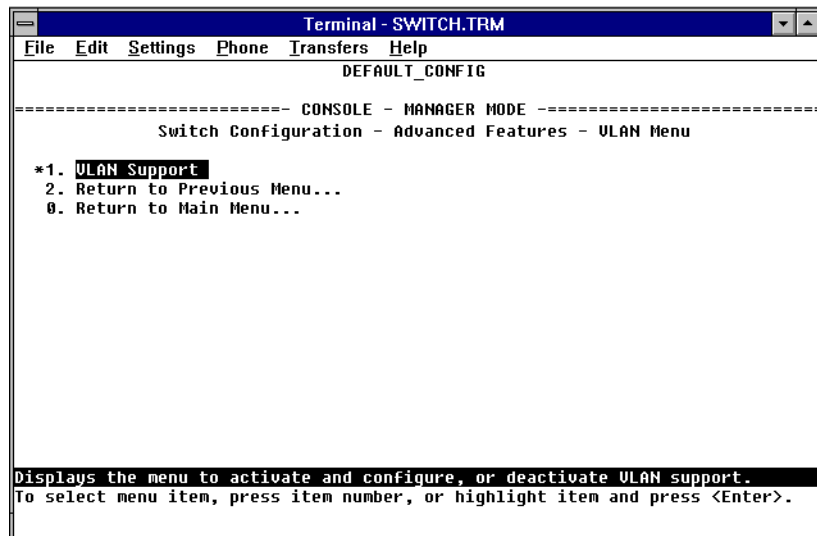


Figure 6-40. VLAN Menu After VLAN Support is Enabled

7. Reboot the switch now by pressing **[0]** to return to the Main menu, then pressing **[6]** to reboot the switch.

Note

After the reboot, all changes to the VLAN configuration, including adding and deleting VLANs, changing port assignments, and configuring various features on the VLANs are dynamic and require no additional switch reboot.

8. Add one or more new VLANs now, as described in the next section, "Adding or Editing VLAN Names".

Adding or Editing VLAN Names

Use this procedure to add a new VLAN or to edit the name of an existing VLAN.

1. From the Main Menu select:

- 3. Switch Configuration**
- 5. Advanced Features**
- 6. VLAN Menu ...**
- 2. VLAN Names**

If multiple VLANs are not yet configured you will see a screen similar to the one shown next.

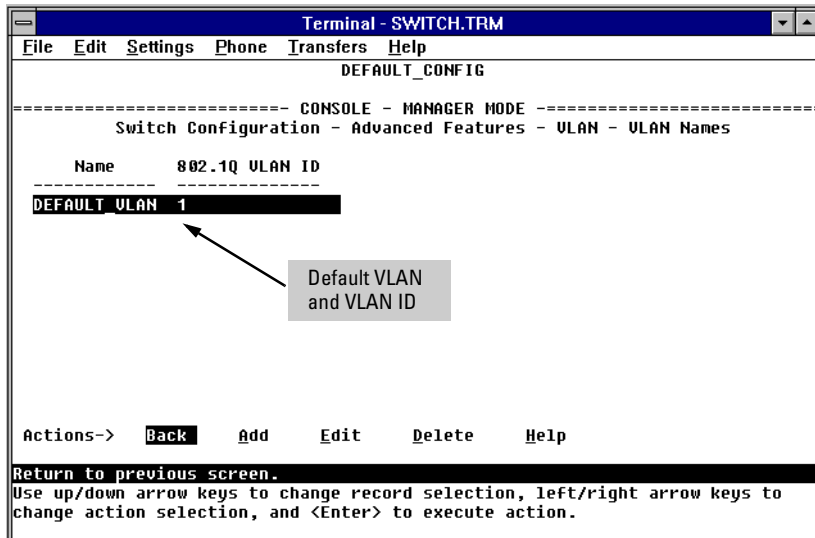


Figure 6-41. The (Default) VLAN Names Screen

2. Press **[A]** (for **Add**). You will then be prompted for a new VLAN name and VLAN ID:

Name : _
802.1Q VLAN ID : 1

3. Type the name (up to 12 characters, with no spaces) of a new VLAN that you want to add.
4. Press **↓** to move the cursor to the **802.1Q VLAN ID** line and type in a VLAN ID number, then press **Enter**. (This can be any number between 1 and 4095 that is not already being used by another VLAN.) Remember that a VLAN *must* have the same VLAN ID in every switch in which you configure that same VLAN.
5. Press **S** (for **Save**). You will then see the VLAN Names screen with the new VLAN listed.

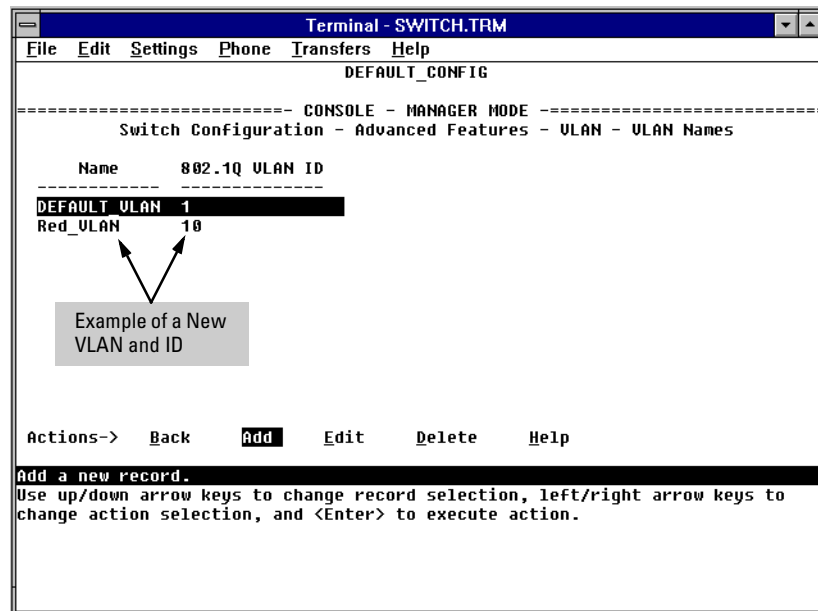


Figure 6-42. Example of the VLAN Names Screen with a New VLAN Added

6. Repeat steps 2 through 5 to add more VLANs. Remember that you will be allowed to add only as many VLANs as you specified in the **Total Number of VLANs** field on the VLAN Support screen (see step 4 on page 6-57).
7. Return to the VLAN Menu to assign ports to the new VLAN(s) as described in the next section, “Adding or Changing a VLAN Port Assignment”.

Adding or Changing a VLAN Port Assignment

Use this procedure to add ports to a VLAN or to change the VLAN assignment(s) for any port. (Ports not specifically assigned to a VLAN are automatically in the default VLAN.)

1. From the Main Menu select:

3. Switch Configuration

5. Advanced Features

6. VLAN Menu ...

3. VLAN Port Assignment

You will then see a VLAN Port Assignment screen similar to the following:

In this example, the "Red_VLAN" has been defined, but no ports have yet been assigned to it. ("No" means the port is not assigned to that VLAN.)

A port can be assigned to several VLANs, but only one of those assignments can be "Untagged".

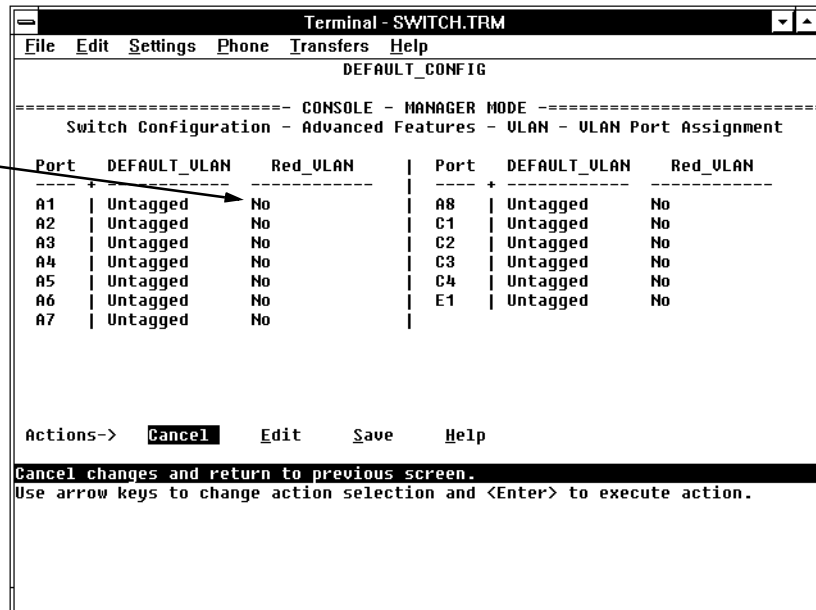


Figure 6-43. Example of the VLAN Port Assignment Screen

2. To change a port's VLAN assignment(s):
 - a. Press **[E]** (for **E**dit).
 - b. Use the arrow keys to select a VLAN assignment you want to change.
 - c. Press the Space bar to make your assignment selection (**No**, **Tagged**, or **Untagged**).

Note

Only one untagged VLAN is allowed per port. Also, there must be at least one VLAN assigned to each port. In the factory default configuration, all ports are assigned to the default VLAN (DEFAULT_VLAN).

For example, if you wanted ports A4 and A5 to belong to both the DEFAULT_VLAN and the Red_VLAN, and ports A6 and A7 to belong only to the Red_VLAN, your selections could look like this:

Ports A4 and A5 are assigned to both VLANs.

Ports A6 and A7 are assigned only to the Red VLAN.

All other ports are assigned only to the Default VLAN.

Port	DEFAULT_VLAN	Red_VLAN	Port	DEFAULT_VLAN	Red_VLAN
A1	Untagged	No	A8	Untagged	No
A2	Untagged	No	C1	Untagged	No
A3	Untagged	No	C2	Untagged	No
A4	Untagged	Tagged	C3	Untagged	No
A5	Untagged	Tagged	C4	Untagged	No
A6	No	Untagged	E1	Untagged	No
A7	No	Untagged			

Actions-> Cancel Edit Save Help

Figure 6-44. Example of VLAN Assignments for Specific Ports

For information on VLAN tags (“Untagged” and “Tagged”), refer to “VLAN Tagging Information” below.

- d. If you are finished assigning ports to VLANs, press **[Enter]** and then **[S]** (for **S**ave) to activate the changes you've made and to return to the Configuration menu. (The console then returns to the VLAN menu.)
3. Return to the Main menu. (It is not necessary to reboot the switch for changes in port VLAN assignments; they are implemented when you do the “save” in the preceding step.)

VLAN Tagging Information

VLAN tagging enables traffic from more than one VLAN to use the same port. (Even when two or more VLANs use the same port they remain as separate domains and cannot receive traffic from each other without going through a router.) As mentioned earlier, a “tag” is simply a unique VLAN identification number (VLAN ID) assigned to a VLAN at the time that you configure the VLAN name in the switch. In the Switches 1600M/2424M/4000M/8000M the tag can be any number from 1 to 4095 that is not already assigned to a VLAN. When you subsequently assign a port to a given VLAN, you need to implement the VLAN tag (VLAN ID) only if the port will carry traffic for more than one VLAN. Otherwise, the port VLAN assignment can remain “untagged” because the tag is not needed. On a given switch, this means you should use the “Untagged” designation for a port VLAN assignment where the port is connected to non 802.1Q-compliant device or is assigned to only one VLAN. Use the “Tagged” designation when the port is assigned to more than one VLAN or the port is connected to a device that *does* comply with the 802.1Q standard.

For example, if port X7 on an 802.1Q-compliant switch is assigned to only the Red VLAN, the assignment can remain “untagged” because the port will forward traffic only for the Red VLAN. However, if both the Red and Green VLANs are assigned to port X7, then at least one of those VLAN assignments must be “tagged” so that Red VLAN traffic can be distinguished from Green VLAN traffic. The following illustration demonstrates this concept:

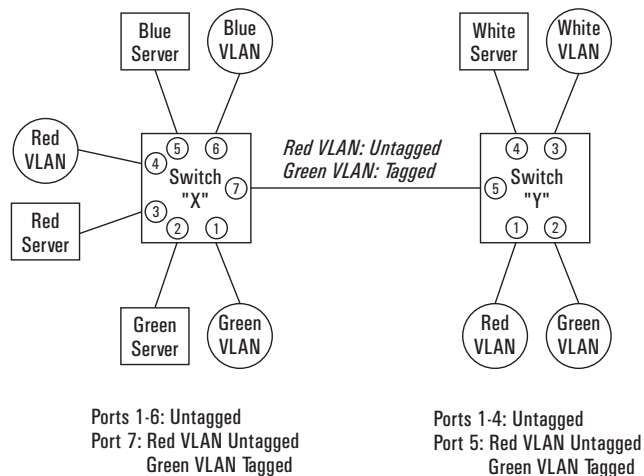


Figure 6-45. Example of Tagged and Untagged VLAN Port Assignments

- In switch X:
 - VLANs assigned to ports X1 - X6 can all be untagged because there is only one VLAN assignment per port. Red VLAN traffic will go out only the Red ports; Green VLAN traffic will go out only the Green ports, and so on. Devices connected to these ports do not have to be 802.1Q-compliant.
 - However, because both the Red VLAN and the Green VLAN are assigned to port X7, at least one of the VLANs must be tagged for this port.
- In switch Y:
 - VLANs assigned to ports Y1 - Y4 can all be untagged because there is only one VLAN assignment per port. Devices connected to these ports do not have to be 802.1Q-compliant.
 - Because both the Red VLAN and the Green VLAN are assigned to port Y5, at least one of the VLANs must be tagged for this port.
- In both switches: The ports on the link between the two switches must be configured the same. That is, the Red VLAN must be untagged on port X7 and Y5 and the Green VLAN must be tagged on port X7 and Y5, or vice-versa.

Note

Each 802.1Q-compliant VLAN must have its own unique VLAN ID number, and that VLAN *must* be given the same VLAN ID in every device in which it is configured. That is, if the Red VLAN has a VLAN ID of 10 in switch X, then 10 must also be used for the Red VLAN ID in switch Y.

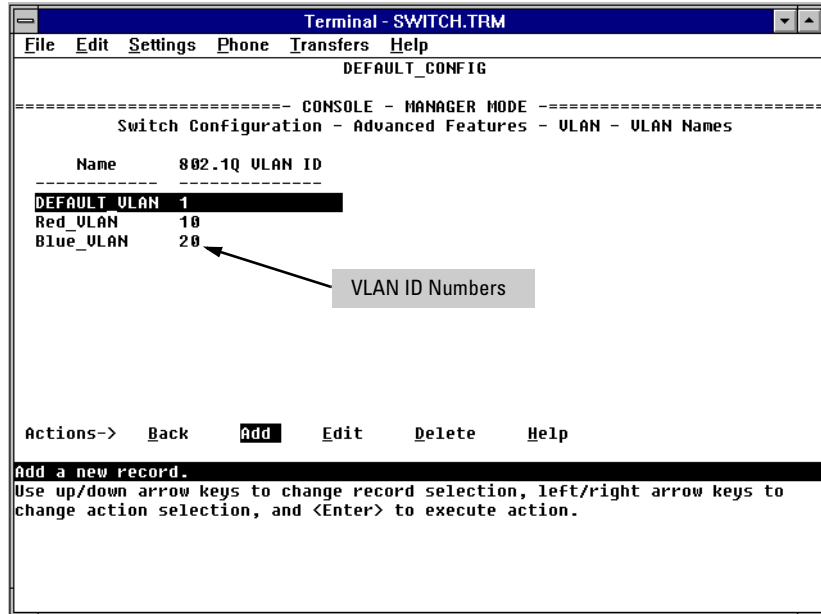


Figure 6-46. Example of VLAN ID Numbers Assigned in the VLAN Names Screen

VLAN tagging gives you several options:

- Since the purpose of VLAN tagging is to allow multiple VLANs on the same port, any port that has only one VLAN assigned to it can be configured as “Untagged” (the default).
- Any port that has two or more VLANs assigned to it can have one VLAN assignment for that port as “Untagged”. All other VLANs assigned to the same port must be configured as “Tagged”. (There can be no more than one Untagged VLAN on a port.)
- If all end nodes on a port comply with the 802.1Q standard and are configured to use the correct VLAN tag number, then, you can configure all VLAN assignments on a port as “Tagged” if doing so makes it easier to manage your VLAN assignments, or for security reasons.

For example, in the following network, switches X and Y and servers S1 and S2 are 802.1Q-compliant. (Server S3 could also be 802.1Q-compliant, but it makes no difference for this example.)

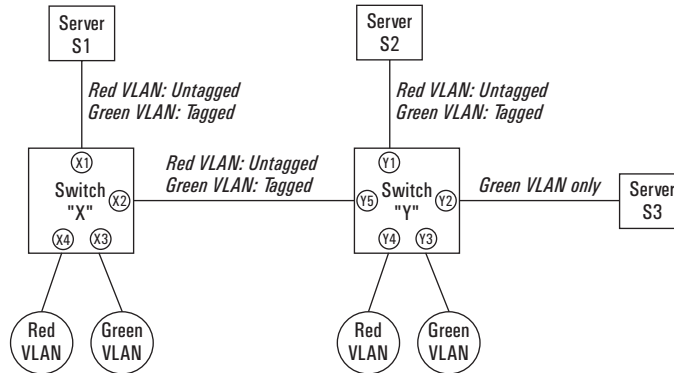


Figure 6-47. Example of Networked 802.1Q-Compliant Devices with Multiple VLANs on Some Ports

The VLANs assigned to ports X3, X4, Y2, Y3, and Y4 can all be untagged because there is only one VLAN assigned per port. Port X1 has multiple VLANs assigned, which means that one VLAN assigned to this port can be untagged and any others must be tagged. The same applies to ports X2, Y1, and Y5.

Switch X			Switch Y		
Port	Red VLAN	Green VLAN	Port	Red VLAN	Green VLAN
X1	Untagged	Tagged	Y1	Untagged	Tagged
X2	Untagged	Tagged	Y2	No*	Untagged
X3	No*	Untagged	Y3	No*	Untagged
X4	Untagged	No*	Y4	Untagged	No*
			Y5	Untagged	Tagged

*"No" means the port is not a member of that VLAN. For example, port X3 is not a member of the Red VLAN and does not carry Red VLAN traffic.

Note

VLAN configurations on ports connected by the same link must match. Because ports X2 and Y5 are opposite ends of the same point-to-point connection, both ports must have the same VLAN configuration; that is, both ports configure the Red VLAN as "Untagged" and the Green VLAN as "Tagged".

To summarize:

VLANs Per Port	Tagging Scheme
1	Untagged or Tagged
2 or More	1 VLAN Untagged; all others Tagged or All VLANs Tagged

A given VLAN *must* have the same VLAN ID on any 802.1Q-compliant device in which the VLAN is configured.

The ports connecting two 802.1Q devices should have identical VLAN configurations, as shown for ports X2 and Y5, above.

Effect of VLANs on Other Switch Features

Spanning Tree Protocol Operation with VLANs

Because the Switches 1600M/2424M/4000M/8000M follow the 802.1Q VLAN recommendation to use single-instance spanning tree, STP operates across the switch instead of on a per-VLAN basis. This means that if redundant physical links exist between the switch and another 802.1Q device, all but one link will be blocked, regardless of whether the redundant links are in separate VLANs. However, you can use port trunking or switch meshing to prevent STP from unnecessarily blocking ports (and to improve overall network performance). Refer to “STP Operation with 802.1Q VLANs” on page 6-44.

Note that STP operates differently in different devices. For example, in the (non-802.1Q) HP Switch 2000 and the HP Switch 800T, STP operates on a per-VLAN basis, allowing redundant physical links as long as they are in separate VLANs. Thus, redundant links connecting a Switch 1600M/2424M/4000M/8000M to the Switch 2000 or Switch 800T in a VLAN environment will not be blocked if the links are in different VLANs.

IPX and IP Interfaces

There is a one-to-one relationship between a VLAN and an IP or IPX network interface. Since the VLAN is defined by a group of ports, the state (up/down) of those ports determines the state of the IP or IPX network interface associated with that VLAN. When a VLAN comes up because one or more of its ports is up, the IP or IPX interface for that VLAN is also activated. Likewise, when a VLAN is deactivated because all of its ports are down, the corresponding IP or IPX interface is also deactivated.

VLAN MAC Addresses

The switch has one unique MAC address for each of its VLAN interfaces. You can send an 802.2 test packet to this MAC address to verify connectivity to the switch. Likewise, you can assign an IP address to the VLAN interface, and when you Ping that address, ARP will resolve the IP address to this MAC address. (For IPX networks, each VLAN interface is automatically assigned a node address that is equivalent to the MAC address for that VLAN interface.) The switch allows up to 30 VLAN MAC addresses (one per possible VLAN).

Port Trunks

When assigning a port trunk to a VLAN, all ports in the trunk are automatically assigned to the same VLAN. You cannot split trunk members across multiple VLANs. Also, a port trunk is tagged, untagged, or excluded from a VLAN in the same way as for individual, untrunked ports.

Port Monitoring

If you designate a port on the switch for network monitoring, this port will appear in the Port VLAN Assignment screen and can be configured as a member of any VLAN. For information on how broadcast, multicast, and unicast packets are tagged inside and outside of the VLAN to which the monitor port is assigned, refer to page 8-10.

VLANs and Switch Meshing

The non-meshed ports on an Edge switch can be assigned to individual VLANs. The meshed ports are automatically assigned as a group to all VLANs configured on the switch. When configuring a VLAN in your network, ensure that you configure the VLAN on each meshed switch, even if no ports on that switch are assigned to the VLAN. This is because all ports in the mesh domain must be members of all VLANs on the network. This allows any port in the mesh domain to forward VLAN traffic. Failing to assign all VLANs to all meshed switches could result in traffic from any unassigned VLANs not getting through the mesh. For more information, refer to “802.1Q VLANs in Meshed Switches” on page 6-91.

VLAN Restrictions

- A port must be a member of at least one VLAN. In the factory default configuration, all ports are assigned to the default VLAN (DEFAULT_VLAN).
- A port can be assigned to several VLANs, but only one of those assignments can be untagged. (The “Untagged” designation enables VLAN operation with non 802.1Q-compliant devices.)
- An external router must be used to communicate between VLANs.
- Duplicate MAC addresses on different VLANs are not supported and can cause VLAN operating problems. These duplicates are possible and common in situations involving Sun workstations with multiple network interface cards, with DECnet routers, and with certain Hewlett-Packard routers using OS versions earlier than A.09.70 where any of the following are enabled:
 - IPX
 - IP Host-Only
 - STP
 - XNS
 - DECnet

Currently, the problem of duplicate MAC addresses in IPX and IP Host-Only environments is addressed through the HP router OS version described below. However, for XNS and DECnet environments, a satisfactory solution is not available from any vendor at this time.

Note

Operating problems associated with duplicate MAC addresses are likely to occur in VLAN environments where XNS and DECnet are used. For this reason, using VLANs in XNS and DECnet environments is not currently supported.

-
- Before you can delete a VLAN, you must first remove all of its unmeshed ports from the VLAN and re-assign all ports in the VLAN to another VLAN.

HP Router Requirements. *Use the Hewlett-Packard version A.09.70 (or later) router OS release if any of the following Hewlett-Packard routers are installed in networks in which you will be using VLANs:*

- HP Router 440 (formerly Router ER)
- HP Router 470 (formerly Router LR)
- HP Router 480 (formerly Router BR)
- HP Router 650

Release A.09.70 (or later) is available electronically through the HP BBS service and the World Wide Web. Refer to the Customer Support/Warranty booklet shipped with the switch.

Symptoms of Duplicate MAC Addresses in VLAN Environments

There are no definitive events or statistics to indicate the presence of duplicate MAC addresses in a VLAN environment. However, one symptom that may occur is that the duplicate MAC address can be seen in the Port Address Table for more than one port. You can do a search for the suspected MAC address in the switch's address table and if there is a duplicate MAC address problem, the address will be found in the table associated with one port at one moment, and then later associated with a different port.

Load Balancing: Port Trunking

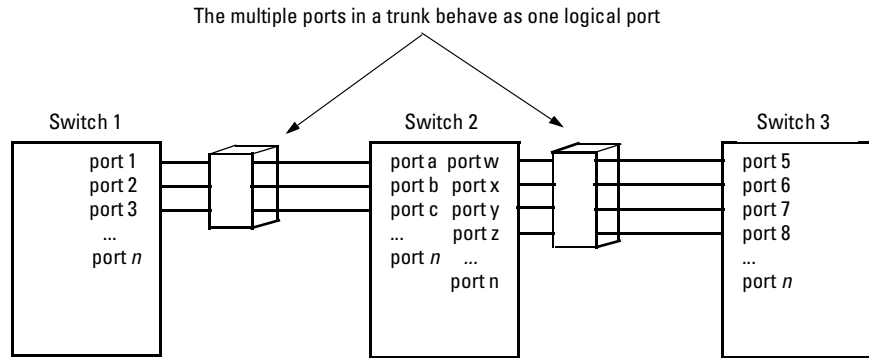


Figure 6-48. Conceptual Illustration of Port Trunking

Port trunking allows up to four ports to be connected together to function as a single, higher-speed link that dramatically increases bandwidth. This capability can be applied to connections between backbone devices as well as connections in other network areas where traffic bottlenecks have developed. With full-duplex operation in a four-port trunk, this enables the following bandwidth capabilities:

- 10 Mbps links: Up to 80 Mbps
- 100 Mbps links: Up to 800 Mbps
- 1000 Mbps (gigabit) links: Up to 8000 Mbps

The Switches 1600M/2424M/4000M/8000M support up to ten four-port trunks.

Caution

To avoid broadcast storms or loops in your network while configuring trunks, first disable or disconnect all ports you want to add or remove from both sides of the trunk. After you finish configuring the trunk, enable or reconnect the ports.

Traffic distribution across the links in a port trunk is based on source/destination or source-only address forwarding methods described later in this section. This results in load balancing based on distribution of source and/or destination addresses across the links in a trunk. Because the amount of traffic coming from or going to various nodes in a network can vary widely, it is possible for one link in a trunk to be fully utilized while others in the same trunk have unused bandwidth capacity even though the address assignments

are evenly distributed across the links in a trunk. In actual networking environments, this is rarely a problem. However, if it becomes a problem, you can use the HP TopTools for Hubs & Switches network management software available from Hewlett-Packard to quickly and easily identify the sources of heavy traffic (top talkers) and make adjustments to improve performance.

Fault Tolerance: If a link in a port trunk fails, traffic originally destined for that link will be redistributed to the remaining links in the trunk. The trunk remains operable as long as there is at least one link in operation. If a link is restored, that link is automatically included in the traffic distribution again.

Port Connections and Configuration: All port trunk links must be point-to-point connections between the Switches 1600M/2424M/4000M/8000M and another switch, router, server, or workstation. It is important to note that ports on both ends of a port trunk should be configured with the same trunk type, mode, flow control, and broadcast limit settings.

Note

Using more than one media type and/or link speed in a port trunk is not supported. The console interface allows only links of the same media type within the same trunk. Similarly, it is recommended that all links in the same trunk have the same speed. You should also apply these rules when using a network management application to configure a port trunk.

Use with Spanning Tree and Advanced Features. A configured trunk appears as a single port (labeled **Trk1**, **Trk2...**, **Trk9**, **Trk0**) on other configuration screens, such as the Spanning Tree, IP Multicast (IGMP), and VLAN port assignment screens. When Spanning Tree forwards on a trunk, all ports in the trunk will be forwarding. Conversely, when Spanning Tree blocks a trunk, all ports in the trunk are blocked. Also, when a trunk port is assigned to a VLAN, all ports in that trunk are assigned to the same VLAN. (If you assign a trunk to a VLAN, and then remove a port from the trunk, that port will automatically be assigned to the same VLAN as the trunk.)

When you add a port to a trunk, the port takes on the properties of the trunk. If you remove a port from a trunk, the port retains the trunk properties (except for the filtering properties, which are returned to their previous state). For example, if you:

1. use ports A1, A2, and A3 to create trunk 1 in the Red VLAN.
2. move trunk 1 to the Blue VLAN.
3. remove port A3 from the trunk.

then port A3 will be a member of the Blue VLAN instead of the original Red VLAN.

However, if filters were in use on port A3, it will return to filtering as it did before joining the trunk:

- If, for example, port A3 was configured with filters to *drop* specific packets *before* it became a member of trunk 1 and . . .
- If trunk 1 was configured to *forward* those packets, then port A3 will also forward the packets while it is a member of trunk 1.
- However, if you subsequently remove port A3 from trunk 1, then port A3 will resume dropping the specific packets according to its original filter configuration.

Interoperability

The Switches 1600M/2424M/4000M/8000M provide a broad set of port trunking capabilities that enable trunking with the HP switch products listed on the next page. These switches also offer trunking interoperation with products offered by some other vendors.

Note

When this manual was released, an IEEE standard for port trunking was not yet available. Thus, standards compliance cannot yet be used to determine how successfully various vendors' implementations of port trunking will interoperate with the Switches 1600M/2424M/4000M/8000M. (However, note that the Trunk option uses the IEEE 802.3 standards for auto-negotiating half- or full-duplex operation and auto-sensing 10 Mbps, 100 Mbps links.) For more on trunking to non-HP devices, see the Technical Support area of HP's ProCurve Networking website at www.hp.com/go/procurve.

Trunk Configuration Options

There are three trunk configuration types from which to select:

Type	Traffic Distribution Method	Recommended Switch 1600M/2424M/4000M/8000M Configuration for Trunking to:
Trunk	Source Address/Destination Address (SA/DA)	<ul style="list-style-type: none"> • Another Switch 1600M/2424M/4000M/8000M • HP Switch 2000A/B • HP Switch 800T • SA/DA forwarding devices such as the Sun Trunk Server and some vendors' switches • Windows NT and HP-UX workstations and servers
SA-Trunk	Source-Address Distribution	Forwarding devices such as low-end switches or devices that do not support SA/DA port trunks.
FEC	Fast EtherChannel®	Forwarding devices that also offer FEC, such as some Cisco® switches, routers, and some HP-UX and Windows NT servers.

Configuring Port Trunks from the Switch Console

Important Note. Use this procedure to configure port trunking *before* you connect the trunked links between switches. Otherwise, a broadcast storm could occur. (If you need to connect the ports before configuring them for trunking, you can use the Port Settings feature—page 6-30—to temporarily disable the ports until the trunk is configured.)

To Access Port Trunking:

1. Follow the procedures in the Important Note above.
2. From the Main Menu, Select:
 3. **Switch Configuration**
 5. **Advanced Features**
 2. **Load Balancing (Meshing, FEC, Trunks)**
3. Press **[E]** (for **Edit**) to access the load balancing parameters.

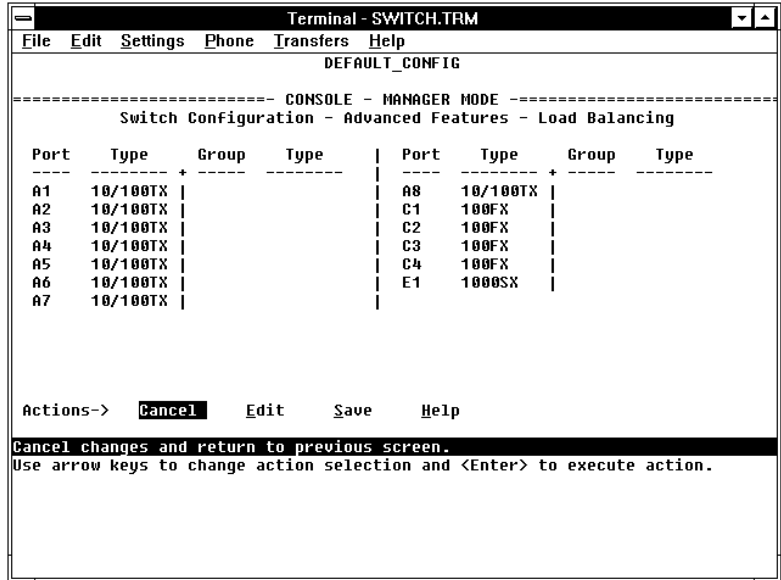


Figure 6-49. Example of the Screen for Configuring Ports for Load Balancing

4. In the Group column, move the cursor to the port you want to configure.
 5. Use the Space bar (or type the trunk name, such as **trk5**) to choose a trunk assignment for the selected port.
 - All ports in a trunk should have the same media type and mode (such as 10/100TX set to 100HDx, or 100FX set to 100FDx). The flow control and broadcast limit settings should also be the same for all ports in a given trunk. To verify these settings, refer to “Port Settings” on page 6-30.
 - You can configure up to ten different trunks (**Trk1...Trk9,Trk0**), with one, two, three, or four ports per trunk. A port can be assigned to only one trunk. However, you can move ports between trunks. If multiple VLANs are configured, all ports within a given trunk will be assigned to the same VLAN or set of VLANs. (With the 802.1Q VLAN capability built into the switch, more than one VLAN can be assigned to a trunk. Refer to “Port-Based Virtual LANs (VLANs)” on page 6-51.)
- (To return a port to a non-trunk status, keep pressing the Space bar until a blank appears in the highlighted Group value for that port.)

```

Terminal - SWITCH.TRM
File Edit Settings Phone Transfers Help
-----
                DEFAULT_CONFIG
-----
Switch Configuration - Advanced Features - Load Balancing

Port  Type  Group  Type  |  Port  Type  Group  Type
-----+-----+-----+-----|-----+-----+-----+-----
A1   10/100TX | Trk1  |  A8   10/100TX |
A2   10/100TX | Trk1  |  C1   100FX   | Trk3
A3   10/100TX | Trk1  |  C2   100FX   | Trk3
A4   10/100TX | Trk1  |  C3   100FX   |
A5   10/100TX |      |  C4   100FX   |
A6   10/100TX | Trk2  |  E1   1000SX  |
A7   10/100TX | Trk2  |

Actions->  CANCEL  EDIT  SAVE  HELP

Select whether the port is part of a trunk or Mesh.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
    
```

Figure 6-50. Example of Trunk Group Assignments for Several Ports

6. Move the cursor to the Type column for the selected port and use the Space bar to select the trunk type:
 - Trunk (Source Address/Destination Address trunk; the default type if you do not select a type)—page 6-77.
 - SA-Trunk (Source-Address trunk)—page 6-78
 - FEC (Fast EtherChannel[®] trunk)—page 6-79

All ports in the same trunk must have the same Type (**Trunk**, **SA-Trunk**, or **FEC**).

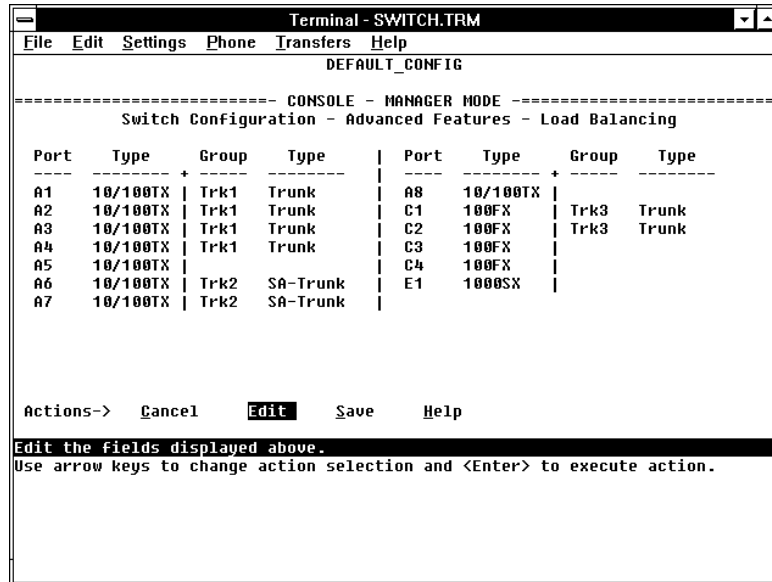


Figure 6-51. Example of trunks with different trunk types

7. When you are finished assigning ports to trunks, press **Enter**, then **S** (for **Save**) and return to the Main Menu. (It is not necessary to reboot the switch.)

During the Save process, traffic on the ports configured for trunking will be delayed for several seconds. If the Spanning Tree Protocol is enabled, the delay may be up to 15 seconds.

8. Connect the trunked ports on the switch to the corresponding ports on the opposite device. If you previously disabled any of the trunked ports on the switch, enable them now. (Refer to “Port Settings” on page 6-30.)
9. Check the Event Log (page 8-12) and the Switch Mesh Information screen (page 7-22) to verify that the trunked ports are operating properly.

Operating Information

This section describes port usage and how traffic is distributed by the various trunking options.

Trunk Operation Using the “Trunk” Option

This method provides the best means for evenly distributing traffic over trunked links to devices.

Configuring the Trunk (source address/destination address or SA/DA) option for a port trunk causes the switch to distribute traffic in a sequential manner to the links within the trunk on the basis of source/destination address pairs. That is, traffic from the same source address to the same destination addresses will travel over the same trunked link. Traffic from the same source address but meant for different destination addresses will be distributed across different links. Likewise, traffic for the same destination address but from different source addresses will be distributed across different links. Because of this feature, broadcasts, multicasts, and floods from different source addresses are distributed evenly across the links. As links are added or deleted, traffic will be redistributed across the trunk. For example, in the three-port trunk shown below, traffic could be assigned as shown in the table below.

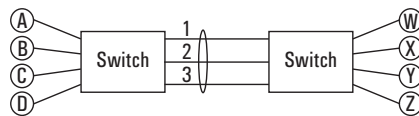


Figure 6-52. Example of Port-Trunked Network

Example of Link Assignments in a Trunk ((SA/DA Distribution))

Source:	Destination:	Link:
Node A	Node W	1
Node B	Node X	2
Node C	Node Y	3
Node D	Node Z	1
Node A	Node Y	2
Node B	Node W	3

Trunk Operation Using the “SA-Trunk” Option

This option is less efficient than the SA/DA option described above. However, it is useful for trunking to devices that do not have built-in support for the SA/DA-trunking method.

Configuring the SA-Trunk option for a port trunk causes the switch to distribute traffic in a sequential manner to the links within the trunk on the basis of source address only. That is, traffic from the same source address will travel over the same trunked link regardless of destination address. Traffic from other sources to the same or different destinations may travel over different links within the same trunk. This prevents the source address from appearing on different ports in the non-trunking device.

Example of Link Assignments in an SA-Only Trunk (refer to figure 6-45 above)

Source Nodes:	Destination Nodes:	Link:
Node A	Node W	1
Node B	Node X	2
Node C	Node Y	3
Node D	Node Z	1
Node A	Node Y	1
Node B	Node W	2

*Source Nodes A and D
Always Appear on Port 1*

Caution

SA/DA Trunking and SA-only Trunking are not compatible. If you are trunking an SA-only device to a Switch 1600M/2424M/4000M/8000M, make sure the involved switch ports are configured as **SA-Trunk**.

Trunk Operation Using the “FEC” Option

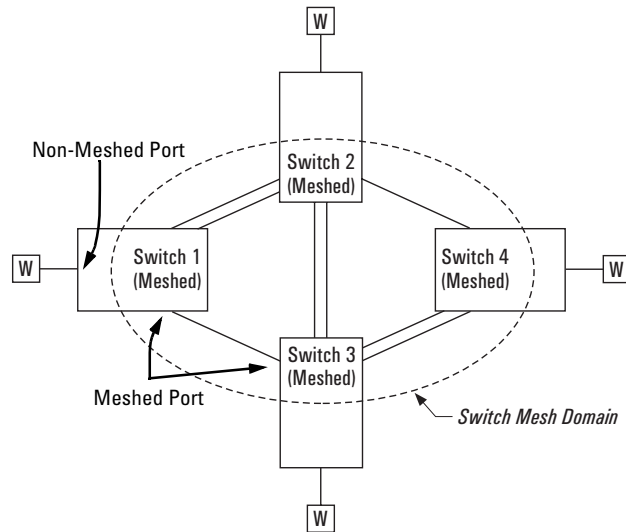
This is the most flexible method for distributing traffic over trunked links when connecting to devices that use the FEC (Fast EtherChannel[®]) technology. HP FEC trunks offer the following benefits:

- Provide trunked connectivity to a FEC-compliant server, switch, or router.
- Enable quick convergence to remaining links when a failure is detected on a trunked port link.
- Depending on the capabilities of the device on the other end of the trunk, negotiate the forwarding mechanism on the trunk to either SA-Trunk or SA/DA (Trunk).
- When auto-negotiated to the SA/DA forwarding mechanism, provide higher performance on the trunk for broadcast, multicast, and flooded traffic through distribution in the same manner as SA/DA trunking.
- Support FEC automatic trunk configuration mode on other devices. That is, when connecting HP FEC trunks to FEC-capable servers, switches, or routers having FEC automatic trunk configuration mode enabled, the HP FEC trunks allow these other devices to automatically form trunk groups.

Load Balancing: Switch Meshing

Switch meshing is a load-balancing technology that enhances reliability and performance in these ways:

- Provides significantly better bandwidth utilization than either Spanning Tree Protocol (STP) or standard port trunking.
- Uses redundant links that remain open to carry traffic, removing any single point of failure for disabling the network, and allowing quick responses to individual link failures. This also helps to maximize investments in ports and cabling.
- Unlike trunked ports, the ports in a switch mesh can be of different types and speeds. For example, a 10Base-FL port and a 1Gps port can be included in the same switch mesh.



The mesh-configured ports in switches 1-4 form a Switch Mesh Domain

Figure 6-53. Example of Switch Meshing

Finding the Fastest Path. Using multiple switches redundantly linked together to form a *meshed switch domain*, switch meshing dynamically distributes traffic across load-balanced switch paths by seeking the fastest paths for new traffic between nodes. In actual operation, the switch mesh periodically determines the best (lowest latency) paths, then assigns these paths as the need arises. The path assignment remains until the related MAC address entry times out. The mesh sees later traffic between the same nodes as new traffic, and may assign a different path, depending on conditions at the time. For example, at one time the best path from node A to node B is through switch 2. However, if traffic between node A and node B ceases long enough for the path assignment to age out, then the next time node A has traffic for node B, the assigned path between these nodes may be through switch 3 if network conditions have changed significantly. (The **Address Age Interval** parameter in the System Information screen—**3. Switch Configuration/1. System Information** menu, page 6-29—determines how long an inactive path assignment remains in memory.)

Because Redundant Paths Are Active, Meshing Adjusts Quickly to Link Failures. If a link in the mesh fails, the fast convergence time designed into meshing typically has an alternate route selected in less than a second for traffic that was destined for the failed link.

Meshing Allows Scalable Responses to Increasing Bandwidth Demand. As more bandwidth is needed in a LAN backbone, another switch and another set of links can be added. This means that bandwidth is not limited by the number of trunk ports allowed in a single switch.

Switch Meshing Fundamentals

Meshed Switch Domain. This is a group of switches exchanging meshing protocol packets. Paths between these switches can have multiple redundant links without creating broadcast storms. A meshed switch can have some ports in the meshed domain and others outside the meshed domain. Meshed links must be point-to-point switch links. Hub links between meshed switch links are not allowed. Within any meshed switch, all ports belong to the same meshed domain.

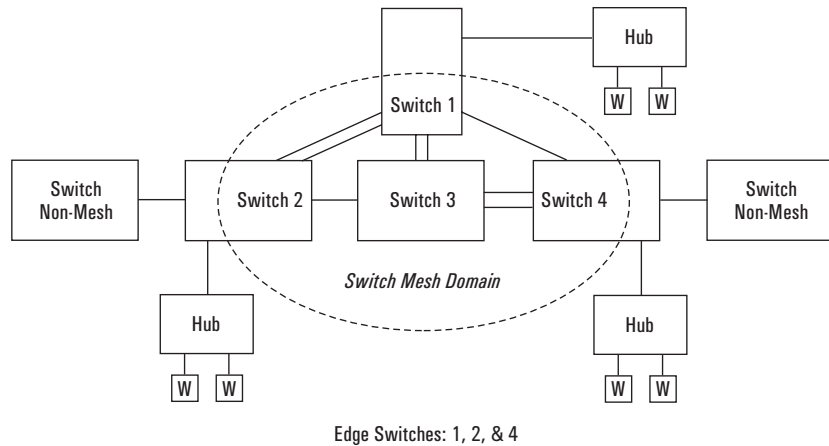


Figure 6-54. Example of a Switch Mesh Domain in a Network

Note

Hubs, switches that are not configured for load balancing, and non load-balanced ports in a switch that does have some load-balanced ports are not allowed in switch mesh domains. Inserting a non-mesh device into the mesh causes the meshed switch port(s) connected to that device to shut down.

Edge Switch. This is a switch that has some ports in the switch meshing domain and some ports outside of the domain. (See figure 6-54, above.)

Multiple meshed domains require separation by either a non-meshed switch or a non-meshed link. For example:

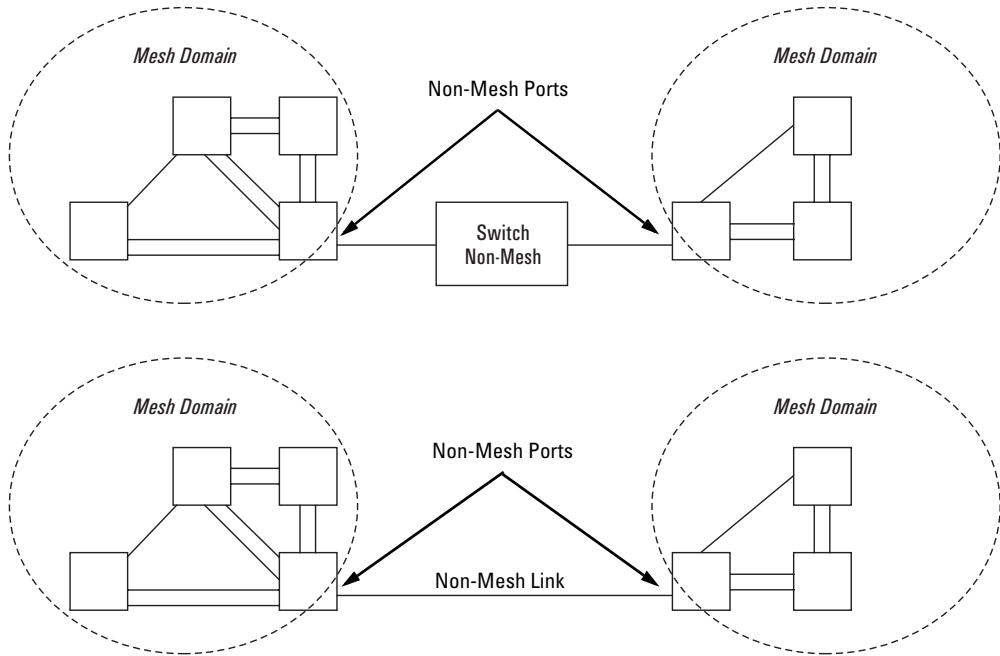


Figure 6-55. Example of Multiple Meshed Switch Domains Separated by a Non-Mesh Switch or a Non-Mesh Link

Configuration Requirements. Before configuring switch meshing on any ports in the Switches 1600M/2424M/4000M/8000M, it is necessary to activate VLAN support. Notice that this does not require that you configure multiple VLANs; only that VLAN support is activated. (See “Using the Console To Configure Switch Meshing” on page 6-84.)

Bringing Up a Switch Mesh Domain: When a meshed port detects a non-meshed port on the opposite end of a point-to-point connection, the link will be blocked. Thus, as you bring up switch meshing on various switches, you may temporarily experience blocked ports where meshed links should be running. These conditions should clear themselves after all switches in the mesh have been configured for meshing and then rebooted. To reduce the effect of blocked ports during bring-up, configure meshing before installing the meshed switches in the network.

Further Information:

- For further operating information and restrictions, refer to “Operating Notes for Switch Meshing” on page 6-87.
- For further explanation and examples of switch meshing, refer to HP’s Network City site at the following URL on the world wide web:

<http://www.hp.com/go/procurve>

Using the Console To Configure Switch Meshing

Note

If VLAN support is not currently activated in the switch, use the instructions under “To Activate VLANs” on page 6-56 to activate VLAN support before continuing here. (VLAN support must be activated before you configure switch meshing, even if multiple VLANs are not configured.)

To Access Switch Meshing

1. Before configuring switch meshing, ensure that VLAN support is enabled on the switch.
2. From the Main Menu, select:
 - 3. Switch Configuration**
 - 5. Advanced Features**
 - 2. Load Balancing (Meshing, FEC, Trunks)**
3. Press **[E]** (for **Edit**) to access the load balancing parameters.

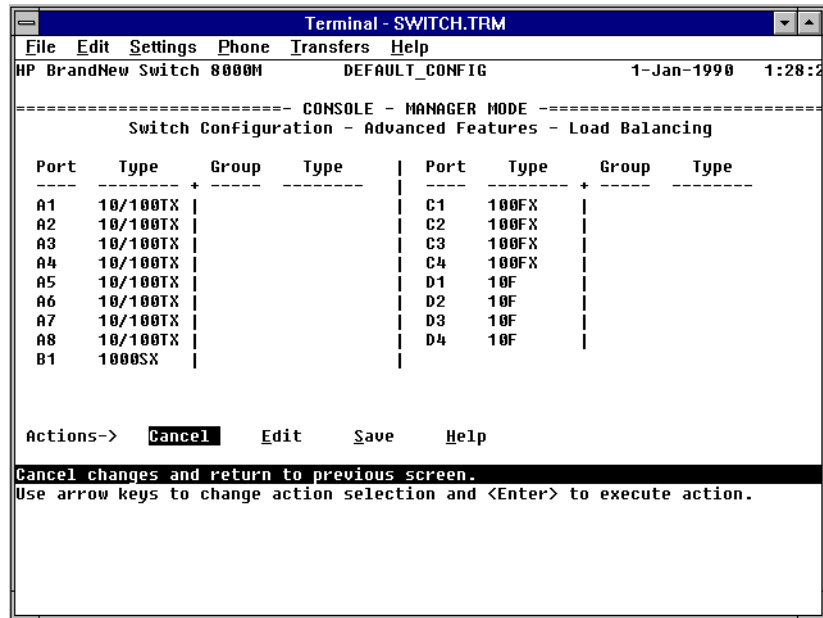


Figure 6-56. Example of the Screen for Configuring Ports for Load Balancing

- In the Group column, move the cursor to the port you want to assign to the switch mesh.
- Use the Space bar (or press **[M]**) to choose **Mesh** for the selected port.

If you are configuring switch meshing, all meshed ports in the switch will belong to the same mesh domain. (See figure 6-54 on page 6-82.)

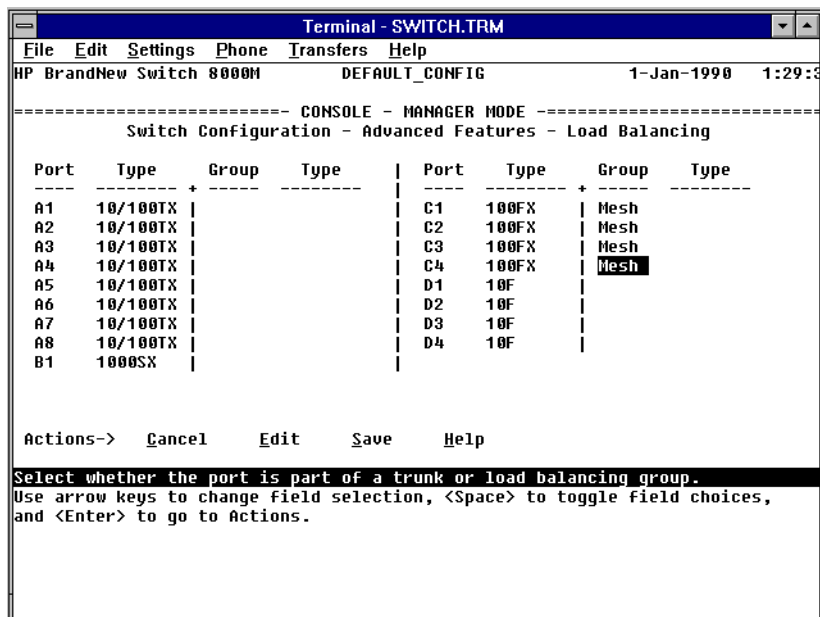


Figure 6-57. Example of Mesh Group Assignments for Several Ports

- When you are finished assigning ports to the switch mesh, press **Enter**, then **S** (for **Save**) and return to the Main Menu.

Note

For meshed ports, leave the “Type” setting blank. (Meshed ports do not accept a Type setting.)

- To activate the mesh assignment(s) from the Main Menu, reboot the switch by pressing the following keys:
 - 6** (for **Reboot Switch**)
 - Space bar
 - Enter**

(The switch cannot dynamically reconfigure ports to enable or disable meshing, so it is always necessary to reboot the switch after adding or deleting a port in the switch mesh.)

Operating Notes for Switch Meshing

In a switch mesh domain traffic is distributed across the available paths with an effort to keep latency the same from path to path. The path selected at any time for a connection between a source node and a destination node is based on these latency and throughput cost factors:

- Outbound queue depth, or the current outbound load factor for any given outbound port in a possible path
- Port speed, such as 10Mbps versus 100Mbps; full-duplex or half-duplex
- Inbound queue depth, or how busy is a destination switch in a possible path
- Increased packet drops, indicating an overloaded port or switch

Paths having a lower cost will have more traffic added than those having a higher cost. Alternate paths and cost information is discovered periodically and communicated to the switches in the mesh domain. This information is used to assign traffic paths between devices that are newly active on the mesh. This means that after an assigned path between two devices has timed out, new traffic between the same two devices may take a different path than previously used.

To display information on the operating states of meshed ports and the identities of adjacent meshed ports and switches, see “Switch Mesh Information” on page 7-22.

Flooded Traffic

Broadcast and multicast packets will always use the same path between the source and destination edge switches unless link failures create the need to select new paths. (Broadcast and multicast traffic entering the mesh from different edge switches are likely to take different paths.) When an edge switch receives a broadcast from a non-mesh port, it floods the broadcast out all its other non-mesh ports, but sends the broadcast out only those ports in the mesh that represent the path from that edge switch through the mesh domain. (Only one copy of the broadcast packet gets to each edge switch for broadcast out of its nonmeshed ports. This helps to keep the latency for these packets to each switch as low as possible.)

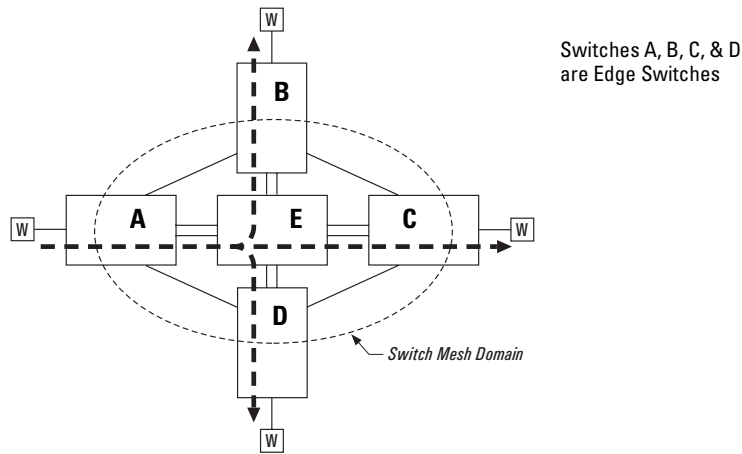


Figure 6-58. Example of a Broadcast Path Through a Switch Mesh Domain

Any mesh switches that are not edge switches will flood the broadcast packets only through ports (paths) that link to separate edge switches in the controlled broadcast tree. The edge switches that receive the broadcast will flood the broadcast out all non-meshed ports. (Note that if multiple VLANs are configured, a broadcast path through the mesh domain leads only to ports that are in the same VLAN as the device originating the broadcast. Refer to “802.1Q VLANs in Meshed Switches” on page 6-91.) Some variations on broadcast/multicast traffic patterns include:

- If multiple VLANs are configured, a broadcast path through the mesh domain leads only to ports that are in the same VLAN as the device originating the broadcast. Refer to “802.1Q VLANs in Meshed Switches” on page 6-91.
- Broadcast control features such as layer 3 (Automatic Broadcast Control) proxy replies and RIP/SAP filtering will reduce broadcast traffic by preventing the need for many of the broadcasts from crossing the switch mesh domain in the first place.

Unicast Packets with Unknown Destinations

A meshed switch receiving a unicast packet with an unknown destination does not flood the packet onto the mesh. Instead, the switch sends a query on the mesh to learn the location of the unicast destination. The meshed switches then send 802.2 test packets through their non-meshed ports. When the unicast destination is found and reported, the unicast packet is then forwarded through the mesh to its destination. By increasing the Address Age Interval in the System Information screen, you can cause the switch address table to

retain device addresses longer. Because the switches in a mesh exchange address information, this will help to decrease the number of unicast packets with unknown destinations, which will improve latency within the mesh. Also, in an IP environment, it is recommended that you configure meshed switches with their own IP addresses. This makes the discovery mechanism more robust, which contributes to decreased latency.

Spanning Tree Operation with Switch Meshing

Using STP with several switches and no switch meshing configured can result in unnecessarily blocking links and reducing available bandwidth. For example:

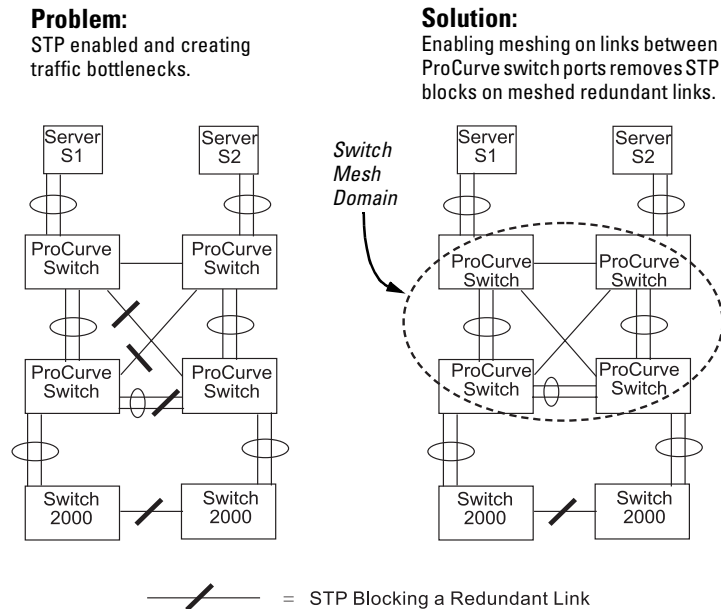


Figure 6-59. Example Using STP Without and With Switch Meshing

If you enable STP in a network that includes switch meshing, you should enable STP on the meshed switches as well as the non-meshed devices. STP sees a meshed domain as a single port. However, on edge switches in the domain, STP will manage non-meshed redundant links from other devices. For example:

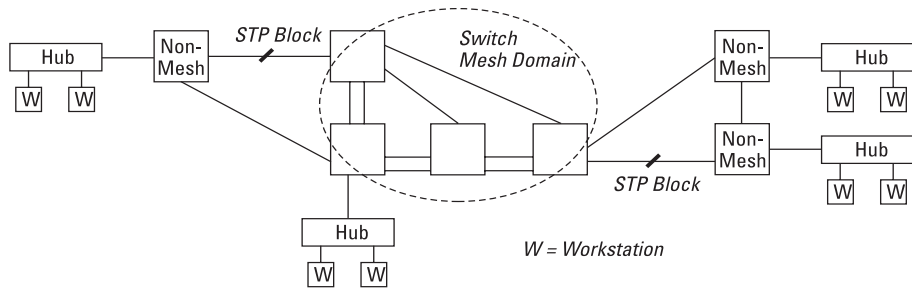


Figure 6-60. Connecting a Switch Mesh Domain to Non-Meshed Devices

STP should be configured on non-mesh devices that use redundant links to interconnect with other devices or with multiple switch mesh domains. For example:

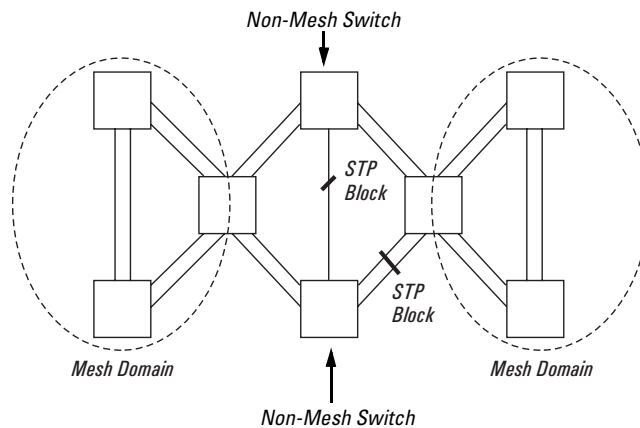


Figure 6-61. Interconnecting Switch Mesh Domains with Redundant Links

In the above case of multiple switch meshes linked with redundant trunks there is the possibility that STP will temporarily block a mesh link. This is because it is possible for STP to interpret the cost on an external trunked link to be less than the cost on a meshed link. However, if this condition occurs, the meshed switch that has a blocked link will automatically increase the STP cost on the external (non-meshed) link to the point where STP will block the external link and unblock the meshed link. This process typically resolves itself in approximately 30 seconds.

Caution

Because the switch automatically gives faster links a higher priority, the default STP parameter settings are usually adequate for spanning tree operation. Because incorrect STP settings can adversely affect network performance, you should avoid making changes without having a strong understanding of how STP operates. For more on STP, refer to “Spanning Tree Protocol (STP)” (page 6-39), and examine the IEEE 802.1d standard.

Filtering/Security in Meshed Switches

Because paths through the mesh can vary with network conditions, configuring filters on meshed ports can create traffic problems that are difficult to predict, and is not recommended. However, configuring filters on nonmeshed ports in an edge switch provides you with control and predictability.

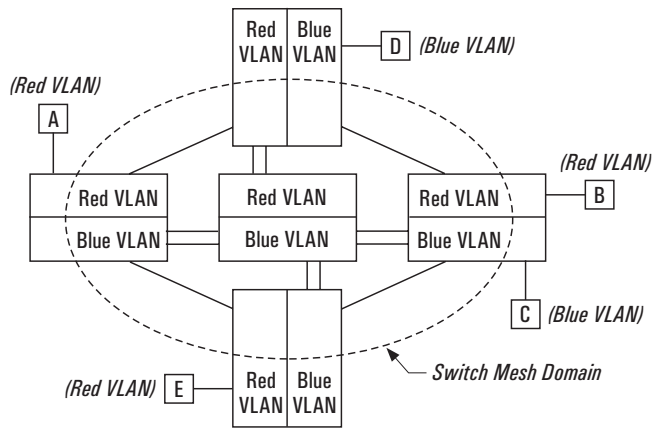
IP Multicast (IGMP) in Meshed Switches

Like trunked ports, the switch mesh domain appears as a single port to IGMP. However, unlike trunked ports, IGMP protocol and multicast traffic may be sent out over several links in the mesh in the same manner as broadcast packets.

802.1Q VLANs in Meshed Switches

In a network having a switch mesh domain and multiple VLANs configured, all VLANs must be configured on each meshed switch, even if no ports on the switch are assigned to any VLAN. (The switch mesh is a member of all VLANs configured on the network.)

When VLANs are configured and activated, the mesh is seen as a single entity by each VLAN. All ports in the mesh domain are members of all VLANs and can be used to forward traffic for any VLAN. However, the non-mesh ports on edge switches that allow traffic to move between the mesh and non-meshed devices belong to specific VLANs and do not allow packets originating in a specific VLAN to enter non-meshed devices that do not belong to that same VLAN. (It is necessary to use a router to communicate between VLANs.) For example, in the following illustration, traffic from host A entering the mesh can only exit the mesh at the port for hosts B and E. Traffic from host A for any other host (such as C or D) will be dropped because only hosts B and E are in the same VLAN as host A.



All ports inside the mesh domain are members of all VLANs.

Figure 6-62. VLAN Operation with a Switch Mesh Domain

Using Automatic Broadcast Control In Meshed Switches

To avoid duplicate replies, switch meshing does not allow ABC proxy replies from within a switch mesh. However, an edge switch can learn of the existence of a device on the other side of the mesh and provide a proxy reply to inquiries. For this reason, it is recommended that you configure ABC in all meshed switches.

Requirements and Restrictions

- **Number of Meshed Ports Configured in a Switch:** You can configure up to 24 meshed ports on the Switches 1600M/2424M/4000M/8000M.
- **Mesh Domain Size:** Up to 12 switches are supported in a switch mesh domain. The following example illustrates a meshed backbone where the maximum meshed switch hop count is 3.

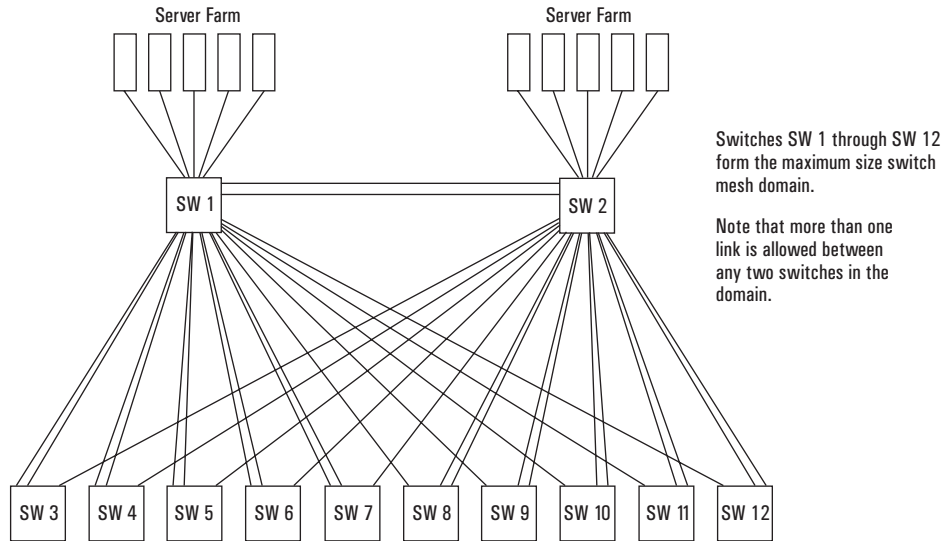


Figure 6-63. Example of a Backbone Using the Maximum Number of Meshed Switches

- **Mesh Support Within the Domain:** All switches in the mesh domain, including edge switches, must support the HP switch meshing protocol. For further information, contact your HP-authorized LAN dealer or refer to HP's ProCurve Networking website at:
<http://www.hp.com/go/procurve>
- **Switch Hop Count in the Mesh Domain:** A maximum (meshed) switch hop count of five is allowed in the path connecting two nodes via a switch mesh domain topology.

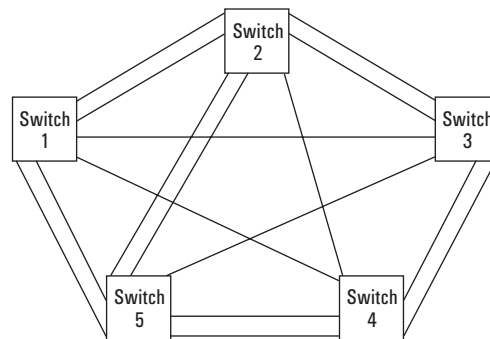


Figure 6-64. Example of the Maximum Meshed Switch Hop Count

- **Connecting Mesh Domains:** To connect two separate switch meshing domains, you must use non-meshed ports. (The non-meshed link can be a port trunk or a single link.) Refer to figure 6-55 on page 6-83.
- **Fast EtherChannel® (FEC):** This cannot be configured on a meshed port. (You can configure FEC on non-meshed ports in a switch that also has meshed ports.)
- **Multiple Links Between Meshed Switches:** Multiple mesh ports can be connected between the same two switches, to provide higher bandwidth. Each port that you want in the mesh domain should be configured as **Mesh** in the Group column of the Load Balancing screen (and not as a trunk—**Trk**). Note that if you configure a port as **Mesh**, there is no “Type” selection.
- **Automatic Broadcast Control:** To use ABC with switch meshing, all edge switches in the mesh must have ABC enabled. Also, proxy replies from the switch are not sent out meshed ports.
- **Network Monitor Port:** If a network monitor port is configured, broadcast packets may be duplicated on this port if more than one port is being monitored and ABC or switch meshing is enabled.

IP Multicast (IGMP) Features— Multimedia Traffic Control

In a network where IP multicast traffic is transmitted for various multimedia applications, you can use the switch to reduce unnecessary bandwidth usage on a per-port basis by configuring IGMP (Internet Group Management Protocol). In the factory default state (IGMP disabled), the switch forwards all IGMP traffic to all ports, which can cause unnecessary bandwidth usage on ports not belonging to multicast groups. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch.

IGMP is useful in multimedia applications such as LAN TV, desktop conferencing, and collaborative computing, where there is multipoint communication; that is, communication from one to many hosts, or communication originating from many hosts and destined for many other hosts. In such multipoint applications, IGMP will be configured on the hosts, and multicast traffic will be generated by one or more servers (inside or outside of the local network). Switches in the network (that support IGMP) can then be configured to direct the multicast traffic to only the ports where needed. If multiple VLANs are configured, you can configure IGMP on a per-VLAN basis.

Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. If no other querier is detected, the switch will then also function as the querier. (If you need to disable the querier feature, you can do so through the IGMP configuration MIB. Refer to “Changing the Querier Configuration Setting” on page 6-105.)

Note

In order for IGMP service to take effect, an IP address must be configured and active. If multiple VLANs are configured, an IP address must be configured for the VLAN in which you are configuring IGMP. Refer to “IP Configuration” on page 6-4.

For more information on IGMP operation, refer to “How IGMP Operates” on page 6-100.

Configuring IGMP from the Web Browser Interface

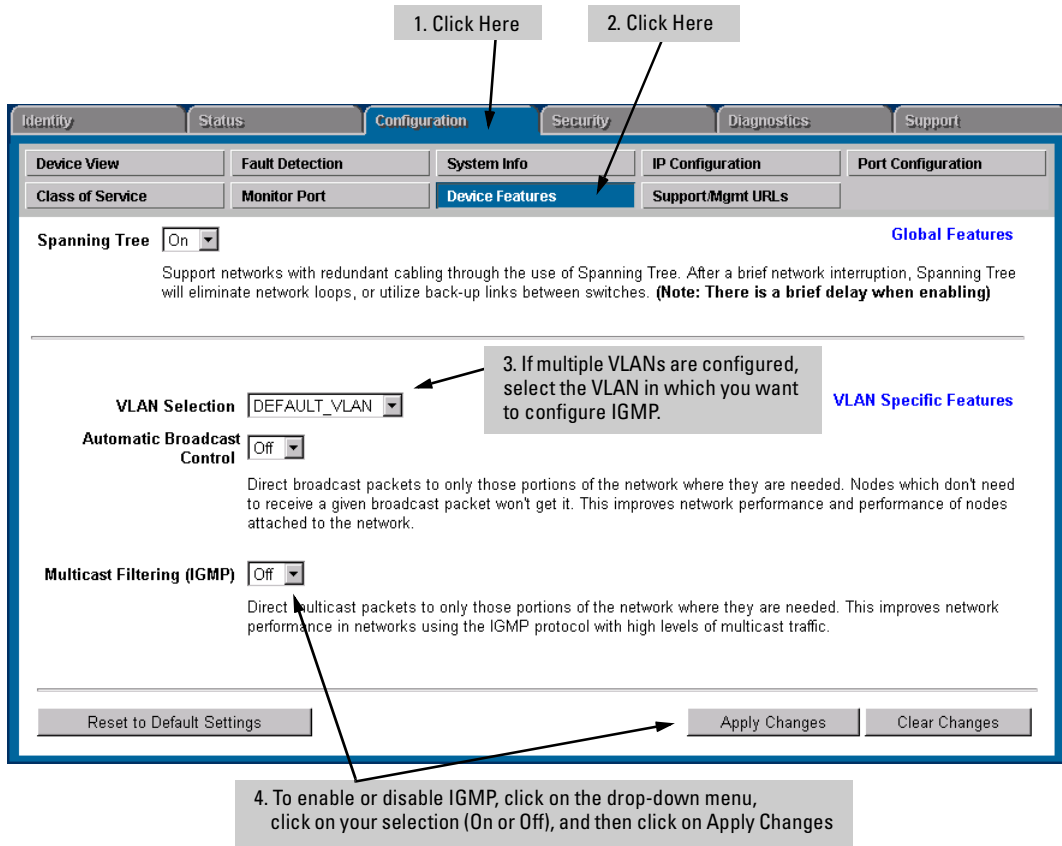


Figure 6-65. Configuring IGMP on the Web Browser Interface

Parameter	Description
<p>Multicast Filtering (IGMP)</p> <p>Default: Off</p>	<p>Determines whether the switch or VLAN uses IGMP on a per-port basis to manage IP Multicast traffic. If multiple VLANs are configured, you can configure IGMP separately for each VLAN. To access a VLAN using the HP web browser interface, enter that VLAN's IP address as the URL.</p> <p>When Off, all ports on the switch or VLAN simply forward IP multicast traffic.</p> <p>When On, enables each port on the switch or VLAN to detect IGMP queries and report packets, and to manage IP multicast traffic.</p> <p>When you use the web browser interface to enable Multicast Filtering, the default operation is for each port in the switch or VLAN to automatically forward or drop IGMP traffic, depending on whether there are any IGMP hosts or multicast routers on the port.</p>
<p>Further Options Available in the Switch Console</p>	<p>By using the switch console, you can make these further changes to IGMP operation:</p> <ul style="list-style-type: none"> • On a per-port basis, block or forward all IP multicast traffic. • For all ports on the switch or VLAN, forward IP multicast traffic at high priority. (The default is for the switch or VLAN to process IGMP traffic, along with other traffic, in the order received.) • Change the querier configuration setting. (By default, the switch will act as a querier if a multicast router is not present to perform this function.) <p>For more information, refer to “Configuring IGMP from the Switch Console” (page 6-98) and “How IGMP Operates” (page 6-100.).</p>

Configuring IGMP from the Switch Console

In the factory default configuration, IGMP is disabled. If multiple VLANs are configured, you can configure IGMP on a per-VLAN basis. When you use either the console or the web browser interface to enable IGMP on the switch or a VLAN, the switch forwards IGMP traffic only to ports belonging to multicast groups. Using the console enables these additional options:

- **Forward with High Priority.** Disabling this parameter (the default) causes the switch or VLAN to process IP multicast traffic, along with other traffic, in the order received. Enabling this parameter causes the switch or VLAN to give a higher priority to IP multicast traffic than to other traffic.
- **Auto/Blocked/Forward:** You can use the console to configure individual ports to any of the following states:
 - **Auto** (the default): Causes the switch to interpret IGMP packets and to filter IP multicast traffic based on the IGMP packet information for ports belonging to a multicast group. This means that IGMP traffic will be forwarded on a specific port only if an IGMP host or multicast router is connected to the port.
 - **Blocked:** Causes the switch to drop all IGMP transmissions received from a specific port and to block all outgoing IP Multicast packets for that port. This has the effect of preventing IGMP traffic from moving through specific ports.
 - **Forward:** Causes the switch to forward all IGMP and IP multicast transmissions through the port.

For more information, refer to “How IGMP Operates” on page 6-100.

To Access IGMP Service:

Use this procedure to configure or edit the IGMP settings for a switch or VLAN.

1. From the Main Menu, select:
 - 3. Switch Configuration**
 - 5. Advanced Features**
 - 3. IP Multicast (IGMP) Service**

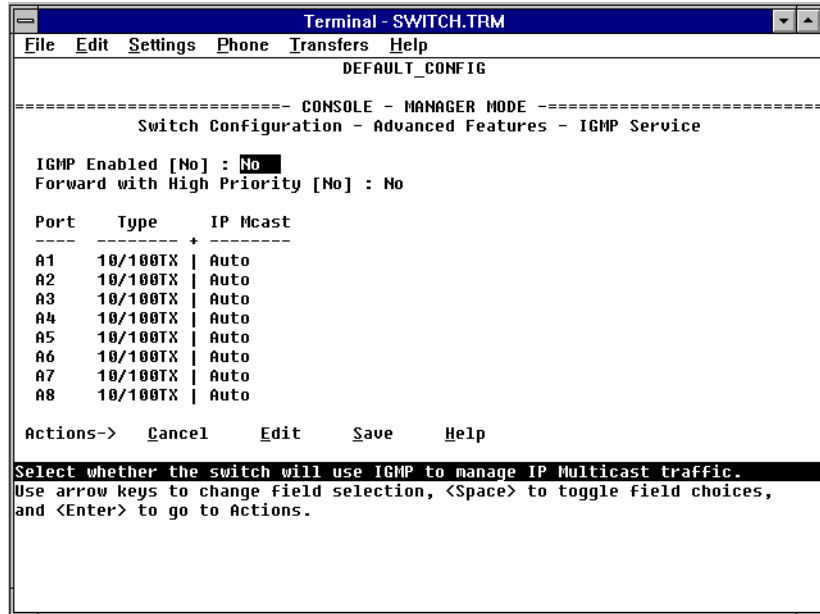


Figure 6-66. Example of the (Default) IGMP Service Screen

2. Press the Space bar to select **Yes** (to enable IGMP).
3. Use to highlight the **Forward with High Priority** parameter.
4. If you want IGMP traffic to be forwarded with a higher priority than other traffic on the switch or VLAN, use the Space bar to select **Yes**. Otherwise, leave this parameter set to **No**.
5. Use to highlight the **IP Mcast** parameter setting for a port you want to reconfigure. (The options are: **Auto**, **Blocked**, and **Forward**. Refer to the previous page or online Help for further information on these choices.)
6. Repeat step 5 for each port you want to configure.
7. When you are finished configuring the **IP Mcast** parameter for the displayed ports, press and (for **Save**) to activate the changes you've made to the IGMP configuration.
8. Return to the Main Menu. (It is not necessary to reboot the switch. The new IGMP configuration is implemented when you select "Save" in step 7.)

How IGMP Operates

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, multicast routers, and hosts that support IGMP. (In Hewlett-Packard's implementation of IGMP, a multicast router is not necessary as long as a switch is configured to support IGMP with the querier feature enabled.) A set of hosts, routers, and/or switches that send or receive multicast data streams to or from the same source(s) is termed a *multicast group*, and all devices in the group use the same multicast group address. The multicast group running version 2 of IGMP uses three fundamental types of messages to communicate:

- **Query:** A message sent from the querier (multicast router or switch) asking for a response from each host belonging to the multicast group. If a multicast router supporting IGMP is not present, then the switch must assume this function in order to elicit group membership information from the hosts on the network. (If you need to disable the querier feature, you can do so through the console, using the IGMP configuration MIB. Refer to “Changing the Querier Configuration Setting” on page 6-105.)
- **Report:** A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
- **Leave Group:** A message sent by a host to the querier to indicate that the host has ceased to be a member of a specific multicast group.

Thus, IGMP identifies members of a multicast group (within a subnet) and allows IGMP-configured hosts (and routers) to join or leave multicast groups.

IGMP Data. To display data showing active group addresses, reports, queries, querier access port, and active group address data (port, type, and access), see “IP Multicast (IGMP) Status” on page 7-19.

Role of the Switch

When IGMP is enabled on the switch, it examines the IGMP packets it receives:

- To learn which of its ports are linked to IGMP hosts and multicast routers/queriers belonging to any multicast group
- To become a querier if a multicast router/querier is not discovered on the network

Once the switch learns the port location of the hosts belonging to any particular multicast group, it can direct group traffic to only those ports, resulting in bandwidth savings on ports where group members do not reside. The following example illustrates this operation.

Figure 6-67 on page 6-102 shows a network running IGMP.

- PCs 1 and 4, switch 2, and all of the routers are members of an IP multicast group. (The routers operate as queriers.)
- Switch 1 ignores IGMP traffic and does not distinguish between IP multicast group members and non-members. Thus, it is sending large amounts of unwanted multicast traffic out the ports to PCs 2 and 3.
- Switch 2 is recognizing IGMP traffic and learns that PC 4 is in the IP multicast group receiving multicast data from the video server (PC X). Switch 2 then sends the multicast data only to the port for PC 4, thus avoiding unwanted multicast traffic on the ports for PCs 5 and 6.

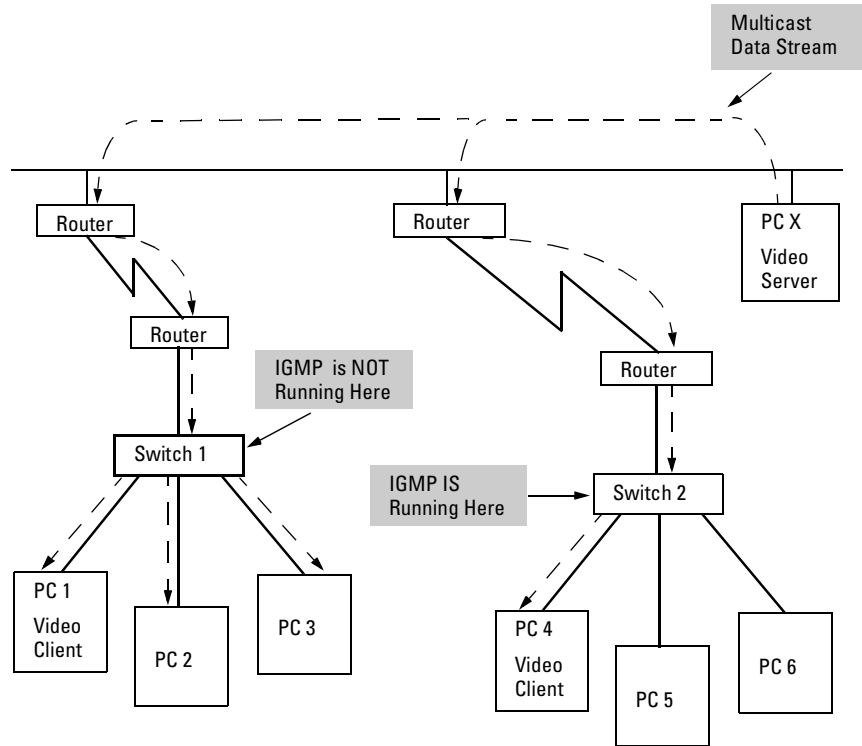


Figure 6-67. The Advantage of Using IGMP

The next figure (6-68) shows a network running IP multicasting using IGMP without a multicast router. In this case, the IGMP-configured switch runs as a querier.

PCs 2, 5, and 6 are members of the same IP multicast group.

IGMP is configured on switches 3 and 4. Either of these switches can operate as querier because a multicast router is not present on the network. (If an IGMP switch does not detect a querier, it automatically assumes this role, assuming the querier feature is enabled—the default—within IGMP.)

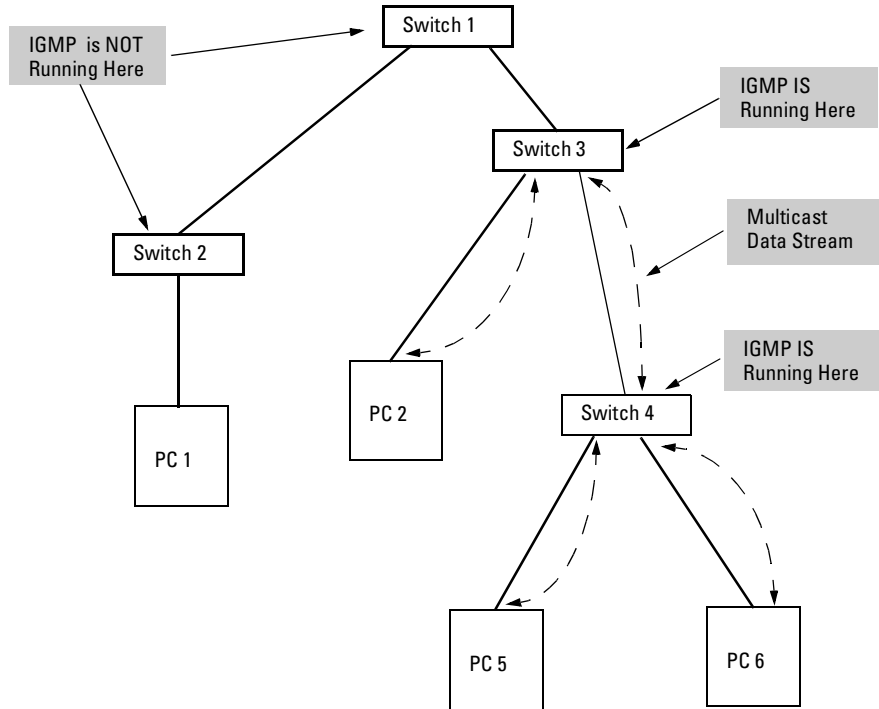


Figure 6-68. Isolating IP Multicast Traffic in a Network

- In the above figure, the multicast group traffic does not go to switch 1 and beyond because either the port on switch 3 that connects to switch 1 has been configured as blocked or there are no hosts connected to switch 1 or switch 2 that belong to the multicast group.
- For PC 1 to become a member of the same multicast group without flooding IP multicast traffic on all ports of switches 1 and 2, IGMP must be configured on both switches 1 and 2, and the port on Switch 3 that connects to Switch 1 must be unblocked.

Note:

IP Multicast Filters. IP multicast addresses occur in the range from 224.0.0.0 through 239.255.255.255 (which corresponds to the Ethernet multicast address range of 01005e-000000 through 01005e-7fffff). Any static Traffic/Security filters (page 6-46) configured with a “Multicast” filter type and a “Multicast Address” in this range will continue in effect unless IGMP learns of a multicast group destination in this range. In that case, IGMP takes over the filtering function for the multicast destination address(es) for as long as the IGMP group is active. If the IGMP group subsequently deactivates, the static filter resumes control over traffic to the multicast address formerly controlled by IGMP.

Reserved Addresses Excluded from IP Multicast (IGMP) Filtering.

Traffic to IP multicast groups in the IP address range of 224.0.0.0 to 224.0.0.255 will always be flooded because addresses in this range are “well known” or “reserved” addresses. Thus, if IP Multicast is enabled and there is an IP multicast group within the reserved address range, traffic to that group will be flooded instead of filtered by the switch.

Number of IP Multicast Addresses Allowed

Multicast filters and IGMP filters (addresses) together can total up to 255 in the switch. If multiple VLANs are configured, then each filter is counted once per VLAN in which it is used.

Interaction with Multicast Traffic/Security Filters.

IGMP-controlled filters override multicast filters defined in the Traffic/Security Filters screen (page 6-47) and having the same multicast address as specified by IGMP.

Changing the Querier Configuration Setting

The Querier feature, by default, is enabled and in most cases should be left in this setting. If you need to change the querier setting, you can do so using the IGMP Configuration MIB. To disable the querier setting, select the Command Prompt from the Diagnostics Menu and enter this command:

```
setmib hpSwitchIcmpQuerierState.<vlan number> -i 2
```

To enable the querier setting, select the Command Prompt from the Main Menu and enter this command:

```
setmib hpSwitchIcmpQuerierState.<vlan number> -i 1
```

To view the current querier setting, select the Command Prompt from the Main Menu and enter this command:

```
getmib hpSwitchIcmpQuerierState.<vlan number>
```

where:

<vlan number> is the sequential (index) number of the specific VLAN. If no VLANs are configured, use “1”. For example:

```
getmib hpSwitchIcmpQuerierState.1
```

Note

The above commands are case-sensitive.

Whenever IGMP is enabled, the switch generates an Event Log message indicating whether querier functionality is enabled.

Automatic Broadcast Control (ABC) Features

ABC reduces the amount of IP and/or IPX broadcast traffic within a broadcast domain without adding the levels of cost and latency normally associated with routers. To get this result, the switch serves as a proxy for IP ARP, IPX NSQ, and IPX GetLocal Target, and limits the forwarding of IP RIP, and IP RIP/ SAP packets to only those ports where the broadcasts are needed. This reduces the number of ports over which IP and/or IPX broadcasts are sent, increases the amount of network bandwidth available for other purposes, and can reduce the need for routers within a network. These factors can lower costs and reduce latency in the network. (While communication between VLANs—broadcast domains—still requires a router, ABC functions within VLANs and, by using multiple subnets per VLAN—multi-netting, can reduce or eliminate the need for routers within the VLAN.)

When enabled, ABC also sets the broadcast limit parameter (**Bcast Limit**) in the Port Configuration screen of the console (figure 6-21) for all ports on the switch (or selected VLAN, if VLANs are configured) that have not already been set to a nonzero value.

In the factory default state, ABC is disabled.

Note

ABC does not control AppleTalk and DECnet broadcasts. To limit these protocols, use the protocol filter option available with Traffic/Security filters. Refer to “Traffic/Security Filters” on page 6-46.

For further operating information and restrictions, refer to “How ABC Operates” on page 6-113.

Configuring ABC from the Web Browser Interface

The screenshot shows the configuration page for the switch. The 'Configuration' tab is selected, and the 'Device Features' sub-tab is active. The 'Spanning Tree' is set to 'On'. Under 'Global Features', there is a section for 'Spanning Tree' with a note: 'Support networks with redundant cabling through the use of Spanning Tree. After a brief network interruption, Spanning Tree will eliminate network loops, or utilize back-up links between switches. (Note: There is a brief delay when enabling)'. Below this, under 'VLAN Specific Features', there is a 'VLAN Selection' dropdown menu set to 'DEFAULT_VLAN' and an 'Automatic Broadcast Control' dropdown menu set to 'Off'. Arrows point to these elements with labels: '1. Click Here' points to the 'Configuration' tab, '2. Click Here' points to the 'Device Features' sub-tab, '3. If VLANs are configured, select VLAN.' points to the 'VLAN Selection' dropdown, and '4. Enable ABC' points to the 'Automatic Broadcast Control' dropdown. Below the 'Automatic Broadcast Control' dropdown, there is a description: 'Direct broadcast packets to only those portions of the network where they are needed. Nodes which don't need to receive a given broadcast packet won't get it. This improves network performance and performance of nodes attached to the network.'

Parameter	Description
VLAN Selection	If multiple VLANs are configured on the switch, select the VLAN in which you want to enable ABC. (If only the DEFAULT_VLAN exists, then all ports on the switch belong to the same broadcast domain and it is not necessary to select a VLAN before enabling ABC.)
Automatic Broadcast Control	Enables or disables ABC for both IP and IPX protocols. When you enable ABC, it automatically resets the default (0) broadcast limits for each port to 30 (%) to help minimize the effects of broadcast storms. Other ABC-related options are also available through the console. Refer to "Configuring ABC from the Switch Console" (page 6-108) and "How ABC Operates" (page 6-113).

Configuring ABC from the Switch Console

In the factory default configuration, ABC is disabled and all broadcasts are sent out either all ports in the switch or, if VLANs are configured, out all ports in VLANs where ABC is enabled. If multiple VLANs are configured, you can configure ABC on a per-VLAN basis. Otherwise, the configuration is for all ports in the switch. You can enable ABC for IP only, IPX only, or for both. When you enable ABC, the broadcast limits on each switch port (or on the selected VLAN, if VLANs are configured) are automatically set to 30% to help minimize the effects of broadcast storms (if the limit has not already been set manually through the Port Settings screen). If you disable ABC, the broadcast limit is reset to 0 on all ports except those ports on which the limit was manually set. (However, if ABC is disabled on one VLAN, but remains active on another VLAN, the broadcast limit will not be changed on any port that belongs to both VLANs.)

ABC Option	Effect of Enabling ABC	Automatic Per-Port Broadcast Limit
IP Only	Causes the switch to send a proxy ARP reply for hosts whose addresses the switch has learned. Enabling for IP also allows you to choose whether to enable ABC for IP RIP Control. If enabled, IP RIP Control causes IP RIP broadcasts to be forwarded only to ports where IP RPs have been previously received. This avoids sending IP RIP broadcasts to ports where there is no indication of devices that would use them.	For ports where the Bcast Limit parameter is set to 0, activates a broadcast limit of 30 percent. (If VLANs are configured, affects only the ports in the selected VLAN). You can accept the default automatic broadcast limit or use the Port Settings screen—page 6-33—to change it or turn it off.) Disabling ABC returns these ports to a 0 percent setting unless they have been manually reset to a value other than the automatic 30 percent.
IPX Only	Causes the switch to send a proxy NSQ (nearest server query) reply for services the switch has learned. Enabling for IPX also allows you to choose whether to enable IPX RIP/SAP control. If enabled, IPX RIP/SAP control causes IPX RIP and SAP broadcasts to be forwarded only to ports where IPX RPs and SAPs have previously been received. This avoids sending IPX RIP and SAP broadcasts to ports where there is no indication of devices that would use them.	Same as above.
IP and IPX	Causes the switch to send a proxy IP ARP reply for hosts whose addresses the switch has learned, or to send a proxy NSQ (nearest server query) reply for services the switch has learned. Enabling for both IP and IPX also allows you to enable ABC for IP RIP Control and/or IPX RIP/SAP control, as described above.	Same as above.

To Access ABC:

1. From the Main Menu, Select:
 3. Switch Configuration
 5. Advanced Features
 4. Automatic Broadcast Control (ABC)

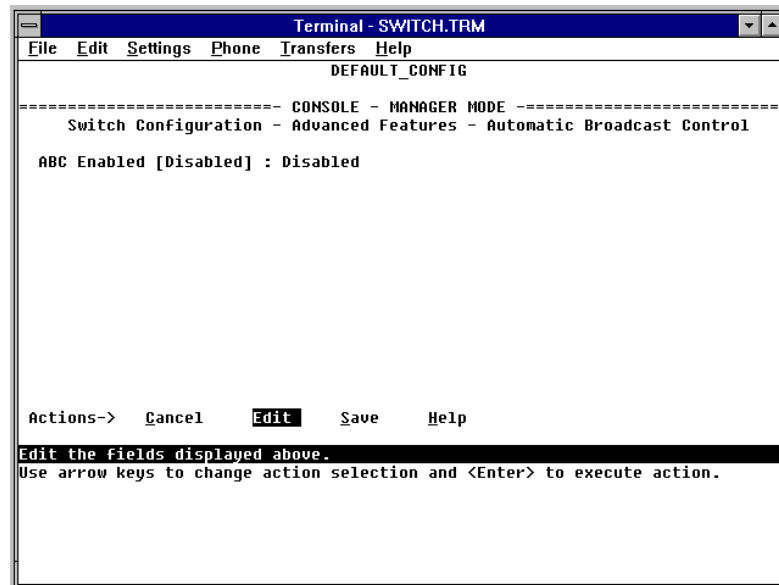


Figure 6-69. The Default ABC Screen (No VLANs Configured)

2. If no VLANs are configured, go to step 3. If VLANs are configured, press **Edit**, then select the VLAN in which you want to configure ABC.

Note

The rest of this procedure assumes that VLANs are *not* configured. If you have VLANs configured on your switch, you can still use this procedure. The screen layout will be different than shown here, but the parameters are the same.

3. Press **E** (for **Edit**).
4. Use the Space bar to enable ABC. Select one of these options:
 - **IP_IPX**: Enables ABC for both the IP and IPX protocols.
 - **IP**: Enables ABC for the IP protocol only.
 - **IPX**: Enables ABC for the IPX protocol only.

Configuring the Switch

Automatic Broadcast Control (ABC) Features

5. Press the \rightarrow key to display the remaining ABC parameters. Then do *one* of the following:
 - If you enabled ABC for IP_IPX and pressed \rightarrow (figure 6-70, below):

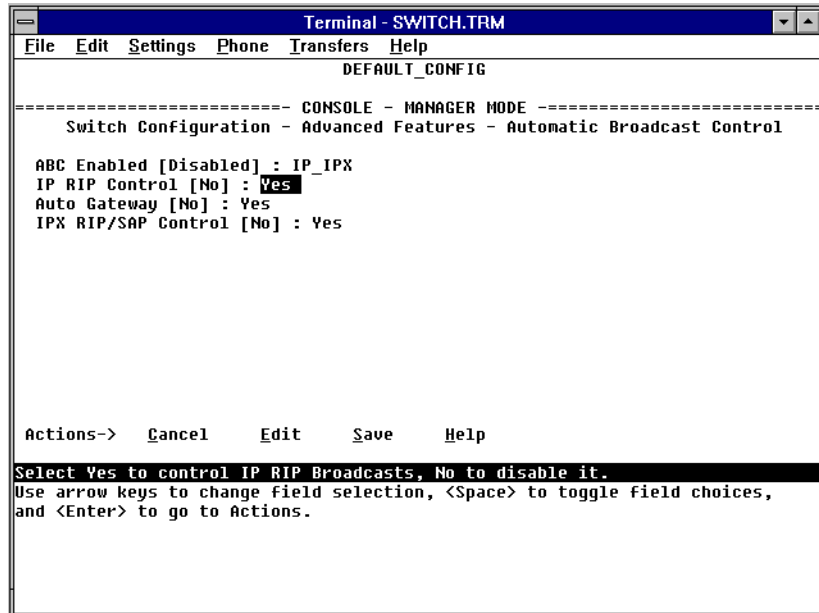


Figure 6-70. ABC Enabled With Default IP_IPX Option (No VLANs Configured)

- i. If you want IP RIP broadcast control, then select the **IP RIP Control** parameter and use the Space bar to select **Yes**.
- ii. If your network uses DHCP to manage IP addressing and you want to automatically configure hosts on the network to be their own gateways, select **Auto Gateway** and use the Space bar to select **Yes**. (For more information, refer to “Automatic Gateway Configuration” on page 6-115.)
- iii. If you want IPX RIP/SAP broadcast control, select the **IPX RIP/SAP Control** parameter and use the Space bar to select **Yes**.
- iv. Go to step 6 on page 6-112.

Note

ABC automatically sets a global broadcast limit of 30% for all ports in the switch or selected VLAN (if VLANs are configured) that have not already been manually set to another value. If you want to set broadcast limits on a per-port basis, you can override the automatic setting by going to the Port Settings screen (page 6-33) and setting the broadcast limit individually for one or more ports.

- If you enabled ABC for IP (figure 6-64, below):

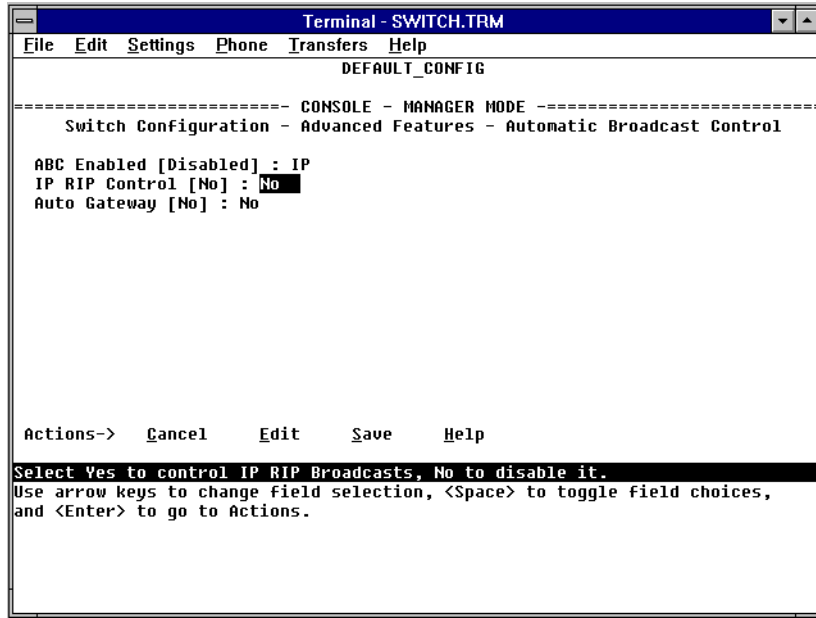


Figure 6-71. ABC Enabled With Default IP Option (No VLANs Configured)

- i. If you want IP RIP broadcast control, then select the **IP RIP Control** parameter and use the Space bar to select **Yes**.
 - ii. If your network uses DHCP to manage IP addressing and you want to automatically configure hosts on the network to be their own gateways, select **Auto Gateway** and use the Space bar to select **Yes**. (For more information, refer to “Automatic Gateway Configuration” on page 6-115.)
 - iii. Go to step 6 on page 6-112.
- If you enabled ABC for IPX (figure 6-72, below):

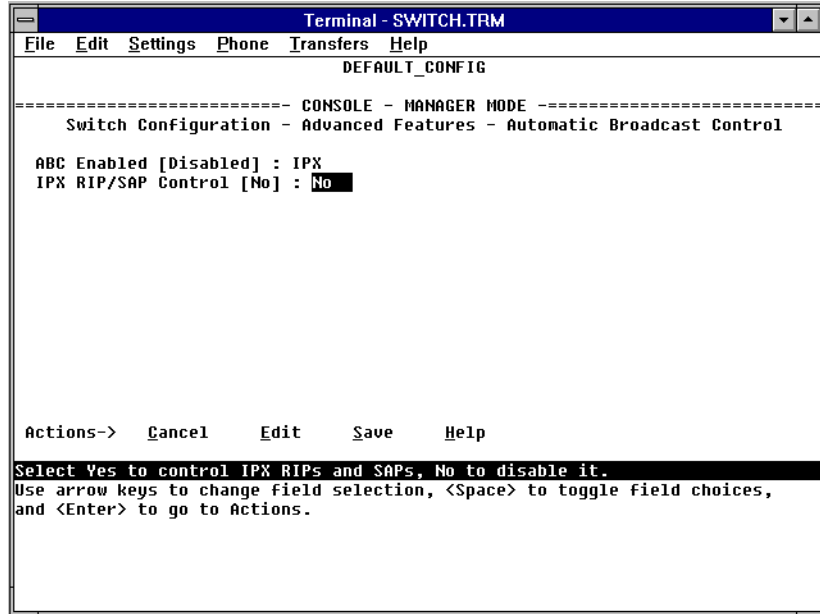


Figure 6-72. ABC Enabled With Default IPX Option (No VLANs Configured)

- i. If you want IPX RIP/SAP control, then select the **IPX RIP/SAP Control** parameter.
 - ii. Use the Space bar to select **Yes**.
 - iii. Go to step 6, below.
6. Press **[Enter]** to return to the **Actions** menu.
7. Press **[S]** (for **Save**) to activate the changes you have made.
8. Return to the Main Menu. (It is not necessary to reboot the switch. The new ABC configuration activates when you select the “Save” in step 7.)

How ABC Operates

Layer 2 (MAC level) broadcast packets can become a large percentage of the traffic on a network. These broadcasts not only use up network bandwidth, but also use up processing power on every client that receives the broadcast. Routers reduced this problem by introducing broadcast domains to reduce broadcast propagation through a network. However routers also introduced increased costs and latency, with reduced throughput.

Using a Hewlett-Packard switch equipped with Automatic Broadcast Control instead of using a router overcomes the latency and throughput problems at a lower cost and with greater ease of management.

Reducing ARP Broadcast Traffic

When enabled on the switch or a VLAN, ABC does the following to reduce ARP (Address Resolution Protocol) broadcast traffic:

1. Learns which port various hosts reside on by reading the address information in broadcast ARP (Address Resolution Protocol) packets and unicast ARP response packets
2. Proxy responds to subsequent ARP broadcast requests for those hosts from other devices instead of forwarding such requests out all ports and requiring each host to respond

For example, assume that host A has traffic for host D.

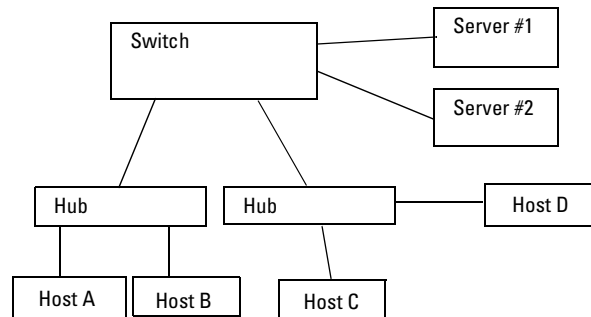


Figure 6-73. Example of a Network Using ABC

To learn host D's MAC address, host A sends a broadcast ARP request. Because the switch does not yet know the location of host D, it floods the request out all ports. However, the switch also learns from the ARP request the location of host A and stores this information in its ARP cache. Host D receives the ARP request (as will all other hosts connected to the switch), and responds

with a unicast packet through the switch to host A. The switch monitors this response, learns the location of host D, and stores this information in its ARP cache. Thus, the switch now knows the address information for both host A and host D. Now, hosts A and D can send unicast packets to each other because they have learned each other's addresses.

Suppose that host C now wants to communicate with host A. C sends a broadcast ARP request to the switch. Because the switch already has A's address information, it does not flood C's ARP request out all ports, but instead sends a proxy ARP reply to C that tells C the address information for host A. Host C can now send unicast packets directly to host A. From these packets, host A will learn host C's addressing information and be able to respond with unicast packets addressed to host C. The result is reduced network traffic because host C's broadcast ARP request was not flooded on the switch's ports.

Similarly, for IPX networks, the switch learns service and route information from SAPs and RIPs respectively, and maintains SAP and RIP tables that contain the addresses of known servers. Using this data, the switch sends proxy responses to NSQ requests for these servers instead of flooding the requests on all ports.

Note

The switch sends proxy ARP replies to hosts (ARP initiators) that are on a different port than the target host. However, the switch does not send a proxy ARP reply when both the initiator and the target host are on the same port. For example, the switch does not send a proxy ARP reply for host B (figure 6-73) in replying to an ARP request from host A.

The switch does not translate encapsulation types (such as 802.2 to SNAP in IPX). As a result, if a host client sends an NSQ request for a server, the switch will always send a proxy response containing the address of a server supporting the same encapsulation type. If the switch has not learned of a server using the same encapsulation type as the host client, then the switch will flood the host client's NSQ request to all ports. However, if a local server supporting the same encapsulation type exists on a port from which the NSQ request is received, the switch will not forward the request to other ports.

Reducing RIP and SAP Broadcast Traffic

You can also configure ABC to limit IP RIP and IPX RIP and SAP broadcasts, which can further reduce broadcast traffic on your network. RIP and SAP broadcasts are normally forwarded on all ports. However, with ABC enabled and additional RIP and SAP parameters configured, the switch forwards IP RIP and IPX RIP and SAP broadcasts only to the ports on which these types of broadcasts have been received earlier. This means that other ports are relieved of some unnecessary traffic because the RIP and SAP broadcasts will be forwarded only to ports where there are routers or servers that would use the broadcast information.

Automatic Gateway Configuration for Networks Using DHCP To Manage IP Addresses.

When using ABC, each client in a multi-subnet structure can be configured as its own gateway so that traffic from the client can be sent directly to target nodes. (This reduces traffic to and from a multinetted router or it allows inter-subnet communication without needing a router.)

Note

If you are using ABC *without* substituting a switch for a router, or if you are adding a switch to enhance performance without replacing a router, then clients do not need to be reconfigured as their own gateways.

You can automatically reconfigure the gateway for clients in a network that meets the following two conditions:

- DHCP is the automatic configuration protocol used to manage IP addresses on the network.
- the DHCP request travels through the switch on its path to the DHCP server.

If you are replacing a router with a switch, one of your tasks is to change the default gateway configuration on all of the clients in the network. Also, some DHCP servers do not have an option allowing a client to be configured as its own gateway. The **Auto Gateway** parameter available with the IP-related ABC options modifies DHCP replies from the server so that the gateway IP address will be set to the client's own IP address.

Note

Clients may not implement a gateway address change without rebooting. Thus, after implementing the automatic gateway feature on the switch, reboot all DHCP clients connected to the switch.

The **Auto Gateway** parameter does not affect operation of hosts on the same port as the DHCP server. This is because such hosts receive responses directly from the server instead of responses from the switch. To prevent this problem, connect the DHCP servers directly to the switch.

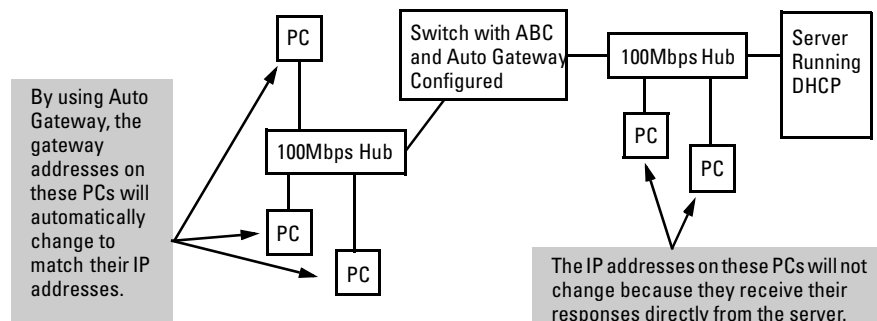


Figure 6-74. DHCP Server Responses Must Come Through the Switch

Restrictions

- **Default Gateway Configuration:** For inter-subnet communication to operate properly in a multi-subnet structure in which there are no routers, all IP hosts in the network or VLAN must be their own default gateways. This means that in an IP host, the IP address of the default gateway must be the IP address assigned to that IP host. Refer to “Automatic Gateway Configuration for Networks Using DHCP To Manage IP Addresses” on page 6-115. For troubleshooting information, see “Automatic Broadcast Control Problems” on page 8-6.
- **Automatic Gateway Configuration:** Operates only for hosts designed and configured for the Bootp/DHCP Router Option (Option 3, as described in RFC 2132). Other hosts must be manually configured.
- **Switch Meshing:** To use ABC with switch meshing, all edge switches in the mesh must have ABC enabled. This is because proxy replies from the switch are not sent out meshed ports. For more on ABC operation with other switch features, see HP’s ProCurve Networking site at the following URL on the World Wide Web:

<http://www.hp.com/go/procurve>

- **IPX Networks:**
 - Only four IPX networks (with four different encapsulation types) are allowed per VLAN.
 - The IPX server chosen in the proxy response is always the first nearest server in the SAP table.
- **Server Selection:** The switch does not support encapsulation translations (such as from 802.2 to SNAP in IPX). For this reason, the switch always responds to a client request by providing a proxy reply to a server supporting the same encapsulation type.
- **AppleTalk and DECnet:** Packets from these protocols are forwarded (bridged) without any broadcast controls. To limit distribution of packets carrying these protocols, use the protocol filter capability described under “Traffic/Security Filters” on page 6-46.

Configuring and Monitoring Port Security

Using Port Security, you can configure each switch port with a unique list of the MAC addresses of devices that are authorized to access the network through that port. This enables individual ports to detect, prevent, and log attempts by unauthorized devices to communicate through the switch.

Basic Operation

The default port security setting for each port is “off”. That is, any device can access a port without causing a security reaction. However, on a per-port basis, you can configure security measures to block unauthorized connections or “listening”, and to send notice of security violations. Once you have configured port security, you can then monitor the network for security violations through one or more of the following:

- Alert flags that are captured by network management tools such as HP TopTools for Hubs & Switches
- Alert Log entries in the switch’s web browser interface
- Event Log entries in the console interface
- Intrusion Log entries in either the switch’s web browser interface or console interface

For any port, you can configure the following:

- **Authorized Addresses:** Specify up to eight devices (MAC addresses) that are allowed to send inbound traffic through the port. This feature:
 - Closes the port to inbound traffic from any unauthorized devices that are connected to the port.
 - Automatically sends notice of an attempted security violation to the switch’s Intrusion Log and to the Alert Log in the switch’s web browser interface.
 - Sends an SNMP trap notifying of an attempted security violation to a network management station. (For more on configuring the switch for SNMP management, see page 6-14.)

- **Prevent Eavesdropping:** Block outbound traffic with unknown destination addresses from exiting through the port. This prevents an unauthorized device on the port from eavesdropping on the flooded unicast traffic intended for other devices.

Note

The switch security measures block unauthorized traffic without disabling the port. This implementation enables you to apply the security configuration to ports on which hubs or other switches are connected, and to maintain security while also maintaining network access to authorized users.

Configuring Port Security

Planning

1. Plan your port security configuration and monitoring according to the following:
 - a. On which ports do you want to configure intruder security?
 - b. Which devices (MAC addresses) are authorized on each port (up to 8 per port)?
 - c. For each port, what security actions do you want? You can do one or both of the following:
 - Block intruders from transmitting to the network
 - Prevent intruders from eavesdropping on network traffic
 - d. How do you want to learn of the security violation attempts the switch detects? You can use one or more of these methods:
 - Through network management (That is, do you want an SNMP trap sent to a net management station when a port detects a security violation attempt?)
 - Through the switch's web browser interface (Alert Log and Intrusion Log)
 - Through the Event Log and the Intrusion Log in the switch console interface
2. Use the web browser interface and/or the switch console to configure port security. The following table describes the parameters.

Table 6-5. Port Security Control Parameters

Parameter	Description
Port	Identifies the switch port to view or configure for port security.
Learn Mode	<p>Specifies how the port will acquire its list of authorized addresses.</p> <p>Continuous (the default): Allows the port to learn addresses from inbound traffic from any device(s) to which it is connected. In this state, the port accepts as authorized any device(s) to which it is connected. Addresses learned this way appear in the switch and port address tables and age out according to the Address Age interval in the System Information configuration screen.</p> <p>Static: Enables you to specify how many devices are authorized on the port and to enter the MAC addresses of the authorized devices. If you enter fewer MAC addresses than you authorized, the port learns the remaining addresses from the inbound traffic it receives. (See “Authorized Addresses” at the end of this table.)</p> <p>Note: When you configure Learn Mode to Static, all devices (MAC addresses) in the port’s address table are deleted (from both the port’s address table and the switch’s address table) and replaced by the authorized devices for this port.</p>
Address Limit	When Learn Mode is set to Static, specifies how many authorized devices (MAC addresses) to allow. Range: 1 (the default) to 8.
Eavesdrop Prevention	<p>Specifies whether the port will block outbound traffic addressed to devices unknown to the port (that is, flooded unicast traffic). This is recommended for use on secure ports with known (static) MAC addresses, which make it unnecessary for these ports to transmit flooded unicast traffic for unknown destinations.</p> <p>Disabled (the default): Allow the port to transmit all outbound traffic it receives, regardless of whether the traffic is addressed to devices that are known to the port.</p> <p>Enabled: Allows the port to transmit only the outbound traffic addressed to devices that are known to the port. (Outbound traffic to devices unknown to the port is dropped.) Devices known to the port include all devices (MAC addresses) the port has detected and listed in its address table, and any devices configured in the Authorized Addresses table. (You can view the port’s address table from the console Status and Counters menu. The Authorized Addresses table appears if the Learn Mode parameter is set to Static.)</p> <p>Note: This feature is not recommended for applications in which a port’s Learn Mode is configured to Continuous.</p>
Action	<p>Specifies whether an SNMP trap is sent to a network management station when Learn Mode is configured to Static and the port detects an unauthorized device.</p> <p>None (the default): Prevents an SNMP trap from being sent.</p> <p>Send Alarm: Causes the switch to send an SNMP trap to a network management station. For information on configuring the switch for SNMP management, see page 6-14.</p>

Parameter	Description
Authorized Addresses	<p>Appears when Learn Mode is set to Static. Enables you to enter up to eight authorized devices (MAC addresses) per port, depending on the value specified in the Address Limits field. If you enter fewer devices than you specified in the Address Limits field, the port learns the remaining addresses from the inbound traffic it receives. For example, if you specify four devices, but enter only two MAC addresses, the first two (non-specified) devices subsequently detected on the port will be added to the Authorized Address list, and all subsequent (non-specified) devices detected on the port will be handled as “unauthorized”.</p> <p>Caution: If you enter fewer devices (MAC addresses) than specified in the Address Limits parameter, it is possible to unintentionally allow a device to become “authorized” that you do not want to include in your Authorized Address list. This can occur because the port, in order to fulfill the number of devices allowed by the Address Limits parameter, will automatically add devices it detects until the specified limit is reached. For this reason it is recommended that you configure the Address Limit to allow only as many devices as you plan to type in to the Authorized Addresses list.</p>

Using the Web Browser Interface to Configure Port Security

1. Display the Port Security Screen

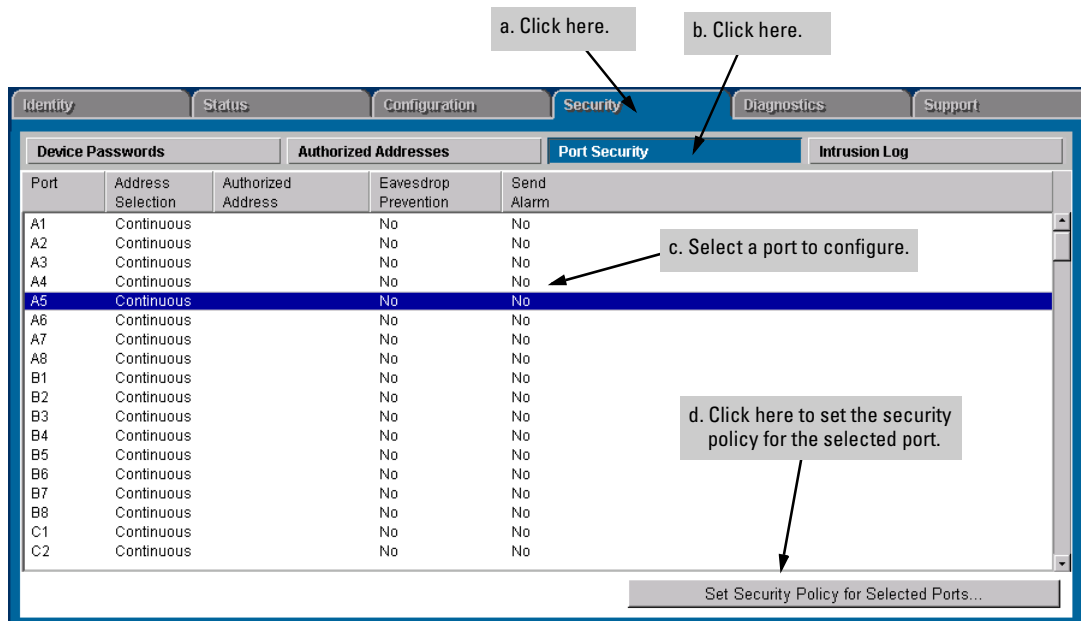


Figure 6-75. Example of the Port Security Overview Screen

2. Set the security policy for the selected port.

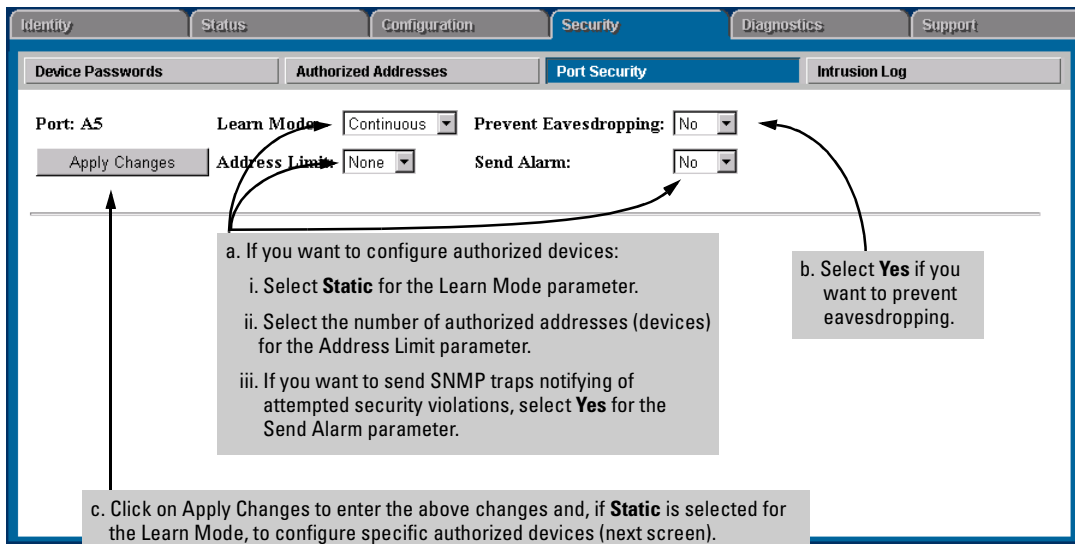


Figure 6-76. Example of the Default Security Configuration Screen for a Selected Port

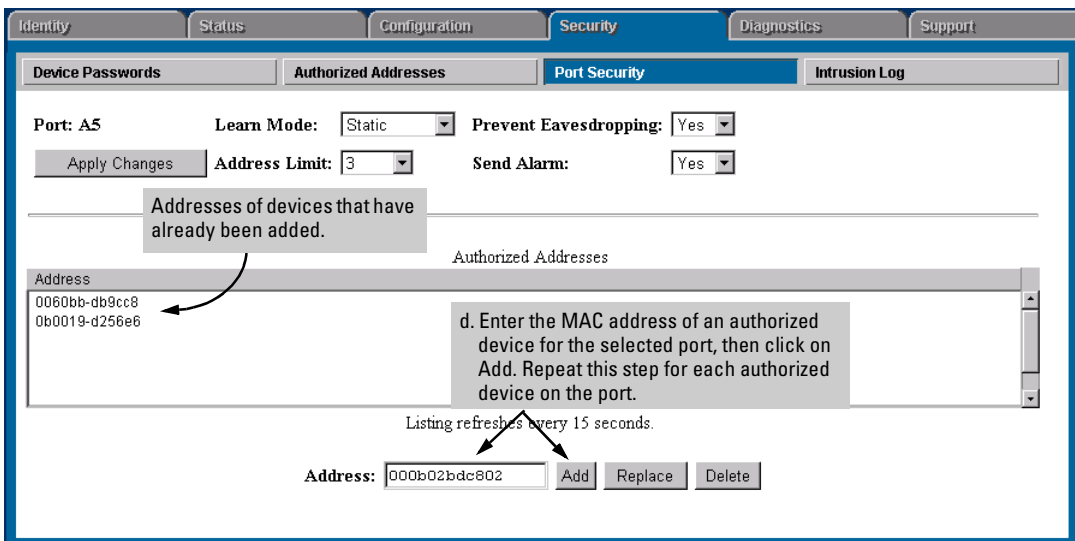


Figure 6-77. Example of Adding Authorized Devices

Using the Switch Console To Configure Port Security

From the Main Menu, select:

3. Switch Configuration ...
5. Advanced Features ...
5. Port Security

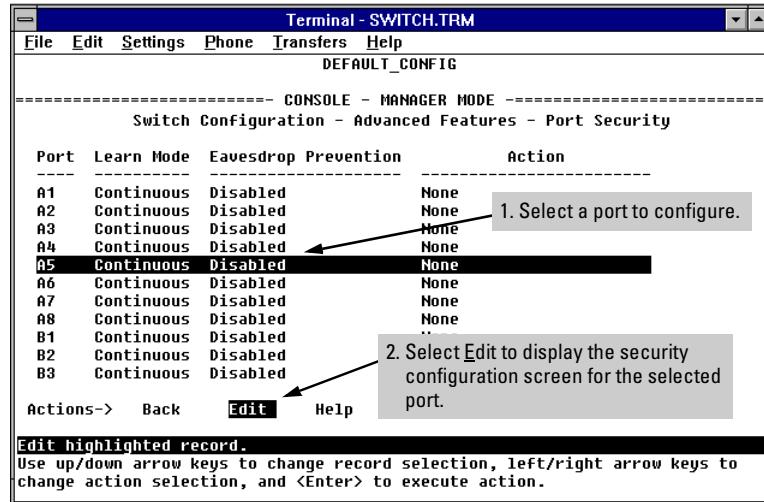


Figure 6-78. Example of the Console Port Security Overview Screen

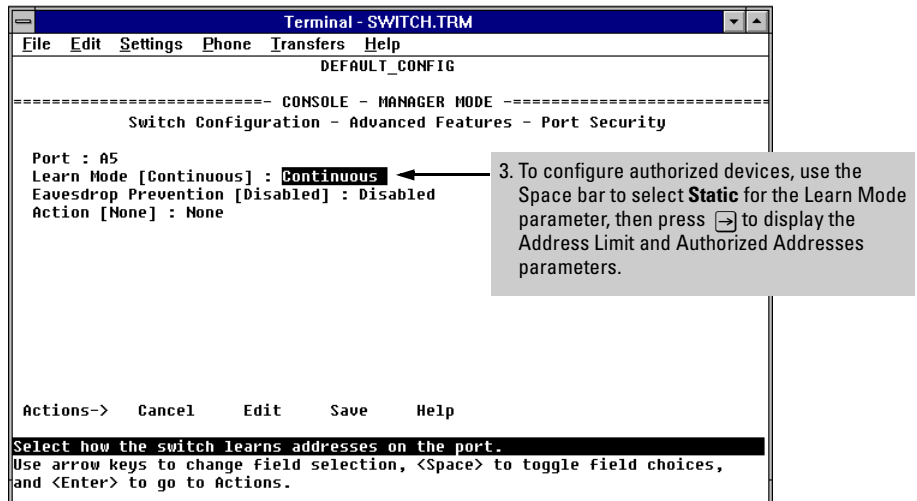


Figure 6-79. Example of the Default Security Configuration Screen for a Selected Port

```
Terminal - SWITCH.TRM
File Edit Settings Phone Transfers Help
-----
                DEFAULT_CONFIG
-----
Switch Configuration - Advanced Features - Port Security

Port : A5
Learn Mode [Continuous] : Static      Address Limit [1] : 3
Eavesdrop Prevention [Disabled] : Enabled
Action [None] : Send Alarm

Authorized Addresses
-----
0050a2-393dda
0060b0-8544ce
00906d-fdcc00

Actions->  Cancel  Edit  Save  Help

Save changes and return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.

4. Configure Address Limit to the number of
   authorized devices you want on the port.
   Note: If the Address Limit parameter
   is more than the number of Authorized
   Addresses, the port automatically adds
   devices in addition to the one(s) you
   specified in the Authorized Address list.
   See the Caution for "Authorized
   Addresses" at the end of table 6-5
   (starts on page 6-120).

5. Enable Eavesdrop Prevention if you
   want to prevent an unauthorized
   device from using the port to
   eavesdrop on the network.

6. Configure the Action parameter to
   send an alarm if you want an SNMP
   trap sent if the switch detects a
   security violation attempt.

7. Type the MAC addresses of the
   authorized device(s) you want on
   the port.

8. Press [Enter], then [S] (for
   Save) to return to the Port
   Security screen.
```

Figure 6-80. Example of a Modified Security Configuration Screen for a Selected Port

Reading and Resetting Intrusion Alarms

When an attempted security violation occurs on a port configured for Port Security, the port drops the packets it receives from the unauthorized device.

Notice of Security Violations

When a security violation occurs on a port configured for Port Security, the switch responds in the following ways to notify you:

- The switch sets an alert flag for that port. This flag remains until:
 - You use either the console or web browser interface to reset the flag.
 - The switch is reset to its factory default configuration.
- The web browser and console interfaces notify you of the intrusion.
 - In the web browser interface:
 - The Alert Log displays a Security Violation entry, with the system date and time, and the port on which the violation occurred (figure 6-81, below).
 - The Intrusion Log lists the port number, the MAC address of the intruding device, and the system time and date when the intrusion occurred (figure 6-82 on page 6-126).

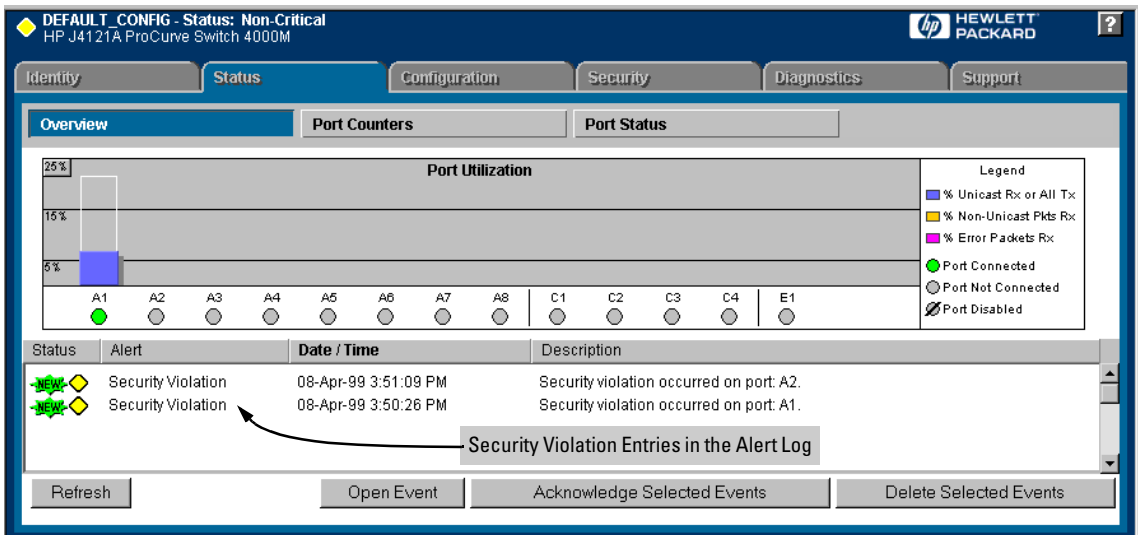


Figure 6-81. Example of Security Violation Entries in the Alert Log of the Switch's Web Browser Interface

Configuring the Switch

Configuring and Monitoring Port Security

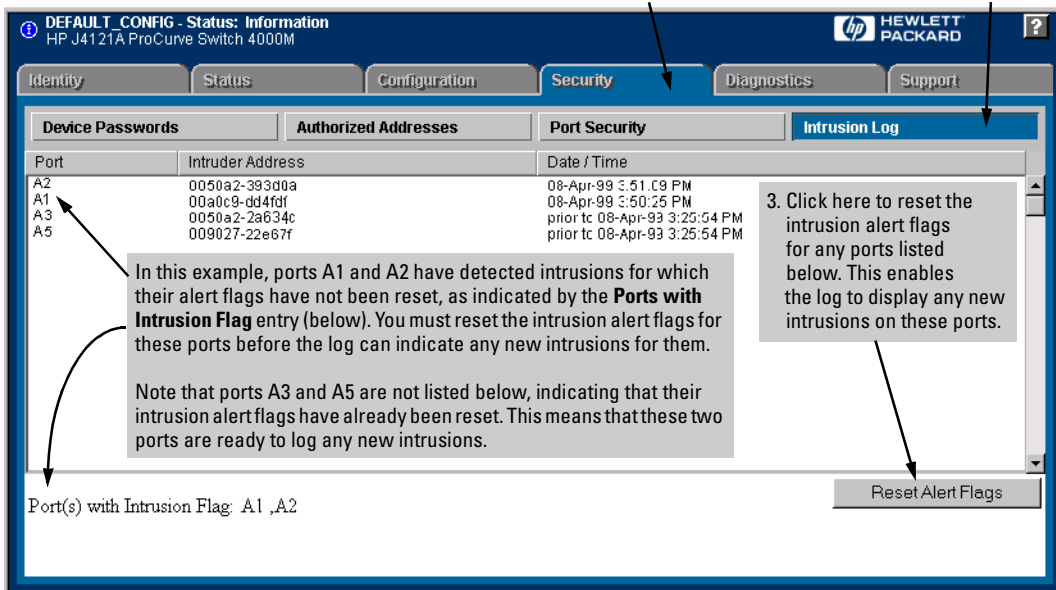


Figure 6-82. Example of the Intrusion Log with Intrusions Entered for Ports A1 and A2

- In the switch console:
 - The switch console Event Log, accessed from the Main Menu, displays the intrusion as an FFI (Find, Fix, and Inform) Security Violation event with the related port number (figure 6-83, below).

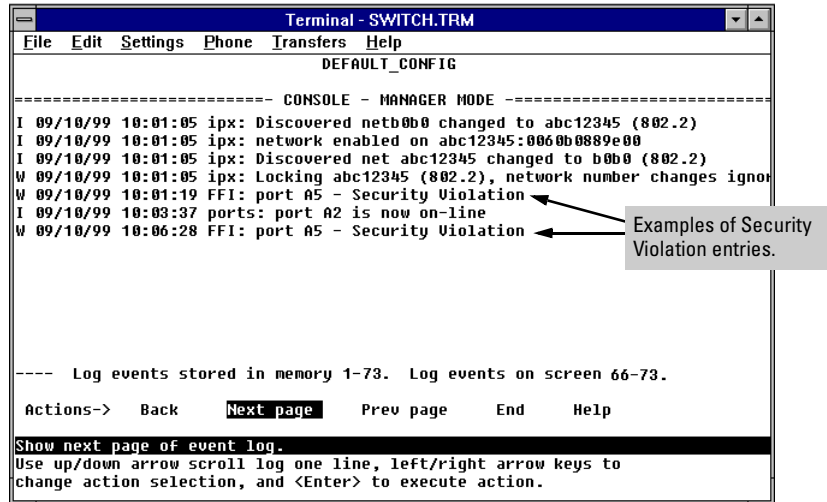


Figure 6-83. Example of the Switch Console Event Log with Security Violation Entries

- The Intrusion Alert column in the console's Port Status screen displays **Yes** for the port on which the violation occurred (figure 6-84, below).

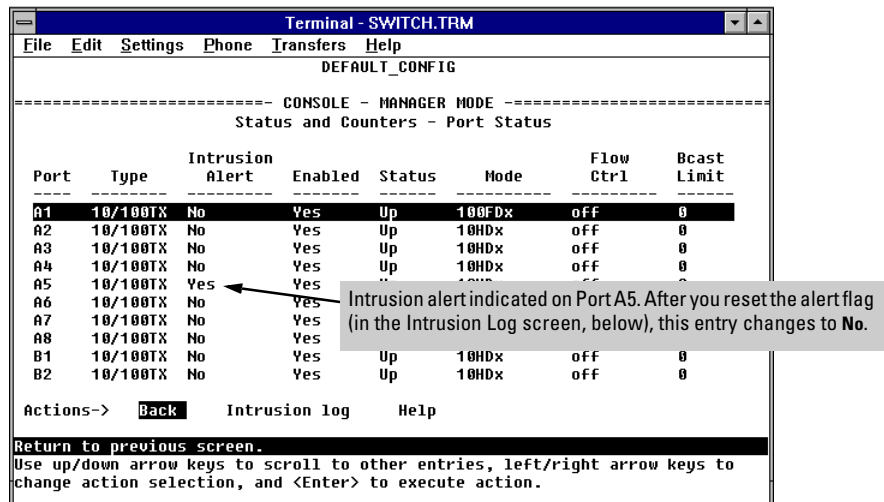


Figure 6-84. Example of Port Status Screen with Intrusion Alert on Port A5

- The console's Intrusion Log lists the port number, the MAC address of the intruding device, and the system time and date when the intrusion occurred (figure 6-85, below).

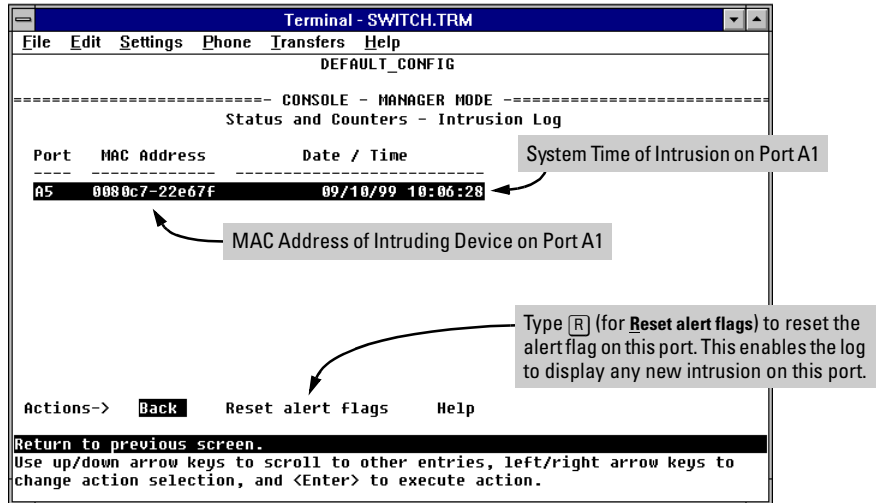


Figure 6-85. Example of the Intrusion Log with an Intrusion Listed for Port A5

How the Intrusion Log Operates

The Intrusion Log gives you a list of the 20 most recent security violation attempts, and appears in both the web browser interface and the switch console. The log shows the most recent intrusion at the top of the listing. You cannot delete Intrusion Log entries. Instead, if the log is filled when the switch detects a new intrusion, the oldest entry is dropped off the listing and the newest entry appears at the top of the listing.

Keeping the Intrusion Log Current by Resetting Alert Flags. When a violation occurs on a port, an alert flag is set for that port and the violation is entered in the Intrusion Log. The switch can detect and handle subsequent intrusions on that port, but will not log another intrusion on the port until you go to the Intrusion Log and use the Reset Alert Flags button to reset the port's alert flag.

Operating Notes for Port Security

Identifying the IP Address of an Intruder. The Intrusion Log lists intruders by MAC address. If you are using HP TopTools for Hubs & Switches to manage your network, you can use the TopTools inventory reports to link MAC addresses to their corresponding IP addresses. (Inventory reports are organized by device type; hubs, switches, servers, etc.)

Proxy Web Servers. If you are using the switch's web browser interface through a switch port configured for Static port security, and your browser access is through a proxy web server, then it is necessary to do the following:

- Enter your PC or workstation MAC address in the port's Authorized Addresses list.
- Enter your PC or workstation's IP address in the switch's IP Authorized Managers list. See "Enhancing Security by Configuring Authorized Managers" on page 6-21.)

Without both of the above configured, the switch detects only the proxy server's MAC address, and not your PC or workstation MAC address, and interprets your connection as unauthorized.

Security Violations. If you reset the switch (using the Reset button, Device Reset, or Reboot Switch), the Intrusion Log will list the time of all currently logged intrusions as "prior to" the time of the reset.

Alert Flag Status for Entries Forced Off of the Intrusion Log. If the Intrusion Log is full of entries for which the alert flags have not been reset, a new intrusion will cause the oldest entry to drop off the list, but will not change the alert flag status for the port referenced in the dropped entry. This means that, even if an entry is forced off of the Intrusion Log, no new intrusions can be logged on the port referenced in that entry until you reset the alert flags.

Class of Service (CoS): Managing Bandwidth More Effectively

As the term suggests, *network policy* refers to the network-wide controls you can implement to ensure uniform and efficient traffic handling throughout your network. One goal of network policy is to keep the most important traffic moving at an acceptable speed, regardless of current bandwidth usage.

While adding bandwidth is always a good idea, it is not always feasible and does not completely eliminate the potential for network congestion. There will always be points in the network where multiple traffic streams merge or where network links will change speed and capacity. The impact and number of these congestion points will increase over time as more applications and devices are added to the network.

When (not *if*) network congestion occurs, it is important to move traffic on the basis of relative importance. However, without *Class of Service (CoS)* prioritization, less important traffic can consume network bandwidth and slow down or halt the delivery of more important traffic. That is, without CoS, most traffic received by the switch is forwarded with the same priority it had upon entering the switch. In many cases, such traffic is “normal” priority and competes for bandwidth with all other normal-priority traffic, regardless of its relative importance to your organization’s mission.

This section gives an overview of CoS operation and benefits, and describes how to configure CoS in the console interface.

Class of Service is a general term for classifying and prioritizing traffic throughout a network. That is, CoS enables you to establish an end-to-end traffic priority policy to improve control and throughput of important data. You can manage available bandwidth so that the most important traffic goes first.

You can use the console and web browser interface to configure CoS on individual switches having the C.07. XX software release. You can also configure CoS for these same switches on a network policy basis (using release N.01.03 or later of HP TopTools for Hubs & Switches network management software).

CoS is implemented in the form of rules or policies that are configured on the switch. While you can use CoS to prioritize only the outbound traffic moving through the switch, you derive the maximum benefit by using CoS in an 802.1Q VLAN environment (with 802.1p priority tags), where CoS can set priorities that are supported by downstream devices.

By management through prioritizing, CoS supports growth of traffic on the network while optimizing the use of existing resources—and delaying the need for further investments in equipment and services. That is, CoS enables you to:

- Specify which traffic has higher or lower priority, regardless of current network bandwidth or the relative priority setting of the traffic when it is received on the switch.
- Change (upgrade or downgrade) the priority of outbound traffic.
- Override “illegal” packet priorities set by upstream devices or applications that use 802.1Q VLAN tagging with 802.1p priority tags.
- Avoid or delay the need to add higher-cost NICs (network interface cards) to implement prioritizing. (Instead, control priority through network policy.)

Definitions

Term	Use in This Document
downstream device	A device linked directly or indirectly to an outbound switch port. That is, the switch <u>sends traffic to</u> downstream devices.
inbound port	Any port on the switch through which traffic enters the switch.
outbound port	Any port on the switch through which traffic leaves the switch.
outbound port queue	For any port, a buffer that holds outbound traffic until it can leave the switch through that port. There is a “high priority” queue and a “normal priority” queue for each port in the switch. Traffic in a port’s high priority queue leaves the switch before any traffic in the port’s normal priority queue.
precedence bits	The upper three bits in the Type of Service (ToS) field of an IP packet.
upstream device	A device linked directly or indirectly to an inbound switch port. That is, the switch <u>receives traffic from</u> upstream devices.
802.1p priority	A traffic priority setting carried only in packets in 802.1Q tagged VLANs. This setting can be from 0 - 7.
802.1Q tagged VLAN	A virtual LAN (VLAN) that complies with the 802.1Q standard and is configured as “tagged”. (For more on VLANs, see page 6-51.)

Basic Operation

CoS settings operate on two levels:

- **Controlling the priority of outbound packets:** Each switch port has two outbound traffic queues; “normal” priority and “high” priority. (High-priority packets leave the switch port first. Normal-priority packets leave the switch port after the port’s high-priority queue is emptied.) With no CoS control, all traffic (except IGMP traffic configured for high priority) goes through the “normal” outbound port queues. However, with a CoS configuration, you can determine the outbound priority queue to which a packet is sent. (In an 802.1Q tagged VLAN environment, if CoS is *not* configured on the switch, but *is* configured on an upstream device, high priority traffic received by the switch is forwarded through high priority queues.)
- **Configuring the 802.1p priority of outbound packets in a tagged VLAN environment for use by downstream devices:** If an outbound packet is in an 802.1Q tagged VLAN environment (that is, if the packet is assigned to a tagged VLAN on the outbound port), then the packet carries an 802.1p priority setting that was configured in the switch. This priority setting can range from 0 to 7, and can be used by downstream devices having up to eight queues. Thus, while packets within the switch move only at high or normal priority, they still can carry the 802.1p priority that can be used by downstream devices having more than two priority levels. Also, if the packet enters the switch with an 802.1p priority setting, CoS can override this setting if configured to do so.

Note: If you are not using multiple tagged VLANs in your network, you can still use the tagged VLAN feature by configuring the default VLAN as a tagged VLAN.

You can configure a CoS priority of 0 through 7 for an outbound packet. When the packet is then sent to a port, the CoS priority determines which outbound queue the packet uses:

CoS Setting	Outbound Port Queue	Operation
0 — 3	normal priority	Packets in this queue leave the port after the high-priority queue is emptied.
4 — 7	high priority	Packets in this queue leave the port first.

If a packet is not in an 802.1Q tagged VLAN environment, the above settings control only to which outbound queue the packet goes, and no 802.1p priority is added to the packet. However, if the packet is in an 802.1Q tagged VLAN environment, then the above setting is also added to the packet as an 802.1p priority that can be used by downstream devices and applications, as indicated in the next table.

Table 6-6. Mapping Priority Settings to Device Queues

Priority Setting in the Switch	Outbound Port Queues in the Switch	802.1p Priority Setting Added to Tagged VLAN Packet Leaving the Switch	Queue Assignment in Downstream Devices With:		
			8 Queues	4 Queues	2 Queues
1	Normal	1 (low priority)	Queue 1	Queue 1	Queue 1
2	Normal	2	Queue 2	Queue 2	
0	Normal	0 (normal priority)	Queue 3		
3	Normal	3	Queue 4	Queue 3	Queue 2
4	High	4	Queue 5		
5	High	5	Queue 6	Queue 4	
6	High	6	Queue 7		
7	High	7 (high priority)	Queue 8		

Criteria for Prioritizing Outbound Packets

You can configure CoS prioritization on the basis of five packet criteria, evaluated in the following order:

1. Device Priority (destination or source IP address)
2. IP Type of Service (ToS) field
3. Protocol Priority (IP, IPX, ARP, DEC LAT, AppleTalk, SNA, and NetBeui)
4. VLAN Priority
5. Incoming 802.1p Priority (present in tagged VLAN environments)

If more than one criteria is present in a packet, the switch applies a precedence scheme to the criteria and then uses only the CoS configuration for the packet criteria that has the highest precedence. For example, if CoS assigns high priority to “red” VLAN packets, but normal priority to IP packets, since Protocol Priority has precedence over VLAN priority, IP packets on the “red” VLAN will be set to normal priority. See Table 6-7. Priority Criteria and Precedence on page 6-134 for more information.

Table 6-7. Priority Criteria and Precedence

Precedence	Criteria	Overview									
1	Device Priority (IP Address)	<p>You can specify a priority for any outbound packet having a particular destination or source IP address. CoS allows up to 30 IP addresses. If an outbound packet has an IP address as the destination, it takes precedence over another outbound packet that has the same IP address as a source. (This can occur, for example, on an outbound port in a switch mesh environment.) Default state: No IP address prioritization.</p> <p>If a packet does not meet the criteria for device priority, then precedence defaults to IP Type of Service (ToS) criteria, below.</p>									
2	IP Type-of-Service (ToS)	<p>Applies only to IP packets. The ToS field in an IP packet is configured by an upstream device or application before the incoming packet enters the switch, and is not altered by the switch. CoS reads the packet's Type of Service (ToS) field and prioritizes the packet (if specified in the CoS configuration) for outbound transmission. For more on this topic, see "Using Type of Service (ToS) Criteria To Prioritize IP Traffic" on 6-143. Default state: Disabled.</p> <p>If a packet does not meet the criteria for ToS priority, then precedence defaults to Protocol criteria, below.</p>									
3	Protocol Priority	<p>CoS can prioritize outbound packets for one or more of these network protocols: IP, IPX, ARP, DEC LAT, AppleTalk, SNA, and NetBeui. Default state: No override for any protocol.</p> <p>If a packet does not meet the criteria for Protocol priority, then precedence defaults to VLAN criteria, below.</p>									
4	VLAN Priority	<p>Enables packet priority based on the name of the VLAN in which the packet exists. For example, if the default VLAN (DEFAULT_VLAN) and the "Blue" VLAN are both assigned to a port, and Blue VLAN traffic is more important, you can configure CoS to give Blue VLAN traffic a higher priority than default VLAN traffic. (Priority is applied on the outbound port.) Default state: No override.</p> <p>If a packet does not meet the criteria for VLAN priority, then precedence defaults to Incoming 802.1p criteria, below.</p>									
5	Incoming 802.1p Priority	<p>Where a packet enters the switch on a tagged VLAN, if CoS is not configured to apply to the packet's priority setting, the switch uses the packet's existing 802.1p priority (assigned by an upstream device or application) to determine which outbound port queue to use. If the packet leaves the switch on a tagged VLAN, then there is no change to its 802.1p priority setting. If the packet leaves the switch on an untagged VLAN, the 802.1p priority is dropped.</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Entering (Inbound) 802.1p Priority</th> <th>Outbound Port Queue</th> <th>Exiting (Outbound) 802.1p Priority</th> </tr> </thead> <tbody> <tr> <td>0 - 3</td> <td>Normal</td> <td>0 - 3</td> </tr> <tr> <td>4 - 7</td> <td>High</td> <td>4 - 7</td> </tr> </tbody> </table> <p>If a packet does not meet the criteria for Incoming 802.1p priority, then the packet is sent to the "normal" outbound queue of the appropriate port. If the packet did not enter the switch on a tagged VLAN, but exits from the switch on a tagged VLAN, then a tagged VLAN field, including an 802.1p priority of 0 (normal), is added to the packet.</p>	Entering (Inbound) 802.1p Priority	Outbound Port Queue	Exiting (Outbound) 802.1p Priority	0 - 3	Normal	0 - 3	4 - 7	High	4 - 7
Entering (Inbound) 802.1p Priority	Outbound Port Queue	Exiting (Outbound) 802.1p Priority									
0 - 3	Normal	0 - 3									
4 - 7	High	4 - 7									

Configuring the Switch

No Override. By default, the IP ToS, Protocol, and VLAN ID criteria automatically list each of their options with **No override** for priority. This means that if you do not configure a priority for a specific option, CoS does not prioritize packets to which that option applies. For example, if you do not specify a priority for the IP protocol, then the IP protocol will not be a criteria for setting a CoS priority. In this case, the packets will be handled as described above.

How To Configure CoS

You can use CoS regardless of whether your network has tagged VLANs. As described earlier (under “Basic Operation” on page 6-132):

- Using CoS in a tagged VLAN environment controls both of the following:
 - **Outbound port queue:** To which queue (high or normal) a packet will be sent
 - **Outbound 802.1p priority:** Enters a new 802.1p priority setting in an outbound packet or retains the packet’s existing 802.1p setting. This enables the packet to carry an 802.1p priority to the next downstream device.
- Using CoS without a tagged VLAN environment affects only the outbound port queue to which a packet is sent. (That is, it prioritizes traffic flow within the switch.) However, without a tagged VLAN environment, an outbound packet cannot carry an 802.1p priority setting to a downstream device.

To configure CoS, use this procedure:

1. Determine the CoS policy you want to implement. This includes analyzing the types of traffic flowing through your network and identifying one or more traffic types to prioritize. In order of precedence, these are:
 - a. Device Priority—destination or source IP address (Note that destination has precedence over source. See Table 6-7.)
 - b. IP Type of Service
 - c. Protocol Priority
 - d. VLAN Priority (requires at least one tagged VLAN on the network)
 - e. Incoming 802.1p Priority (requires at least one tagged VLAN on the network)

For more on how CoS operates with the above traffic types, see Table 6-7. Priority Criteria and Precedence on page 6-134.)

2. If you want 802.1p priority settings to be included in outbound packets, ensure that tagged VLANs are configured on the appropriate links. (See “Supporting CoS with an 802.1Q Tagged VLAN Environment” on 6-151.)

Configuring the Switch

Class of Service (CoS): Managing Bandwidth More Effectively

3. Determine the actual CoS configuration changes you will need to make on each CoS-capable device in your network in order to implement the desired policy.
4. Configure the desired CoS priorities on the CoS-capable devices in the network. For HP devices, HP recommends that you use TopTools for Hubs & Switches (version N.01.03 or later) to help ensure that your CoS policy is implemented consistently across the network. Otherwise, use the web browser interface or the switch console interface for each device to configure CoS.

Note: If you use TopTools for Hubs & Switches to configure CoS policy in a network, it overrides any CoS settings configured through the console or the web browser interface in any individual HP switch.

The remainder of this section describes the general process for using the web browser interface and the console interface to configure CoS.

Configuring Class of Service from the Web Browser Interface

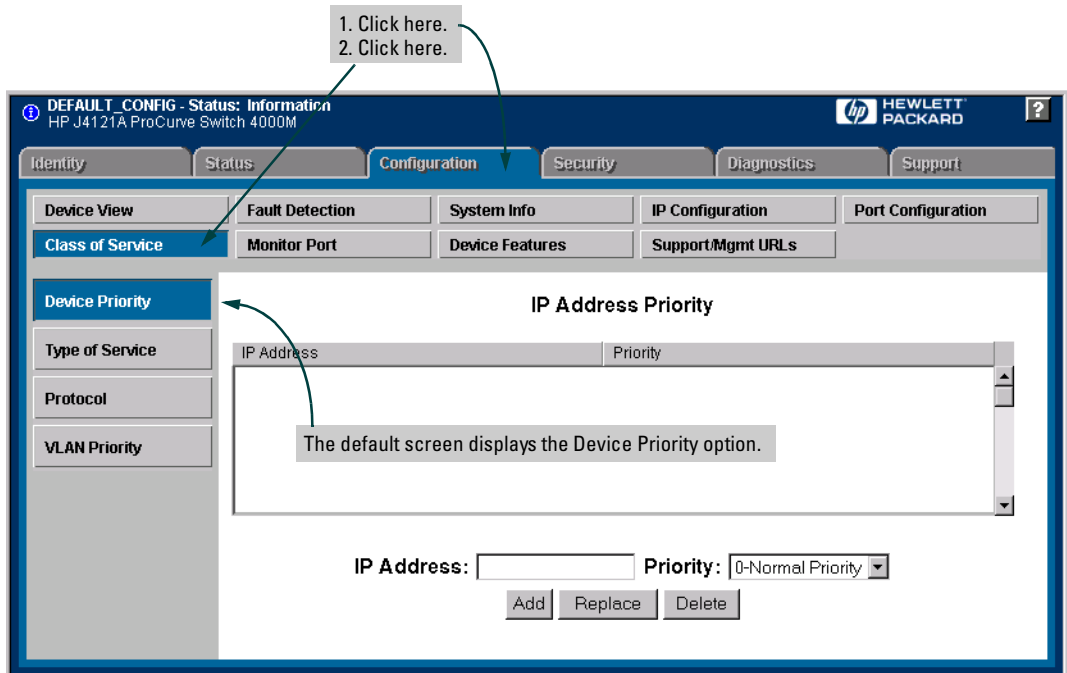


Figure 6-86. The Default Class of Service Configuration Screen

Use Table 6-8., “Steps for Using the Web Browser Interface To Configure CoS Priority” (next page) to guide you in configuring your CoS criteria.

Note

If you select “Differentiated Services” in the Type of Service option, use Telnet (to the console interface) to change the priority for a given IP ToS value.

Table 6-8. Steps for Using the Web Browser Interface To Configure CoS Priority

CoS Options	Priority Configuration Steps
Device Priority	<p>Click on the Device Priority button, then:</p> <p><u>To add an IP address:</u></p> <ol style="list-style-type: none"> 1. Type the address in the IP Address field. 2. Select the desired priority level from the Priority pull-down menu. 3. Click on the Add button. <p><u>To change a configured priority for a device:</u></p> <ol style="list-style-type: none"> 1. Type the device's IP address in the IP Address field. 2. Highlight a replacement priority level in the Priority pull-down menu. 3. Click on the Replace button. <p><u>To delete a device from the Device Priority list:</u></p> <ol style="list-style-type: none"> 1. Click on the device's IP address in the IP Address Priority field. 2. Click on the Delete button.
Type of Service	<p>Click on the Type of Service button. Then:</p> <ol style="list-style-type: none"> 1. Use the pull-down menu to select either IP Precedence or Differentiated Services. 2. Click on the Apply Changes button. <p>If you selected Differentiated Services, you will then need to go to the Device View screen (under the Configuration tab) and Telnet to the switch console interface to change the priority for a given IP ToS value. For more on Type of Service, see "Using Type of Service (ToS) Criteria to Prioritize IP Traffic" on 6-143.</p>
Protocol	<p>Click on the Protocol button. Then:</p> <ol style="list-style-type: none"> 1. Click on the Priority pull-down menu for the desired protocol and select a priority level. 2. Click on the Apply Changes button.
VLAN Priority	<p>Click on the VLAN Priority button. Then:</p> <p>Note: This feature configures the priority on existing VLANs (including the default VLAN). To configure new VLANs, go to the Device View screen (under the Configuration tab) and Telnet to the switch console interface.</p> <ol style="list-style-type: none"> 1. Click on (highlight) the VLAN for which you want to configure a priority. 2. In the Priority pull-down menu, select the priority level you want. 3. Click on Modify VLAN priority.

Configuring the Switch

Configuring Class of Service from the Console

CoS uses dynamic reconfiguration to configure your CoS choices. This means that it is not necessary to reboot the switch after configuring CoS.

To access the CoS console screens, begin at the Main Menu and select the following:

- 3. Switch Configuration . . .
- 5. Advanced Features . . .
- 7. Class of Service (CoS) Menu . . .

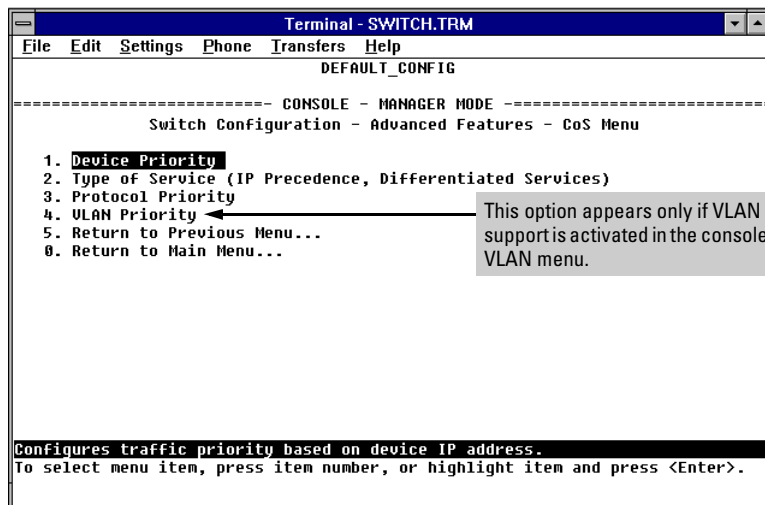


Figure 6-87. The Class of Service Menu

Select the priority option you want to configure for CoS. The following screens show the options with notes on how to configure them.

The CoS Device Priority Screen

CoS uses the criteria you specify per IP address (up to 30) to determine traffic prioritization. Device Priority has higher precedence than any other CoS prioritization criteria. Thus, if traffic from or to the listed devices also carries other CoS criteria, those other criteria will be ignored due to the existence of the Device Priority criteria. (For precedence information, see table 6-7, “Priority Criteria and Precedence”, on 6-134.)

To display the Device Priority screen, select **Device Priority** in the CoS Menu screen (page 6-139).

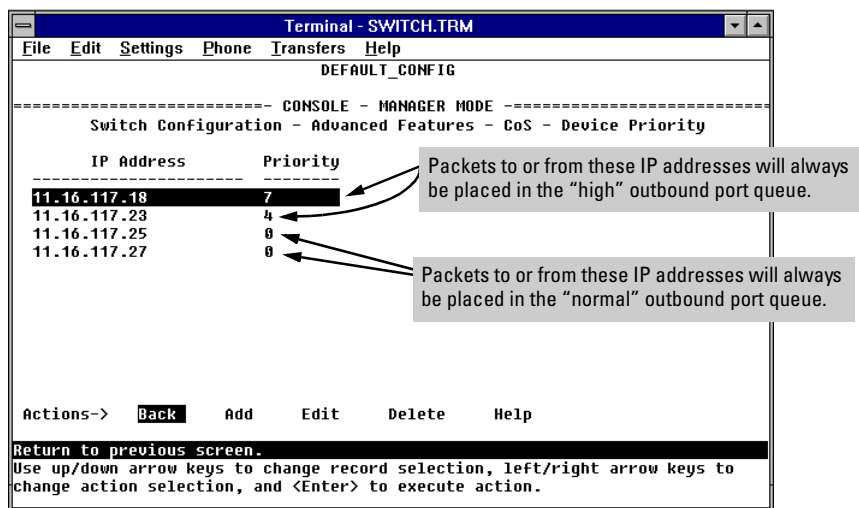


Figure 6-88. Example of the CoS Device Priority Screen

The Device Priority screen shows examples of CoS device priority configurations. The priorities for IP packets to or from the listed devices will always be controlled by these criteria. If packets for the listed devices are outbound in a tagged VLAN environment, then they will carry with them an 802.1p priority that matches the Priority assignment in this screen.

The CoS Type of Service (ToS) Priority Screen

This feature applies only to IP traffic. CoS reads the Type of Service field in IP packets received from other devices and prioritizes the packets accordingly, unless the same traffic has already been prioritized by the Device Priority (IP address) option. For more information on using ToS criteria, refer to “Using Type of Service (ToS) Criteria to Prioritize IP Traffic” on 6-143.

The CoS Protocol Priority Screen

CoS uses protocol criteria to determine traffic priority unless the same traffic has other CoS criteria (configured in other CoS screens) that has a higher precedence. (For precedence information, see Table 6-7. Priority Criteria and Precedence on page 6-134.)

To display the Protocol Priority screen, select **Protocol Priority** in the CoS Menu screen (page 6-139).

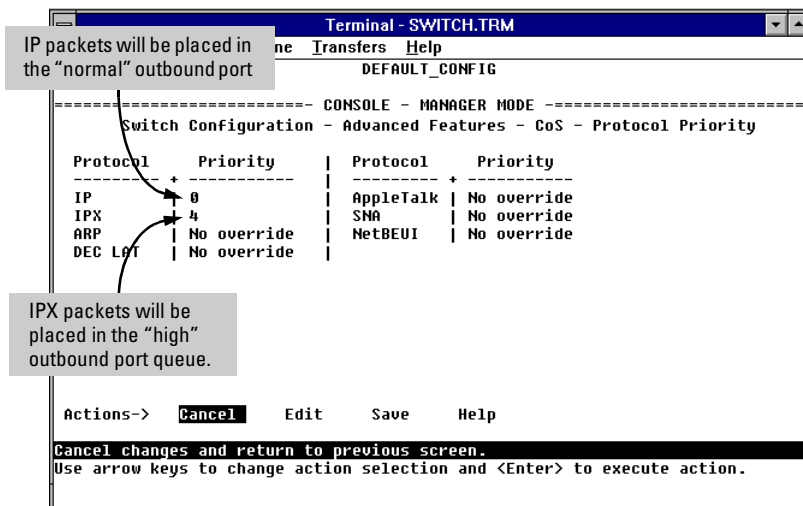


Figure 6-89. Examples of CoS Protocol Priority Configurations

Where a packet in a listed protocol is outbound in a tagged VLAN environment, then it carries with it an 802.1p priority. If a 0-7 priority is configured, the packet carries the equivalent 802.1p priority. If **No override** is configured, and the packet entered the switch through a tagged VLAN, then the packet carries the 802.1p priority it carried when entering the switch. If **No override** is configured and the packet did not enter the switch through a tagged VLAN, then the packet carries an 802.1p priority of 0 (normal priority) when it leaves the switch.

The CoS VLAN Priority Screen

If you configure CoS on this screen, CoS uses the criteria you specify per VLAN to determine traffic prioritization unless the same traffic has other CoS criteria (configured in other CoS screens) that has a higher precedence. (For precedence information, see table 6-7, “Priority Criteria and Precedence”, on 6-134.)

To display the VLAN Priority screen, select **VLAN Priority** in the CoS Menu screen (page 6-139).

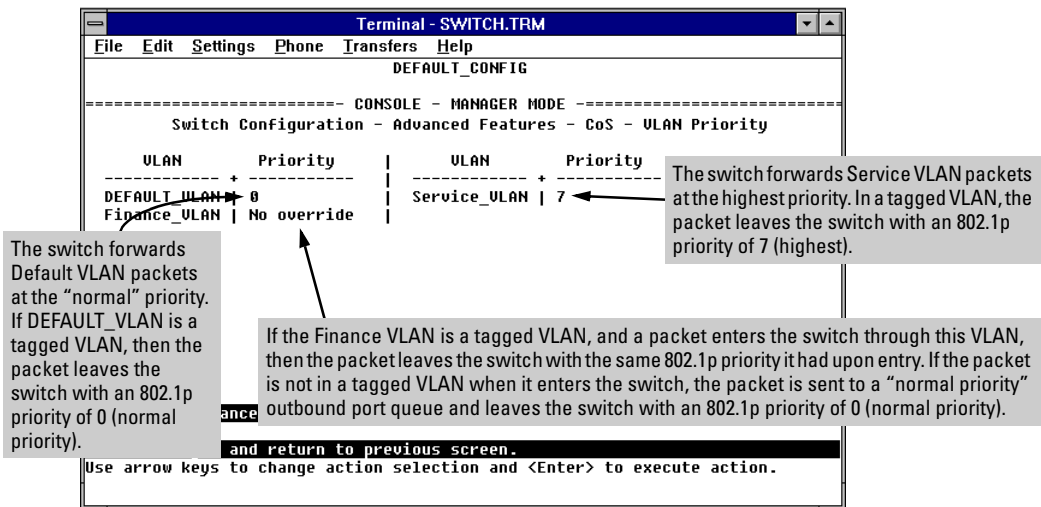


Figure 6-90. The CoS VLAN Priority Screen

Using Type of Service (ToS) Criteria to Prioritize IP Traffic

Every IP packet includes a Type of Service (ToS) field. This field carries priority settings that are read and used, but not altered by the switch. When CoS is configured to use ToS criteria, the switch reads the content of the packet's ToS field and takes actions based on any CoS configuration that applies to the packet.

In order to use ToS to configure priority, you need to anticipate the ToS field settings in IP packets entering the switch from upstream devices. This involves having knowledge of how an upstream device or application will set the bits in the ToS field of IP packets sent to the switch.

The switch can use the ToS field in either of two ways:

- Use the Differentiated Services bits to select the packets to prioritize (ToS Differentiated Services option)
- Use the Precedence bits to prioritize a packet (ToS IP precedence option).

The following shows an example of the ToS field in the header for an IP packet, and illustrates the diffserve bits and precedence bits in the ToS field. (Note that the Differentiated Services bits and the Precedence bits are two different interpretations of the same field.)

Field:	Destination MAC Address	Source MAC Address	IP Identifier	Type & Version	ToS Byte	...
Packet:	FF FF FF FF FF FF	08 00 09 00 00 16	08 00	45	E0	...

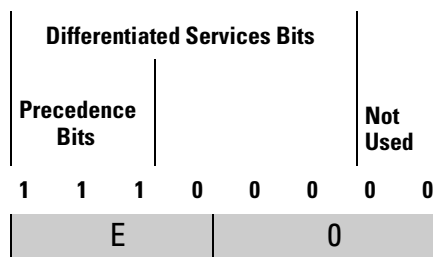


Figure 6-91. The ToS Field (or Byte) in an IP Header

ToS Configuration Options. To display the Type of Service screen, select **Type of Service (IP Precedence, Differentiated Services)** in the CoS Menu screen (page 6-139).

Type of Service includes three possible settings:

- **Disabled (the default):** ToS is disabled and is not a factor in prioritizing packets. (Priority settings in the ToS fields of IP packets received by the switch are ignored.)
- **IP Precedence:** ToS is enabled and the switch uses ToS precedence bits (the upper three bits in the TOS field) to determine packet priority. The value of these bits are in the range of 0 through 7.
- **Differentiated Services:** ToS is enabled and the switch uses the Differentiated Services bits (the upper six bits) of the ToS field. Each possible setting is termed a codepoint, and there are 64 possible codepoints. This means that you can configure a priority (0 - 7) for up to 64 ToS codepoints. If **No override** is specified for a codepoint, then differentiated services prioritization is not used for packets carrying that codepoint.

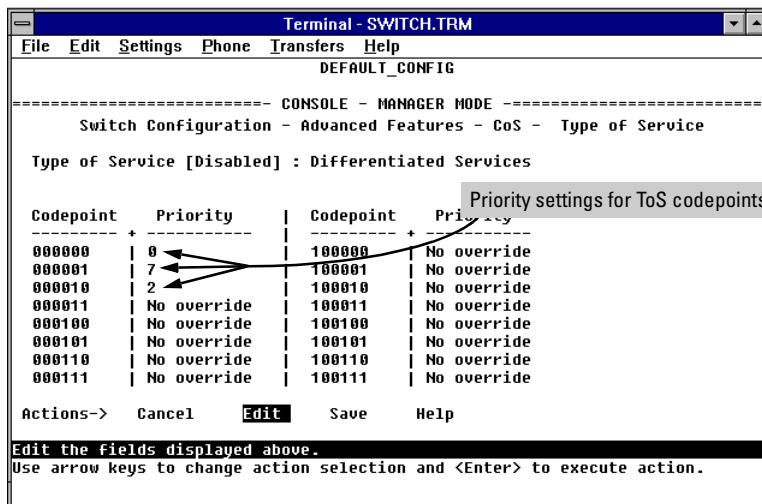


Figure 6-92. Example of the Differentiated Services (diffserve) Screen

In the above example, the first three ToS codepoints have priority settings. Packets arriving in the switch with these codepoints will be prioritized accordingly (if no higher-precedence CoS criteria apply). That is, a priority of 0 - 3 sends the packet to the normal priority outbound queue. A priority of 4 - 7 sends the packet to the high priority outbound queue. If the packet is outbound in a tagged VLAN, then its 802.1p priority will be set to the same value as the codepoint priority setting (0 - 7).

Table 6-9. How the Switch Uses the ToS Configuration

Outbound Port	ToS Option:	
	IP Precedence (Value = 0 - 7)	Differentiated Services
IP Packet in an Untagged VLAN or No VLAN	<p>Depending on the value of the IP Precedence bits in the packet's ToS field, the packet will go to either the high or normal priority outbound port queue in the switch:</p> <ul style="list-style-type: none"> 0 - 3 = normal priority 4 - 7 = high priority 	<p>For a given packet carrying a given codepoint in the ToS field:</p> <ul style="list-style-type: none"> • If a priority (0 - 7) has been configured for that codepoint, the packet will go to either the high or normal priority outbound port queue in the switch: <ul style="list-style-type: none"> 0 - 3 = normal priority 4 - 7 = high priority • If No override (the default) has been configured for that codepoint, then the packet is not prioritized by ToS.
IP Packet in a Tagged VLAN	<p>Same as above, plus the IP Precedence value (0 - 7) will be used to set a corresponding 802.1p priority in the VLAN tag carried by the packet to the next downstream device.</p>	<p>Same as above, plus the user-configured Priority value (0 - 7) will be used to set a corresponding 802.1p priority in the VLAN tag carried by the packet to the next downstream device.</p>

IP Multicast (IGMP) Interaction with CoS

The switch's ability to prioritize IGMP traffic for either a normal or high priority outbound queue overrides any CoS criteria, and does not affect any 802.1p priority settings the switch may assign. For a given packet, if both IGMP high priority and CoS are configured, the CoS configuration overrides the IGMP setting.

IGMP High Priority Configured	CoS Configuration Affects Packet	Switch Port Output Queue	Outbound 802.1p Setting (Requires Tagged VLAN)
Not Enabled	No	Normal	Same as Inbound Setting
Not Enabled	Yes: High Priority (4 - 7)	High	Configured by CoS (4 - 7)
Not Enabled	Yes: Normal Priority (0 - 3)	Normal	Configured by CoS (0 - 3)
Enabled	No	High	Same as Inbound Setting
Enabled	Yes: High Priority (4 - 7)	High	Configured by CoS (4 - 7)
Enabled	Yes: Normal Priority (0 - 3)	High	Configured by CoS (0 - 3)

Summary of CoS Operation

Each of the following four tables provide a hierarchy of CoS criteria and resulting operation, based on one of the four possible tagged VLAN scenarios a packet can encounter while traversing the switch. These scenarios include:

- The packet enters the switch and exits from the switch on a non-VLAN or untagged VLAN port.
- The packet enters the switch in an untagged VLAN and exits from the switch in a tagged VLAN.
- The packet enters the switch in a tagged VLAN and exits from the switch in an untagged VLAN.
- The packet enters the switch and exits from the switch in a tagged VLAN.

In each scenario, only the *first* CoS criteria that applies to a packet is used. All others are ignored.

Packet Enters Switch: On a Non-VLAN Port or in an Untagged VLAN

Packet Exits From Switch: On a Non-VLAN Port or in an Untagged VLAN

(Prioritizing affects only the choice of outbound priority queue. The packet carries no 802.1p priority tag.)

1. Device Priority (IP Address) Option (IP Packets Only):

- If Device Priority does not apply to the packet, then packet priority defers to the ToS policy.
- If Device Priority (0 - 7) is configured and applies to a packet, the packet is assigned to the appropriate queue (high or normal priority) of the outbound port, regardless of any other CoS-configured policy.

2. Type of Service (ToS) Option (IP Packets Only):

- If ToS option is configured to **Disabled**, then packet priority defers to the Protocol Priority policy.
- IP Precedence option: Prioritizes packet (high or normal) according to the value of the ToS precedence bits (upper three bits of ToS field; 0 - 7); 4 - 7 = high, 0 - 3 = normal.
- Differentiated Services option: Prioritizes packet (high or normal) according to Priority setting (0 - 7) for packet's ToS field codepoint. If Priority is set to **No override** (the default), then packet priority defers to the Protocol Priority policy.

See "Using Type of Service (ToS) Criteria to Prioritize IP Traffic" on 6-143.

3. Protocol Priority Option:

- If Protocol Priority does not assign a priority to the packet, then packet priority defers to the VLAN ID policy.
- If Protocol Priority assigns a priority (0 - 7) to a packet, the packet is assigned to the appropriate queue (high or normal priority) of the outbound port.

4. VLAN Priority Option:

- If VLAN Priority does not assign a priority to the packet, then the packet goes to the "normal" priority queue of an outbound port.
- If VLAN Priority assigns a priority (0 - 7) to a packet, the packet is assigned to the appropriate queue (high or normal priority) of the outbound port.

(An outbound packet belonging to an untagged VLAN can be assigned to a high or normal priority queue, but cannot be assigned an 802.1p priority because there is no tagged VLAN field in the packet.)

Configuring the Switch

Class of Service (CoS): Managing Bandwidth More Effectively

Packet Enters Switch: In an Untagged VLAN

Packet Exits From Switch: In a tagged VLAN

(Prioritizing affects both the choice of outbound priority queue and the packet's 802.1p priority tag.)

In this scenario, the outbound packet always carries a tagged VLAN field with an 802.1p priority setting.

1. Device Priority (IP Address) Option (IP Packets Only):

- If Device Priority does not apply to the packet, then packet priority defers to the ToS policy.
- If Device Priority (0 - 7) is configured and applies to a packet, then the packet is assigned to the appropriate queue (high or normal priority) of the outbound port and the priority value is configured in the 802.1p priority tag in the packet's tagged VLAN field.

2. Type of Service (ToS) Option (IP Packets Only):

- If ToS option is configured to **Disabled**, then packet priority defers to the Protocol Priority policy.
- IP Precedence option: Prioritizes packet (high or normal) according to the value of the ToS precedence bits (upper three bits of ToS field; 0 - 7); 4 - 7 = high, 0 - 3 = normal. Also, the Precedence bits are used as follows to configure the 802.1p priority tag in the packet's tagged VLAN field:

IP Precedence Setting:	0	1	2	3	4	5	6	7
802.1p Priority Setting*:	1	2	0	3	4	5	6	7
*To interpret these settings, see Table 6-6. Mapping Priority Settings to Device Queues on page 6-133.								

- Differentiated Services option: Prioritizes packet (high or normal) according to Priority you set (0 - 7) for the packet's ToS field codepoint. Also, the 802.1p priority tag in the packet's tagged VLAN field is configured to the same value as the Priority you set for the ToS field codepoint. If Priority is set to **No override** (the default), then packet priority defers to the Protocol Priority policy.

See "Using Type of Service (ToS) Criteria to Prioritize IP Traffic" on 6-143.

3. Protocol Priority Option:

- If Protocol Priority does not assign a priority to the packet, then packet priority defers to the VLAN ID policy.
- If Protocol Priority assigns a priority (0 - 7) to a packet, the packet is assigned to the appropriate queue (high or normal priority) of the outbound port and the priority value is configured in the 802.1p priority tag in the packet's tagged VLAN field.

4. VLAN Priority Option:

- If VLAN Priority does not assign a priority to the packet, then the packet goes to the "normal" priority queue of an outbound port.
- If VLAN Priority assigns a priority (0 - 7) to a packet, the packet is assigned to the appropriate queue (high or normal priority) of the outbound port and the priority value is configured in the 802.1p priority tag in the packet's tagged VLAN field.

Packet Enters Switch: In a tagged VLAN
Packet Exits From Switch: In an Untagged VLAN

(Prioritizing affects only the choice of outbound priority queue. The 802.1p priority tag carried by the packet when it entered the switch is discarded along with the tagged VLAN field.)

1. Device Priority (IP Address) Policy (IP Packets Only):

- If Device Priority does not apply to the packet, then packet priority defers to the ToS policy.
- If Device Priority (0 - 7) is configured and applies to a packet, the packet is assigned to the appropriate queue (high or normal priority) of the outbound port, regardless of any other CoS-configured policy.

2. Type of Service (ToS) Policy (IP Packets Only):

- If ToS option is configured to **Disabled**, then packet priority defers to the Protocol Priority policy.
- IP Precedence option: Prioritizes packet (high or normal outbound queue) according to the value of the ToS precedence bits (upper three bits of ToS field; 0 - 7); 4 - 7 = high, 0 - 3 = normal.
- Differentiated Services option: Prioritizes packet (high or normal outbound queue) according to Priority setting (0 - 7) for packet's ToS field codepoint. If Priority is set to **No override** (the default), then packet priority defers to the Protocol Priority policy.

See "Using Type of Service (ToS) Criteria to Prioritize IP Traffic" on 6-143.

3. Protocol Priority Policy:

- If Protocol Priority does not assign a priority to the packet, then packet priority defers to the VLAN ID policy.
- If Protocol Priority assigns a priority (0 - 7) to a packet, the packet is assigned to the appropriate queue (high or normal priority) of the outbound port.

4. VLAN Priority Policy:

- If VLAN Priority does not assign a priority to the packet, then packet priority defers to the incoming 802.1p priority value. (See "Incoming 802.1p Priority" in Table 6-7. Priority Criteria and Precedence on page 6-134.)
- If VLAN Priority assigns a priority (0 - 7) to a packet, the packet is assigned to the appropriate queue (high or normal priority) of the outbound port.

(An outbound packet belonging to an untagged VLAN can be assigned to an outbound, high or normal priority queue, but cannot be assigned an 802.1p priority because there is no tagged VLAN field in the packet.)

Configuring the Switch

Class of Service (CoS): Managing Bandwidth More Effectively

Packet Enters Switch: In a tagged VLAN

Packet Exits From Switch: In a tagged VLAN

(Prioritizing affects both the choice of outbound priority queue and the packet's 802.1p priority tag.)

In this scenario, the packet always carries a tagged VLAN field with an 802.1p priority setting, both inbound and outbound.

1. Device Priority (IP Address) Option (IP Packets Only):

- If Device Priority does not apply to the packet, then packet priority defers to the ToS policy.
- If Device Priority (0 - 7) is configured and applies to a packet, then the packet is assigned to the appropriate queue (high or normal priority) of the outbound port and the priority value is configured in the 802.1p priority tag in the packet's tagged VLAN field. This assignment replaces whatever 802.1p priority tag value the packet had when it entered the switch.

2. Type of Service (ToS) Option (IP Packets Only):

- If ToS option is configured to **Disabled**, then packet priority defers to the Protocol Priority policy.
- IP Precedence option: Prioritizes packet (high or normal) according to the value of the ToS precedence bits (upper three bits of ToS field; 0 - 7); 4 - 7 = high, 0 - 3 = normal. Also, the Precedence bits are used as follows to configure the 802.1p priority tag in the packet's tagged VLAN field:

IP Precedence Setting:	0	1	2	3	4	5	6	7
802.1p Priority Setting*:	1	2	0	3	4	5	6	7
*To interpret these settings, see Table 6-6. Mapping Priority Settings to Device Queues on page 6-133.								

This assignment replaces whatever 802.1p priority tag value that the packet had when it entered the switch.

- Differentiated Services option: Prioritizes packet (high or normal) according to Priority you set (0 - 7) for the packet's ToS field Codepoint. Also, the 802.1p priority tag in the packet's tagged VLAN field is configured to the same value as the Priority you set for the ToS field Codepoint. This assignment replaces whatever 802.1p priority tag value the packet had when it entered the switch. If Priority is set to **No override** (the default), then packet priority defers to the Protocol Priority policy.

See "Using Type of Service (ToS) Criteria to Prioritize IP Traffic" on page 6-143.

3. Protocol Priority Option:

- If Protocol Priority does not assign a priority to the packet, then packet priority defers to the VLAN ID policy.
- If Protocol Priority assigns a priority (0 - 7) to a packet, the packet is assigned to the appropriate queue (high or normal priority) of the outbound port and the priority value is configured in the 802.1p priority tag in the packet's tagged VLAN field. This assignment replaces whatever 802.1p priority tag value the packet had when it entered the switch.

4. VLAN Priority Option:

- If VLAN Priority does not assign a priority to the packet, then packet priority defers to the incoming 802.1p priority value. (See "Incoming 802.1p Priority" in Table 6-7. Priority Criteria and Precedence on page 6-134.)
- If VLAN Priority assigns a priority (0 - 7) to a packet, the packet is assigned to the appropriate queue (high or normal priority) of the outbound port and the priority value is configured in the 802.1p priority tag in the packet's tagged VLAN field. This assignment replaces whatever 802.1p priority tag value the packet had when it entered the switch.

Supporting CoS with an 802.1Q Tagged VLAN Environment

Using HP's 802.1Q-compliant switches, you can create either a single tagged VLAN or multiple tagged VLANs. To do either, you need an 802.1Q-compliant device connected to each tagged VLAN port on an HP switch. For more on VLANs, see page 6-51.

Using the Default VLAN to Create a Single Tagged VLAN

1. Activate the switch's VLAN support. To access the VLAN Support option from the Main Menu, select the following:

3. Switch Configuration . . .
5. Advanced Features . . .
6. VLAN Menu . . .
1. VLAN Support

2. From the Main Menu, reboot the switch.
3. In the VLAN Port Assignment screen, reconfigure to **Tagged** every port that is connected to an 802.1Q-compliant device.

To access the VLAN Port Assignment screen, select the following from the Main Menu:

3. Switch Configuration . . .
5. Advanced Features . . .
6. VLAN Menu . . .
3. VLAN Port Assignment

4. Ensure that each 802.1Q-compliant device connected to a port in step 3 is configured as tagged for the default VLAN.

Operating and Troubleshooting Notes

- **For Devices that Do Not Support 802.1Q Tagged VLANs:** For communication between these devices and the switch, connect the device to a switch port configured as **Untagged** for the VLAN in which you want the device's traffic to move.
- **VLAN Tagging Rules:** For a port on the switch to be a member of a VLAN, the port must be configured as either **Tagged** or **Untagged** for that VLAN. (Only one VLAN on a port can be untagged. Otherwise, the switch cannot determine which VLAN should receive untagged VLAN traffic.)
- **Loss of Communication on a Tagged VLAN:** If you cannot communicate with a device in a tagged VLAN environment, ensure that the device either supports tagged VLANs or is connected to a VLAN port that is configured as **Untagged**.

Monitoring and Analyzing Switch Operation

Overview

You can use the switch console (and, in some cases, the web browser interface) to access read-only status and counter information to help you monitor, analyze, and troubleshoot switch operation.

In particular, the web browser interface has an Alert Log that can help that can help you quickly identify network problems. See chapter 3, “Using the Web Browser Interface” for more information about the web browser interface and the Alert Log.

Note

Link test, ping test, browse configuration, and the Command prompt—analysis tools in troubleshooting situations—are described in chapter 8, “Troubleshooting”. See “Diagnostics” on (page 8-17).

The Event Log, a diagnostic tool that is often used for troubleshooting switch operation, is described in chapter 8, “Troubleshooting”. See “Using the Event Log To Identify Problem Sources” on (page 8-12).

Status and Counters Screens

This section describes the status and counters screens available through the switch console interface and/or the web browser interface.

Note

You can access all console screens from the web browser interface via Telnet to the console. See “Configuration Tab” on page 3-24.

Status or Counters Type	Interface	Purpose	Page
General System Information	Console	Lists switch-level operating information.	7-5
Management Address Information	Console	Lists the MAC address, IP address, and IPX network number for each VLAN or, if no VLANs are configured, for the switch.	7-6
Module Information	Console	For each slot, lists the module type (such as 10/100TX) and description.	7-7
Port Status Overview	Browser	Shows port utilization and the Alert Log.	3-14
Port Status	Console/ Browser	Displays the operational status of each port.	7-8
Port Counters	Console/ Browser	Summarizes port activity.	7-10
Address Table (Address Forwarding Table)	Console	Lists the MAC addresses of nodes the switch has detected on the network, with the corresponding switch port.	7-14
Port Address Table	Console	Lists the MAC addresses that the switch has learned from the selected port.	7-15
Spanning Tree Information	Console	Lists Spanning Tree data for the switch and for individual ports. If VLANs are configured, reports on a per-VLAN basis.	7-17
IP Multicast (IGMP) Status	Console	Lists IGMP groups, reports, queries, and port on which querier is located.	7-19
Automatic Broadcast Control (ABC) Information	Console	If VLANs are configured, reports are on a per-VLAN basis.	7-21
Switch Mesh Information	Console	For meshed ports, describes operating state, MAC address of adjacent meshed switch, and identity of peer port on adjacent switch.	7-22
VLAN Information	Console	For each VLAN configured in the switch, lists 802.1Q VLAN ID and up/down status.	7-23

Switch Console Status and Counters Menu

Select **Status and Counters** from the Main Menu to display the Status and Counters menu:

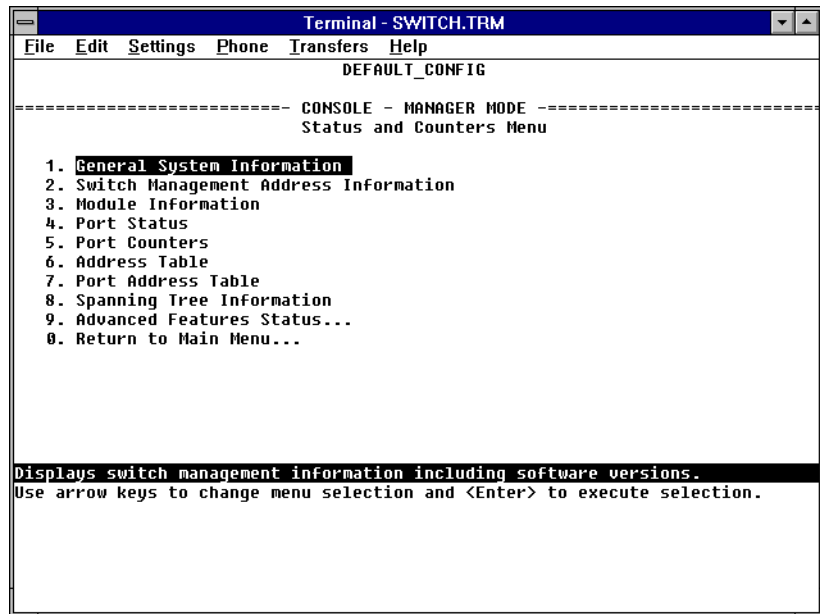


Figure 7-1. The Status and Counters Menu

Each of the above menu items accesses the read-only screens described on the following pages. Refer to the online help for a description of the entries displayed in these screens.

Note

IP Multicast (IGMP) and Automatic Broadcast Control (ABC) are reported on a per-VLAN basis. For these features, if VLANs are configured, you will be prompted to select a VLAN.

Web Browser Interface Status Information

The “home” screen for the web browser interface is the Status Overview screen, as shown in figure 7-2. As the title implies, it provides an overview of the status of the switch, including summary graphs indicating the network utilization on each of the switch ports, symbolic port status indicators, and the Alert Log, which informs you of any problems that may have occurred on the switch.

For more information on this screen, see chapter 3, “Using the HP Web Browser Interface”.

Monitoring and Analyzing
Switch Operation

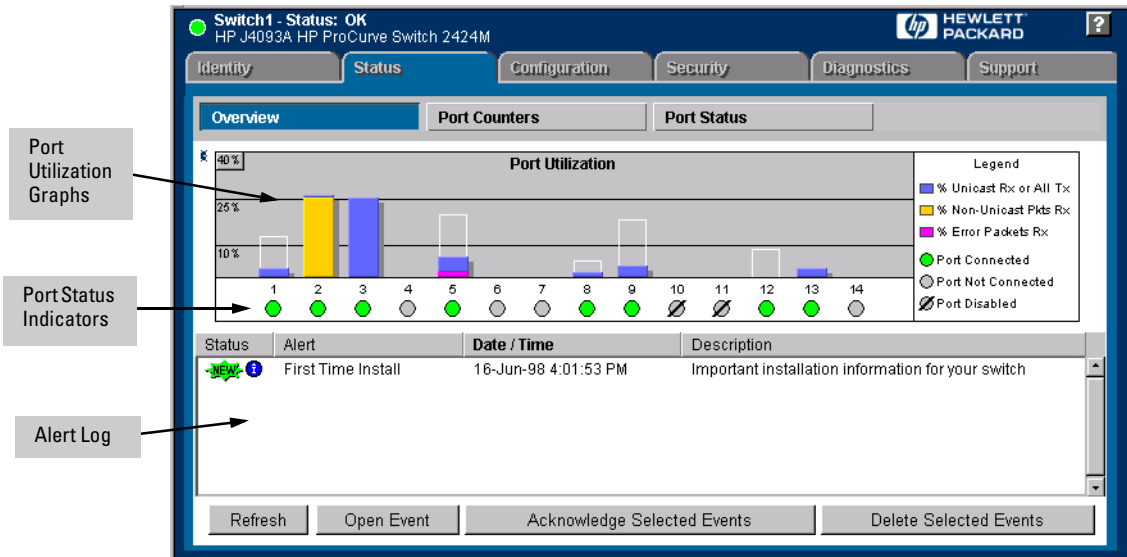


Figure 7-2. Example of a Web Browser Interface Status Overview Screen

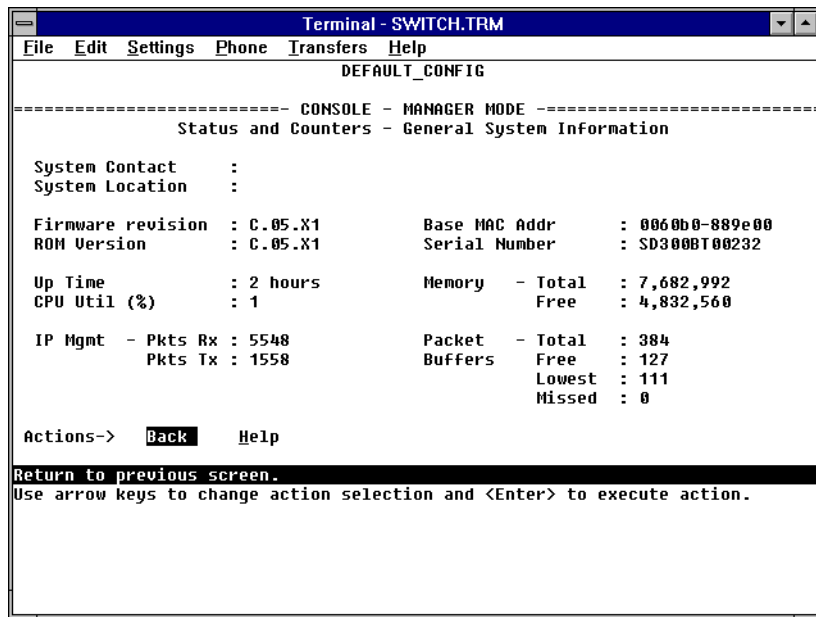
The other web browser interface status screens, Port Counters, and Port Status are described later in this chapter.

General System Information

To access this screen from the console Main Menu, select:

1. Status and Counters

1. General System Information



```
Terminal - SWITCH.TRM
File Edit Settings Phone Transfers Help
DEFAULT_CONFIG
----- CONSOLE - MANAGER MODE -----
Status and Counters - General System Information

System Contact      :
System Location     :

Firmware revision   : C.05.X1          Base MAC Addr      : 0060b0-889e00
ROM Version         : C.05.X1          Serial Number      : SD300BT00232

Up Time             : 2 hours           Memory - Total     : 7,682,992
CPU Util (%)        : 1                 Free               : 4,832,560

IP Mgmt - Pkts Rx   : 5548             Packet - Total     : 384
           Pkts Tx   : 1558             Buffers - Free    : 127
                                           Lowest            : 111
                                           Missed           : 0

Actions-> Back Help
Return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

Figure 7-3. Example of General Switch Information

This screen dynamically indicates how individual switch resources are being used. See the online Help for details.

Switch Management Address Information

To access this screen from the Main Menu, select:

1 Status and Counters

2. Switch Management Address Information

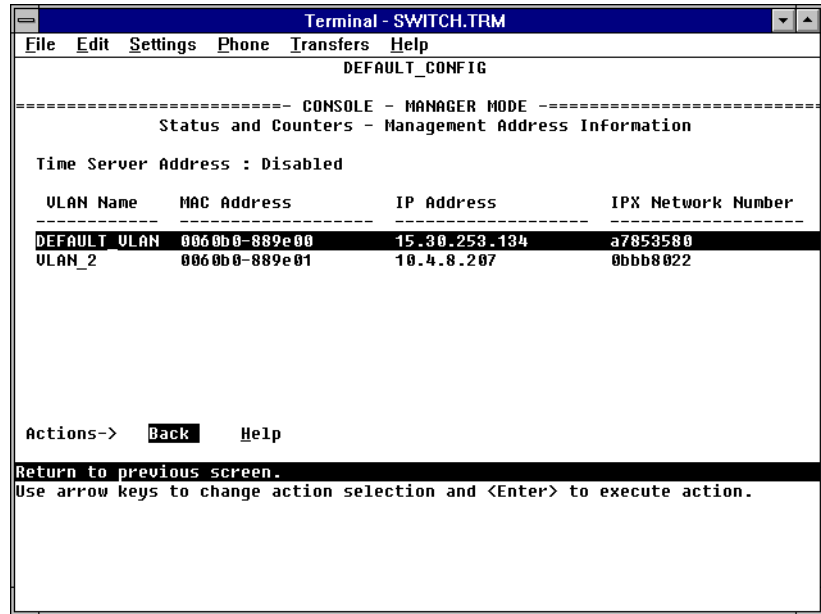


Figure 7-4. Example of Management Address Information with VLANs Configured

This screen displays addresses that are important for management of the switch. If multiple VLANs are *not* configured, this screen displays a single set of addresses for the entire switch. See the online Help for details.

Module Information

To access this screen from the Main Menu, select:

1. Status and Counters

3. Module Information

```
Terminal - SWITCH.TRM
File Edit Settings Phone Transfers Help
DEFAULT_CONFIG
----- CONSOLE - MANAGER MODE -----
                Status and Counters - Module Information
-----
Slot   Module Type                Module Description
-----
A      10/100TX                    HP J4111A 8-port 10/100Base-TX module
B      10/100TX                    HP J4111A 8-port 10/100Base-TX module
C      10/100TX                    HP J4111A 8-port 10/100Base-TX module
D      10/100TX                    HP J4111A 8-port 10/100Base-TX module
E      10/100TX                    HP J4111A 8-port 10/100Base-TX module
F                                     Slot Available
G                                     Slot Available
H                                     Slot Available
I                                     Slot Available
J                                     Slot Available

Actions->  Back  Help

Return to previous screen.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

Figure 7-5. Example of the Module Information Screen (Switch 4000M)

Displays information on the modules installed in the switch. See the online Help for details.

Port Status

The web browser interface and the console interface show the same port status data.

Note

If Automatic Broadcast Control (ABC) has been enabled, all ports where Bcast Limit (broadcast limit) has not already been manually set to a nonzero value will automatically be set to 30(%). See “Port Settings” on page 6-30.

Displaying Port Status from the Web Browser Interface

1. Click here

2. Click here

Port	Port Type	Enabled	Link Status	Current Mode	Flow Ctrl	Bcast Limit
A1	10/1 00TX	Yes	Up	10HDx	off	0
A2	10/1 00TX	Yes	Up	10HDx	off	0
A3	10/1 00TX	Yes	Up	10HDx	off	0
A4	10/1 00TX	Yes	Up	10HDx	off	0
A5	10/1 00TX	Yes	Up	10HDx	off	0
A6	10/1 00TX	Yes	Up	10HDx	off	0
A7	10/1 00TX	Yes	Up	10HDx	off	0
A8	10/1 00TX	Yes	Down	10HDx	off	0
B1	10/1 00TX	Yes	Up	10HDx	off	0
B2	10/1 00TX	Yes	Up	10HDx	off	0
B3	10/1 00TX	Yes	Up	10HDx	off	0
B4	10/1 00TX	Yes	Up	10HDx	off	0
B5	10/1 00TX	Yes	Down	10HDx	off	0
B6	10/1 00TX	Yes	Down	10HDx	off	0
B7	10/1 00TX	Yes	Up	10HDx	off	0
B8	10/1 00TX	Yes	Up	10HDx	off	0

Refresh

Figure 7-6. Example of Port Status on the Web Browser Interface (Switch 4000M)

Displaying Port Status from the Console Interface

To access this screen from the Main Menu, select:

1. Status and Counters

4. Port Status

```

Terminal - SWITCH.TRM
File Edit Settings Phone Transfers Help
DEFAULT_CONFIG
----- CONSOLE - MANAGER MODE -----
                Status and Counters - Port Status
-----
Port   Type   Enabled  Status   Mode   Flow Ctrl  Bcast Limit
-----
A1    10/100TX  Yes     Up       10HDx  off        0
A2    10/100TX  Yes     Up       10HDx  off        0
A3    10/100TX  Yes     Up       10HDx  off        0
A4    10/100TX  Yes     Up       10HDx  off        0
A5    10/100TX  Yes     Up       10HDx  off        0
A6    10/100TX  Yes     Up       10HDx  off        0
A7    10/100TX  Yes     Up       10HDx  off        0
A8    10/100TX  Yes     Down    10HDx  off        0
B1    10/100TX  Yes     Up       10HDx  off        0
B2    10/100TX  Yes     Up       10HDx  off        0
B3    10/100TX  Yes     Up       10HDx  off        0

Actions->  Back  Help

Return to previous screen.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
    
```

Figure 7-7. Example of Port Status on the Console Interface (Switch 4000M)

Port Counters

The web browser interface and the console interface show the same port counter data.

These screens enables you to determine the traffic patterns for each port. Port Counter features include:

- Dynamic display of counters summarizing the traffic on each port since the last reboot or reset
- Option to reset the counters to zero (for the current console session). This is useful for troubleshooting. Refer to the Note, below.
- An option to display the link status and further port activity details for a specific port (console: **Show details** or browser: **Details for Select Port**).

Note

The **Reset** action resets the counter display to zero for the current session, but does not affect the cumulative values in the actual hardware counters. (In compliance with the SNMP standard, the values in the hardware counters are not reset to zero unless you reboot the switch.) Thus, using the **Reset** action resets the displayed counters to zero for the current session only. Exiting from the console session and starting a new session restores the counter displays to the accumulated values in the hardware counters.

Displaying Port Counters from the Web Browser Interface

1. Click here

2. Click here

Port	MCast Rx	MCast Tx	BCast Rx	BCast Tx	Pkts Rx	Pkts Tx	Errors Rx
A1	292	0	11141	20	54447	468	0
A2	0	0	0	0	0	0	0
A3	0	0	0	0	0	0	0
A4	0	0	0	0	0	0	0
A5	0	0	0	0	0	0	0
A6	0	0	0	0	0	0	0
A7	0	0	0	0	0	0	0
A8	0	0	0	0	0	0	0
B1	0	0	0	0	0	0	0
B2	0	0	0	0	0	0	0
B3	0	0	0	0	0	0	0
B4	0	0	0	0	0	0	0
B5	0	0	0	0	0	0	0
B6	0	0	0	0	0	0	0
B7	0	0	0	0	0	0	0
B8	0	0	0	0	0	0	0

3. To view details about the traffic on a particular port, highlight that port number, then click on **Details for Select Port**.

Refresh Details for select Port

4. Click here to return to the Port Counters screen.

Status and Counters - Port Counters - A1

Link Status : Up

Bytes Rx :	39,120,319	Bytes Tx :	154,304
Unicast Rx :	63,372	Unicast Tx :	509
Bcast/Mcast Rx :	15,393	Bcast/Mcast Tx :	20
FCS Rx :	0	Drops Tx :	0
Alignment Rx :	0	Collisions Tx :	79
Runts Rx :	0	Late Colln Tx :	0
Giants Rx :	0	Excessive Colln :	0
Total Rx Errors :	0	Deferred Tx :	22

Return to Summary

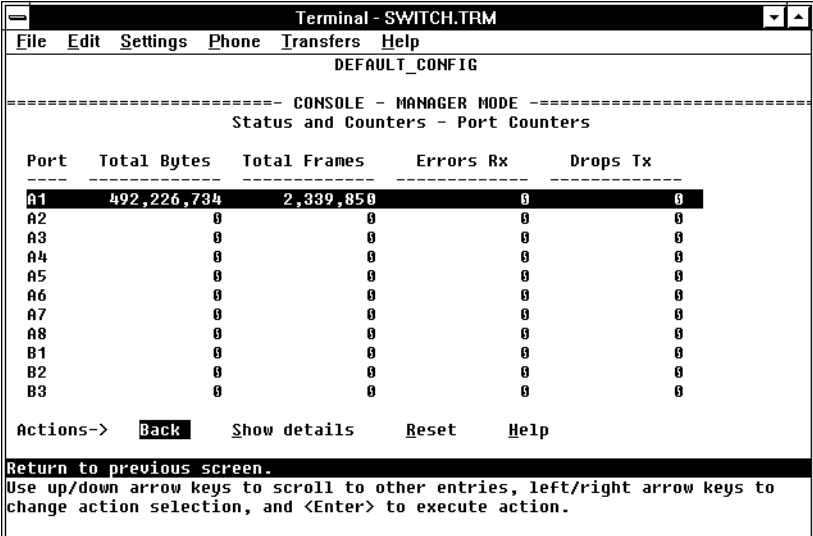
Figure 7-8. Example of Port Counters and Details on the Web Browser Interface

Displaying Port Counters from the Console Interface

To access this screen from the Main Menu, select:

1. Status and Counters

5. Port Counters



```
Terminal - SWITCH.TRM
File Edit Settings Phone Transfers Help
DEFAULT_CONFIG
----- CONSOLE - MANAGER MODE -----
Status and Counters - Port Counters

Port    Total Bytes    Total Frames    Errors Rx    Drops Tx
-----
A1      492,226,734    2,339,850      0            0
A2              0              0            0            0
A3              0              0            0            0
A4              0              0            0            0
A5              0              0            0            0
A6              0              0            0            0
A7              0              0            0            0
A8              0              0            0            0
B1              0              0            0            0
B2              0              0            0            0
B3              0              0            0            0

Actions->  Back    Show details    Reset    Help

Return to previous screen.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

Figure 7-9. Example of Port Counters on the Console Interface

To view details about the traffic on a particular port, highlight that port number (figure 7-9), then select **Show Details**. For example, selecting port A1 displays a screen similar to figure 7-10, on the next page.

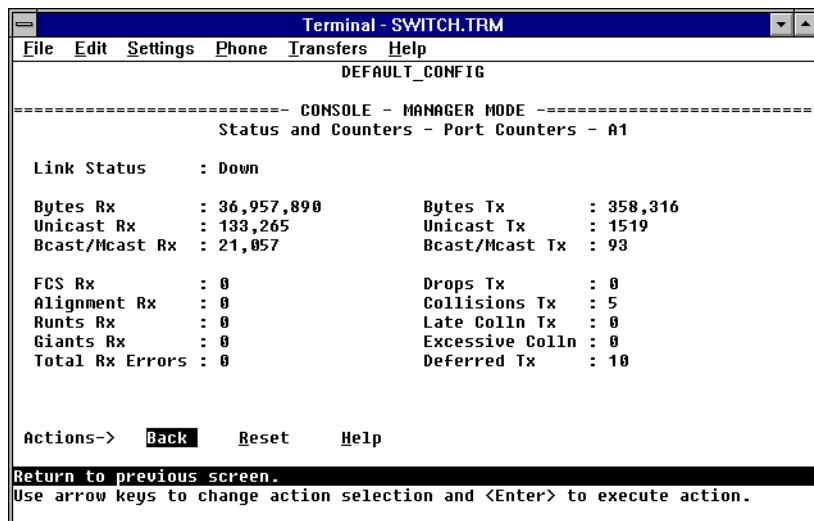


Figure 7-10. Example of the Display for Show details on a Selected Port

This screen also includes the **Reset** action. Refer to the note on page 7-10.

Address Table

To access the Address Table screen from the Main Menu, select:

1. Status and Counters

6. Address Table

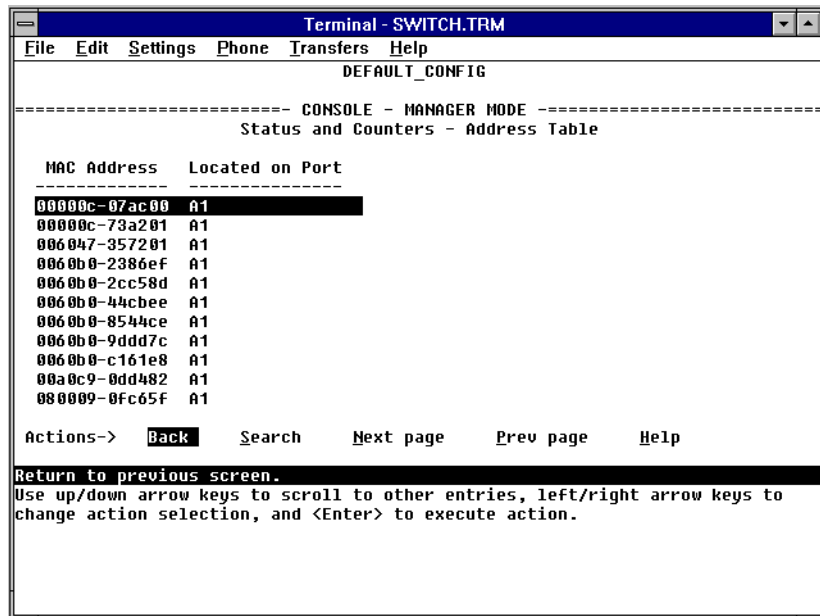


Figure 7-11. Example of the Address Table (Switch 4000M)

This screen lets you determine which switch port is being used to communicate with a specific device on the network. The listing includes:

- The MAC addresses that the switch has learned from network devices attached to the switch
- The port on which each MAC address was learned

Use the **Search** action at the bottom of the screen to locate a specific device (MAC address).

Port Address Table

This screen lets you determine which devices are attached to the selected switch port by listing all of the MAC addresses detected on that port.

To access the port address table:

1. From the Main Menu, select:

1. Status and Counters

7. Port Address Table

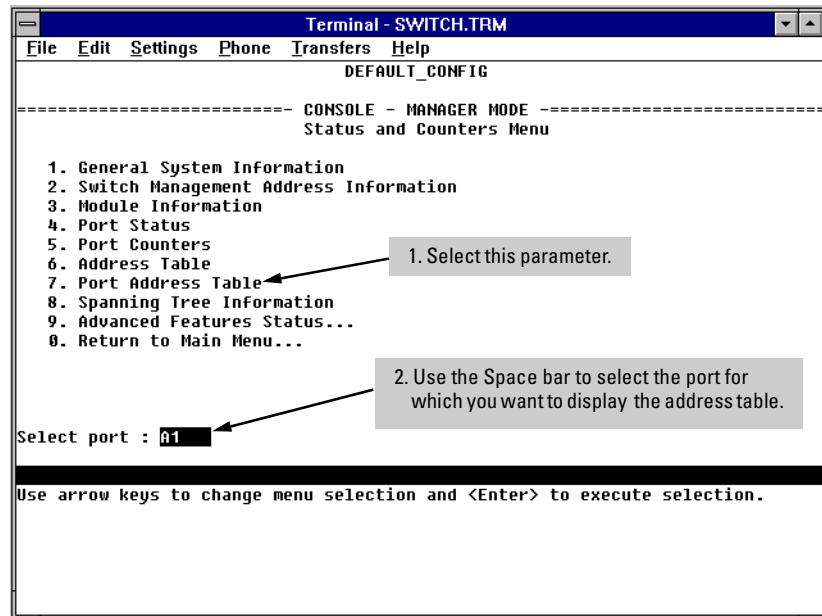


Figure 7-12. Example of How To Access the Port Address Table

2. When the prompt appears, press the Space bar or type the port name to display the port you want to examine, then press **[Enter]**. (See figure 7-12, above.)

You will then see a list of the MAC addresses that have been detected on the selected port, as shown in figure 7-13 on the next page. Each port is identified by the sequential port numbers on the front of the switch.

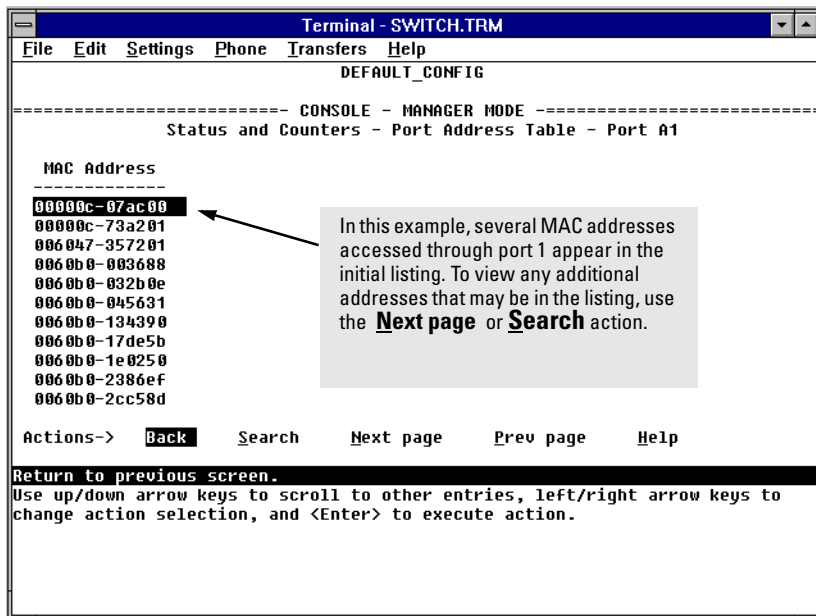


Figure 7-13. Example of a Port Address Table for a Specific Port

Use the **Search** action at the bottom of the screen to determine whether a specific device (MAC address) is connected to the selected port.

Spanning Tree (STP) Information

To access the Spanning Tree Information from the Main Menu, select:

1. Status and Counters

8. Spanning Tree Information

STP must be enabled on the switch to display the following data:

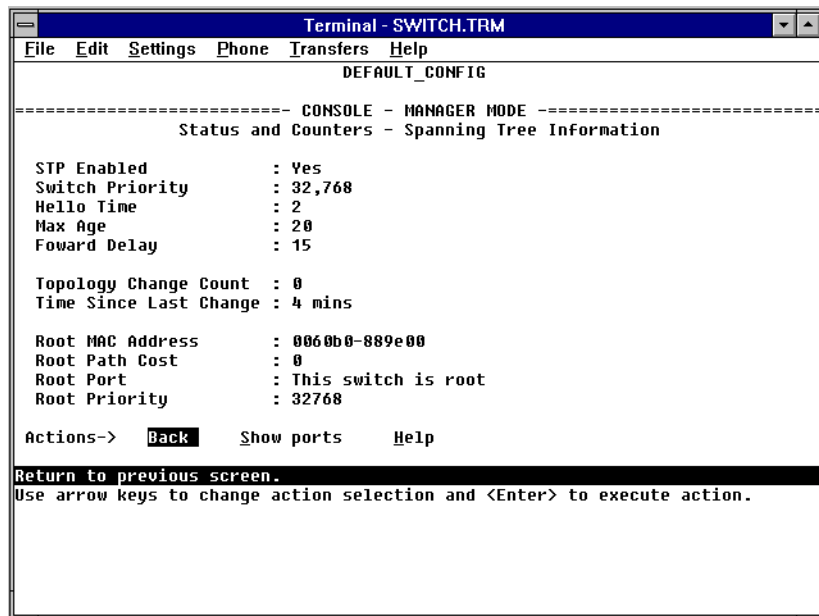


Figure 7-14. Example of Spanning Tree Information

Use this screen to determine current switch-level STP parameter settings and statistics.

You can use the **Show ports** action at the bottom of the screen to display port-level information and parameter settings for each port in the switch (including port type, cost, priority, operating state, and designated bridge) as shown in figure 7-15.

```
Terminal - SWITCH.TRM
File Edit Settings Phone Transfers Help
DEFAULT_CONFIG
----- CONSOLE - MANAGER MODE -----
Status and Counters - Spanning Tree - Port Information
-----
Port      Type      Cost    Priority  State      Designated Bridge
-----
A1       10/100TX  10      128      Forwarding 0060b0-889e00
A2       10/100TX  10      128      Disabled
A3       10/100TX  10      128      Disabled
A4       10/100TX  10      128      Disabled
A5       10/100TX  10      128      Disabled
A6       10/100TX  10      128      Disabled
A7       10/100TX  10      128      Forwarding 0060b0-889e00
A8       10/100TX  10      128      Blocking   0060b0-889e00
E1       100FX     10      128      Disabled
E2       100FX     10      128      Disabled
E3       100FX     10      128      Disabled

Actions->  Back      Help

Return to previous screen.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

Figure 7-15. Example of STP Port Information (Switch 4000M)

IP Multicast (IGMP) Status

To access this screen from the Main Menu, select:

1. Status and Counters

9. Advanced Features Status

1. IP Multicast (IGMP) Status

Note

If multiple VLANs are configured on the switch, you will be prompted to select a VLAN (by using the Space bar, then pressing **[Enter]**) to display this screen.

This screen identifies the active IP multicast groups the switch has detected, along with the number of report packets and query packets seen for each group. It also indicates which port is used for connecting to the querier.

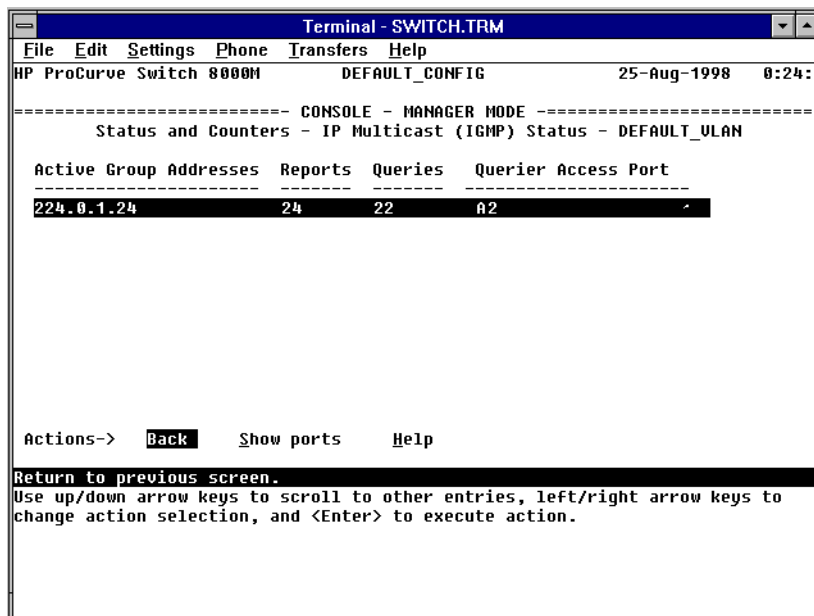


Figure 7-16. Example of IGMP Status Screen

You can also display the port status of the individual multicast groups. (That is, you can display the ports, port types, and whether the IGMP devices connected to the switch via the port are hosts, routers, or both.) To do so, select the group from the above screen and press **[S]** for **Show ports**. For example, suppose you wanted to view the status of the IP multicast group 224.0.1.24 shown in the above screen. You would highlight the row beginning with that group number, then press **[S]**. You would then see a screen similar to the following:

```
Terminal - SWITCH.TRM
File Edit Settings Phone Transfers Help
HP ProCurve Switch 8000M  DEFAULT_CONFIG  25-Aug-1998  0:27:00
----- CONSOLE - MANAGER MODE -----
                Status and Counters - IGMP Status - Ports

Active Group Address : 224.0.1.24

  Port      Type      Access
-----
A1         10/100TX  host
A3         10/100TX  host
A4         10/100TX  host-Router

Actions->  Back      Help

Return to previous screen.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

Figure 7-17. Example of an IGMP Status Screen for a Selected Multicast Group

Automatic Broadcast Control (ABC) Information

To access this screen from the Main Menu, click on:

1. Status and Counters

9. Advanced Features Status

2. Automatic Broadcast Control (ABC) Information

Note

If multiple VLANs are configured on the switch, you will be prompted to select a VLAN (by using the Space bar, then pressing **[Enter]**) to display this screen.

This screen displays the number of IP ARP and IPX NSQ replies sent per port and whether RIP and SAP packets are being forwarded or not forwarded per port. If VLANs are configured, this data is on a per-VLAN basis.

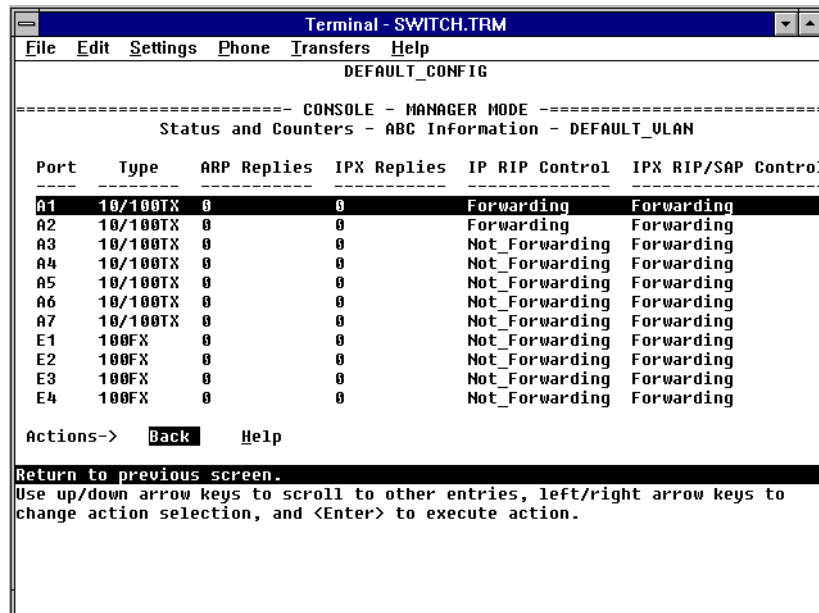


Figure 7-18. Example of Automatic Broadcast Control (ABC) Screen

Switch Mesh Information

To access this screen from the Main Menu, click on:

1. Status and Counters
9. Advanced Features Status
3. Switch Mesh Information

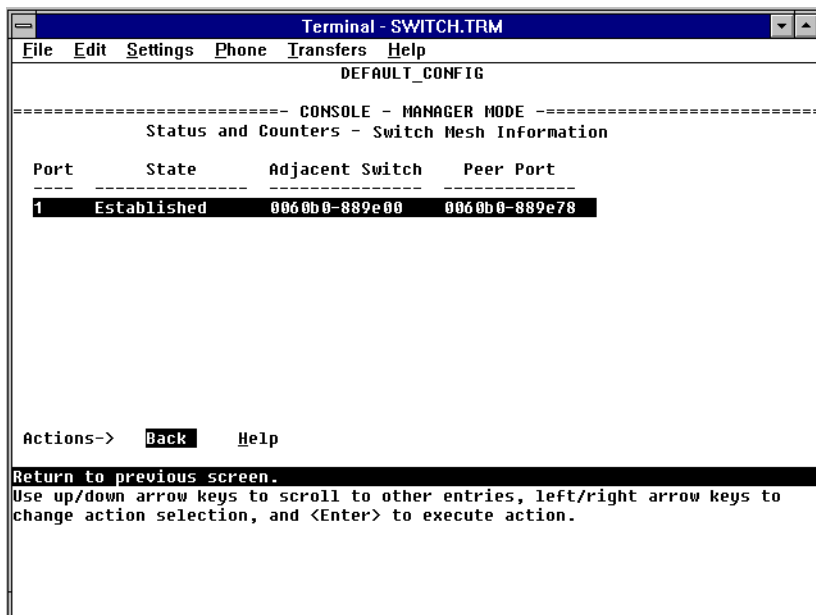


Figure 7-19. Example of Switch Mesh Screen

This screen indicates the current operating states for meshed ports in the switch and identifies adjacent meshed ports and switches. For more information, see the online Help.

VLAN Information

To access this screen from the Main Menu, select:

- 1. Status and Counters
- 9. Advanced Features Status
- 4. VLAN Information

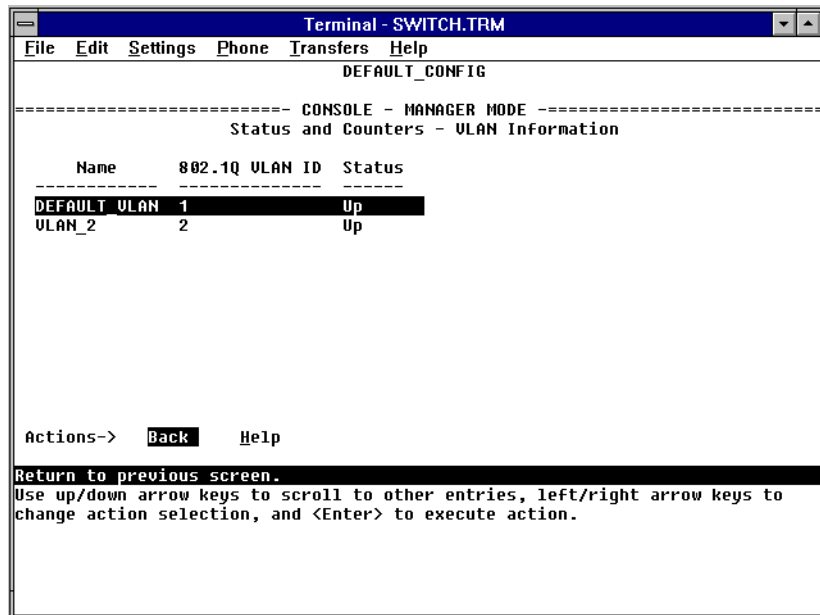


Figure 7-20. Example of VLAN Information Screen

This screen displays the VLAN identification and status for each VLAN configured in the switch.

Troubleshooting

This chapter addresses performance-related network problems that can be caused by topology, switch configuration, and the effects of other devices or their configurations on switch operation. (For switch-specific information on hardware problems indicated by LED behavior, cabling requirements, and other potential hardware-related problems, refer to the installation guide you received with the switch.)

This chapter includes:

- Troubleshooting Approaches (page 8-2)
- Browser or Console Interface Problems (page 8-3)
- Unusual Network Activity (page 8-5)
 - General Problems (page 8-5)
 - Automatic Broadcast Control Problems (page 8-6)
 - IGMP-Related Problems (page 8-7)
 - Switch Mesh Problems (page 8-7)
 - STP-Related Problems (page 8-9)
 - VLAN-Related Problems (page 8-10)
- Using the Event Log To Identify Problem Sources (page 8-12)
- Diagnostics and management tools (page 8-17), including:
 - Link test (page 8-17)
 - Ping test (page 8-18)
 - Browse configuration (page 8-21)
 - Command prompt (page 8-23)
 - Restoring the factory default configuration (page 8-24)

For information on support and warranty provisions, see the Support and Warranty booklet shipped with the switch.

Troubleshooting Approaches

There are six primary ways to diagnose switch problems:

- Check the switch LEDs for indications of proper switch operation:
 - Each switch port has a Link LED that should light whenever an active network device is connected to the port.
 - Problems with the switch hardware and software are indicated by flashing the Fault and other switch LEDs.

See the *Installation Guide* shipped with the switch for a description of the LED behavior and information on using the LEDs for troubleshooting.
- Check the network topology/installation. See the *Installation Guide* shipped with the switch for topology information.
- Check cables for damage, correct type, and proper connections. See the *Installation Guide* shipped with the switch for correct cable types and connector pin-outs.
- Use HP TopTools for Hubs & Switches (if installed on your network) to help isolate problems and recommend solutions. HP TopTools is shipped at no extra cost with the switch.
- Use the Port Utilization Graph and Alert Log in the web browser interface included in the switch to help isolate problems. See chapter 3, “Using the HP Web Browser Interface” for operating information. These tools are available through the web browser interface:
 - Port Utilization Graph
 - Alert Log
 - Port Status and Port Counters screens
 - Diagnostic tools (Link test, Ping test, configuration file browser)
- For help in isolating problems, use the easy-to-access switch console built into the switch or Telnet to the switch console. See chapter 4, “Using the Switch Console Interface” for operating information. These tools are available through the switch console
 - Status and Counters screens
 - Event Log
 - Diagnostics tools (Link test, Ping test, configuration file browser, and advanced user commands)

Browser or Console Access Problems

Cannot access the web browser interface:

- Access may be disabled by the **Web Agent Enabled** parameter in the switch console. Check the setting on this parameter by selecting:

2. Switch Management Access Configuration

4. Console/Serial Link.

- The switch may not have the correct IP address, subnet mask or gateway. Verify by connecting a console to the switch's Console port and selecting:

2. Status Management Access Configuration (IP, SNMP, Console...)

1. IP Configuration

Note: If DHCP/Bootp is used to configure the switch, use **2. Switch Management Address Information** under **1. Status and Counters** to view IP addressing information. If Bootp is in use, check the Bootp configuration file in the Bootp server to verify correct gateway addressing.

- If you are using DHCP to acquire the IP address for the switch, the IP address “lease time” may have expired so that the IP address has changed. For more information on how to “reserve” an IP address, refer to the documentation for the DHCP application that you are using.
- If one or more IP-Authorized managers are configured, the switch allows web browser access only to a device having an authorized IP address. For more information on IP Authorized managers, see “Enhancing Security By Configuring Authorized IP Managers” on page 6-21.
- Java™ applets may not be running on the web browser. They are required for the switch web browser interface to operate correctly. See the online Help on your web browser for how to run the Java applets.

Cannot Telnet into the switch console from a station on the network:

- Telnet access may be disabled by the **Inbound Telnet Enabled** parameter in the switch console. See “Configuring the Console/Serial Link from the Switch Console” on page 6-20.
- The switch may not have the correct IP address, subnet mask, or gateway. Verify by connecting a console to the switch’s Console port and selecting:

2. Status Management Access Configuration (IP, SNMP, Console...)

1. IP Configuration

Note: If DHCP/Bootp is used to configure the switch, see the **Note**, above.

- If you are using DHCP to acquire the IP address for the switch, the IP address “lease time” may have expired so that the IP address has changed. For more information on how to “reserve” an IP address, refer to the documentation for the DHCP application that you are using.
- If one or more IP-Authorized managers are configured, the switch allows inbound telnet access only to a device having an authorized IP address. For more information on IP Authorized managers, see “Enhancing Security By Configuring Authorized IP Managers” on page 6-21.

Unusual Network Activity

Network activity that exceeds accepted norms often indicates a hardware problem with one or more of the network components, possibly including the switch. Unusual network activity is usually indicated by the LEDs on the front of the switch or measured with the switch console interface or with a network management tool such as the HP TopTools for Hubs & Switches. Refer to the *Installation Guide* you received with the switch for information on using LEDs to identify unusual network activity.

General Problems

The network runs slow; processes fail; users cannot access servers or other devices. Broadcast storms may be occurring in the network. These may be due to redundant links between nodes.

- If you are configuring a port trunk, finish configuring the ports in the trunk before connecting the related cables. Otherwise you may inadvertently create a number of redundant links that will cause broadcast storms.
- Turn on Spanning Tree Protocol to block redundant links.

Duplicate IP Addresses. This is indicated by this Event Log message:

ip: Invalid ARP source: *IP address* on *IP address*

where: both instances of *IP address* are the same address, indicating the switch's IP address has been duplicated somewhere on the network.

Duplicate IP Addresses in a DHCP Network. If you use a DHCP server to automatically assign IP addresses in your network and you find a device with a valid IP address that does not appear to communicate properly with the server or other devices, a duplicate IP address may have been issued by the server. This can occur if a client has not released a DHCP-assigned IP address after the intended expiration time and the server “leases” the address to another device. This can also happen, for example, if the server is first configured to issue IP addresses with an unlimited duration, then is subsequently configured to issue IP addresses that will expire after a limited duration. One solution is to configure “reservations” in the DHCP server for specific IP addresses to be assigned to devices having specific MAC addresses. For more information, refer to the documentation for the DHCP server.

One indication of a duplicate IP address in a DHCP network is this Event Log message:

ip: Invalid ARP source: IP address on IP address

where: both instances of *IP address* are the same address, indicating the IP address that has been duplicated somewhere on the network.

The Switch Has Been Configured for DHCP/Bootp Operation, But Has Not Received a DHCP or Bootp Reply. When the switch is first configured for DHCP/Bootp operation, or if it is rebooted with this configuration, it immediately begins sending request packets on the network. If the switch does not receive a reply to its DHCP/Bootp requests, it continues to periodically send request packets, but with decreasing frequency. Thus, if a DHCP or Bootp server is not available or accessible to the switch when DHCP/Bootp is first configured, the switch may not immediately receive the desired configuration. After verifying that the server has become accessible to the switch, reboot the switch to re-start the process.

Automatic Broadcast Control Problems

After Enabling ABC, Some Clients in a DHCP Network Using a Router as a Gateway Cannot Communicate with their Servers or Other Devices. When ABC is enabled in IP or IP-IPX networks, the default

Auto Gateway parameter is set to **Yes**. Generally, this should be used only where you want client-server traffic to remain in the client's broadcast domain. In a DHCP network this causes the switch to intercept DHCP server reply packets, change the default router option field within these packets to match the clients' IP addresses, then forward the modified reply packets to the clients. This effectively configures the clients to be their own gateways. In a DHCP network where a router must serve as a gateway, this causes clients to lose contact with devices that are reached through the router. Possible solutions include:

- Disable the **Auto Gateway** parameter. (See the procedure on page 6-109.)
- On the gateway router, enable Proxy ARP if available.

Note that the Auto Gateway and IP RIP Control are not functional without an IP address and subnet mask.

IGMP-Related Problems

IP Multicast (IGMP) Traffic Does Not Reach IGMP Hosts or a Multicast Router Connected to a Port. IGMP must be enabled on the switch and the affected port must be configured for “Auto” or “Forward” operation.

IP Multicast Traffic Floods Out All Ports; IGMP Does Not Appear To Filter Traffic. The IGMP feature does not operate if the switch or VLAN does not have an IP address configured manually or obtained through DHCP/Bootp. To verify whether an IP address is configured for the switch or VLAN, do either of the following:

- **Try Using the Web Browser Interface:** If you can access the web browser interface, then an IP address is configured.
- **Try To Telnet to the Switch Console:** If you can Telnet to the switch, then an IP address is configured.
- **Using the Switch Console Interface:** From the Main Menu, check the Management Address Information screen by clicking on

1. Status and Counters

2. Switch Management Address Information

Switch Mesh Problems

In a Network Using Meshed Switches, Traffic for a Specific VLAN Does Not Reach Its Destination. The failing VLAN may not be configured on all meshed switches. A VLAN on the network must be configured on all meshed switches, even if a given switch has no ports assigned to that VLAN. Refer to “VLANs and Switch Meshing” on page 6-67.

A Meshed Port Remains Disabled. The cable connecting the port to another meshed port may be defective, or a topology error may exist. For example, the following topology conditions are *not allowed*:

- Using a hub to connect multiple meshed ports

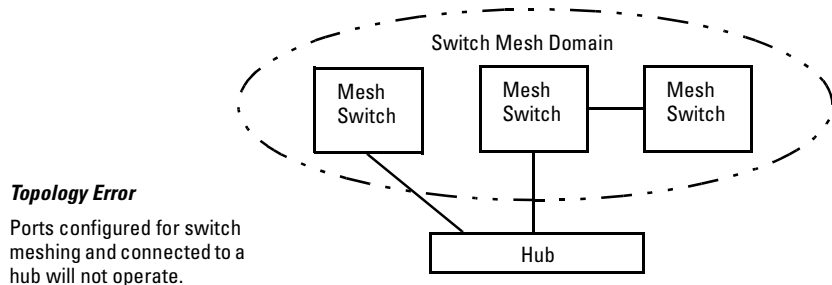


Figure 8-1. Connecting a Hub To Meshed Ports Causes a Topology Error

- A non-meshed switch or port connected to a mesh port

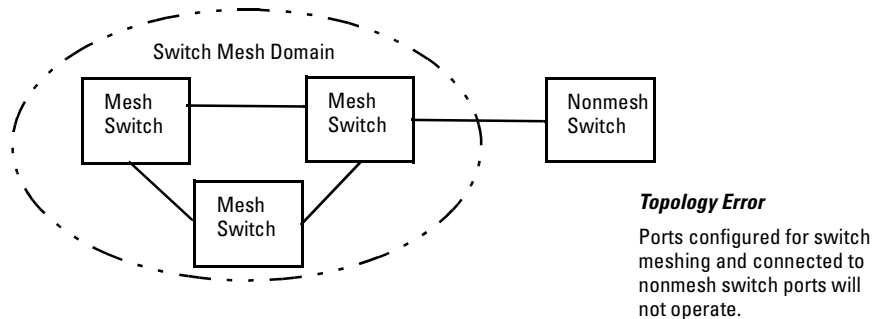


Figure 8-2. Connecting a Non-Meshed Switch Port to a Meshed Port Causes a Topology Error

To view the state, adjacent switch, and peer port for a meshed port, display the Load Balance (LdBal) Information screen. To do so, select the following from the Main Menu of the console interface:

1. Status and Counters
9. Advanced Features Status
3. Switch Mesh Information

A Meshed Port Remains in the “Not Established” State. The meshed port may be connected to a non-meshed port.

STP-Related Problems

Caution

If you enable STP, it is recommended that you leave the remainder of the STP parameter settings at their default values until you have had an opportunity to evaluate STP performance in your network. Because incorrect STP settings can adversely affect network performance, you should avoid making changes without having a strong understanding of how STP operates. To learn the details of STP operation, refer to the IEEE 802.1d standard.

Broadcast Storms and/or Duplicate MAC Addresses Appearing in the Network. This can occur where STP is not detecting physical loops (redundant links). Where this exists, you should enable STP on all bridging devices in the loop in order for the loop to be detected.

The Spanning Tree Cost Configured on a Non-Meshed Port Will Not Stay at the Configured Value. A redundant link situation exists between a non-meshed port and a port in the switch mesh.

The mesh path and the nonmesh path form redundant links. STP will eventually block the nonmesh link because the cost for the nonmeshed path will be automatically increased above that for the meshed path. (Switches "A" and "C" are "edge switches"—refer to page 6-82.)

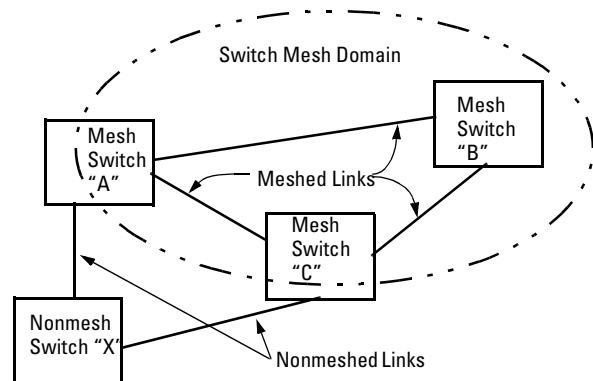


Figure 8-3. Example of Meshed and Nonmeshed Links Forming a Redundant Pair

Spanning Tree attempted to block the meshed port. In this situation, the meshed switch automatically increases the STP cost on the non-meshed redundant link so that STP will block the nonmeshed port and open the meshed port. Refer to "STP Operation with Switch Meshing" on page 6-45.

If you are experienced with STP, then it is recommended that you set up your topology and STP configuration so that one of the meshed switches is the root switch.

STP Blocks a Link in a VLAN Even Though There Are No Redundant Links in that VLAN. In 802.1Q-compliant switches such as the Switch 4000M and Switch 2424M, STP blocks redundant physical links even if they are in separate VLANs. A solution is to use only one, multiple-VLAN link between the devices. Also, if ports are available, you can improve the bandwidth in this situation by using a port trunk. See “STP Operation with 802.1Q VLANs” on page 6-44.

VLAN-Related Problems

Monitor Port. When using the monitor port in a multiple VLAN environment, it can be useful to know how broadcast, multicast, and unicast traffic is tagged. The following table describes the tagging to expect.

	Within Same Tagged VLAN as Monitor Port	Within Same Untagged VLAN as Monitor Port	Outside of Tagged Monitor Port VLAN	Outside of Untagged Monitor Port VLAN
Broadcast	Tagged	Untagged	Untagged	Untagged
Multicast	Tagged	Untagged	Untagged	Untagged
Unicast Flood	Tagged	Untagged	Untagged	Untagged
Unicast Not to Monitor Port	Untagged	Untagged	Untagged	Untagged
Unicast to Monitor Port	Tagged	Untagged	N/A—Dropped	N/A—Dropped

None of the devices assigned to one or more VLANs on an 802.1Q-compliant switch are being recognized. If multiple VLANs are being used on ports connecting 802.1Q-compliant devices, inconsistent VLAN IDs may have been assigned to one or more VLANs. For a given VLAN, the same VLAN ID must be used on all connected 802.1Q-compliant devices.

Link Configured for Multiple VLANs Does Not Support Traffic for One or More VLANs. One or more VLANs may not be properly configured as “Tagged” or “Untagged”. A VLAN assigned to a port connecting two 802.1Q-compliant devices must be configured the same on both ports. For example, VLAN_1 and VLAN_2 use the same link between switch “X” and switch “Y”.

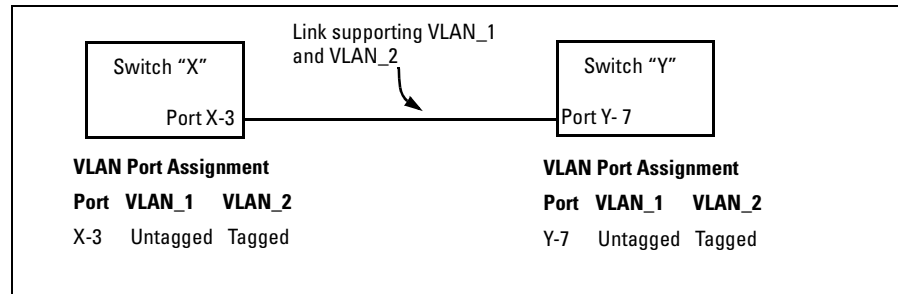


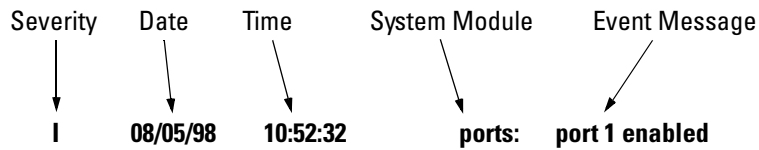
Figure 8-4. Example of Correct VLAN Port Assignments on a Link

1. If VLAN_1 is configured as “Untagged” on port 3 on switch “X”, then it must also be configured as “Untagged” on port 7 on switch “Y”.
2. Similarly, if VLAN_2 is configured as “Tagged on the link port on switch “A”, then it must also be configured as “Tagged” on the link port on switch “B”.

Duplicate MAC Addresses Across VLANs. Duplicate MAC addresses on different VLANs are not supported and can cause VLAN operating problems. There are no explicit events or statistics to indicate the presence of duplicate MAC addresses in a VLAN environment. However, one symptom that may occur is that a duplicate MAC address can appear in the Port Address Table of one port, and then later appear to be linked to another port. (This can also occur in a LAN where there are redundant paths between nodes and Spanning Tree is turned off.) For more information, refer to “VLAN Restrictions” on page 6-68.

Using the Event Log To Identify Problem Sources

The Event Log records operating events as single-line entries listed in chronological order, and serves as a tool for isolating problems. Each Event Log entry is composed of five fields:



Severity is one of the following codes:

- I** (information) indicates routine events.
- W** (warning) indicates that a service has behaved unexpectedly.
- C** (critical) indicates that a severe switch error has occurred.
- D** (debug) reserved for HP internal diagnostic information.

Date is the date in *mm/dd/yy* format that the entry was placed in the log.

Time is the time in *hh:mm:ss* format that the entry was placed in the log.

System Module is the internal module (such as “ports” for port manager) that generated the log entry. If VLANs are configured, then a VLAN name also appears for an event that is specific to an individual VLAN. Table 8-1 on page 8-13 lists the individual modules.

Event Message is a brief description of the operating event.

Table 8-1. Event Log System Modules

Module	Event Description	Module	Event Description
abc	Automatic Broadcast Control	mgr	Console management
addrMgr	Address table	pagp	Port trunks
chassis	switch hardware	ports	Change in port status
bootp	bootp addressing	snmp	SNMP communications
console	Console interface	stp	Spanning Tree
dhcp	DHCP addressing	sys, system	Switch management
download	file transfer	telnet	Telnet activity
FFI	Find, Fix, and Inform) -- available in the console event log and web browser interface alert log	tcp	Transmission control
igmp	IP Multicast	tftp	File transfer for new OS or config.
ip	IP-related	timep	Time protocol
ipx	Novell Netware	vlan	VLAN operations
ldbal	Load balancing (trunking and meshing)	Xmodem	Xmodem file transfer

Entering and Navigating in the Event Log Display. From the Main Menu, select **Event Log**. From the Main Menu, select **Event Log**.

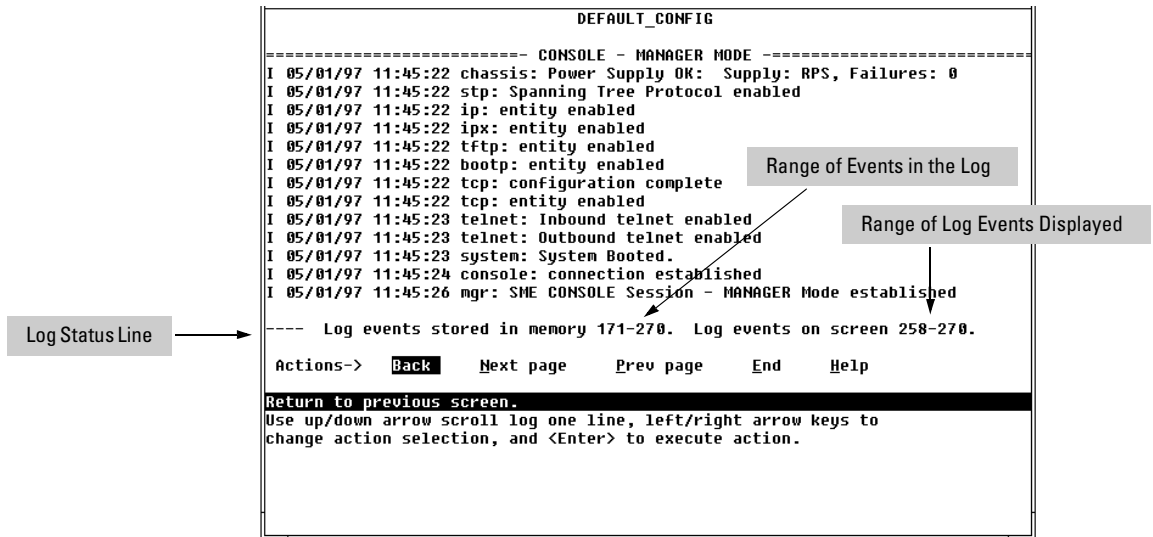


Figure 8-2. Example of an Event Log Display

To display various portions of the Event Log, either preceding or following the currently visible portion, use either the actions listed at the bottom of the display (**Next page**, **Prev page**, or **End**), or the keys described in the following table:

Table 8-2. Event Log Control Keys

Key	Action
N	Advance the display by one page (next page).
P	Roll back the display by one page (previous page).
↓	Advance display by one event (down one line).
↑	Roll back display by one event (up one line).
E	Advance to the end of the log.
H	Display Help for the event log.

The event log holds up to 1000 lines in chronological order, from the oldest to the newest. Each line consists of one complete event message. Once the log has received 1000 entries, it discards the current oldest line each time a new line is received. The event log window contains 14 log entry lines and can be positioned to any location in the log.

The log status line at the bottom of the display identifies where in the sequence of event messages the display is currently positioned.

The event log will be *erased* if any of the following occurs:

- The switch is reset using the Reset button.
- Power to the switch is interrupted.
- A new operating system is downloaded to the switch.

(The event log is *not* erased by using the **Reboot Switch** command in the Main Menu.)

To Change the Severity Level of Event Log Messages

In its default setting, the Event Log displays all event levels. If you want to change the severity level for which events will be displayed in the Event Log, change the setting for the **Displayed Events** parameter in the Console/Serial Link screen. Options include:

Severity Level	Event Log Action
All (default)	Display all events.
None	Display no events.
Not INFO	Display all events except informational-only events.
Critical	Display only critical-level events.
Debug	Reserved for HP internal use only.

1. From the Console Main Menu, Select...
 - 2. Switch Management Access Configuration (IP, SNMP, Console)...**
 - 4. Console/Serial Link Configuration**

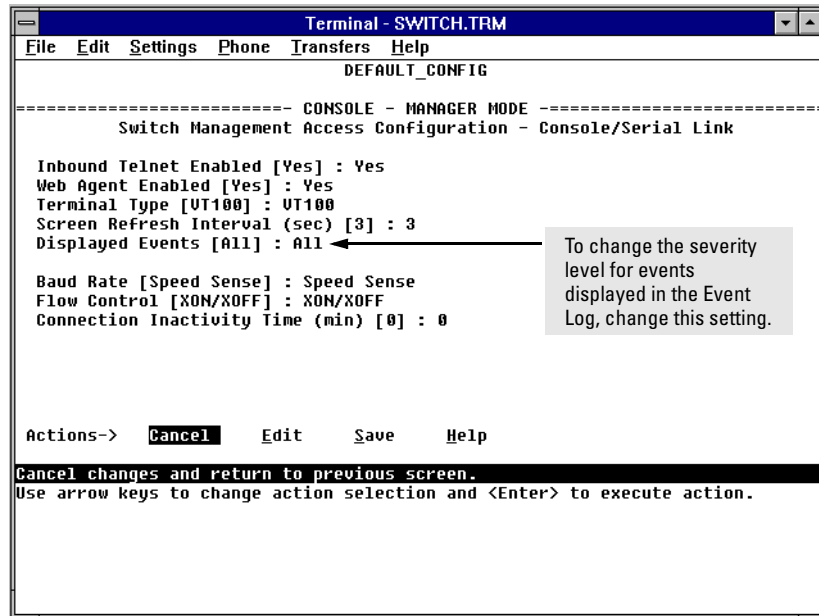


Figure 8-3. The Console/Serial Link Configuration Screen (Default Values)

2. Press **[E]** (for **Edit**). The cursor moves to the **Baud Rate** field.
3. Move the cursor to the **Displayed Events** field.
4. Use the Space bar to select the severity level you want for displayed Event Log messages, then press **[Enter]**.
5. When you have finished making changes in the Console/Serial Link screen, press **[Enter]**, then press **[S]** (for **Save**) to activate the change(s) you've made.
6. Return to the Main Menu.

Diagnostics

The switch's diagnostic tools include the following:

Feature	Switch Console	Web Browser Interface	Page
Link Test	Yes	Yes	8-17
Ping Test	Yes	Yes	8-17
Browse Config File	Yes	Yes	8-21
Command Prompt	Yes	No	8-23

Ping and Link Tests

The Ping test and the Link test are point-to-point tests between your switch and another IEEE 802.3-compliant device on your network. These tests can tell you whether the switch is communicating properly with another device.

Note

To respond to a Ping test or a Link test, the device you are trying to reach must be IEEE 802.3-compliant.

Ping Test. This is a test of the path between the switch and another device on the same or another IP network that can respond to IP packets. (“Ping” is an acronym for “Packet INternet Groper”.)

Link Test. This is a test of the connection between the switch and a designated network device on the same LAN (or VLAN, if configured). During the link test, IEEE 802.3 test packets are sent to the designated network device in the same VLAN or broadcast domain. The remote device returns the data to the switch, where it is compared to the data transmitted. If the received data matches the transmitted data, the test passes.

Executing Ping or Link Tests from the Web Browser Interface

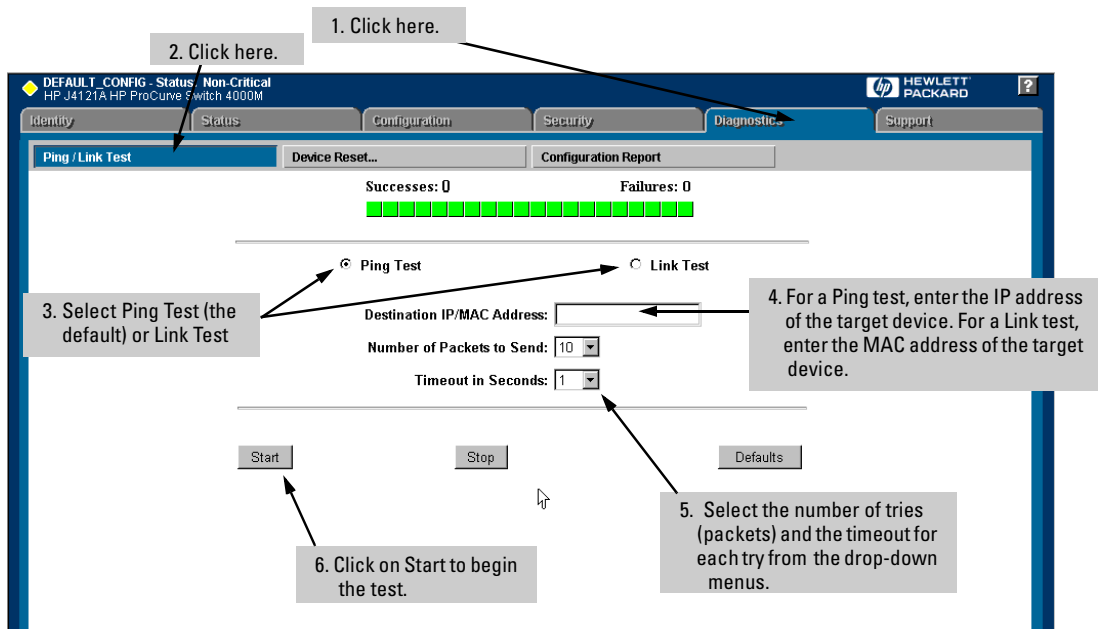


Figure 8-4. Link and Ping Test Screen on the Web Browser Interface

Successes indicates the number of Ping or Link packets that successfully completed the most recent test.

Failures indicates the number of Ping or Link packets that were unsuccessful in the last test. Failures indicate connectivity or network performance problems (such as overloaded links or devices).

Destination IP/MAC Address is the network address of the target, or destination, device to which you want to test a connection with the switch. An IP address is in the X.X.X.X format where X is a decimal number between 0 and 255. A MAC address is made up of 12 hexadecimal digits, for example, 0060b0-080400.

Number of Packets to Send is the number of times you want the switch to attempt to test a connection.

Timeout in Seconds is the number of seconds to allow per attempt to test a connection before determining that the current attempt has failed.

To halt a Link or Ping test before it concludes, click on the Stop button. **To reset the screen** to its default settings, click on the Defaults button.

Executing Ping or Link Tests from the Switch Console

(To cancel a Ping or Link test that is in progress, press **Ctrl** **C**.)

1. From the Main Menu, select:

5. Diagnostics . . .

1. Link Test

or

2. Ping Test

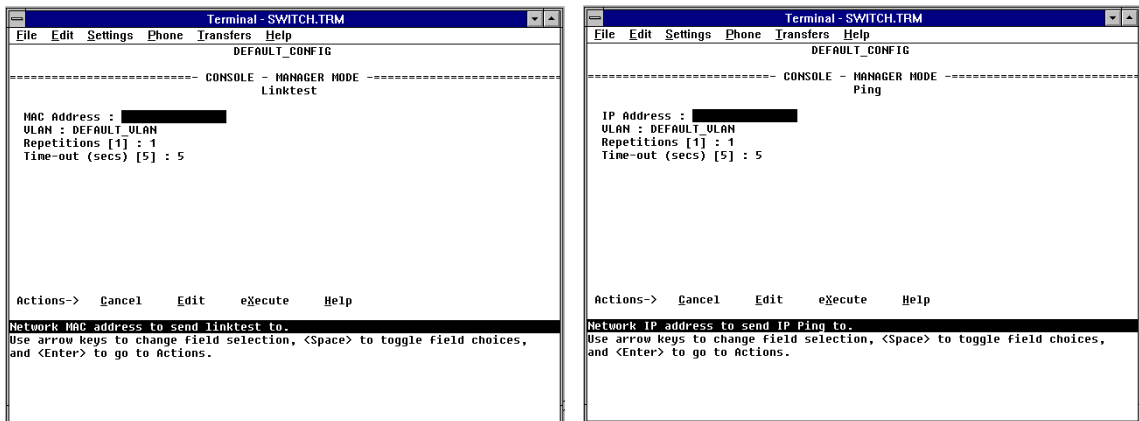


Figure 8-5. Examples of Link Test and Ping Test Screens with VLANs Configured

2. Do one of the following:
 - a. For a Link test, enter the 12-digit hexadecimal MAC address of the target device.
 - b. For a Ping test, enter the IP address of the target device.
3. If the **VLAN** parameter does not appear, multiple VLANs are not configured; go to the next step. If the **VLAN** parameter appears, select it and use the Space bar to select the VLAN of the target device.
4. Select the **Repetitions** parameter and type in the number of times you want the test to be made.
5. Select **Time-out** and select the number of seconds to allow for each test.

The console displays the result of each test. For example, if a Link test succeeds, you will see

Linktest Command Successful.

If the Link test fails, you will see

Linktest Command Timed out.

If a Ping test succeeds, you will see a message indicating the target IP address is “alive”, along with a test counter and elapsed time for each test. For example:

12.10.8.207 is alive, iteration 1, time = 1 ms

If a Ping test fails, you will see a message such as the following:

Ping Failed or Target did not Respond

The Configuration File

The complete switch configuration is contained in a file that you can browse from either the web browser interface or the switch console. It may be useful in some troubleshooting scenarios to view the switch configuration.

Browsing the Configuration File from the Web Browser Interface

To display the currently saved switch configuration through the web browser interface:

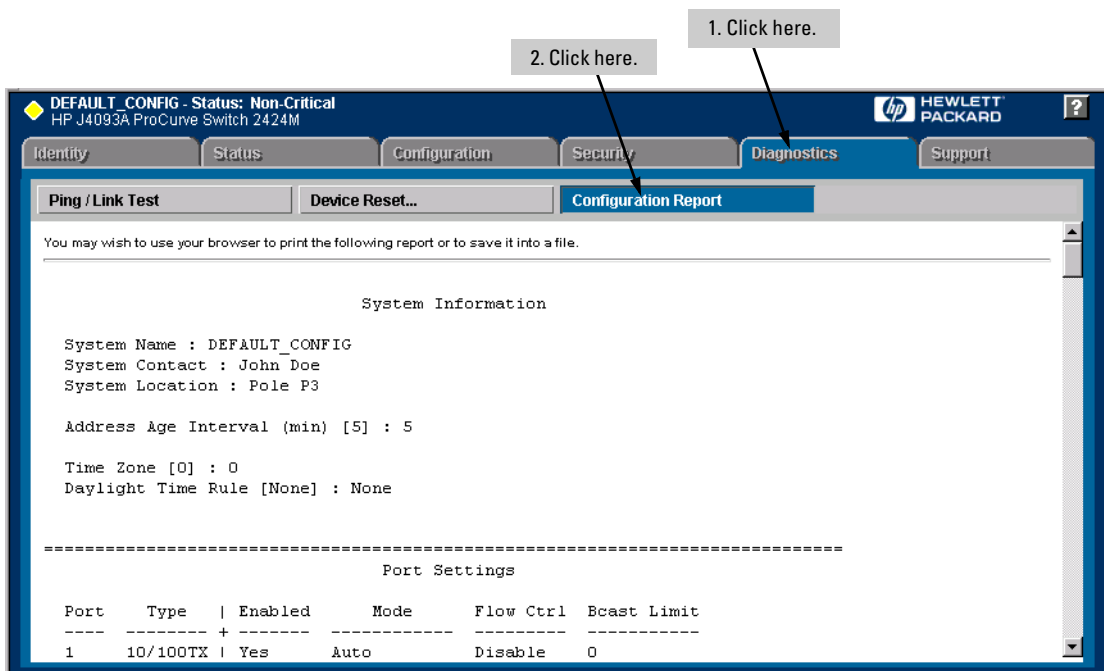


Figure 8-6. Example of the Web Browser Interface Configuration Report

Browsing the Configuration File from the Switch Console

To display the configuration file that is currently saved:

1. From the Main Menu, select:

5. Diagnostics

3. Browse Configuration File

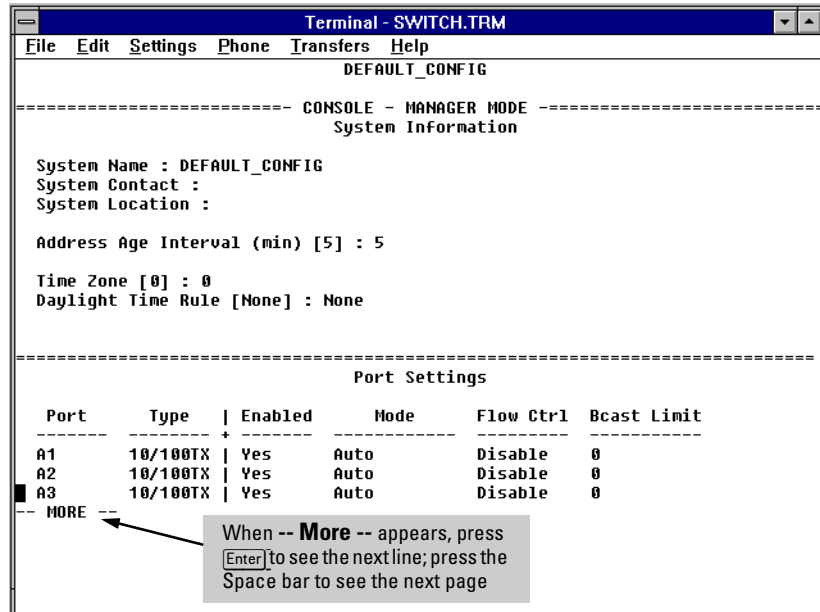


Figure 8-7. Example of the Browse Configuration Display

2. When -- **MORE** -- appears in the display, press **Enter** to see the next line of the configuration, or press the Space bar to display the next page of the configuration.

To halt a configuration listing, press **Q** (for Quit) and then press any key to return to the Diagnostics menu.

Using the Command Prompt

These commands are primarily for the expert user and for diagnostics purposes. Selecting **Command Prompt** from the Diagnostics Menu presents a command prompt from which you can enter the following commands:

List of Commands Available at the Command Prompt			
Help	Show	Log	Version
Exit	Delete	Page	Vlan
Browse	History	Ping	WalkMIB
Config	Kill	Print	Xget
Date	Get	Redo	Xput
Time	Put	GetMIB	romversion
Set	LinkTest	SetMIB	

To get a definition of these commands and their syntax, enter **Help** at the command prompt. When you see -- **MORE** -- at the bottom of the screen:

- To advance the display one line at a time, use `[Enter]`.
- To advance the display one screen at a time, use the Space bar.
- To stop the help listing, press `[Q]`.

How To Use the Command Prompt:

1. From the Main Menu, select **5. Diagnostics ...**, then from the Diagnostics Menu, select **4. Command Prompt**
2. One of the following appears:

- If VLANs are configured, you will see a prompt similar to the following:

Select VLAN : DEFAULT_VLAN

Use the Space bar to select the VLAN in which you want to execute a command, then press `[Enter]` to display the command prompt. The text in the prompt will match the name of the VLAN you select.

- If no VLANs are configured, the command prompt appears near the bottom of the screen. For example:

DEFAULT_CONFIG:

The text in the prompt matches the System Name parameter. In the above example, the factory default configuration name appears because no system name is configured.

3. Type in the command you want to execute and press **[Enter]**. For example, to set the time to 9:55 a.m. you would execute the following command:

DEFAULT_CONFIG: time 9:55 [Enter]

How To Exit from the command prompt:

Type **exit** and press **[Enter]** to return to the Diagnostics Menu.

Restoring the Factory Default Configuration

As part of your troubleshooting process, it may become necessary to return the switch configuration to the factory default settings. This process momentarily interrupts the switch operation, clears any passwords, clears the console event log, resets the network counters to zero, performs a complete self test, and reboots the switch into its factory default configuration including deleting an IP address.

To execute the factory default reset, perform these steps:

1. Using pointed objects, simultaneously press both the Reset and Clear buttons on the front of the switch.
2. Continue to press the Clear button while releasing the Reset button.
3. When the Self Test LED begins to flash, release the Clear button.

The switch will then complete its self test and begin operating with the configuration restored to the factory default settings.

File Transfers

Overview

You can download new switch software (operating system—OS) and upload or download switch configuration files. These features are useful for acquiring periodic switch software upgrades and for storing or retrieving a switch configuration.

This appendix includes the following information:

- downloading an operating system (this page)
- transferring switch configurations (page A-8)

Downloading an Operating System (OS)

HP periodically provides switch operating system (OS) updates through the Network City website (http://www.hp.com/go/network_city) and the HP FTP Library Service. For more information, see the support and warranty booklet shipped with the switch. After you acquire the new OS file, you can use one of the following methods for downloading the operating system (OS) code to the switch:

- The TFTP feature (**Download OS**) command in the Main Menu of the switch console interface (page A-2)
- HP's SNMP Download Manager included in HP TopTools for Hubs & Switches
- A switch-to-switch file transfer
- Xmodem transfer method

Note

Downloading a new OS does not change the current switch configuration. The switch configuration is contained in a separate file that can also be transferred, for example, for archive purposes or to be used in another switch of the same model. See “Transferring Switch Configurations” on page A-8.

Using TFTP To Download the OS File

This procedure assumes that:

- An OS file for the switch has been stored on a TFTP server accessible to the switch. (The OS file is typically available from HP's electronic services—see the support and warranty booklet shipped with the switch.)
- The switch is properly connected to your network and has already been configured with a compatible IP address and subnet mask.
- The TFTP server is accessible to the switch via IP.

Before you use the procedure, do the following:

- Obtain the IP address of the TFTP server in which the OS file has been stored.
- If VLANs are configured on the switch, determine the name of the VLAN in which the TFTP server is operating.
- Determine the name of the OS file stored in the TFTP server for the switch (for example, A_01_01.swi).

Note

If your TFTP server is a Unix workstation, ensure that the case (upper or lower) that you specify for the filename in the switch console Download OS screen is the same case as the characters in the OS filenames on the server.

1. In the console Main Menu, select **Download OS** to display this screen:

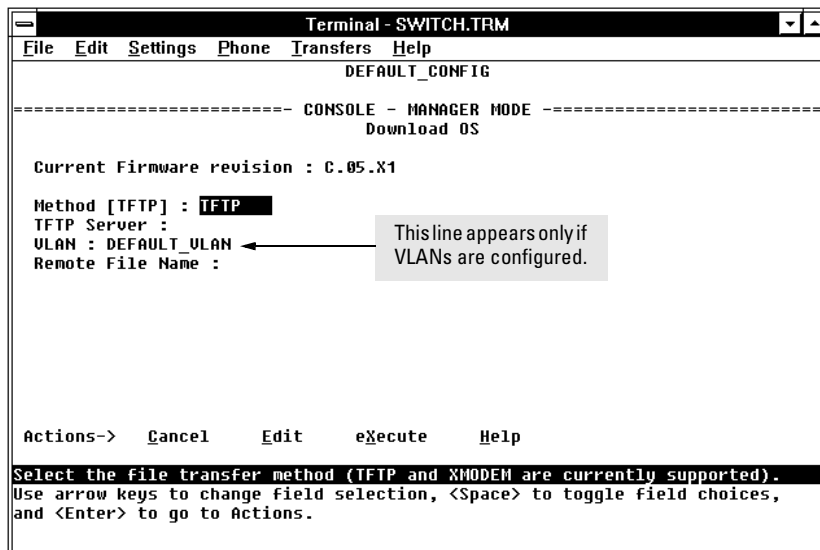


Figure A-1. Example of the Download OS Screen (Default Values)

2. Press **[E]** (for **E**dit).
3. Ensure that the **Method** field is set to **TFTP** (the default).
4. In the **TFTP Server** field, type in the IP address of the TFTP server in which the OS file has been stored.
5. If the **VLAN** field appears, use the Space bar to select the VLAN in which the TFTP server is operating (The VLAN field appears only if multiple VLANs are configured in the switch.)
6. In the **Remote File Name** field, then type the name of the OS file. If you are using a UNIX system, remember that the filename is case-sensitive.
7. Press **[Enter]**, then **[X]** (for **e**Xecute) to begin the OS download. The following screen then appears:

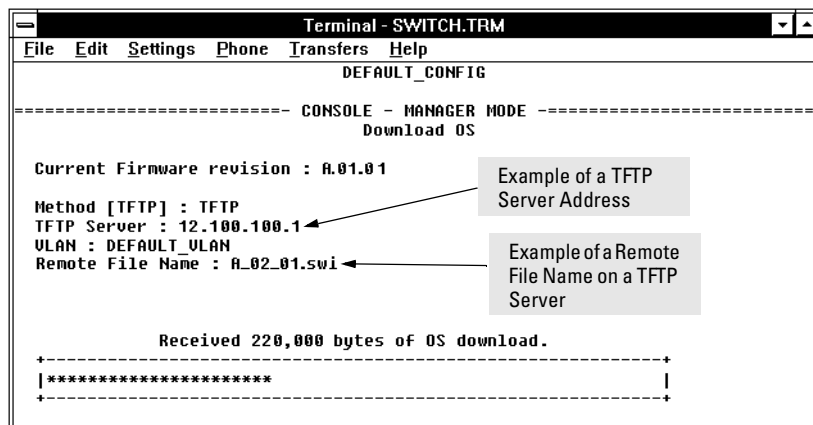


Figure A-2. Example of the Download OS Screen During a Download

8. A “progress” bar indicates the progress of the download. When the entire operating system has been received, all activity on the switch halts and you will see **Transfer completed** followed by **Validating and writing system software to FLASH...**

After the system flash memory has been updated with the new operating system, the switch reboots itself and begins running with the new operating system.

9. To confirm that the operating system downloaded correctly:
 - a. From the Main Menu, select **1. Status and Counters**, and from the Status and Counters menu, select **1. General System Information**
 - b. Check the **Firmware revision** line.

Using the SNMP-Based HP Download Manager

Included with your switch is the HP TopTools for Hubs & Switches CD ROM (available Fall 1998). The HP Download Manager is included with HP TopTools and enables you to initiate a firmware (OS) download over the network to the switch. This capability assumes that the switch is properly connected to the network and has been discovered by HP TopTools. For further information, refer to the documentation and online Help provided with HP TopTools.

Switch-to-Switch Download

If you have two or more Switch 4000Ms and/or Switch 2424Ms networked together, you can download the OS software from one switch to another by using the Download OS feature in the switch console interface. (The Switch 4000M and the Switch 2424M use the same OS.) To do so:

1. From the switch console Main Menu in the switch to receive the download, select **7. Download OS** screen.
2. Ensure that the **Method** parameter is set to **TFTP** (the default).
3. In the **TFTP Server** field, enter the IP address of the remote Switch 4000M or 2424M containing the OS you want to download.
4. Enter “os” for the **Remote File Name**. (Type “os” in lowercase characters.)
5. Press , then (for **eXecute**) to begin the OS download.
6. A “progress” bar indicates the progress of the download. When the entire operating system has been received, all activity on the switch halts and the following messages appear:

Validating and writing system software to FLASH...

Transfer completed

After the system flash memory has been updated with the new operating system, the switch reboots itself and begins running with the new operating system.

7. To confirm that the operating system downloaded correctly:
 - a. From the Main Menu, select

Status and Counters

General System Information

- b. Check the **Firmware revision** line.

Using Xmodem to Download the OS File

This procedure assumes that:

- The switch is connected via the Console RS-232 port on a PC operating as a terminal. (Refer to the Installation Guide you received with the switch for information on connecting a PC as a terminal and running the switch console interface.)
- The switch operating system (OS) is stored on a disk drive in the PC.
- The terminal emulator you are using includes the Xmodem binary transfer feature. (For example, in the Windows 3.1 terminal emulator, you would use the **Send Binary File** option in the **Transfers** dropdown menu.)

To Perform the OS Download:

1. From the console Main Menu, select
7. Download OS
2. Press **[E]** (for **Edit**).
3. Use the Space bar to select **XMODEM** in the **Method** field.
4. Press **[Enter]**, then **[X]** (for **eXecute**) to begin the OS download. The following message then appears:

**Press enter and then initiate Xmodem transfer
from the attached computer....**

5. Execute the terminal emulator command(s) to begin Xmodem binary transfer.

The download can take several minutes, depending on the baud rate used for the transfer.

6. When the download finishes, the switch automatically resets itself and begins running the new OS version.
7. To confirm that the operating system downloaded correctly:
 - a. From the Main Menu, select
1. Status and Counters
 - 1. General System Information**
 - b. Check the **Firmware revision** line.

Troubleshooting TFTP Downloads

If a TFTP download fails, the Download OS screen indicates the failure.

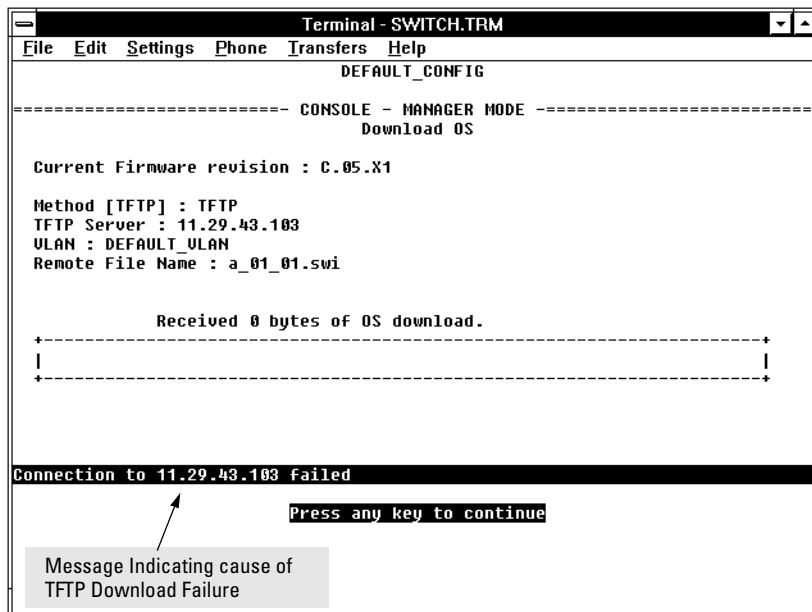


Figure A-3. Example of Message for Download Failure

To find more information on the cause of a download failure, examine the messages in the switch's Event Log. (See "Event Log" on page 8-12.)

Some of the causes of download failures include:

- Incorrect or unreachable address specified for the **TFTP Server** parameter. This may include network problems.
- Incorrect VLAN.
- Incorrect name specified for the **Remote File Name** parameter, or the specified file cannot be found on the TFTP server. This can also occur if the TFTP server is a Unix machine and the case (upper or lower) for the filename on the server does not match the case for the filename entered for the **Remote File Name** parameter in the Download OS screen.
- One or more of the switch's IP configuration parameters are incorrect.

- For a Unix TFTP server, the file permissions for the OS file do not allow the file to be copied.
- Another console session (through either a direct connection to a terminal device or through Telnet) was already running when you started the session in which the download was attempted.

Note

If an error occurs in which normal switch operation cannot be restored, the switch automatically reboots itself. In this case, an appropriate message is displayed in the copyright screen that appears after the switch reboots. You can display the same information by selecting the **Command Prompt** option from the Diagnostics menu and executing the History command.

Transferring Switch Configurations

You can use the following commands to transfer Switch 4000M and Switch 2424M configurations between the switch and a PC or Unix workstation.

Command	Function
Get	Download a switch configuration file from a networked PC or Unix workstation using TFTP.
Put	Upload a switch configuration to a file in a networked PC or Unix workstation using TFTP.
XGet	Uses an Xmodem-compatible terminal emulation program to download a switch configuration file from a PC or Unix workstation connected to the switch's console port.
XPut	Uses an Xmodem-compatible terminal emulation program to upload a switch configuration to a file in a PC or Unix workstation connected to the switch's console port.

Using Get and Put To Transfer a Configuration Between the Switch and a Networked PC or Unix Workstation

To use Get or Put, you need the following:

- The IP address of the remote PC or Unix workstation that is acting as a TFTP server
- The name assigned to the configuration file you will use on the remote PC or Unix workstation

Note

For the “Put” operation, most UNIX TFTP servers require that a file of the same name already exists in the server's TFTP directory, and that the file has “write” permissions.

Get or Xget overwrites the switch's current configuration with the downloaded configuration. The switch then automatically reboots itself.

-
1. From the Main Menu select

5. Diagnostics...

4. Command Prompt

2. At the command prompt, execute the following commands:

To upload a configuration to a file on a PC or Unix workstation:

put *IP_address* CONFIG *remote_file*

To download a configuration from a file on a PC or Unix workstation:

get *IP_address* CONFIG *remote_file*

where: ***IP address*** is the address of the PC or Unix workstation in which the configuration is stored (**get**) or is to be stored (**put**).

remote_file is the name of the configuration file in the PC or Unix workstation

Using XGet and XPut To Transfer a Configuration Between the Switch and a PC or Unix Workstation

The PC or workstation must be operating as a VT-100 or ANSI terminal and connected directly to the switch's console port. Also, the PC or workstation must be running an Xmodem-compatible terminal emulation program. If a manager password has been set, you must log on to the switch using that password in order to execute the Xget or Xput commands.

Note

XGet overwrites the switch's current configuration with the downloaded configuration. The switch then automatically reboots itself.

To use XGet or XPut, you need the name assigned to the configuration file on the PC or workstation.

1. On the PC or workstation, start the Xmodem-compatible terminal emulation program, then follow the instructions provided with the program to prepare for a file transfer.
2. From the switch's Main Menu select:

5. Diagnostics...

Command Prompt

3. At the command prompt, execute one of the following commands:

To upload a configuration to a file on a PC or Unix workstation:

xput config *remote_file* [pc/unix]

To download a configuration from a file on a PC or Unix workstation:

xget config *remote_file* [pc/unix]

where: ***remote_file*** is the name of the file in which the configuration is stored or is to be stored.

[pc/unix] is one of the following optional values:

unix (the default) specifies the Unix file format.

pc specifies the PC file format.

If the PC or workstation does not respond to an XPut or XGet command, the command times out and control returns to the **Command Prompt** line.

MAC Address Management

Overview

The switch assigns MAC addresses in these areas:

- For management functions:
 - One Base MAC address assigned to the switch
 - Additional MAC address(es) corresponding to any VLANs you configure in the switch
- For internal switch operations: One MAC address per port

MAC addresses are assigned at the factory. The switch automatically implements these addresses for VLANs and ports as they are added to the switch

Determining the MAC Addresses

You can use the switch console to determine the switch's base MAC address and the VLAN addresses (if any VLANs are configured on the switch), and the port MAC addresses for the switch. The methods are described in the rest of this appendix.

The Base and VLAN MAC Addresses

These addresses appear in the Management Address Information screen. Also, the Base MAC address appears on a label on the front of the switch.

Note

The Base MAC address is used by the first (default) VLAN in the switch. This is usually the VLAN named “DEFAULT_VLAN” unless the name has been changed (by using the VLAN Names screen).

To display (in hexadecimal format) the switch’s Base MAC address and the MAC Addresses Assigned to any VLANs Configured:

1. From the Main Menu, Select

1. **Status and Counters**

2. **Switch Management Address Information**

If multiple VLANs are not configured, this screen appears. If multiple VLANs are configured, each VLAN is listed with its corresponding address data.

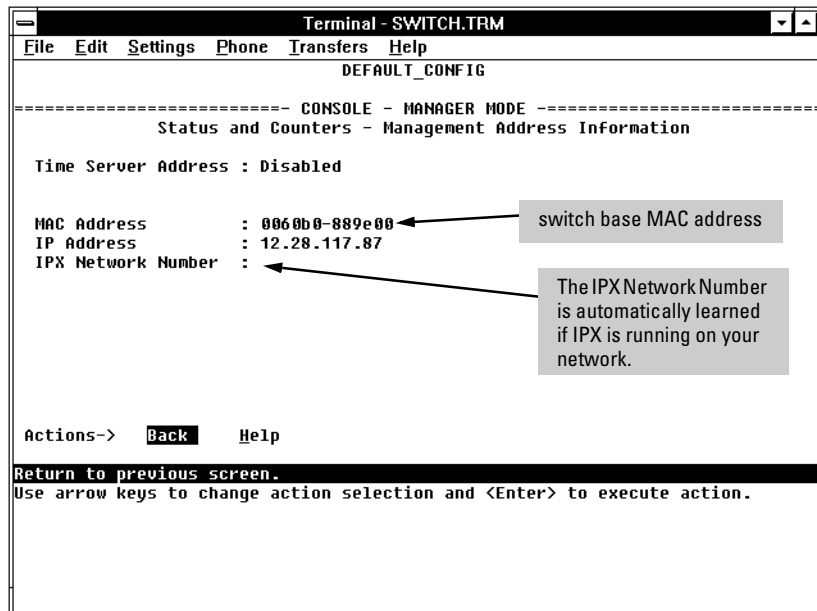


Figure B-1. Example of the Management Address Information Screen

Switch Port MAC Addresses

The MAC address assigned to each switch port is used internally by such features as Flow Control and the Spanning Tree Protocol. Determining the MAC address assignments for individual ports can sometimes be useful when diagnosing switch operation. To display these addresses, use the **walkmib** command at the command prompt

1. From the Main Menu, select **5. Diagnostics** and from the Diagnostics menu, select **4. Command Prompt**
2. If multiple VLANs are configured, use the Space bar to select a VLAN.

Note

This procedure displays the MAC addresses for all ports and existing VLANs in the switch, regardless of which VLAN you select.

3. Type the following command to display the MAC address for each port on the switch: **walkmib ifPhysAddress**

The following figure is an example of the display:

```

Terminal - SWITCH.TRM
File Edit Settings Phone Transfers Help
DEFAULT_CONFIG
----- CONSOLE - MANAGER MODE -----
ifPhysAddress.1 = 00 60 b0 88 9e 7f
ifPhysAddress.2 = 00 60 b0 88 9e 7e
ifPhysAddress.3 = 00 60 b0 88 9e 7d
ifPhysAddress.4 = 00 60 b0 88 9e 7c
ifPhysAddress.5 = 00 60 b0 88 9e 7b
ifPhysAddress.6 = 00 60 b0 88 9e 7a
ifPhysAddress.7 = 00 60 b0 88 9e 79
ifPhysAddress.8 = 00 60 b0 88 9e 78
ifPhysAddress.33 = 00 60 b0 88 9e 5f
ifPhysAddress.34 = 00 60 b0 88 9e 5e
ifPhysAddress.35 = 00 60 b0 88 9e 5d
ifPhysAddress.36 = 00 60 b0 88 9e 5c
ifPhysAddress.49 = 00 60 b0 88 9e 4f
ifPhysAddress.92 = 00 60 b0 88 9e 00
ifPhysAddress.93 = 00 60 b0 88 9e 01

VLAN_2: ← Command Prompt
  
```

ifPhysAddress.1 - 8: A1-A8 (10/100 module)
 ifPhysAddress.33 - 36: Ports E1-E4 (100FX module)
 ifPhysAddress.49 Port G-1 (Gigabit module)
 ifPhysAddress.92 Base MAC Address
 ifPhysAddress.93 MAC Address Assigned to VLAN_2

Figure B-2. Example of Port MAC Address Assignments on the Switch 4000M

Index

Numerics

- 802.1p priority (CoS)
 - definition ... 6-131
- 802.1q VLAN in mesh ... 6-91
- 802.1Q VLAN standard ... 6-3, 6-39
 - use with CoS, definition ... 6-131
- 802.2 ... 6-114
- 802.3u auto negotiation standard ... 6-30

A

- A.09.70 router release ... 6-69
- ABC ... 6-106
 - AppleTalk packets forwarded ... 6-117
 - broadcast limit, automatic ... 6-108, 6-110
 - configuration ... 4-17, 6-107–6-108, 6-112
 - console configuration ... 6-108
 - DECnet packets forwarded ... 6-117
 - edge switch proxy reply ... 6-92
 - enabled on edge switch ... 6-94
 - enabling from the command prompt ... 4-17
 - encapsulation type ... 6-114
 - example ... 6-113
 - gateway ... 8-6
 - gateway configuration ... 6-115
 - in switch mesh ... 6-88
 - IPX option ... 6-109
 - operation ... 6-113
 - proxy reply from mesh ... 6-92
 - reducing RIP/SAP traffic ... 6-115
 - restrictions ... 6-116
 - router ... 6-113
 - VLAN ... 6-108, 6-113
 - web browser interface ... 6-107
 - with IPX ... 6-117
 - with switch meshing ... 6-116
- access
 - manager ... 6-14
 - operator ... 6-14
- access level configuration tasks ... 1-3
- access levels, authorized IP managers ... 6-21
- Actions line ... 4-6–4-8
 - location on screen ... 4-6

- active button ... 3-15
- active path ... 6-39
- active tab ... 3-15
- address
 - authorized for port security ... 6-118
- address aging ... 6-28
- address resolution protocol ... 6-113
- address table, port ... 7-14
- address, manager ... 6-14, 6-16
- address, network manager ... 5-3
- alert log ... 3-15, 3-18–3-19
 - alert types ... 3-20
 - Control bar ... 3-15
 - disabling ... 3-28
 - header bar ... 3-15
 - setting the sensitivity level ... 3-27
 - showing security violations ... 6-125
 - sorting the entries ... 3-19
- analysis, traffic ... 5-1
- ANSI terminal ... A-9
- AppleTalk packets forwarded, ABC ... 6-117
- ARP ... 6-114
 - ARP statistics ... 7-21
 - ARP, proxy ... 6-114, 8-6
 - ARP, proxy response ... 6-113
- ASCII terminal ... 2-2
- asterisk ... 4-7
- authentication trap ... 6-17
- authorized addresses
 - for IP management security ... 6-22
 - for port security ... 6-118
- authorized IP managers
 - access levels ... 6-21
 - building IP masks ... 6-24
 - configuring in browser interface ... 6-23
 - configuring in console ... 6-23
 - definitions of single and multiple ... 6-22
 - effect of duplicate IP addresses ... 6-27
 - IP mask for multiple stations ... 6-25
 - IP mask for single station ... 6-25
 - IP mask operation ... 6-22
 - operating notes ... 6-27
 - overview ... 6-21
 - troubleshooting ... 6-27

Auto Gateway ... 6-115
Auto Gateway parameter ... 8-6
auto port setting ... 6-98
auto-discovery ... 5-4
automatic broadcast control
 See ABC
automatic gateway configuration ... 6-115
auto-negotiation ... 6-30

B

bandwidth
 displaying utilization ... 3-16
 effect of CoS ... 6-130
bandwidth savings, with ABC ... 6-106
bandwidth savings, with IGMP ... 6-101
bandwidth usage, filters ... 6-46
baud rate ... 4-2
blocked link from STP operation ... 6-44
blocked port
 from IGMP operation ... 6-98
 from STP operation ... 6-42
Bootp ... 5-1, 6-4, 6-9
 automatic switch configuration ... 2-2
 Bootp table file ... 6-11
 Bootptab file ... 6-10
 configuring ... 6-12
 effect of no reply ... 8-5
 using with Unix systems ... 6-10
Bootp/DHCP differences ... 6-10
Bootp/DHCP router option ... 6-116
broadcast ... 6-115
broadcast control ... 6-88
broadcast domain ... 6-51
broadcast limit ... 6-31–6-32, 6-108, 6-110
broadcast storm ... 6-3, 6-39, 6-55, 6-70, 6-82, 8-9
broadcast traffic ... 6-87, 6-115
broadcast traffic, IP/IPX ... 6-106
broadcast, restricting ... 6-30
browser interface
 See web browser interface
browsers ... 3-2
button bar ... 3-15

C

Class of Service
 basic operation ... 6-132

 configuring ... 6-135
 configuring in browser interface ... 6-137
 configuring in console ... 6-139
 configuring IP type of service ... 6-140, 6-144
 criteria for prioritizing outbound
 packets ... 6-133
 definitions of terms ... 6-131
 device priority screen ... 6-140
 diffserve configuration screen ... 6-144
 no override definition ... 6-135
 overview ... 6-130
 prioritizing traffic based on IP ToS field ... 6-143
 priority settings map to outbound
 queues ... 6-132
 priority settings mapped to downstream
 devices ... 6-133
 protocol priority screen ... 6-141
 ToS field, diffserve versus IP
 precedence ... 6-143
 type of service screen ... 6-140, 6-144
 using diffserve to prioritize packets ... 6-144
 using IP precedence to prioritize
 packets ... 6-144
 VLAN priority screen ... 6-142
Clear button ... 3-9
 restoring factory default configuration ... 8-24
 to delete password protection ... 4-11
command prompt ... 4-5, 4-14, 8-23
 for troubleshooting ... 8-23
 set commands ... 4-17
 show commands ... 4-18
command prompt, exit ... 4-14, 8-24
communities, SNMP ... 6-15
Community field ... 6-18
comparison, features ... 6-2
configuration ... 4-4, 6-42
 ABC ... 6-107–6-108
 activating ... 5-4
 Bootp ... 6-10, 6-12
 Class of Service ... 6-135
 console ... 6-19
 copying ... A-8
 DHCP, gateway ... 6-115
 DHCP/Bootp ... 2-2
 download ... A-1
 factory default ... 4-14, 6-1, 6-3, 6-39, 6-56, 8-23
 features ... 6-2
 IGMP from the console ... 6-98

- IP ... 2-2, 6-4
- IP address, manually ... 2-2
- mesh ... 6-84
- network monitoring ... 6-34
- port ... 6-30
- port security ... 6-119
- port trunk ... 6-71
- restoring factory defaults ... 8-24
- serial link ... 6-19
- SNMP ... 2-1, 5-3, 6-14
- spanning tree ... 6-39
- spanning tree protocol ... 6-42
- subnet mask ... 2-2
- switch management access ... 4-4
- system ... 6-28
- traffic/security filters ... 6-46
- transfer ... A-8
- transferring ... A-8
- trap receivers ... 6-17
- VLAN ... 6-51
- configuration file
 - browsing for troubleshooting ... 8-21
- connection inactivity time ... 4-9
- console ... 6-19, 8-5
 - ending a session ... 4-3
 - features ... 1-3
 - Main menu ... 4-4
 - navigation ... 4-6-4-7
 - operation ... 4-7
 - security violations ... 6-125
 - starting a session ... 4-2
 - status and counters access ... 4-4
 - switch management access configuration ... 4-4
 - troubleshooting access problems ... 8-3
- console, for configuring
 - ABC ... 6-108
 - authorized IP managers ... 6-23
 - Class of Service ... 6-139
 - IGMP ... 6-98
 - port security ... 6-123
 - STP ... 6-41
 - switch meshing ... 6-84
- control bar, alert log ... 3-15
- copyright screen ... 4-2
- CoS
 - See* Class of Service
- CPU utilization ... 7-5
- crash information ... 4-3

D

- date format ... 8-12
- date parameter ... 6-29
- DECnet packets forwarded, ABC ... 6-117
- default gateway ... 6-116
- DEFAULT_VLAN
 - See* VLAN
- Device Passwords Window ... 3-7
- device, managed ... 2-1
- DHCP ... 6-6, 6-9
 - address problems ... 8-5
 - automatic switch configuration ... 2-2
 - effect of no reply ... 8-5
 - gateway configuration ... 6-115
- DHCP/Bootp differences ... 6-10
- DHCP/Bootp process ... 6-9
- diagnostics tab ... 3-25
- diagnostics tools ... 8-17
 - browsing the configuration file ... 8-21
 - command prompt ... 8-23
 - ping and link tests ... 8-17
- differentiated services field
 - configuration screen ... 6-144
 - definition ... 6-144
- diffserve
 - See* differentiated services field
- disable IP address ... 6-4
- DNS name ... 3-4
- domain ... 6-56
- Domain Name Server ... 3-4
- domains, connecting ... 6-94
- down time ... 4-3
- download
 - configuration ... A-8
 - SNMP-based ... A-4
 - switch-to-switch ... A-4
 - troubleshooting ... A-6
 - Xmodem ... A-5
- download OS ... A-4
- download, TFTP ... A-1-A-2
- downstream device (CoS)
 - definition ... 6-131
 - effect of priority settings ... 6-133
- duplicate IP address
 - effect on authorized IP managers ... 6-27
- duplicate MAC address ... 6-68-6-69, 8-11

E

- eavesdrop prevention
 - port security configuration ... 6-119
- edge switch ... 6-92
- ending a console session ... 4-3
- event log ... 4-3, 4-5, 6-17, 8-12, 8-14
 - causes of erasure ... 8-14
 - navigation ... 8-13
 - severity level ... 6-20, 8-12
 - use during troubleshooting ... 8-12
- exiting from command prompt ... 4-14, 8-24
- extended RMON ... 5-4

F

- factory default configuration ... 6-3
 - restoring ... 8-24
- failure, OS download ... A-6
- Fast EtherChannel
 - See* FEC
- fast mode
 - spanning tree ... 6-43
- fault detection ... 3-7
- fault detection policy ... 3-7, 3-27
- fault detection policy, setting ... 3-27
- fault detection window ... 3-27
- fault-tolerance ... 6-71
- feature comparison ... 6-2
- FEC
 - benefits ... 6-79
- filters
 - effect of IGMP ... 6-49, 6-104
 - IGMP override ... 6-104
 - maximum allowed ... 6-104
 - multicast ... 6-49
 - protocol ... 6-50
 - RIP/SAP ... 6-88
 - source port ... 6-50
 - static ... 6-46
 - types ... 6-46
- firmware version ... 7-5
- flow control ... 6-31
- flow control, terminal ... 6-19
- format, date ... 8-12
- format, time ... 8-12
- forwarding port, IGMP ... 6-98

G

- gateway ... 6-6
- gateway (IP) address ... 6-4, 6-8
- gateway, client ... 6-115
- gateway, DHCP configuration ... 6-115
- Get command for file transfer ... A-8
- getmib ... 6-105
- graphs area, web browser interface ... 3-15

H

- header bar, alert log ... 3-15
- Help ... 3-10, 4-8
- Help line, about ... 4-6
- Help line, location on screens ... 4-6
- help, online inoperable ... 3-10
- History command ... A-7
- hop count, mesh switch ... 6-92
- host-only ... 6-68
- HP extended RMON ... 5-4
- HP ProCurve
 - support URL ... 3-12
- HP proprietary MIB ... 5-2
- HP Router 440 ... 6-69
- HP Router 470 ... 6-69
- HP Router 480 ... 6-69
- HP Router 650 ... 6-69
- HP TopTools
 - See* TopTools
- HP web browser interface ... 1-2

I

- IEEE 802.1 standard ... 6-91
- IEEE 802.1d ... 6-39, 6-41, 8-9
- IGMP
 - benefits ... 6-95
 - configuration ... 6-96
 - configuration from console ... 6-98
 - configure per VLAN ... 6-98
 - console configuration ... 6-98
 - effect on filters ... 6-49, 6-104
 - enabling from the command prompt ... 4-17
 - example ... 6-101–6-102
 - filter override ... 6-104
 - high priority forwarding ... 6-99
 - high-priority forwarding ... 6-98
 - host not receiving ... 8-7

- in switch mesh domain ... 6-91
 - IP address required ... 6-95
 - IP multicast address range ... 6-49, 6-104
 - leave group ... 6-100
 - maximum address count ... 6-104
 - multicast group ... 6-100, 6-103
 - multimedia ... 6-95
 - not working ... 8-7
 - operation ... 6-100
 - port states ... 6-98
 - querier setting, changing ... 6-105
 - query ... 6-100
 - report ... 6-100
 - statistics ... 7-19
 - status ... 6-100
 - traffic ... 6-98
 - in-band ... 2-1
 - in-band security ... 6-46
 - inbound port (CoS)
 - definition ... 6-131
 - Inbound Telnet Enabled parameter ... 8-4
 - interfaces listed ... 1-1
 - intrusion alarms
 - reading and resetting ... 6-125
 - IP
 - address for IGMP ... 6-95
 - address for mesh switch ... 6-89
 - address function ... 2-1
 - authorized IP managers ... 6-21
 - broadcast traffic reduction with ABC ... 6-106
 - configuration ... 6-4
 - DHCP/Bootp ... 6-4
 - disable ... 6-4
 - duplicate address ... 8-5
 - duplicate address, DHCP network ... 8-5
 - effect when address not used ... 6-8
 - gateway ... 6-6
 - gateway (IP) address ... 6-4
 - global assignment ... 6-13
 - globally assigned addressing ... 6-13
 - subnet mask ... 6-4, 6-7
 - traffic priority based on ToS field ... 6-143
 - using for web browser interface ... 3-4
 - VLAN ... 6-4
 - web browser interface ... 6-5–6-6
 - IP address
 - See* IP
 - IP host-only ... 6-68
 - IP masks
 - building ... 6-24
 - for multiple authorized manager stations ... 6-25
 - for single authorized manager station ... 6-25
 - operation ... 6-22
 - IP precedence field
 - used for prioritizing packets ... 6-144
 - IP, for SNMP ... 5-1
 - IP, type of service
 - configuring priority ... 6-140, 6-144
 - IPX
 - 802.2 to SNAP ... 6-117
 - broadcast traffic ... 6-106
 - encapsulation type ... 6-117
 - network number ... 7-6, B-2
 - proxy reply ... 6-117
 - proxy response ... 6-117
- J**
- Java ... 3-3–3-4
- L**
- latency ... 6-113
 - reducing with ABC ... 6-106
 - reducing with switch meshing ... 6-89
 - layer 3
 - See* ABC
 - learning bridge ... 6-1
 - leave group
 - See* IGMP
 - legacy VLAN ... 6-53
 - link failure ... 6-80
 - link speed, port trunk ... 6-71
 - link status, port ... 7-10
 - link test ... 8-17
 - for troubleshooting ... 8-17
 - link, redundant ... 6-3
 - link, serial ... 6-19
 - links, multiple in mesh ... 6-94
 - load balancing
 - See* port trunk
 - loop, network ... 6-39, 6-42, 6-55, 6-70
 - lost password ... 3-9

M

- MAC address ... 6-10, 7-5, B-1
 - duplicate ... 6-68–6-69, 8-9, 8-11
 - learned ... 7-14
 - port ... 7-15, B-1–B-2
 - switch ... B-1
 - VLAN ... 6-67, B-1
 - Main menu, console ... 4-4
 - managed device ... 2-1
 - management
 - access configuration from console ... 4-4
 - interfaces described ... 1-1
 - server URL ... 3-12–3-13
 - server URL default ... 3-10
 - manager access ... 6-14
 - manager address ... 6-14, 6-16
 - Manager Address field ... 5-3
 - manager password ... 3-8–3-9, 4-9, 4-11
 - Manual, IP address ... 6-7
 - media type, port trunk ... 6-71
 - mesh
 - ABC on edge switches ... 6-94
 - ABC proxy reply ... 6-92
 - benefits ... 6-80
 - blocked ports ... 6-83
 - broadcast control ... 6-88
 - broadcast storm ... 6-82
 - broadcast traffic ... 6-87
 - broadcast tree ... 6-88
 - configuration ... 6-84
 - configuring from the console ... 6-84
 - connecting domains ... 6-94
 - connecting multiple domains ... 6-82
 - domain ... 6-81
 - edge switch ... 6-82, 6-87, 6-92
 - filtering ... 6-91
 - hop count ... 6-92
 - hub not allowed ... 6-82
 - increase STP cost ... 6-90
 - IP address ... 6-89
 - link blocked ... 6-90
 - link to non-mesh switch ... 6-89
 - links, multiple ... 6-94
 - maximum domain size ... 6-92
 - maximum ports ... 6-92
 - multicast traffic ... 6-87
 - multiple mesh domains ... 6-90
 - multiple VLANs ... 6-88
 - no Type selection ... 6-94
 - operating details ... 6-87
 - operating notes ... 6-87
 - port trunk ... 6-94
 - port types ... 6-80
 - problems ... 8-7
 - proxy reply not sent ... 6-94
 - redundant link ... 6-90
 - redundant paths ... 6-81
 - spanning tree ... 6-89, 8-9
 - STP operation ... 6-45
 - switch hop count ... 6-93
 - Type setting ... 6-86
 - unicast ... 6-88
 - utilization ... 6-87
 - VLAN ... 6-67, 6-91
 - VLAN requirement ... 6-83
 - when ABC used ... 6-116
 - with IGMP ... 6-91
 - with network monitor port ... 6-94
 - message, system down ... 4-3
 - MIB ... 5-2, 6-105
 - MIB listing ... 5-2
 - MIB, HP proprietary ... 5-2
 - MIB, standard ... 5-2
 - Microsoft Internet Explorer ... 3-3
 - Monitor parameter ... 6-37
 - monitoring a VLAN ... 6-38
 - monitoring traffic ... 6-34
 - monitoring, traffic ... 5-1
 - multicast address, spanning tree protocol ... 6-50
 - multicast filter ... 6-46, 6-49
 - multicast group
 - See* IGMP
 - multicast traffic ... 6-87
 - multimedia
 - See* IGMP
 - multiple VLAN ... 5-1
 - multi-port bridge ... 6-1
- ## N
- navigation, console interface ... 4-6–4-7
 - navigation, event log ... 8-14
 - Netscape ... 3-3
 - network management functions ... 5-4
 - network manager address ... 5-3
 - network monitoring

- traffic overload ... 6-34
- VLAN monitoring parameter ... 6-38
- Network Monitoring Port screen ... 6-34
- network slow ... 8-5
- notes on using VLANs ... 6-54
- NSQ reply, proxy ... 6-108
- NSQ request ... 6-114
- NSQ statistics ... 7-21

O

- online help ... 3-10
- online help location ... 3-13
- operating notes
 - authorized IP managers ... 6-27
 - port security ... 6-129
 - switch meshing ... 6-87
- operator access ... 6-14
- operator mode ... 4-10
- operator password ... 3-8–3-9, 4-9, 4-11
- OS
 - version ... A-3–A-5
- OS download
 - effect on event log ... 8-14
 - failure indication ... A-6
 - switch-to-switch download ... A-4
 - troubleshooting ... A-6
 - using TFTP ... A-2
- outbound port (CoS)
 - definition ... 6-131
- outbound port queue (CoS)
 - definition ... 6-131
- out-of-band ... 1-3
- Overview window
 - active button ... 3-15
 - active tab ... 3-15
 - alert log ... 3-15
 - alert log control bar ... 3-15
 - alert log header bar ... 3-15
 - button bar ... 3-15
 - graphs area ... 3-15
 - Status bar ... 3-15

P

- password ... 3-7, 3-9, 4-2
 - browser/console access ... 4-9
 - case-sensitive ... 4-11

- creating ... 3-8
- delete ... 3-9, 4-11
- deleting with the Clear button ... 4-11
- if you lose the password ... 3-9, 4-11
- incorrect ... 4-10
- length ... 4-11
- lost ... 3-9
- manager ... 3-8
- operator ... 3-8
- setting ... 3-8, 4-10
- using to access browser and console ... 3-9
- path cost ... 6-42
- ping test ... 8-17
 - for troubleshooting ... 8-17
- port
 - address table ... 7-14
 - Address Table screen ... 6-69
 - auto, IGMP ... 6-98
 - auto-negotiation ... 6-30
 - blocked by STP operation ... 6-42
 - blocked in mesh ... 6-83
 - blocked, IGMP ... 6-98
 - cost
 - See* spanning tree protocol.
 - counters ... 7-10
 - counters, reset ... 7-10
 - enabling from the command prompt ... 4-17
 - forwarding, IGMP ... 6-98
 - MAC address ... B-2–B-3
 - monitoring ... 6-67
 - monitoring, VLAN ... 6-35
 - numbering ... 6-30
 - security configuration ... 6-118
 - state, IGMP control ... 6-98
 - traffic patterns ... 7-10
 - utilization ... 3-16
 - web browser interface ... 3-16
- port security
 - authorized address definition ... 6-118
 - basic operation ... 6-118
 - configuring ... 6-119
 - configuring in browser interface ... 6-121
 - configuring in console ... 6-123
 - eavesdrop prevention definition ... 6-119
 - notice of security violations ... 6-125
 - operating notes ... 6-129
 - overview ... 6-118
 - reading and resetting intrusion alarms ... 6-125

- resetting the alert flag ... 6-128
 - security violations in browser alert log ... 6-125
- port trunk ... 6-70
 - configuration ... 6-71
 - FEC ... 6-79
 - interoperation ... 6-72
 - limit ... 6-70
 - media type ... 6-71
 - meshed switch ... 6-94
 - network management ... 6-71
 - SA/DA ... 6-77
 - SA-trunk ... 6-78
 - spanning tree protocol ... 6-71
 - VLAN ... 6-67, 6-71
- port, maximum for mesh ... 6-92
- power interruption, effect on event log ... 8-14
- precedence bits (CoS)
 - definition ... 6-131
- priority ... 6-98
 - See* spanning tree
- priority (CoS)
 - criteria for prioritizing packets ... 6-133
 - device priority screen ... 6-140
 - protocol priority screen ... 6-141
 - type of service screen ... 6-140, 6-144
 - VLAN priority screen ... 6-142
- proprietary MIB ... 5-2
- protocol filters ... 6-50
- protocol priority (CoS)
 - configuring ... 6-141
- proxy ARP ... 6-114, 8-6
- proxy NSQ reply ... 6-108
- proxy replies ... 6-88
- proxy reply ... 6-115
- proxy reply, IPX ... 6-117
- proxy reply, not sent ... 6-94
- proxy response to ARP ... 6-113
- proxy response, IPX ... 6-117
- public SNMP community ... 5-3–5-4
- Put command for file transfers ... A-8

Q

- querier ... 6-105
- query
 - See* IGMP

R

- reboot ... 4-5, 4-7, 4-12, 5-4
- reconfigure ... 4-7
- redundant link ... 6-3, 6-90
- redundant link, non-meshed ... 6-89
- redundant links ... 6-82
- redundant path ... 6-39, 6-42
 - spanning tree ... 6-39
- report
 - See* IGMP
- reset ... 4-12
- Reset button
 - effect on event log ... 8-14
 - restoring factory default configuration ... 8-24
- reset port counters ... 7-10
- resetting the switch
 - factory default reset ... 8-24
- restricted access ... 6-14
- restricted write access ... 6-14
- RFC
 - See* MIB
 - RFC 1213 ... 5-2
 - RFC 1493 ... 5-2
 - RFC 1515 ... 5-2
 - RFC 1573 ... 5-2
 - RFC 1757 ... 5-2
 - RFC 2132 ... 6-116
- RIP ... 6-115
- RIP statistics ... 7-21
- RIP/SAP filtering ... 6-88
- RMON ... 5-1
- RMON groups supported ... 5-4
- router ... 6-69, 6-100
 - gateway ... 6-8
- router release A.09.70 ... 6-69
- router, Bootp/DHCP ... 6-116
- router, with ABC enabled ... 6-115
- RS-232 ... 1-3

S

- SAP ... 6-115
- SAP statistics ... 7-21
- SAP table ... 6-117
- security ... 3-9
 - authorized IP managers ... 6-21
 - per port ... 6-118
- security filters ... 6-46

- security violations
 - notices of ... 6-125
 - resetting ... 6-128
- security, in-band ... 6-46
- Self Test LED
 - behavior during factory default reset ... 8-24
- send authentication traps ... 6-18
- Serial Link Configuration screen ... 6-19
- serial number ... 7-5
- server
 - DHCP/Bootp ... 6-6
 - effect of ABC on server access ... 8-6
 - TFTP ... A-8
 - Timep ... 6-7
- set commands ... 4-17
- setmib ... 6-105
- setting a password ... 4-10
- setting fault detection policy ... 3-27
- severity code, event log ... 8-12
- show commands ... 4-18
- slow network ... 8-5
- SNAP ... 6-114
- SNMP ... 5-1
 - communities ... 5-3, 6-14–6-15
 - Communities screen ... 6-14
 - community
 - configure ... 5-3
 - IP ... 5-1
 - manager address ... 6-14, 6-16
 - public community ... 5-4, 6-14
 - restricted access ... 6-14
 - traps ... 5-1
 - v1 agent ... 5-2
- SNMP-based download ... A-4
- software version ... 7-5
- sorting alert log entries ... 3-19
- source port filter ... 6-46
- source port filters ... 6-50
- spanning tree ... 6-39
 - blocked link ... 6-44
 - blocked port ... 6-42
 - blocking in VLANs ... 6-3
 - causing duplicate MAC address ... 6-68
 - caution about filtering ... 6-50
 - configuring from the command prompt ... 4-17
 - configuring from the console ... 6-41
 - description of operation ... 6-42
 - enabling from the browser interface ... 6-40
 - fast mode ... 6-43
 - global information ... 7-17
 - information screen ... 7-17
 - link priority ... 6-39, 6-91
 - operating with switch meshing ... 6-45
 - operation with switch meshing ... 6-89
 - port cost ... 6-42
 - port priority automatic setting ... 6-42
 - problems related to ... 8-9
 - statistics ... 7-17
 - using with port trunking ... 6-71
 - VLAN effect on ... 6-66
- standard MIB ... 5-2
- starting a console session ... 4-2
- static filter limit ... 6-46
- statistical sampling ... 5-1
- statistics ... 4-4, 7-2
- statistics, clear counters ... 4-12
- status and counters
 - access from console ... 4-4
- status and counters menu ... 7-3
- Status bar ... 3-15
- status overview screen ... 3-5
- STP
 - cost change by mesh switch ... 6-90
 - switch mesh ... 8-9
- subnet ... 6-100
- subnet address ... 6-51
- subnet mask ... 2-3, 6-4, 6-6–6-7
 - See also* IP
- subnetting, multiple ... 6-106
- Sun workstation ... 6-68
- support
 - changing default URL ... 3-12
 - URL ... 3-12
 - URL Window ... 3-12
- support/mgmt URLs ... 3-24
- switch console
 - See* console
- switch management
 - access configuration ... 4-4
- switch meshing
 - See* mesh
- switch-to-switch download ... A-4
- system configuration screen ... 6-28
- system down ... 4-3
- system name
 - when none is specified ... 4-14, 8-23

System Name parameter ... 6-29

T

Tab bar, web browser interface ... 3-15

tagged VLAN

See VLAN

Telnet ... 4-2

Telnet, problem ... 8-4

terminal type ... 6-19

terminal, ANSI ... A-9

terminal, VT-100 ... A-9

TFTP

download ... A-1–A-2

OS download ... A-2

server ... A-8

threshold setting ... 5-4

time command, how to enter ... 4-14, 8-24

time format ... 8-12

time parameter ... 6-28

Time Protocol Enabled ... 6-29

Time Protocol parameter ... 6-7

time server ... 6-4

Timep ... 6-4, 6-7

Timep Poll Interval ... 6-7

Timep Server ... 6-7

TopTools ... 1-4

TopTools access ... 3-4

TopTools system requirements ... 3-3

TopTools, main screen ... 1-4

traffic analysis ... 5-1

traffic monitoring ... 5-1, 5-4

traffic, monitoring ... 6-34

traffic, port ... 7-10

trap ... 3-28, 6-17

authentication trap ... 6-17

event levels ... 6-18

limit ... 6-17

SNMP ... 6-17

Trap Receivers Configuration screen ... 6-17

trap receiver ... 5-3–5-4

troubleshooting ... 7-1

approaches ... 8-2

authorized IP managers ... 6-27

browsing the configuration file ... 8-21

command prompt ... 8-23

console access problems ... 8-3

diagnosing unusual network activity ... 8-5

diagnostics tools ... 8-17

OS download ... A-6

ping and link tests ... 8-17

restoring factory default configuration ... 8-24

unusual network activity ... 8-5

using the event log ... 8-12

web browser access problems ... 8-3

trunk

See port trunk

Type of Service

using to prioritize IP traffic ... 6-143

Type of Service field (IP)

configuring packet priority ... 6-140, 6-144

diffserve versus IP precedence ... 6-143

how the switch uses it ... 6-145

Type, meshed port ... 6-86

types of alert log entries ... 3-20

U

unauthorized access ... 6-17

unicast in switch mesh ... 6-88

Universal Resource Locator

See URL

Unix, Bootp ... 6-10

unrestricted write access ... 6-14

unusual network activity ... 8-5

up time ... 7-5

upload configuration ... A-8

upstream device (CoS)

definition ... 6-131

URL ... 3-10

browser interface online help location ... 3-13

HP ProCurve ... 3-12

management ... 3-13

management server ... 3-12–3-13

online help ... 3-13

support ... 3-12

URL, support/mgmt ... 3-24

user name, using for browser or console

access ... 3-8–3-9

using the passwords ... 3-9

utilization, port ... 3-16

V

version, OS ... A-3–A-5

VLAN ... 6-4, 6-37–6-38, 6-51, 6-66–6-69, 8-11, B-1

- 802.1Q ... 6-44
- ABC ... 6-108–6-109, 6-113
- address ... 5-1
- Bootp ... 6-10
- Bootp or DHCP ... 6-9
- configuring Bootp ... 6-10
- default ... 2-2
- DEFAULT_VLAN ... 2-2, 6-54, 6-56
- deleting ... 6-68
- device not seen ... 8-10
- effect on spanning tree ... 6-66
- event log entries ... 8-12
- IGMP configuration ... 6-98
- IP address ... 2-2, 6-4
- IPX with ABC configured ... 6-117
- limit ... 6-56
- link blocked ... 8-10
- MAC address ... 6-67
- mesh ... 6-67
- mesh domain ... 6-45
- monitoring ... 6-35, 6-38
- multiple ... 5-1
- multiple in switch mesh ... 6-88
- multiple VLANs on port ... 6-64
- network monitoring ... 6-34
- notes on using ... 6-54
- OS download ... A-2
- port assignment ... 6-60
- port configuration ... 6-65, 8-10
- port monitoring ... 6-67
- port trunk ... 6-67, 6-71
- prioritizing traffic from with CoS ... 6-142
- reboot ... 6-57
- required for mesh ... 6-83–6-84
- restrictions ... 6-68
- source port filters ... 6-50
- spanning tree operation ... 6-44
- Switch 2000 ... 6-66
- Switch 800T ... 6-66
- switch capacity ... 6-51
- switch mesh ... 6-82
- tagged ... 6-52
- tagging ... 6-62, 6-64
- tagging broadcast, multicast, and unicast traffic ... 8-10
- untagged ... 6-53, 6-61
- VLAN ID ... 6-64
- VT-100 terminal ... 2-2, 6-19, A-9

W

- warranty ... ii
- web agent enabled ... 3-1
- web agent,
 - advantages ... 1-2
- web browser interface
 - access parameters ... 3-7
 - active button ... 3-15
 - active tab ... 3-15
 - alert log ... 3-5, 3-15, 3-18–3-19
 - alert log control ... 3-22
 - alert log control bar ... 3-15
 - alert log details ... 3-21
 - alert log header bar ... 3-15
 - alert types ... 3-20
 - bandwidth adjustment ... 3-17
 - bar graph adjustment ... 3-17
 - Button bar ... 3-15
 - button bar ... 3-15
 - configuration tab ... 3-24
 - configuration, support URL ... 3-10
 - diagnostics tab ... 3-25
 - disable access ... 3-1
 - enabling ... 3-3
 - error packets ... 3-16
 - fault detection policy ... 3-7, 3-27
 - fault detection window ... 3-27
 - features ... 1-2
 - first-time install ... 3-6
 - first-time tasks ... 3-6
 - graphs area ... 3-15
 - help via TopTools ... 3-10
 - identity tab ... 3-23
 - main screen ... 3-14
 - management server URL ... 3-10
 - online help ... 3-10
 - online help location specifying ... 3-13
 - online help, inoperable ... 3-10
 - overview ... 3-14
 - Overview window ... 3-14
 - password lost ... 3-9
 - password, setting ... 3-8
 - port status ... 3-18
 - port utilization ... 3-16
 - port utilization and status displays ... 3-16
 - screen elements ... 3-14
 - screen layout ... 3-14
 - security ... 3-1, 3-7

- security tab ... 3-25
- showing security violations ... 6-125
- standalone ... 3-3
- Status bar ... 3-15
- status bar ... 3-26
- status indicators ... 3-26
- status overview screen ... 3-5
- status tab ... 3-23
- support tab ... 3-26
- system requirements ... 3-2-3-3
- troubleshooting access problems ... 8-3
- URL default ... 3-10
- URL, management server ... 3-11
- URL, support ... 3-11
- web browser interface, for configuring
 - ABC ... 6-107
 - authorized IP managers ... 6-23
 - Class of Service ... 6-137
 - IGMP ... 6-96
 - port security ... 6-121
 - STP ... 6-40
- web site, HP ... 5-2
- world wide web site, HP
 - See* HP ProCurve
- write access ... 6-14

X

- Xmodem OS download ... A-5
- XNS ... 6-68
- XPut ... A-8

Technical information in this document
is subject to change without notice.

©Copyright Hewlett-Packard Company
1999. All rights reserved. Reproduction,
adaptation, or translation without prior
written permission is prohibited except
as allowed under the copyright laws.

Printed in Singapore 9/99

Manual Part Number
5969-2320

