
HP ProCurve Switch 1600M and
HP ProCurve Switch 8000M

Management and Configuration Guide

© Copyright 1998 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

5967-2142
June 1998

Applicable Product

HP J4110A, HP J4120A

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. EtherChannel is a registered trademark of Cisco Systems, Inc. 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

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 Switch 1600M and Switch 8000M Documentation

This guide describes how to use the browser interface and console interface for the HP ProCurve Switch 1600M and HP ProCurve Switch 8000M (hereafter referred to as the “Switch 1600M and Switch 8000M”).

- If you need information on specific parameters in the console interface, refer to the online help provided in the console 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 3-9.
- If you need further information on Hewlett-Packard switch technology, refer to HP’s Network City website at:

http://www.hp.com/go/network_city

Contents

1 Selecting a Management Interface

| | |
|--|-----|
| Understanding Management Interfaces | 1-1 |
| Advantages of Using the HP Web Browser Interface | 1-3 |
| Advantages of Using the Console Interface | 1-4 |
| HP TopTools for Hubs and Switches | 1-5 |

2 Configure an IP Address on the Switch

| | |
|--|-----|
| Methods for Configuring an IP Address and Subnet Mask | 2-2 |
| Manually Configuring an IP Address | 2-3 |
| Where To Go From Here | 2-5 |

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 | 3-5 |
| Viewing the “First Time Install” Window | 3-6 |
| Creating Usernames and Passwords in the Browser Interface | 3-7 |
| Using the Passwords | 3-8 |
| Using the User Names | 3-8 |
| If You Lose a Password | 3-8 |
| Online Help for the HP Web Browser Interface | 3-9 |
| The Web Browser Interface Screen Layout | 3-11 |
| The Overview Window | 3-11 |
| The Port Utilization and Status Displays | 3-12 |
| Port Utilization | 3-13 |
| Port Status | 3-14 |

| | |
|---|------|
| The Alert Log | 3-14 |
| Sorting the Alert Log Entries | 3-15 |
| Alert Types | 3-16 |
| Viewing Detail Views of Alert Log Entries | 3-17 |
| The Alert Control Bar | 3-18 |
| The Tab Bar | 3-19 |
| Identity Tab | 3-19 |
| Status Tab | 3-19 |
| Configuration Tab | 3-20 |
| Security Tab | 3-21 |
| Diagnostics Tab | 3-21 |
| The Support Tab | 3-21 |
| The Status Bar | 3-22 |
| Setting Fault Detection Policy | 3-23 |
| Working With Fault Detection | 3-23 |

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 | 4-5 |
| Using Password Security | 4-9 |
| To set Manager and Operator passwords: | 4-10 |
| Rebooting the Switch | 4-13 |
| The Command Prompt | 4-15 |

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

| | |
|---|-----|
| SNMP Management Features | 5-1 |
| SNMP Configuration Process | 5-3 |

6 Configuring the Switch

| | |
|--|------|
| Overview | 6-1 |
| Configuration Features | 6-2 |
| Support URLs Feature | 6-4 |
| Support URL | 6-4 |
| Management Server URL | 6-5 |
| IP Configuration | 6-6 |
| Configuring IP Addressing Parameters from the Web Browser Interface 6-7 | |
| Configuring IP Addressing Parameters from the Switch Console ... | 6-8 |
| To Access IP Addressing: | 6-9 |
| How IP Addressing Affects Switch Operation | 6-10 |
| DHCP/Bootp Operation | 6-10 |
| Overview | 6-10 |
| The DHCP/Bootp Process | 6-11 |
| Configuring DHCP/Bootp | 6-13 |
| Globally Assigned IP Network Addresses | 6-14 |
| SNMP Communities | 6-15 |
| Configuring SNMP Communities from the Switch Console | 6-15 |
| To View, Edit, or Add SNMP Communities: | 6-16 |
| Trap Receivers | 6-18 |
| Configuring SNMP Communities from the Console | 6-18 |
| To Access Trap Receivers: | 6-18 |
| Console/Serial Link | 6-20 |
| Using the Switch Console To Configure the Console/Serial Link ... | 6-21 |
| To Access Console/Serial Link Features | 6-21 |
| System Information | 6-22 |
| Configuring System Parameters from the Web Browser Interface . | 6-22 |
| Configuring System Information from the Console | 6-23 |
| To Access System Information: | 6-23 |
| Port Settings | 6-24 |
| Configuring Port Parameters from the Web Browser Interface | 6-25 |
| Configuring Port Parameters from the Switch Console | 6-27 |
| To Access IP Addressing: | 6-27 |

| | |
|---|------|
| Network Monitoring Port Features | 6-29 |
| Configuring Port Monitoring from the Web Browser Interface | 6-29 |
| Configuring Port Monitoring from the Switch Console | 6-31 |
| To Access Port Monitoring: | 6-31 |
| Spanning Tree Protocol (STP) | 6-34 |
| Configuring STP from the Web Browser Interface | 6-35 |
| Using the Switch Console To Configure STP | 6-36 |
| To Access STP: | 6-36 |
| How STP Operates | 6-37 |
| STP Operation with 802.1Q VLANs | 6-38 |
| STP Operation with Switch Meshing | 6-38 |
| Further Information | 6-39 |
| Traffic/Security Filter Features | 6-40 |
| Configuring Port Monitoring from the Switch Console | 6-40 |
| To Access Traffic/Security Filters | 6-40 |
| Filter Types and Operation | 6-43 |
| Multicast Filters | 6-43 |
| Protocol Filters | 6-44 |
| Source Port Filters | 6-44 |
| Port-Based Virtual LANs (VLANs) | 6-45 |
| Overview of Using VLANs | 6-48 |
| VLAN Support and the Default VLAN | 6-48 |
| Further Information | 6-49 |
| Using the Switch Console To Configure VLAN Parameters | 6-49 |
| To Activate or De-Activate VLANs | 6-50 |
| To Activate VLANs: | 6-50 |
| How To Create or Edit a VLAN. | 6-52 |
| To Add or Remove a Port VLAN Assignment | 6-54 |
| Further VLAN Operating Information | 6-56 |
| VLAN Tagging | 6-56 |
| Effect of VLANs on Other Switch Features | 6-60 |
| Spanning Tree Protocol Operation with VLANs | 6-60 |
| IPX and IP Interfaces. | 6-61 |
| VLAN MAC Addresses | 6-61 |
| Port Trunks | 6-61 |
| Port Monitoring | 6-61 |
| VLANs and Switch Meshing | 6-61 |
| VLAN Restrictions | 6-62 |
| Symptoms of Duplicate MAC Addresses in VLAN Environments | 6-63 |

| | |
|--|------|
| Load Balancing: Port Trunking | 6-64 |
| Interoperability | 6-66 |
| Trunk Configuration Options | 6-66 |
| Using the Console To Configure Port Trunks | 6-67 |
| To Access Port Trunking: | 6-67 |
| Operating Information | 6-70 |
| Trunk Operation Using the Trunk (Source Address/Destination Address, or SA/DA) Option | 6-71 |
| Trunk Operation Using the SA-Trunk (Source-Address Distribution) Option | 6-72 |
| Trunk Operation Using the FEC (Fast EtherChannel®) Option | 6-72 |
| Load Balancing: Switch Meshing | 6-74 |
| Switch Meshing Fundamentals | 6-75 |
| Using the Console To Configure Switch Meshing | 6-78 |
| To Access Switch Meshing | 6-78 |
| Operating Notes for Switch Meshing | 6-81 |
| Flooded Traffic | 6-81 |
| Unicast Packets with Unknown Destinations | 6-82 |
| Spanning Tree Operation with Switch Meshing | 6-83 |
| Filtering/Security in Meshed Switches | 6-85 |
| IP Multicast (IGMP) in Meshed Switches | 6-85 |
| 802.1Q VLANs in Meshed Switches. | 6-85 |
| Using Automatic Broadcast Control in a Switch Mesh Environment | 6-86 |
| Requirements and Restrictions | 6-86 |
| IP Multicast (IGMP) Service Features—Multimedia Traffic Control | 6-89 |
| Configuring IGMP from the Web Browser Interface | 6-90 |
| Using the Switch Console To Configure IGMP | 6-92 |
| To Access IGMP Service: | 6-93 |
| How IGMP Operates | 6-94 |
| Role of the Switch | 6-94 |
| Number of IP Multicast Addresses Allowed | 6-98 |
| Interaction with Multicast Traffic/Security Filters. | 6-98 |
| Changing the Querier Configuration Setting | 6-98 |

| | |
|---|-------|
| Automatic Broadcast Control (ABC) Features—Layer 3 Switching | 6-100 |
| Using the HP Web Browser Interface To Configure | |
| ABC Parameters | 6-101 |
| Using the Switch Console To Configure ABC Parameters | 6-102 |
| To Access ABC: | 6-104 |
| How ABC Operates | 6-107 |
| Reducing ARP Broadcast Traffic | 6-108 |
| Reducing RIP and SAP Broadcast Traffic | 6-109 |
| Automatic Gateway Configuration for Networks Using DHCP To | |
| Manage IP Addresses. | 6-110 |
| Restrictions | 6-111 |

7 Monitoring and Analyzing Switch Operation

| | |
|---|------|
| Overview | 7-1 |
| Status and Counter Screens | 7-2 |
| General System Information | 7-4 |
| Switch Management Address Information | 7-5 |
| Module Information | 7-6 |
| Port Status | 7-7 |
| Displaying Port Status from the Web Browser Interface | 7-7 |
| Displaying Port Status from the Console Interface | 7-8 |
| Port Counters | 7-9 |
| Displaying Port Counters from the Web Browser Interface | 7-10 |
| Displaying Port Counters from the Console Interface | 7-11 |
| Address Table | 7-13 |
| Port Address Table | 7-14 |
| Spanning Tree (STP) Information | 7-16 |
| IP Multicast (IGMP) Status | 7-18 |
| Automatic Broadcast Control (ABC) Information | 7-20 |
| Switch Mesh Information | 7-21 |
| VLAN Information | 7-22 |
| Diagnostics | 7-23 |
| Ping and Link Tests | 7-23 |
| Executing Ping or Link Tests from the Web Browser Interface | 7-24 |
| Executing Ping or Link Tests from the Console Interface | 7-25 |
| Browse Configuration File | 7-27 |
| Using the Command Prompt | 7-28 |

8 Troubleshooting

| | |
|--|------|
| Troubleshooting Approaches | 8-2 |
| Browser or Console Interface Problems | 8-3 |
| Unusual Network Activity | 8-3 |
| General Problems | 8-3 |
| Automatic Broadcast Control Problems | 8-4 |
| IGMP-Related Problems | 8-5 |
| Switch Mesh Problems | 8-5 |
| STP-Related Problems | 8-7 |
| VLAN-Related Problems | 8-8 |
| Using the Event Log To Identify Problem Sources | 8-10 |

A File Transfers

| | |
|--|------|
| Overview | A-1 |
| Downloading an Operating System (OS) | A-2 |
| Using TFTP To Download the OS File | A-2 |
| Using the SNMP-Based HP Download Manager | A-5 |
| Switch-to-Switch Download | A-5 |
| Using Xmodem to Download the OS File | A-6 |
| To Perform the OS Download: | A-6 |
| Troubleshooting TFTP Downloads | A-7 |
| Transferring Switch Configurations | A-9 |
| Using Get and Put To Transfer a Configuration Between the Switch and a Networked PC or Unix Workstation | A-9 |
| Using XGet and XPut To Transfer a Configuration Between the Switch and a PC or Unix Workstation | A-10 |

B MAC Address Management

| | |
|---|-----|
| Overview | B-1 |
| The Primary and VLAN MAC Addresses | B-2 |
| The Port MAC Addresses | B-3 |

Index

Selecting a Management Interface

This chapter describes the following:

- Management interfaces for the Switch 8000M and the Switch 1600M
- Advantages of using each interface

Understanding Management Interfaces

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

The Switch 8000M and the Switch 1600M 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 “System Requirements” on page 3-2.
- The switch console—an ASCII 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—available Fall 1998)

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 included in the user’s guide included on the HP TopTools CD.

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 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 for the Switch 8000M and Switch 1600M, refer to "Online Help for the Web Browser Interface" on page 3-9.

Advantages of Using the HP Web Browser Interface

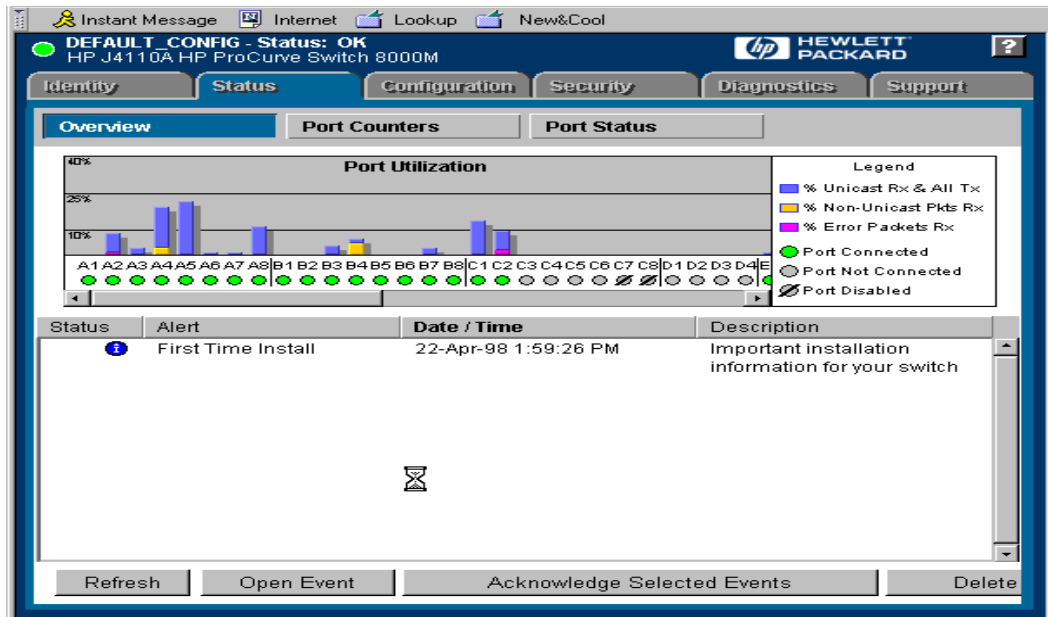


Figure 1-1. Example of the HP Web Browser Interface Display

- **Easy access** to the switch from anywhere on the network
- **Familiar browser interface**—locations of window objects consistent with commonly used browsers
- **Faster configuration**, avoid cycling through a series of screens—requires less keystrokes, uses mouse clicking for navigation; no terminal setup; Telnet access to the switch console
- **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 Console Interface

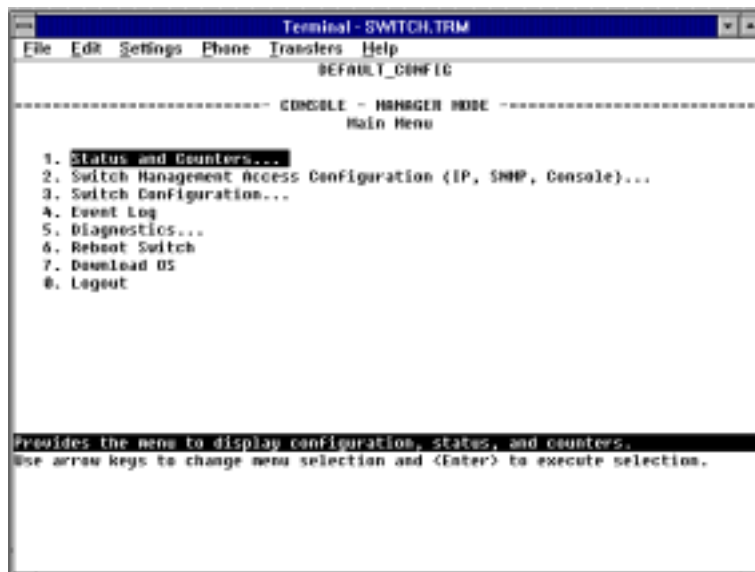


Figure 1-2. Example of the Console Interface Display

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

HP TopTools for Hubs and 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 (formerly HP AdvanceStack Assistant) is the answer to your management challenges.



Figure 1-3. Example of HP TopTools Main Screen

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 right 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.

Configure an IP Address on the Switch

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 the HP Web browser interface built into the switch, and to other HP proactive networking features available in the switch or through the HP TopTools for Hubs & Switches network management software (available Fall, 1998). For a listing of switch features available with and without an IP address, refer to “How IP Addressing Affects Switch Operation” on page 6-10.

This chapter helps you to quickly assign an IP address and subnet mask to the switch. (Without an IP address and subnet mask—the factory default configuration—the switch operates as a multi-port transparent bridge, managed only by using the direct RS-232 Console port.)

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

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, using the switch's RS-232 console port:** 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 ASCII terminal. Refer to "Manually Configuring an IP Address" on the next page.
- **Automatically, using the DHCP/Bootp process:** This method is used to download a configuration from a Bootp or DHCP server (console not needed). To use this method, refer to "DHCP/Bootp Operation" on page 6-10.

An IP address and subnet mask for the switch should be assigned by your network administrator and be compatible with the IP addressing used in your network. The purpose of this section is to help you quickly configure an IP address and subnet mask in the switch. For more information about IP addressing, refer to "IP Configuration" on page 6-6.

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 6-14.

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 6-45.

1. Use the instructions in your switch installation manual to connect a PC running a terminal emulator, or a terminal, to the RS-232 Console port on the switch, and display the Main Menu.

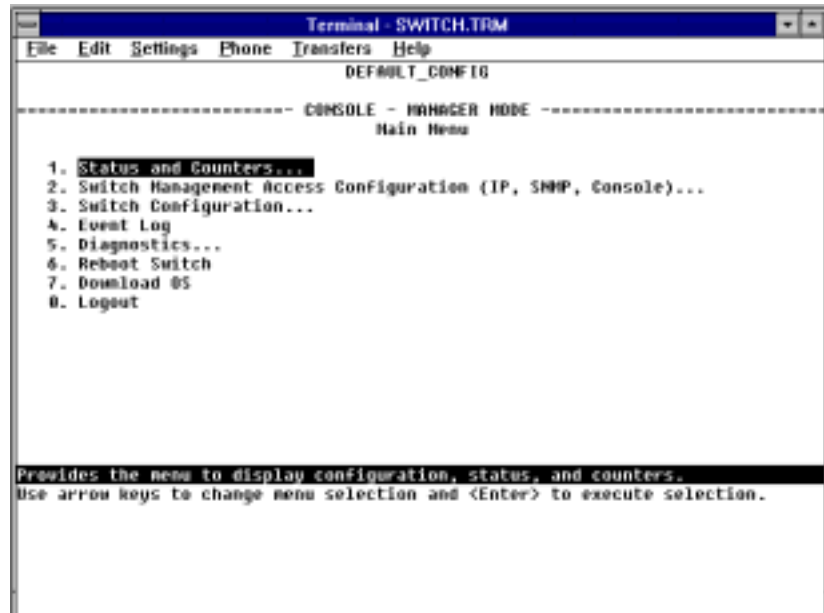


Figure 2-1. The Main Menu

2. From the Main Menu, select
2. Switch Management Access Configuration
 1. IP Configuration.
3. Press **[E]** to select **Edit**, then use the downarrow key (**[↓]**) to select **IP Config [DHCP/BOOTP]**.
4. Use the Space bar to display **Manual** at the **IP Config** parameter.
5. Press the downarrow key (**[↓]**) to display these three parameters and select the **IP Address** field:

IP Address
Subnet Mask
Gateway

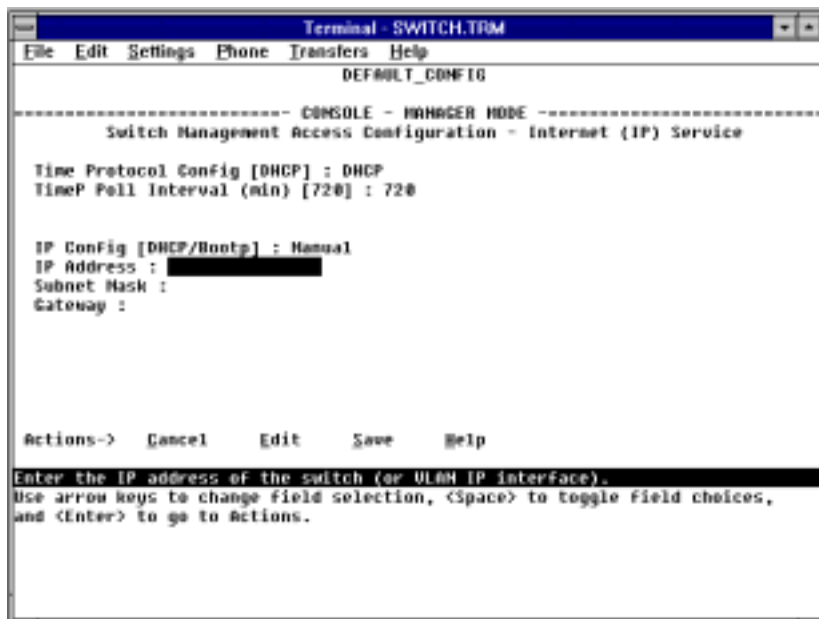


Figure 2-2. The Internet (IP) Service Screen

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. Press **[Enter]**, then **[S]** (for **Save**).
9. Press **[0]** to return to the Main Menu.

10. Do the following to reboot the switch:
 - a. Press **[6]** to select **Reboot Switch**.
 - b. When prompted, press **[Y]** for “Yes” and press **[Enter]**.

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 “Using the Switch Console To Configure the Console/Serial Link” on page 6-21.
 - To use Telnet to access the switch console from the browser interface, click on the **Configuration** tab in the browser interface, then click on **telnet session to the switch console**. If you need information on how to access the switch via the 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 3-5)
 - Creating usernames and passwords in the web browser interface (page 3-7)
 - Selecting the fault detection configuration for the Alert Log operation (page 3-23)
 - Getting access to online help for the web browser interface (page 3-9)
- Description of the web browser interface:
 - Overview window and tabs (page 3-11)
 - Port Utilization and Status displays (page 3-12)
 - Alert Log and Alert types (page 3-14)
 - Setting the Fault Detection Policy (page 3-23)

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 6-20.

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: Netscape Communicator 4.03 or later UNIX: Netscape Navigator 3.1 or later |
| PC Operating System | Microsoft Windows® 95 and Windows NT | |
| UNIX® Operating System | Standard UNIX® OS | |
| * For notes on using Netscape and Microsoft web browsers, go to HP's Network City web site, http://www.hp.com/go/network_city . | | |

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, "Configure 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 **[Enter]**. (It is not necessary to include **http://**.)

Using the HP Web Browser Interface

Starting an HP Web Browser Interface Session with the Switch

switch8000 (example of a DNS-type name)

10.11.12.195 (example of an IP address)

Note

After you begin a web browser interface session with the switch, you can use the browser to Telnet to the switch console interface. To do so, click on the Configuration tab, then click on **telnet session to the switch console** in the Device view.

If you are using a Domain Name Server (DNS), your device may have a name associated with it (for example, **switch8000**) 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 or DNS name and has been discovered by HP TopTools. (For more on assigning an IP address, refer to chapter 2, "Configure 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).
3. 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.

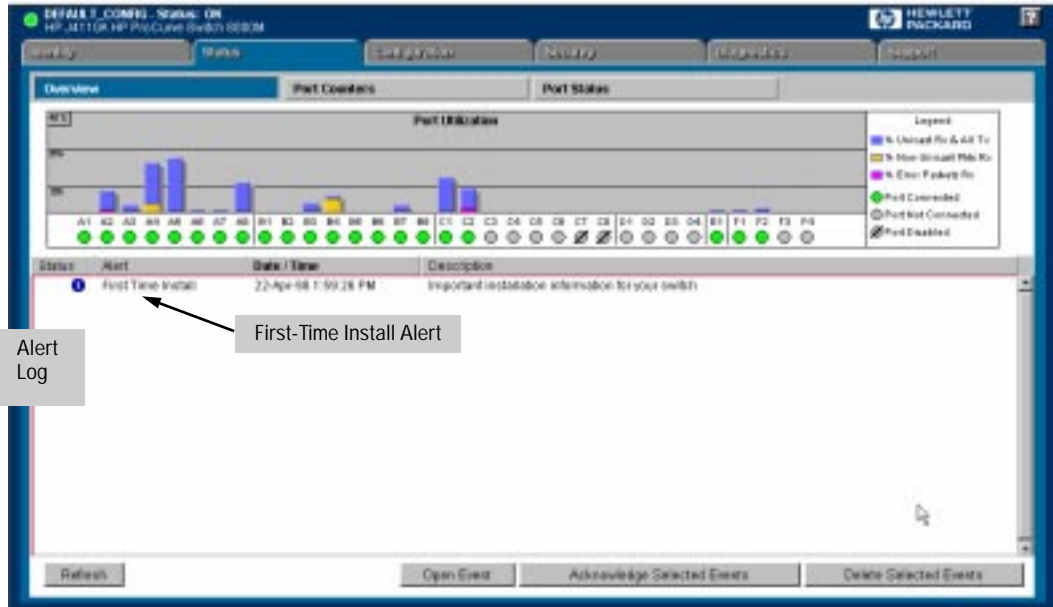


Figure 3-1. Status Overview Screen

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.

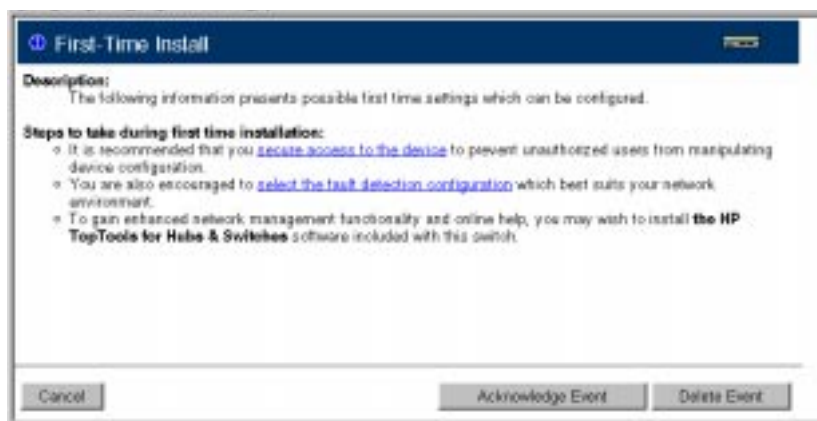


Figure 3-2. First-Time Install Window

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 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

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 3-23.

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.

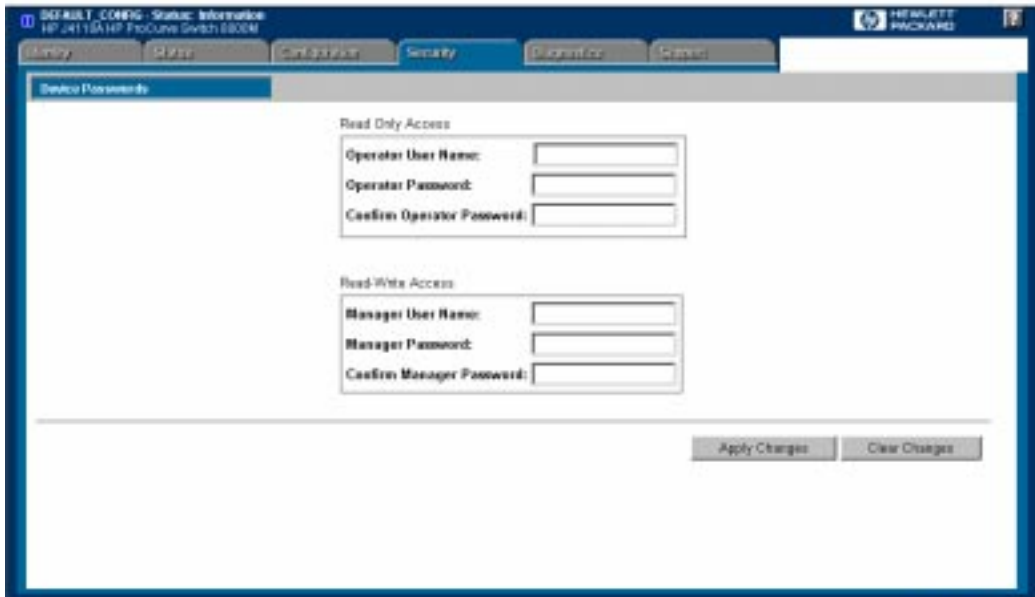


Figure 3-3. The Device Passwords Window

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 and then the Device Passwords button.

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 **Apply Changes** 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 and 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. That is, the switch is shipped with the URL needed to retrieve online Help through the World Wide Web. However, if HP TopTools is installed on your network and discovers the switch, the Management Server URL is automatically changed to retrieve the Help from your TopTools management station.

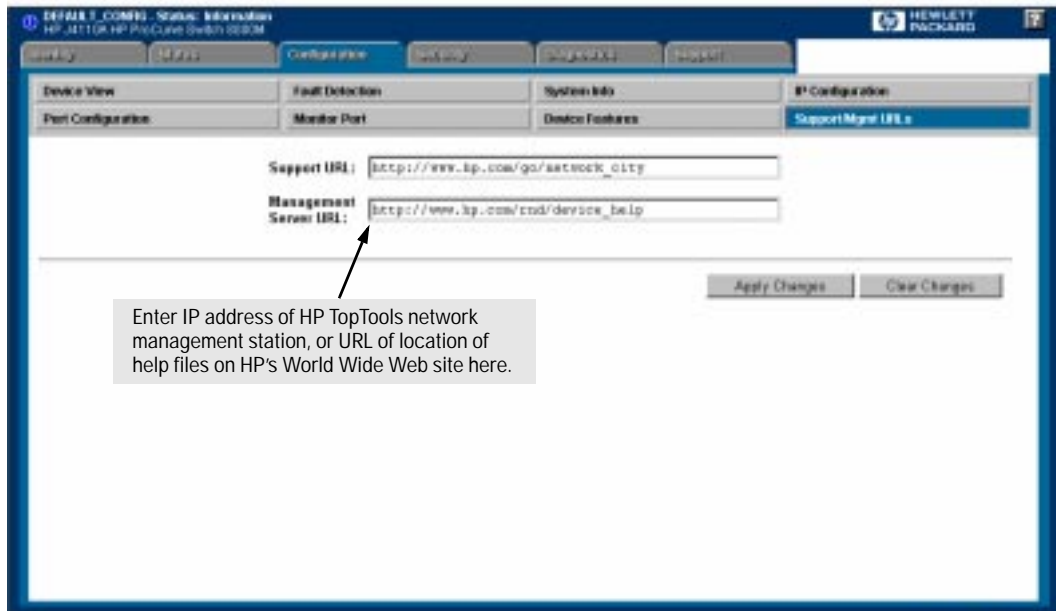
If Online Help Fails To Operate. Do one of the following:

- 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 3-10.
- 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 3-10:

`http://www.hp.com/rnd/device_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 browser interface will not be available.

Using the HP Web Browser Interface Tasks for Your First HP Web Browser Interface Session



Enter IP address of HP TopTools network management station, or URL of location of help files on HP's World Wide Web site here.

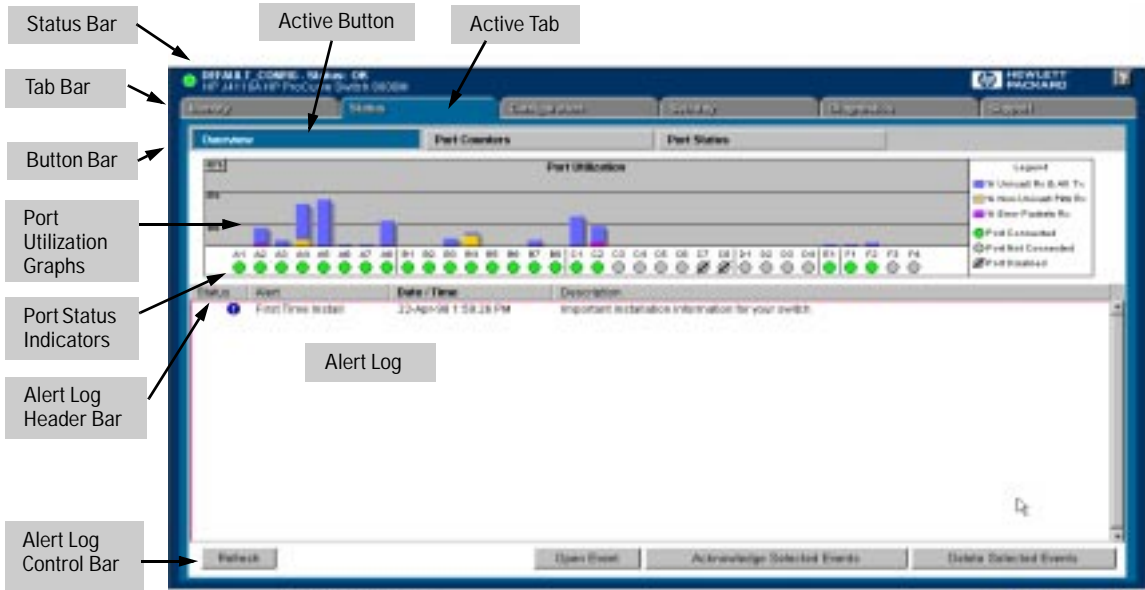
Figure 3-4. How To Access Web Browser Interface Online Help

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 details the different pieces to it.



Using the HP Web Browser Interface

Figure 3-5. 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 Browser Interface Top Level menus.
- **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 3-14.
- **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.

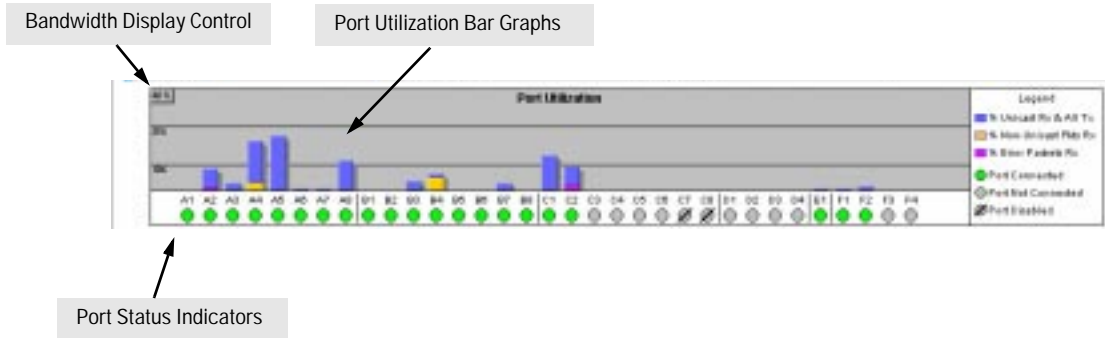


Figure 3-6. The Graphs Area

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 device connected to the indicated port and needing attention.

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.

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%). 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.

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 6, “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 are shown in Table 4-3. (If HP TopTools for Hubs & Switches is running on the network, it receives alerts from the web browser interface.)



Figure 3-7. 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 Browser Interface. This value is shown in the format: *DD-MM-YY HH:MM:SSAM/PM*, for example, **12-Sep-97 3:57:20 PM**.
- **Description** – A short narrative statement that describes the event. For example, **Lost connection to multiple devices on port 1**.

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. |
| Problem Driver or NIC | Problem software driver or LAN adapter detected on port. |
| Problem XCVR or NIC | Problem transceiver or LAN adapter card detected on port. |
| Problem Cable | Problem cable or duplex mismatch (full-duplex configured on one end of the link, half-duplex configured on the other) detected on port. |
| Cable Length/Repeater Hops | <ul style="list-style-type: none">• Problem cable detected on port.• Packet loss detected, which could be due to excessive number of gateways to traverse or to duplex mismatch (full-duplex configured on one end of the link, half-duplex configured on the other). |
| Over Bandwidth | Excessive network traffic on port. |
| Broadcast Storm | Excessive broadcasts detected on port. |
| Fault-Disabled Port | The port has been automatically disabled due to a detected fault condition, for example, an incorrect transceiver installed in a transceiver slot. |
| Polarity Reversal | Miswired cable detected on port. |
| Network Loop | Network loop detected by switch. Network loop detected on port. |
| Loss of Link | Lost connection to multiple devices on port. |

Note

When troubleshooting the sources of alerts, it may be helpful to check the switch's Port Status and Port Counter windows (page 7-7 and page 7-9) and the Event Log in the console interface (page 8-10).

Viewing Detail Views of Alert Log Entries

By double clicking on Alert Entries, the 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 a Loss of Link alert is shown here.



Figure 3-8. 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.



Figure 3-9. The Alert Control Bar

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 browser interface tab bar 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

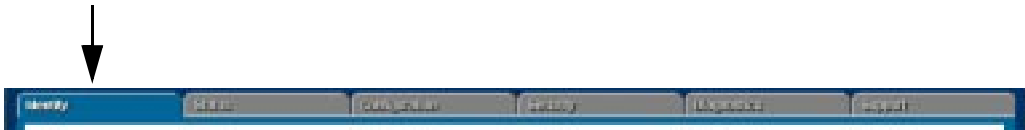


Figure 3-10. The Identity Tab

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 6-4).

Status Tab



Figure 3-11. The Status Tab and Buttons

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 Browser Interface. Displays the screen shown in figure 4-4.

- **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



Figure 3-12. The Configuration Tab and Buttons

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.
- **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.** Enables you to change existing value for an IP address, subnet mask, and the gateway address for the switch.
- **Monitor Port.** Enables you to designate a port for monitoring traffic on one or more other ports or on a VLAN configured on the switch.
- **Port Configuration.** Enables you to enable and disable ports in addition to viewing the security and source address information.
- **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 6-5). The Support URL is configured to automatically access HP's Network City 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



Figure 3-13. The Security Tab and Buttons

This tab displays the Security Button Bar which contains the button that enables you view and set operator names and passwords to restrict access to your switch. The button displayed is:

- **Device Passwords.** Enables you to set operator and manager-level user names and passwords for the switch.

Diagnostics Tab



Figure 3-14. The Diagnostics Tab and Buttons

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.

The Support Tab



The URL for this window is set in the Configuration|Support|Mgmt URLs option. By default, it is set to Hewlett-Packard's Network City web page, but you can change it to the URL for another location, such as an internal support resource.

The Status Bar

The Status Bar is displayed in the upper left corner of the browser interface screen. Figure 3-14 shows an expanded view of the status bar.

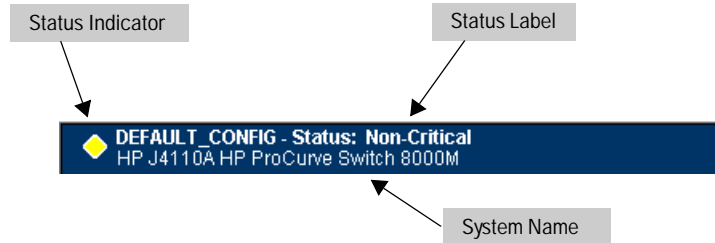





Figure 3-15. The Status Bar

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 | Gauge Severity Region | Status Indicator Shape |
|--------|-----------------------|--|
| Green | Normal Activity |  |
| Yellow | Warning |  |
| Red | Critical |  |

- **System Name.** Indicates the name of product name of the switch for which you have created your current browser interface session.
- **Status Label.** Indicates, by test string, the severity of the most critical alert in the current display of the Alert Log.
- **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.

Setting Fault Detection Policy

One of the powerful features in the 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 3-15).

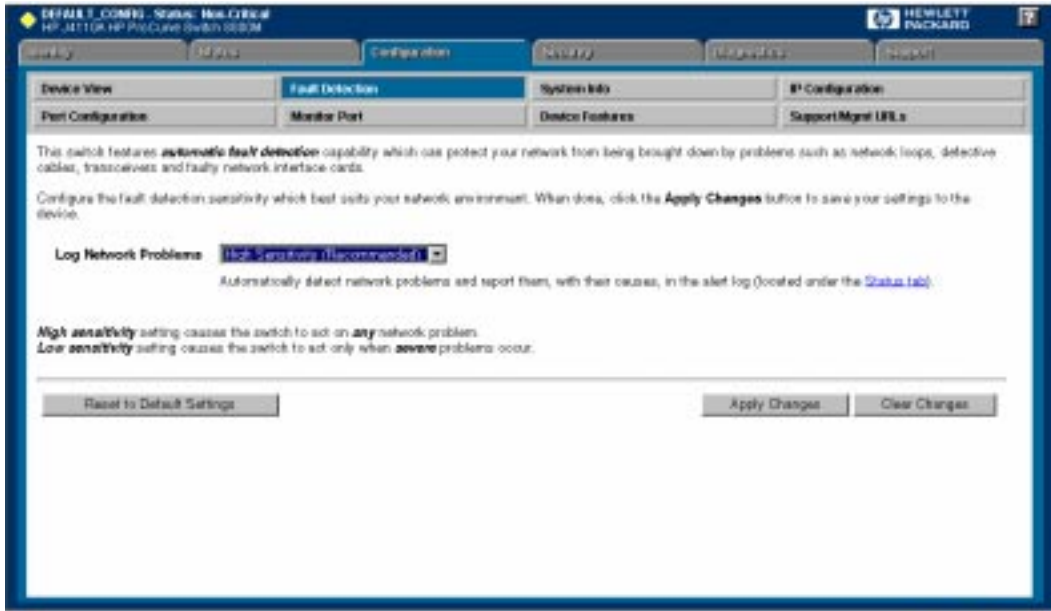


Figure 3-16. The Fault Detection Window

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.

The sensitivity levels for both list boxes are:

- Never
- Low Sensitivity
- Medium Sensitivity
- High Sensitivity

The recommended sensitivity level for Log Network Problems is High Sensitivity to provide the most information on network problems in the Alert Log. 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.

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 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 4-5)
 - Using password security (page 4-9)
 - Rebooting the switch (page 4-13)
 - Using the command prompt (page 4-15)
-

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 6-29)
- Control console security by configuring passwords. (See "Using Password Security" on page 4-9.)
- Download new software to the switch (appendix A.)

You can access the switch console interface using either:

- The Console RS-232 port, as described in the installation guide you received with the switch.
- Via Telnet from the web browser interface on a networked workstation (if an IP address and subnet mask have already been configured on the switch—see chapter 2).

Configuration changes made through the console overwrite previous changes made through the web browser interface. Similarly, configuration changes made through the web browser interface overwrite any prior changes made through the console. The console gives you access to all switch configuration parameters. 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

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 *HP Switch 8000M and 1600M Installation Guide*) 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 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 4-14.)

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

Main Menu Features

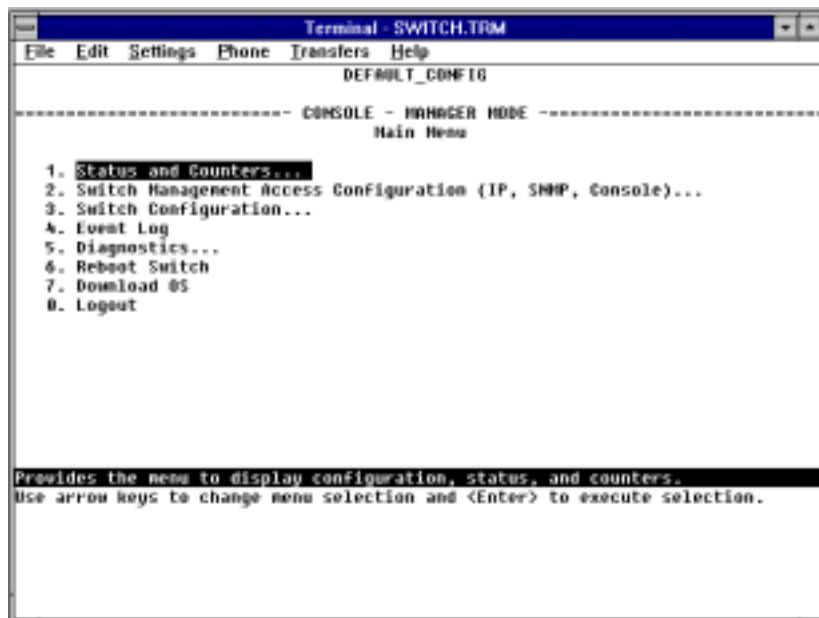


Figure 4-1. The Main Menu

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. A listing of Event Log messages is included on the CD shipped with your switch. (Refer to “Event Log” in chapter 7, “Monitoring and Analyzing Switch Operation”.)
- **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 chapter 8, “Troubleshooting”.)
- **Reboot Switch:** Performs a “soft” reboot, which is the minimum required (in some cases) to activate configuration changes that have been made. (Refer to “Rebooting To Activate Configuration Changes” on page 4-14.) Using this option, the reboot cycle is slightly faster because, instead of running a new self-test, it accepts the self-test results from the most recent “hard” reboot caused by cycling the power or pressing the Reset button.
- **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:

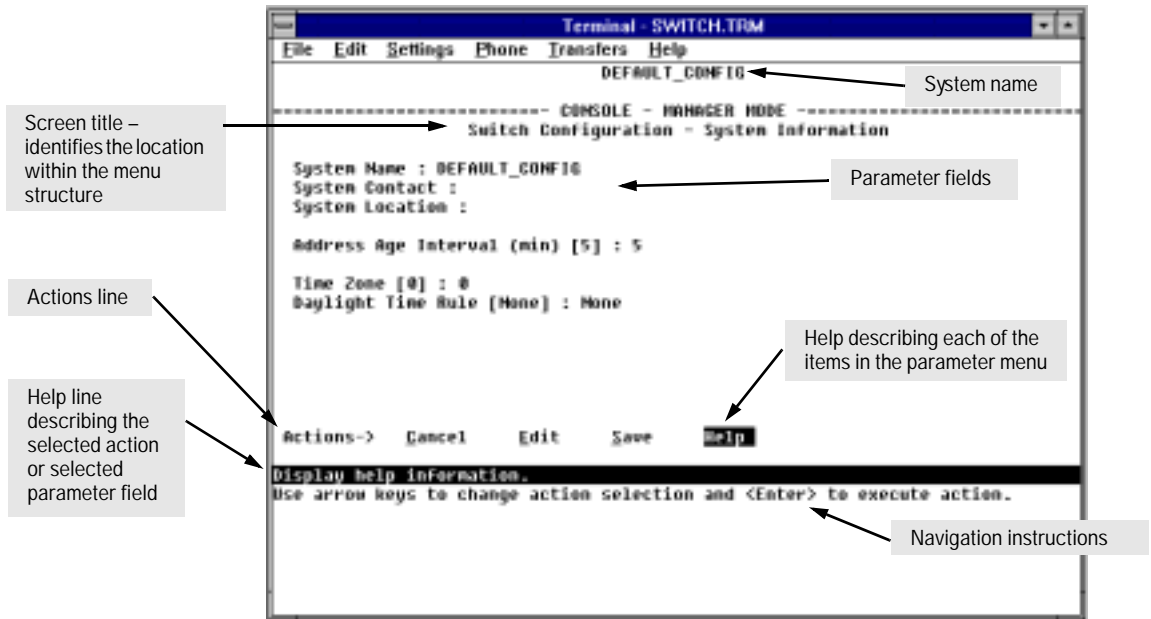


Figure 4-2. Elements of the Screen Structure

“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 **Edit** action.
2. Navigate through the screen making ALL the necessary configuration changes.
3. Press **[Enter]** to return to the Actions line. From there you can save the configuration changes or to cancel the changes. Cancel returns the configuration to the values you saw when you first entered the screen.

The next page provides specific instructions on using the console screens.

Table 4-1. How To Navigate in the Console

| Task: | Actions: |
|---|--|
| Execute an action from an "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. (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 Action line and do one of the following: <ul style="list-style-type: none"> • To save any configuration changes you have made (or if you have made no changes), press S (for the Save action). • To exit from the screen without saving any changes that you have made, 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:

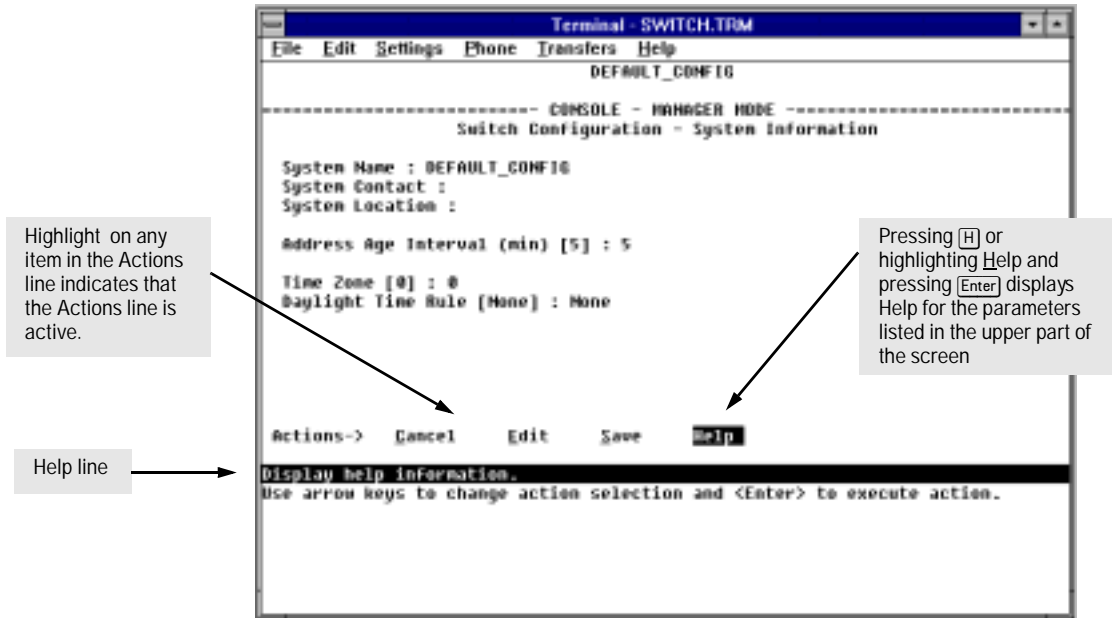


Figure 4-3. Example Showing How To Display Help

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 configuration screen, see the instructions provided at the bottom of the screen, or refer to “Screen Structure and Navigation” on page 4-5.)

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, Event Log, and minimal Configuration capabilities. On the Operator level, the Command Prompt, Set Passwords, Download OS, and Reboot options are not available in the Main Menu. |

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 6-21). 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**

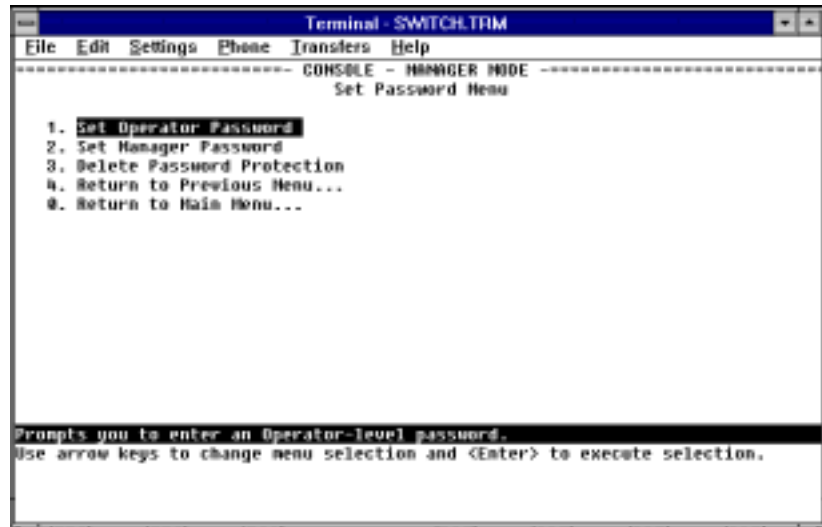


Figure 4-4. The Set Password Screen

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 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 7-11.)

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, you enter an Operator password at the password prompt.)

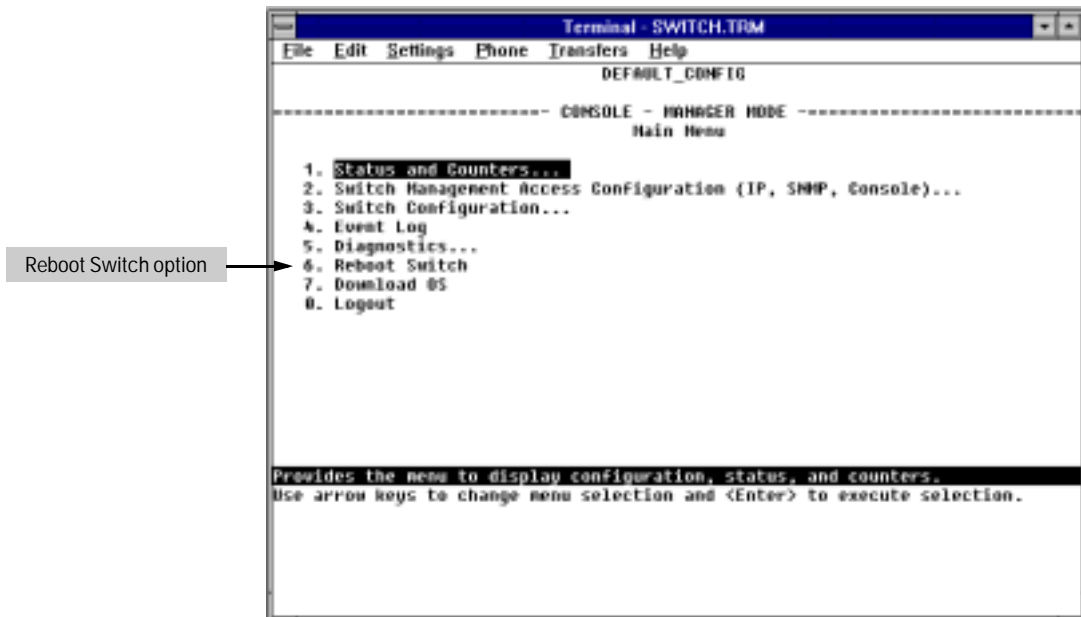


Figure 4-5. The Reboot Switch Option in the Main Menu

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 Switch Management Access Configuration 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:

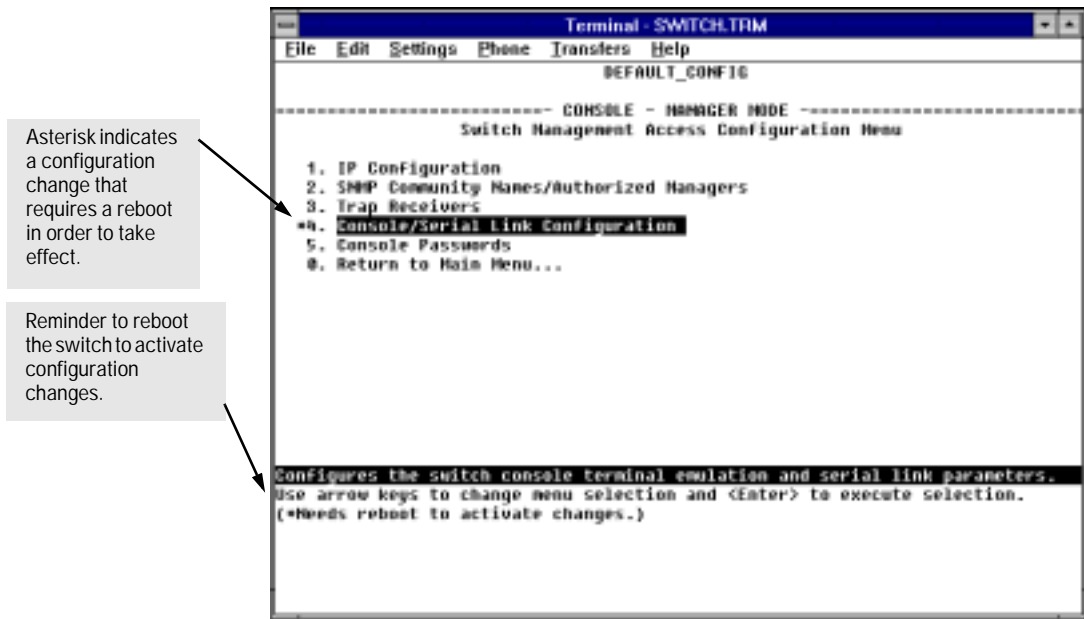


Figure 4-6. Example of a Configuration Change Requiring a Reboot

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. For more information, refer to “Using the Command Prompt” on page 7-28.

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 and 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 and provides 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”.

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 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. This chapter provides an overview of SNMP management for the switch and describes the configuration process for the various features. For parameter-specific information, refer to the Help provided in the individual configuration screens.

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 8000M and Switch 1600M configuration (config.mib)
- HP VLAN configuration information (vlan.mib) supporting hpVlanGeneralGroup
- HP EASE 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/network_city

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 6-10.)

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 6-10.)
 - Manually configure an IP address. (Refer to chapter 2, “Configure 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 6-15.)
4. Configure the appropriate trap receivers. (For more on configuring trap receivers, refer to “Trap Receivers” on page 6-18.)

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 4-13.)

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 Console Interface”

Why Reconfigure? In its factory default configuration, the switch operates as a multiport learning bridge with network connectivity provided by 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 will most likely 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 Interface | Page |
|---|----------------|-----------------------|----------|
| Time Protocol | Yes | — | 6-8 |
| IP Configuration | Yes | Yes | 6-6 |
| SNMP Communities | Yes | — | 6-15 |
| Authentication Traps Trap Receivers | Yes | — | 6-18 |
| Fault Detection | No | Yes | 3-14 |
| Console/Serial Link | | | 6-20 |
| • Enable Inbound Telnet to Console | Yes | — | 6-21 |
| • Enable Web Browser Interface Access | Yes | — | 6-21 |
| • Terminal settings | Yes | — | 6-21 |
| Operator and Manager Usernames | — | Yes | 3-7 |
| Operator and Manager Passwords | Yes | Yes | 3-7, 4-9 |
| System Information | Yes | Yes | 6-22 |
| Address Age Interval | Yes | — | |
| System Time | Yes | — | |
| Port Settings | Yes | Yes | 6-24 |
| Network Monitoring Port | Yes | Yes | 6-29 |
| Spanning Tree Enable/Disable | Yes | Yes | 6-34 |
| Spanning Tree Parameters | Yes | — | |
| Traffic/Security Filters | Yes | — | 6-40 |
| Enable/Disable VLANs | Yes | — | 6-45 |
| VLAN Names and Port Assignment | Yes | — | |
| Load Balancing: Port Trunking | Yes | — | 6-64 |
| Load Balancing: Switch Meshing | Yes | — | 6-74 |
| IP Multicast (IGMP) Enable/Disable | Yes | Yes | 6-89 |
| IGMP Priority and Port Settings | Yes | — | |
| Automatic Broadcast Control Enable/Disable | Yes | Yes | 6-100 |
| RIP, SAP, and Gateway Parameters | Yes | — | |

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 6-74 and “Spanning Tree Protocol” on page 6-34.

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.

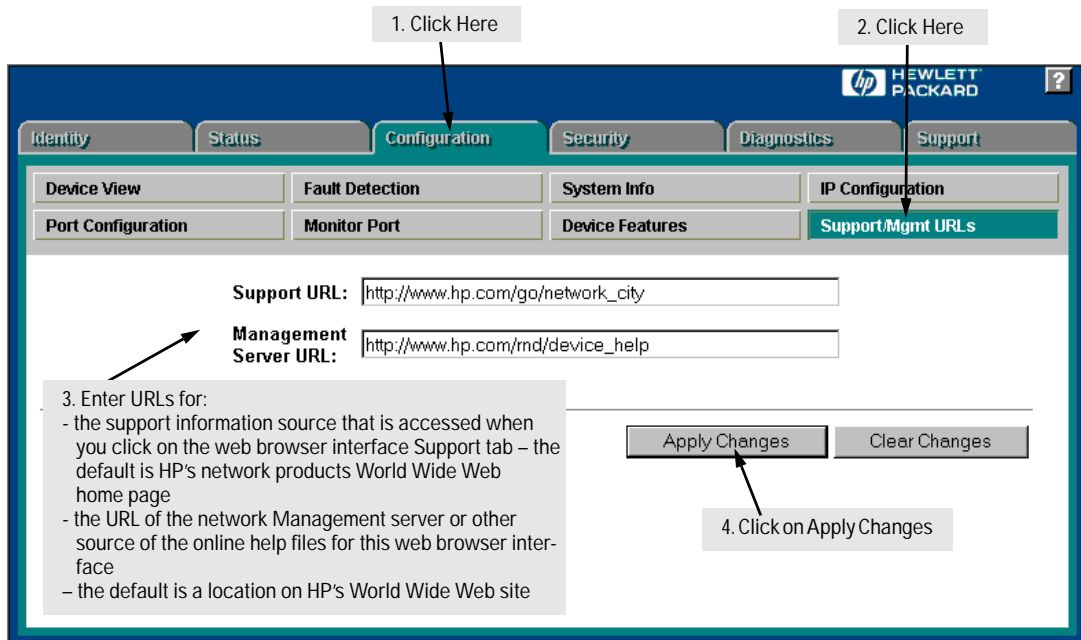


Figure 6-1. The Support/Mgmt URLs Window

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/network_city

which is the World Wide Web site for Hewlett-Packard's networking products. Click on the Support button on that page, and you can get to support information regarding your switch including white papers, code 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 **Support** tab.

Management Server URL

This field serves two purposes:

- The location of online help for the web browser interface
- 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 the URL location.

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 3-9. (HP Top Tools for Hubs & Switches has the capability to perform network-wide policy management and configuration of your switch. For more information, refer to the documentation provided on the HP TopTools CD shipped with the switch—available Fall, 1998.)

IP Configuration

Enables you to configure:

- 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)

If VLANs are not configured, then enable IP once for the entire switch. If VLANs are configured, then enable IP on a “per VLAN” basis. This is because each VLAN is a separate network and requires a unique IP address, plus a subnet mask. A gateway (IP) address is optional. For more on VLANs, refer to “Virtual LANs (VLANs)” on page 6-45.

The switch can receive IP addressing from a DHCP/Bootp server or manually using the Web Browser Interface or console interface. A third option is to disable the IP configuration. (Refer “DHCP/Bootp Operation” on page 6-10 for information on setting up automatic configuration from a server.)

The IP addressing used in the switch should be compatible with your network. (The IP address must be unique; the subnet mask must be the same for all devices on the network.)

Note

If you plan to connect to other networks that use globally administered IP addressing, refer to “Globally Assigned IP Addresses” on page 6-14.

For information on how IP addressing affects switch performance, refer to “How IP Addressing Affects Switch Operation” on page 6-10.

Configuring IP Addressing Parameters from the Web Browser Interface

1. Click here.

2. Click here.

3. If multiple VLANs are configured, select a VLAN.

4. To enable manual entry of the IP address, set this to "Manual".

5. Enter an IP address, subnet mask, and, if needed, the IP address of the default gateway.

6. Click on this to activate the changes you made in steps 3 - 5.

Warning: Changing IP configuration could result in loss of browser connectivity to the switch.

The default setting for Time Protocol Config is DHCP. Setting it to **Manual**, then pressing **↓** or **Tab** causes the Time 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 6-10.

Figure 6-2. Configuring IP Addressing on the Web Browser Interface

| HP-WBI 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 service configuration. <ul style="list-style-type: none"> DHCP/Bootp: 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. |

| HP-WBI 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. |
| 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 Parameters 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 and subnet mask 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 6-10.

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.

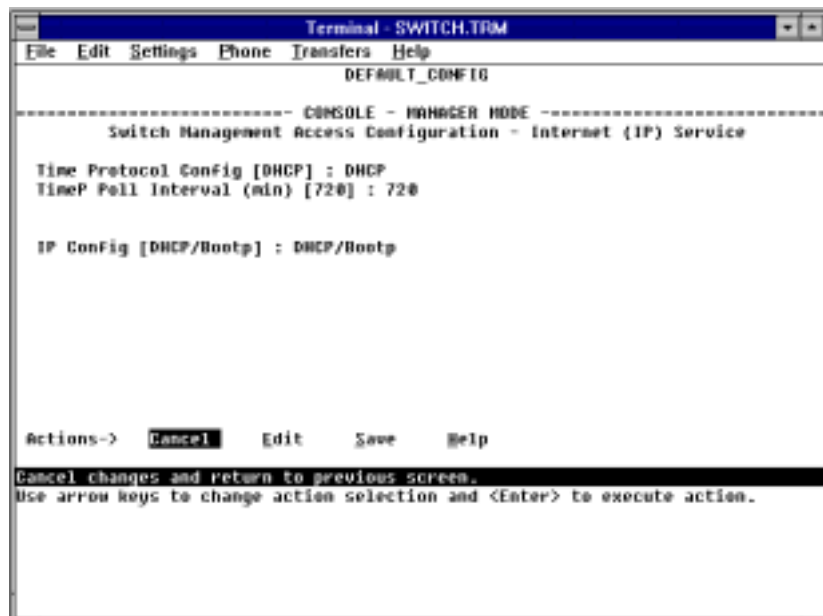


Figure 6-3. Example of the IP Service Configuration Screen

2. Press **[E]** (for **E**dit).
3. Select the **IP ConFig** field and use the Space bar to select **Manual**.
4. Select the **IP Address** field and enter the IP address for the switch.
5. Select the **Subnet Mask** field and enter the subnet mask for the IP address.
6. If you want to reach off-subnet destinations, select the **Gateway** field and enter the IP address of the gateway router.
7. Press **[Enter]**, then **[S]** (for **S**ave).
8. 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 • Bootp or DHCP support for automatic 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 or downloading from another switch) | <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 • DHCP time serve 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. Either a minimal IP configuration or a full configuration can be retrieved from the server.

Note

The Switch 8000M and Switch 1600M are compatible with both DHCP and Bootp servers.

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 all local networks. (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. (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 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.

DHCP Operation. A significant difference between a DHCP configuration and a Bootp configuration is that an IP address assignment from a DHCP server is temporarily leased. Periodically the switch is 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 the following:

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

For more information, 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. 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. An 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:

```
j4110switch:\
  ht=ether:\
  ha=080009123456:\
  sm=255.255.248.0:\
  lg=11.22.33.44:\
  hn:\
  ip=55.66.77.88:\
  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:

```
j4110switch:\
  ht=ether:\
  ha=080009123456:\
  sm=255.255.248.0:\
  lg=11.22.33.44:\
  hn:\
  ip=55.66.77.88:\
  T144="switch.cfg":\
  vm=rfc1048
```

where:

- | | |
|-------------|---|
| j4110switch | 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 Switch 8000M and Switch 1600M, 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. |
| sm | is the subnet mask of the subnet in which the switch (or VLAN) is installed. |
| lg | TFTP server address (source of final configuration file) |
| hn | send nodename (boolean flag, no "=value" needed) |
| ip | is the IP address to be assigned to the switch (or VLAN). |
| 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 Switch 8000M and Switch 1600M, set this parameter to **rfc1048**.
- ts is the IP address of the time server.

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 a DHCP/Bootp database record has already been entered into an appropriate DHCP/Bootp server, and that the necessary network connections are in place.

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 Help server and Timep server.
- 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 DHCP/Bootp database configuration record and that the DHCP/Bootp database record is correctly configured.)

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

Enables you to 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

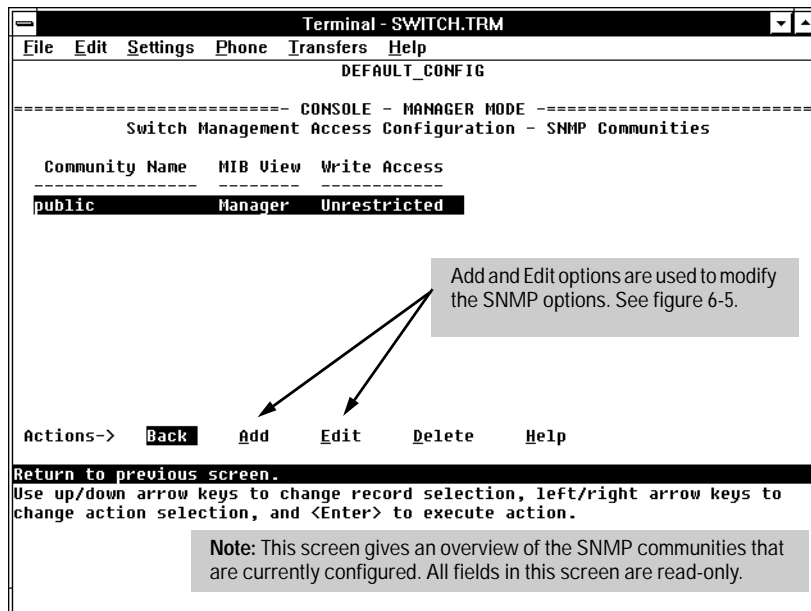


Figure 6-4. The SNMP Communities Screen (Default Values)

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.

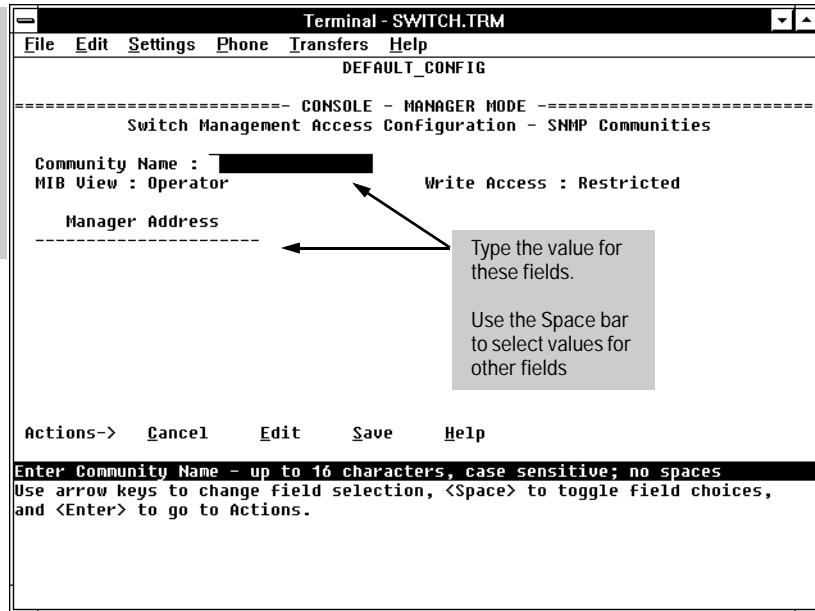


Figure 6-5. The SNMP Add or Edit Screen

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

Enables 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. An authentication trap is sent if a management station attempts an unauthorized access. 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 8-10.)

Configuring SNMP Communities from the Console

To Access Trap Receivers:

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

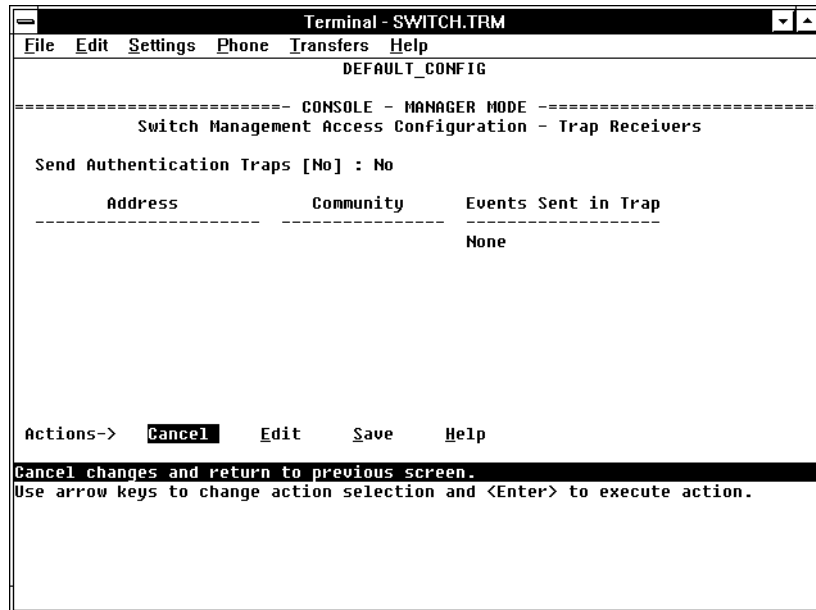


Figure 6-6. The Trap Receivers Configuration Screen (Default Values)

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

This screen configures console terminal emulation and communication with the switch in the following ways:

- Enable or disable inbound Telnet access (default: enabled)
- Enable or disable HP Web Browser Interface access (default: enabled)
- Specify:
 - Terminal type (default: VT100)
 - 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)
- Adjust the Console RS-232 configuration to customize the connection with the PC or terminal you are using for console access.
 - Baud Rate (default: Speed Sense)
 - Flow Control (default: XON/XOFF)
 - Connection Inactivity Time (default: 0—off)

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.

Using the Switch Console To Configure the Console/Serial Link

This screen enables you to:

- Enable or disable inbound Telnet and Web Browser Interface access
- 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

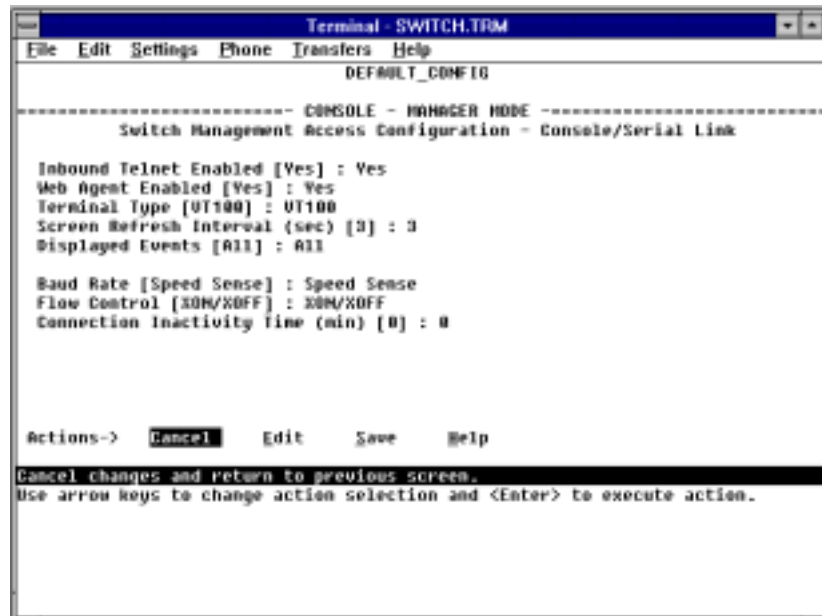


Figure 6-7. The Console/Serial Link Configuration Screen (Default Values)

2. Press **[E]** (for **E**dit). The cursor moves to the **Baud Rate** 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

System Information

Configures 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.

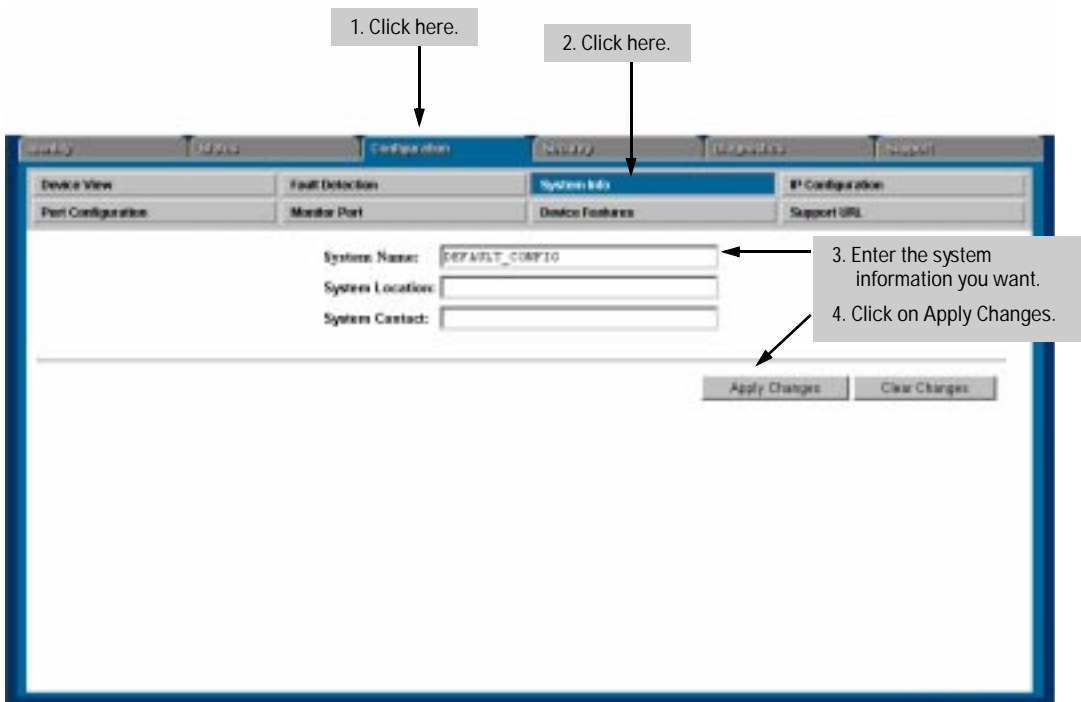


Figure 6-8. Example of System Info Screen on the Web Browser Interface

Configuring System Information from the Console

To Access System Information:

1. From the Console Main Menu, Select...
 2. Switch Configuration...
 1. System Information

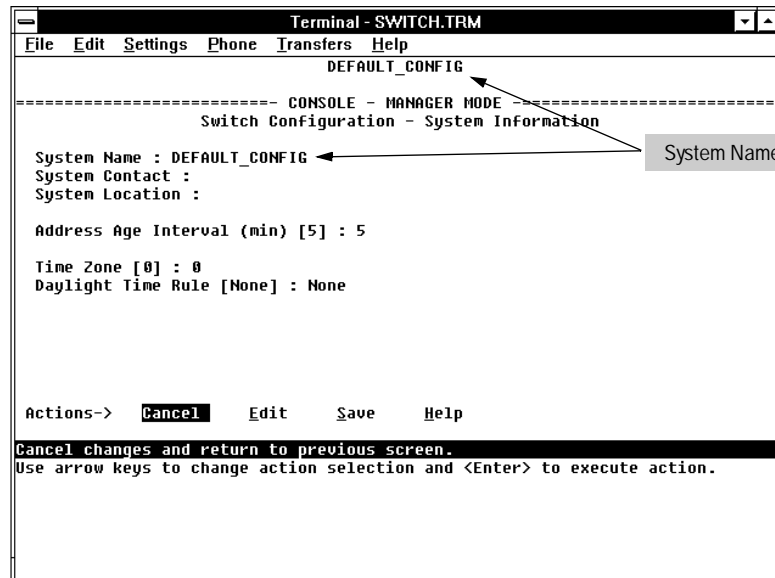


Figure 6-9. The System Configuration Screen (Default Values)

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 6-6) for your time server or use the time and date commands described in chapter 6, “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

Configures 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 names 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.

| Mode: | Port Types: | | | |
|-----------------------------|---------------------------------|----------------------------------|---------------------------------|-----------------------------|
| | 10/100TX | 10FL | 100Fx | Gigabit |
| 10 or 100 Mbps | Auto (default) or Manual Select | 10 only | 100 only | n/a |
| Half/Full Duplex | Auto (default) or Manual Select | Manual only Default: Half Dx | Manual only Default: Half Dx | Full Duplex only |
| Enable/Disable Flow Control | Auto (default) or Manual Select | Manual only. Default: Disable | | Disable (default) or Enable |

Auto (Auto-Negotiation): This feature complies with the IEEE 802.3u Auto Negotiation standard, and is the default setting for 10/100TX ports on the switch. Using Auto, the port automatically selects the network speed (10- or 100Mbps) and the data transfer operation (full- or half-duplex) for the connection to another device, provided that the other device also complies with the IEEE 802.3u Auto Negotiation protocol and is set to Auto. 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.

Note

Both ports in a link must be configured with the same settings.

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 6-100 and following) if ABC is enabled. Setting the broadcast limit (Bcast 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

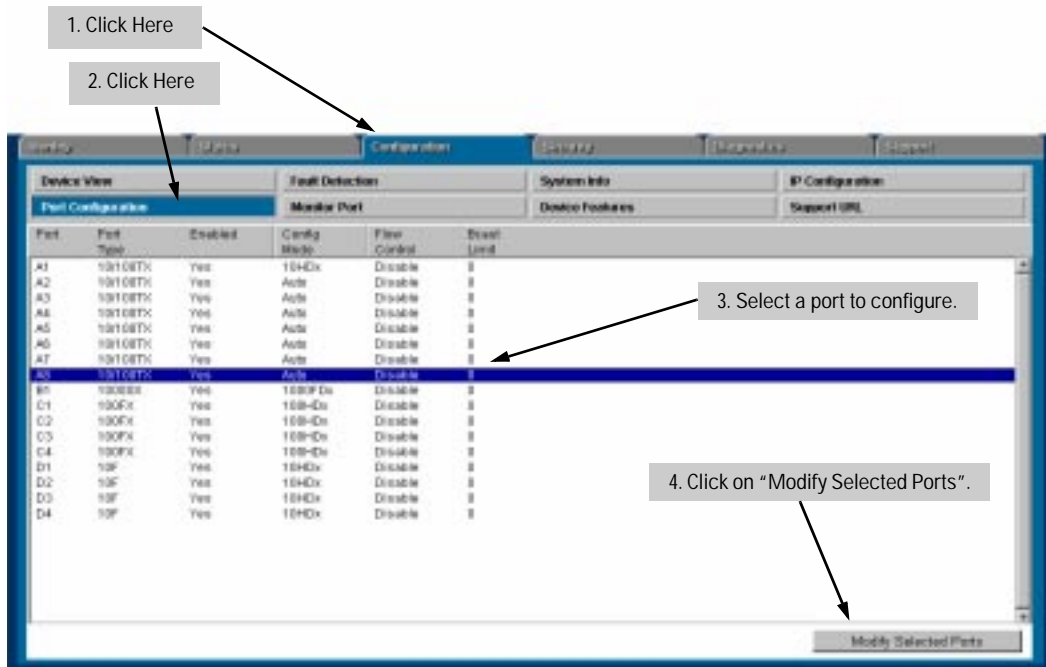


Figure 6-10. Example of Port Configuration Screen on the Web Browser Interface

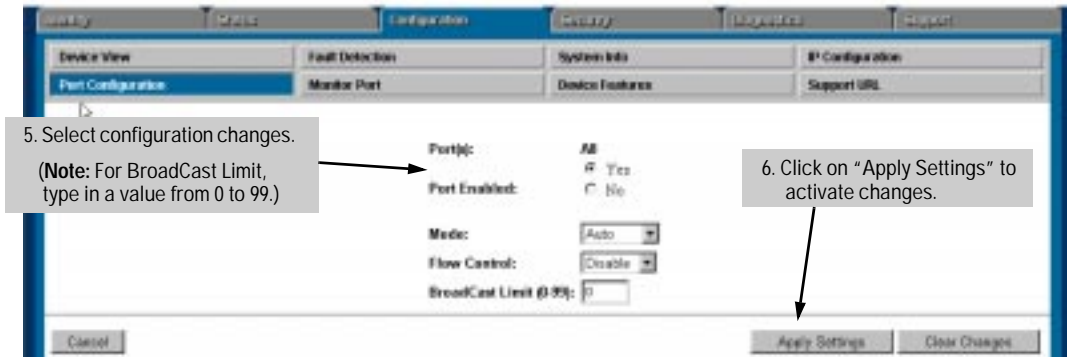


Figure 6-11. Example of Port Modification Screen on the Web Browser Interface

| HP-WBI Parameter | Description |
|------------------------|--|
| Enabled | Determines whether the port can be used. Yes (default) |
| Config Mode 1000SX: | The operational mode of the port. 1000FDx (default): 1gbps, Full-Duplex Auto : The port operates at 1000FDx and auto-negotiates flow control with the device connected to the port. |
| 10/100TX | Auto (default): Auto-negotiates with the port at the other end of the link for speed (10Mbps or 100Mbps) 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. 10HDx : 10Mbps, Half-Duplex 100HDx : 100Mbps, Half-Duplex 10FDx : 10Mbps, Full-Duplex 100FDx : 100Mbps, Full-Duplex |
| 100FX | 100HDx (default): 100Mbps, Half-Duplex 100FDx : 100Mbps, Full-Duplex |
| 10F | 10HDx :(default): 10Mbps, Half-Duplex 10FDx : 10Mbps, Full-Duplex |
| Flow Control | Maximizes circuit efficiency by enabling negotiation of packet parameters with the device to which the port is connected. When enabled, the port uses 802.3x Link Layer Flow Control, generates flow control packets and processes received flow control packets. When disabled, the port will not generate flow control packets and drops received flow control packets. Default: Disable |

| HP-WBI Parameter | Description |
|------------------|---|
| Bcast Limit | 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. If Automatic Broadcast Control is enabled, this value is automatically set to 30 (%) if it has not already been manually set to a nonzero value. |

Configuring Port Parameters from the Switch Console

To Access IP Addressing:

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

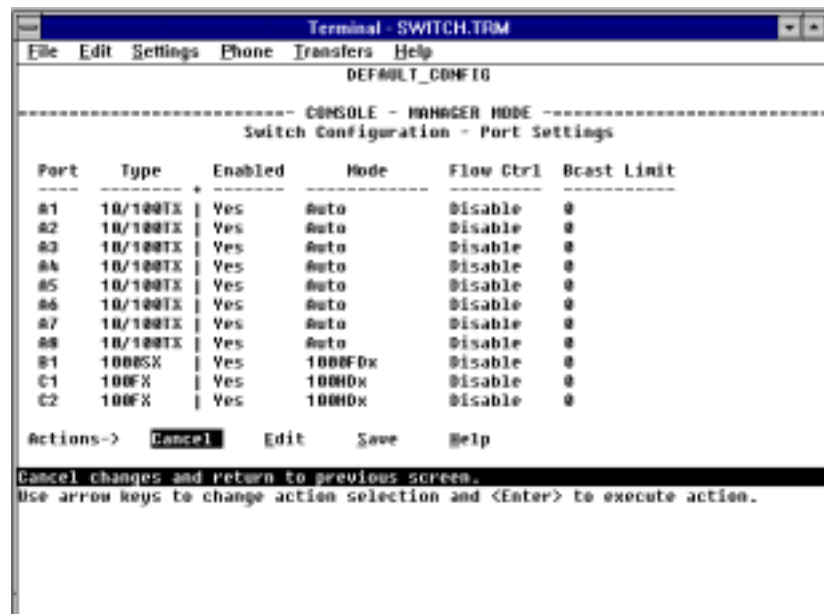


Figure 6-12. Example of the Port Configuration Screen

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 **Save**) and return to the Main Menu

Network Monitoring Port Features

Lets you designate a port for monitoring traffic on one or more other ports or on a VLAN configured on the switch. This is accomplished by copying all traffic from the specified ports or VLAN to the designated monitoring port.

Note

When monitoring multiple ports in a busy network, some frames may not be copied to the monitoring port.

Configuring Port Monitoring from the Web Browser Interface

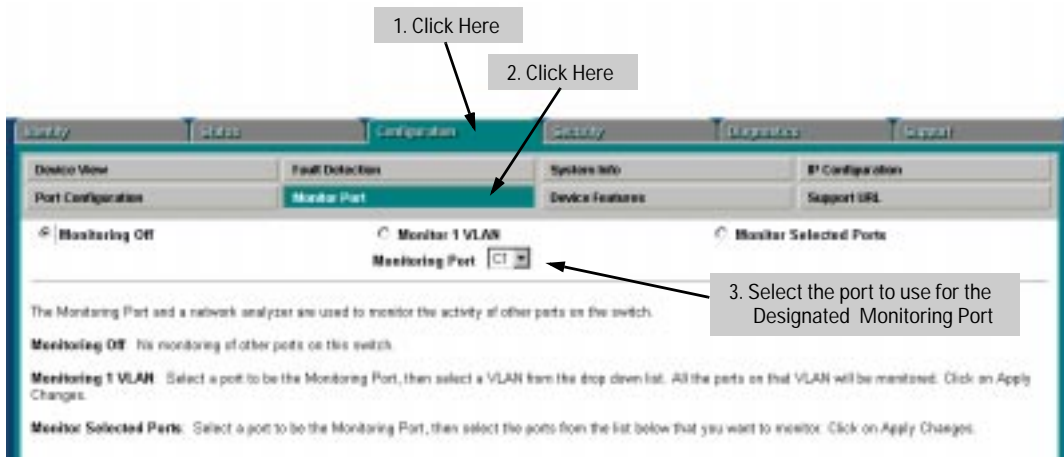


Figure 6-13. Setting Up Port Monitoring on the Web Browser Interface

4. Do one of the following:
 - If you want to monitor one port or several consecutive ports, click on the **Monitor Selected Ports** button. (See figure 6-14, below.)
 - If you want to monitor VLAN traffic, click on the **Monitor 1 VLAN** button. (See figure 6-15, below.)

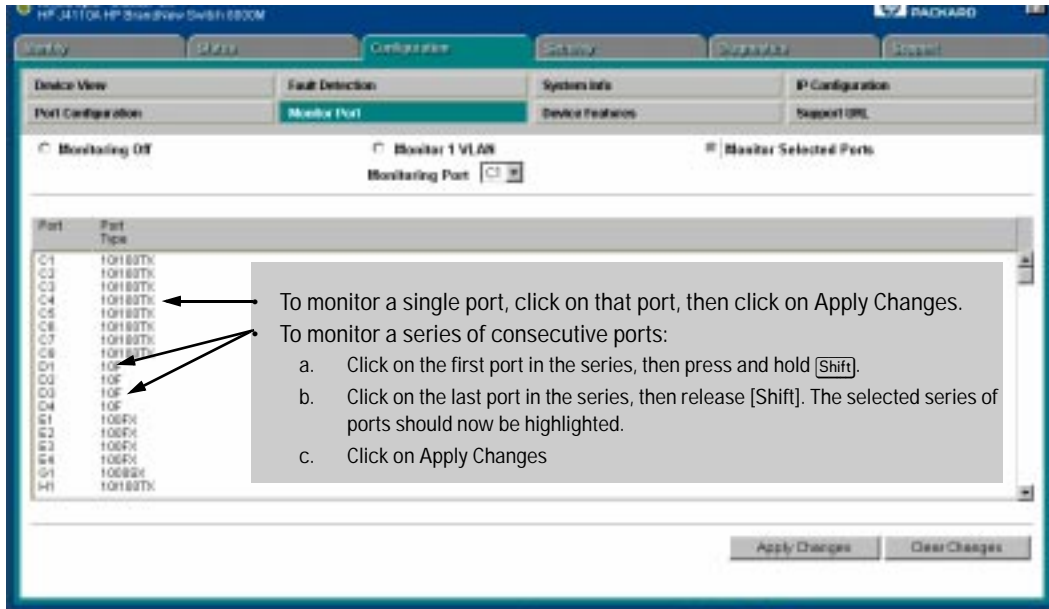


Figure 6-14. Selecting the Port(s) To Monitor

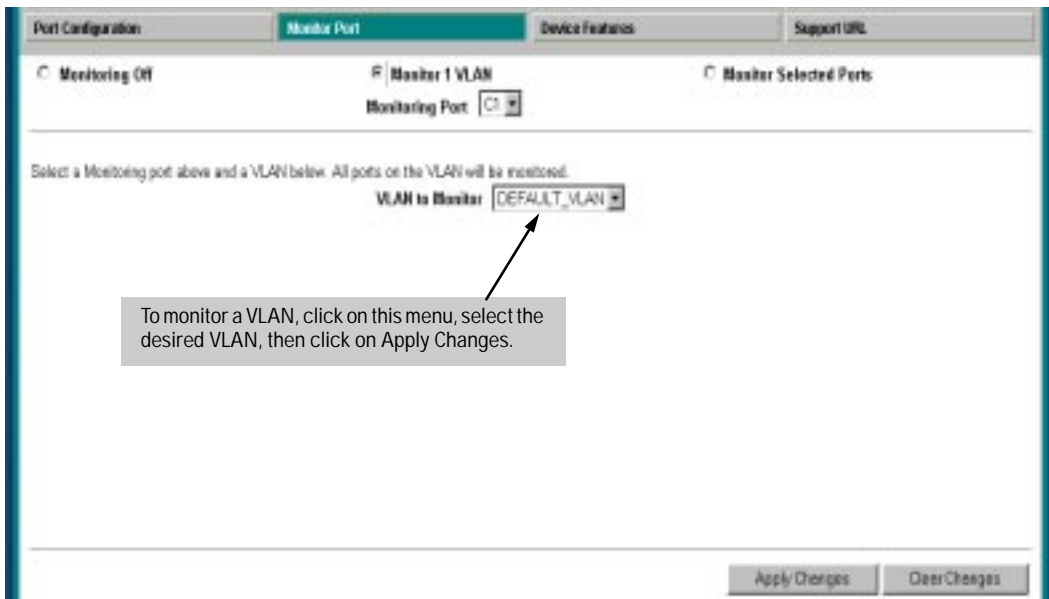


Figure 6-15. Selecting a VLAN To Monitor

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

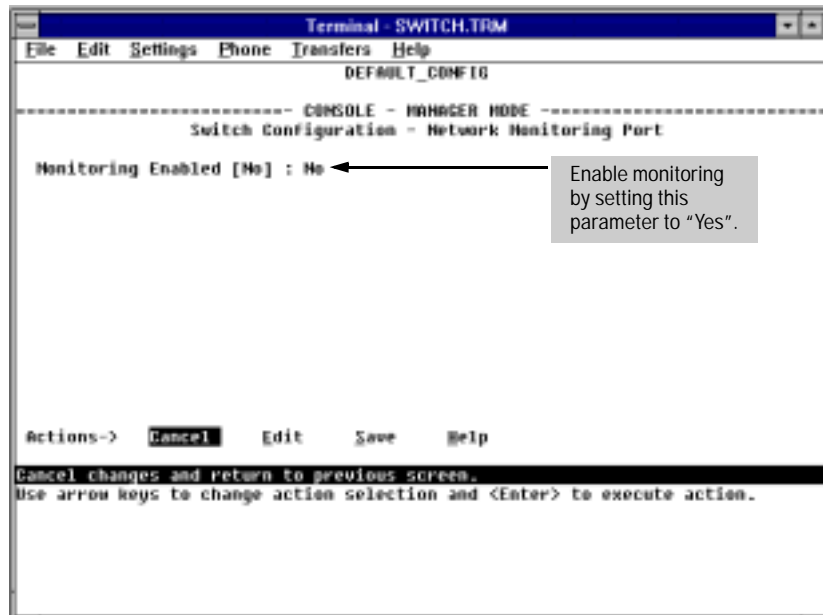


Figure 6-16. The Default Network Monitoring Configuration Screen

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.

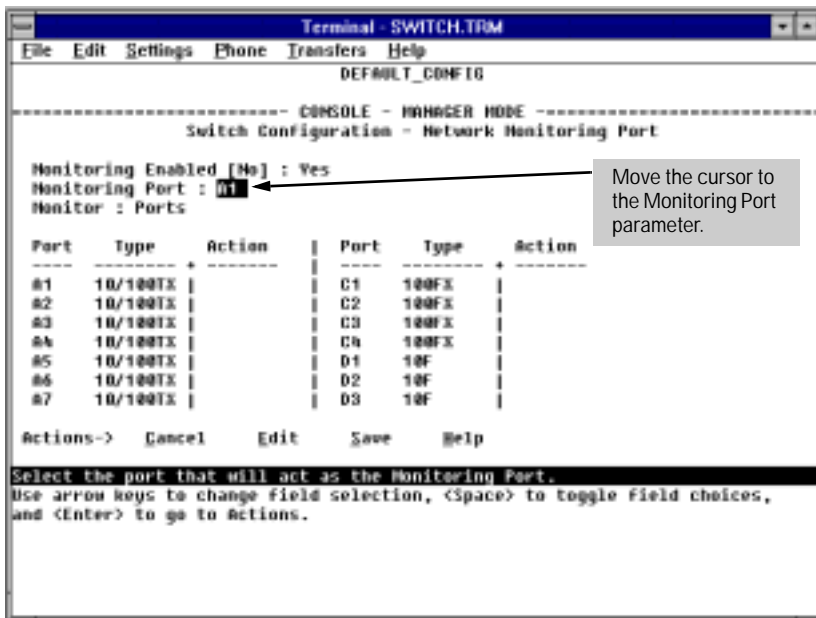


Figure 6-17. Example of Selecting a Monitoring Port

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 **Enter**, then press **S** (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 6-18 on page 6-33). Then press the Space bar again to select the VLAN that you want to monitor. When you are finished, press **Enter**, then press **S** (for **Save**) to save your changes and exit from the screen.
7. Return to the Main Menu.

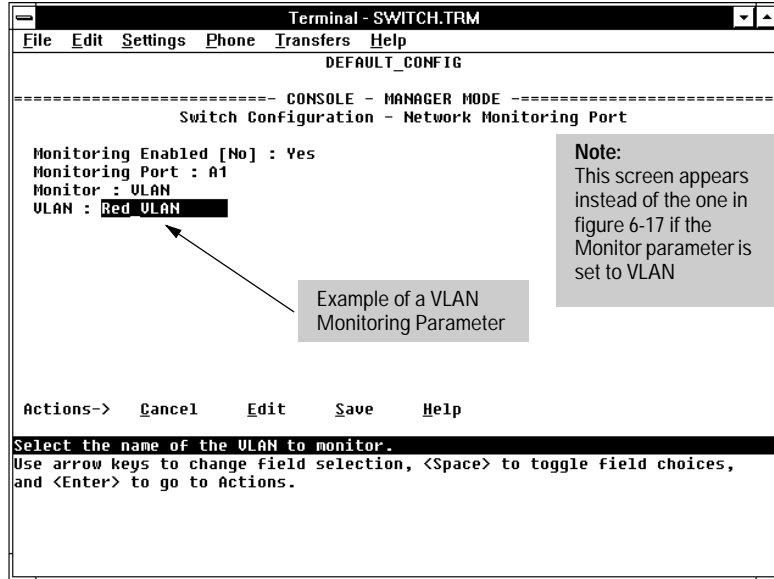


Figure 6-18. Example of Selecting a VLAN to Monitor

Note

It is possible 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.

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 a switch detecting the same node on more than one port. This results in duplication of messages, leading to a “broadcast storm” that can bring down the network.

Note

You should enable STP in any Switch 8000M or Switch 1600M 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.)

As recommended in the IEEE 802.1Q VLAN standard, STP on the Switch 8000 and Switch 1600 use single-instance STP. Thus, these switches do not distinguish between VLANs when identifying redundant physical links. However, STP sees a switch mesh domain as a single port, which enables you to use both STP without blocking switch ports that you want to remain open. These topics are covered in more detail under “How STP Operates” on page 6-37.

You can activate the IEEE 802.1D Spanning Tree Protocol (STP) and adjust STP parameters. In the factory default configuration, STP is off. Thus, if a redundant link (loop) exists between nodes in your network, you should set the Spanning Tree Enabled parameter to Yes. This ensures that all redundant ports (those providing backup parallel connections) are in a blocking state and not used to forward data. In the event of a topology change such as a switch, bridge, or data link failure, STP develops a new spanning tree that may result in changing some ports from the blocking state to the forwarding state.

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.

Configuring STP from the Web Browser Interface

This procedure enables or disables STP on the switch.

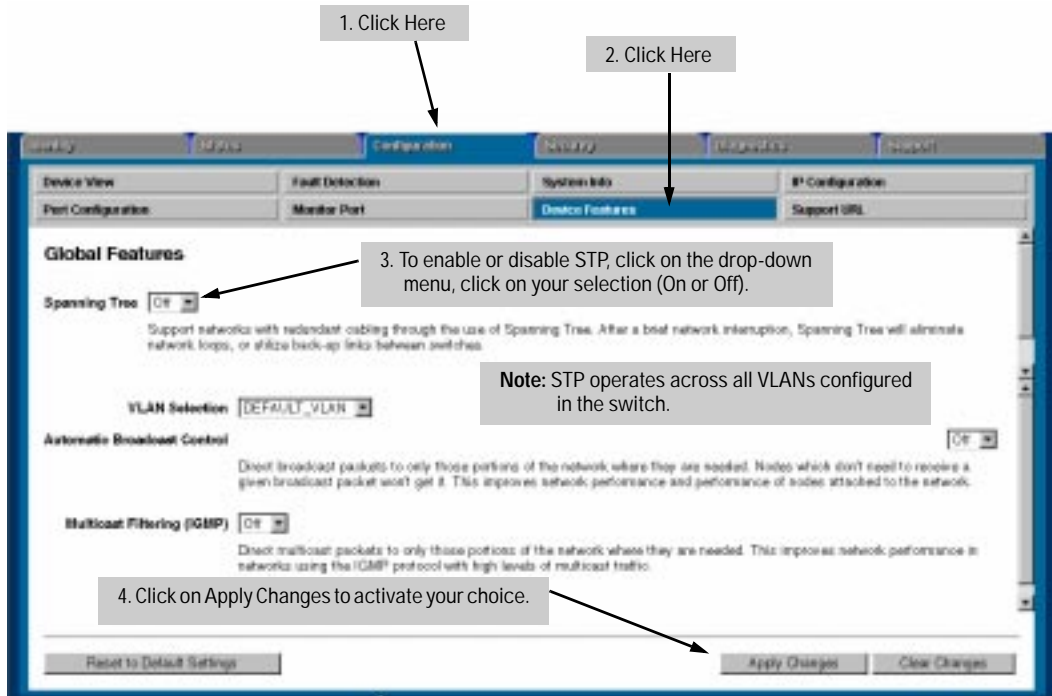


Figure 6-19. Configuring STP from the Web Browser Interface

| WBI 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 6-37. |
| Default: Off | |

Using the Switch Console To Configure STP

In most cases, the default STP parameter settings are adequate. In cases where it is 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:

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

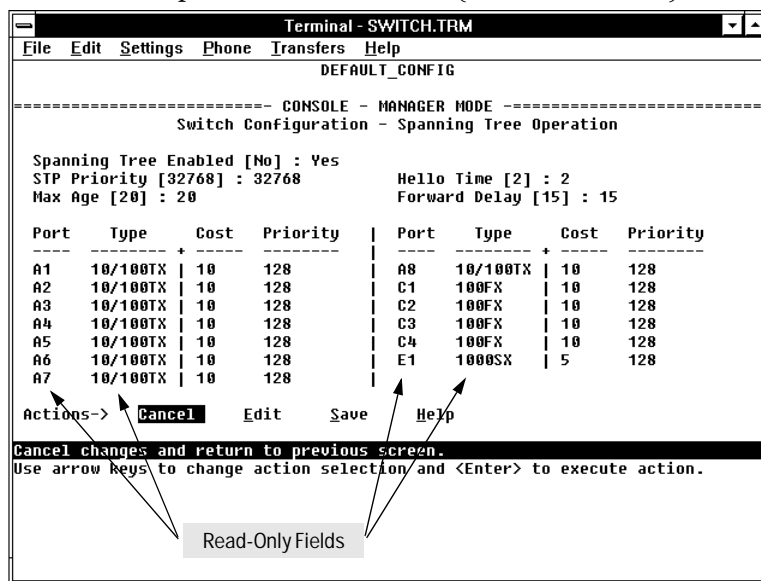


Figure 6-20. Example of the STP Configuration Screen with Ethernet Modules Installed in the Switch

4. 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. (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.
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 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. (STP sees a switch mesh domain as a single path.) 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

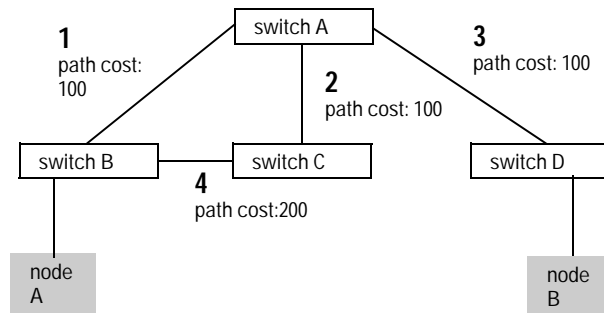


Figure 6-21. Example of Logical and Redundant Paths Between Two Nodes

STP Operation with 802.1Q VLANs

As recommended in the IEEE 802.1Q VLAN standard, 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 8000M or Switch 1600M 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.

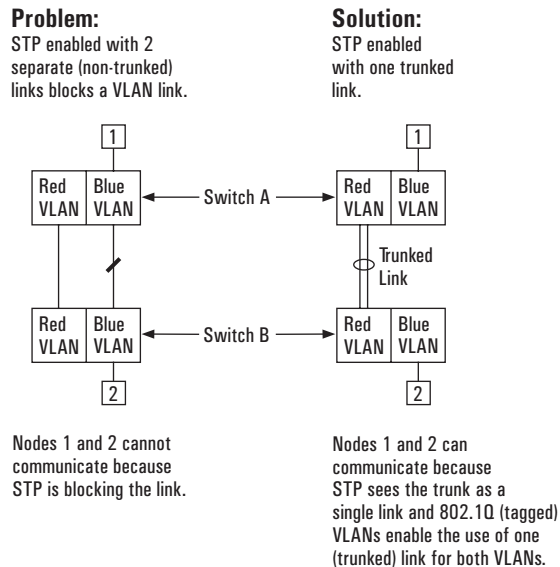


Figure 6-22. Example of Using a Trunked Link with STP and VLANs

For more information, refer to “Spanning Tree Protocol Operation with VLANs” on page 6-60.

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 6-83.

Further Information

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

http://www.hp.com/go/network_city

Traffic/Security Filter Features

To enhance bandwidth usage and in-band security, configure static per-port filters to forward desired traffic or drop unwanted traffic, as described below.

Table 6-2. 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 141 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 6-43.

Configuring Port Monitoring 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

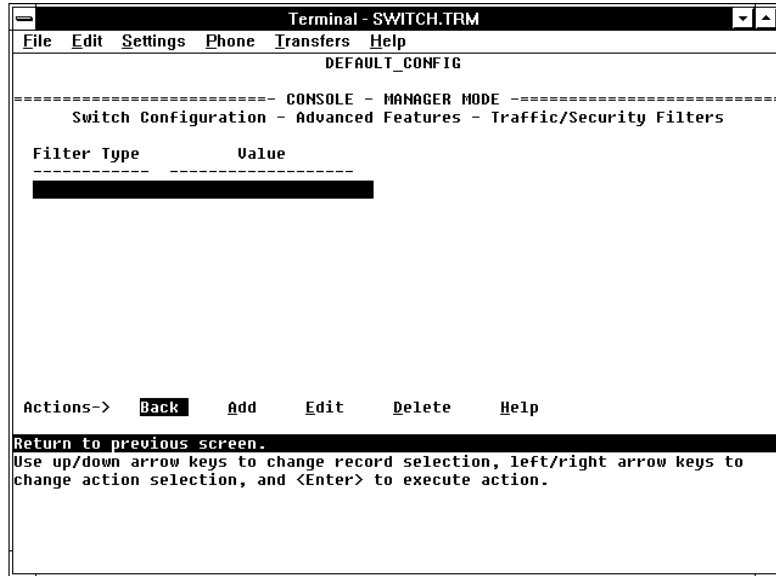


Figure 6-23. The Traffic/Security Filters List Screen (Default Values)

- In the Actions line, press **[A]** (for **Add**) to display the Traffic/Security Filters Configuration screen shown in figure 6-24.

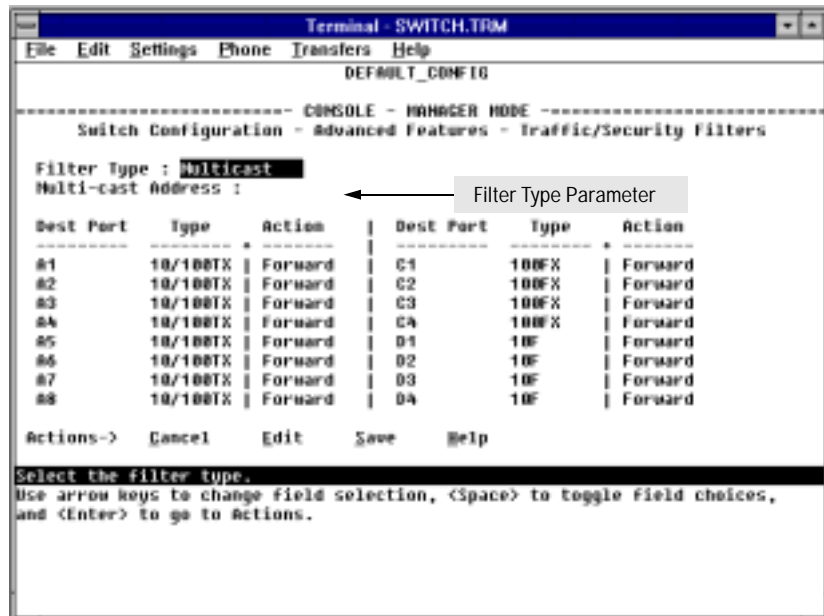


Figure 6-24. Example of the Traffic/Security Filters Configuration Screen

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:

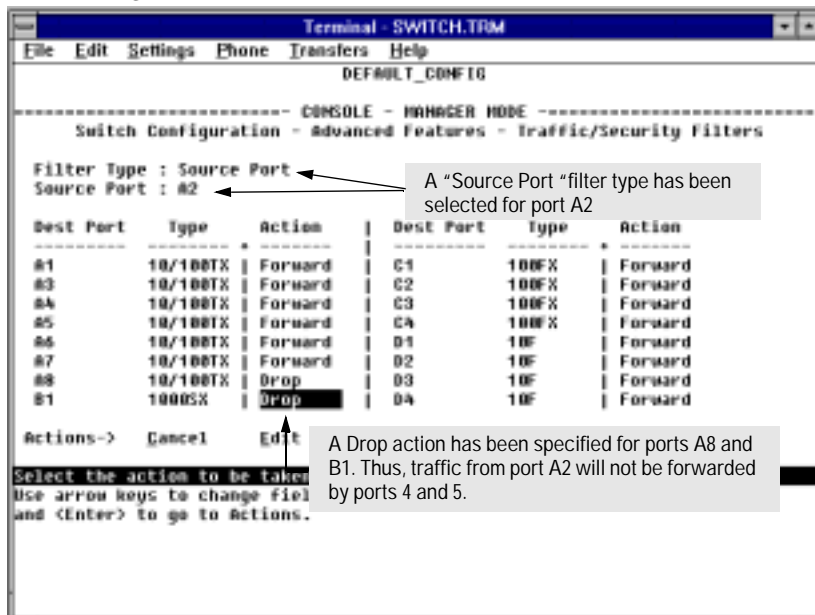


Figure 6-25. Example of Specifying Filter Actions for Individual Ports

- 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 6-89).

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

IP multicast addresses occur in the range from 224.0.0.0 through 239.255.255.255. Any static Traffic/Security filters (page 6-40) 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 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 formerly controlled by IGMP.

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
- NetBIOS
- 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 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 Switch 8000M and the Switch 1600M enable you to configure up to 8 port-based, 802.1Q-compatible VLANs. This enables you to use the same port for two or more VLANs and still 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 increased security. By using port groupings, traffic is isolated to specific domains. A group of network users assigned to a VLAN are a separate traffic domain so that 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, 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.

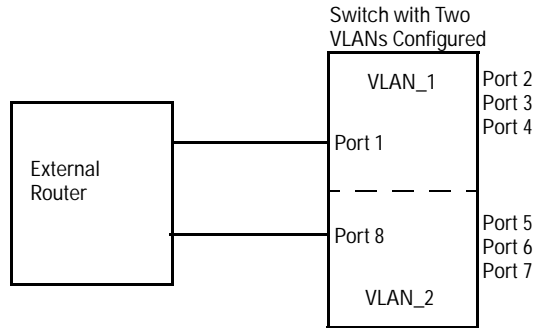


Figure 6-26. Example of Routing Between VLANs via an External Router

Overlapping (Tagged) VLANs. A port on the Switch 8000M or Switch 1600M can be a member of more than one VLAN if the device(s) to which it is connected comply 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 use the server *over the same link*. Where VLANs overlap in this way, VLAN “tags” are used to distinguish between traffic from different VLANs.

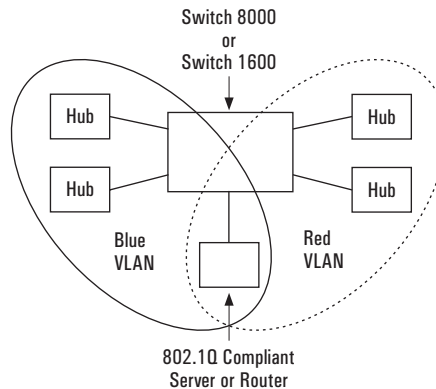


Figure 6-27. Example of Overlapping VLANs Using the Same Server

Similarly, using 802.1Q-compliant switches, you can connect multiple VLANs through the same link.

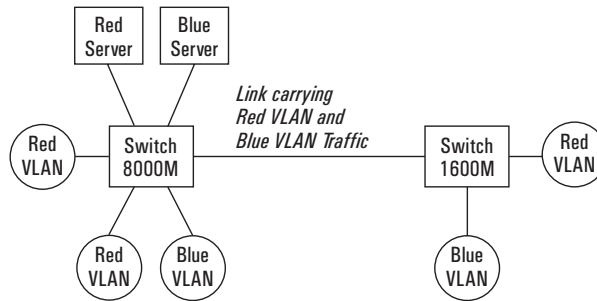


Figure 6-28. Example of Connecting Multiple VLANs Through the Same Link

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.

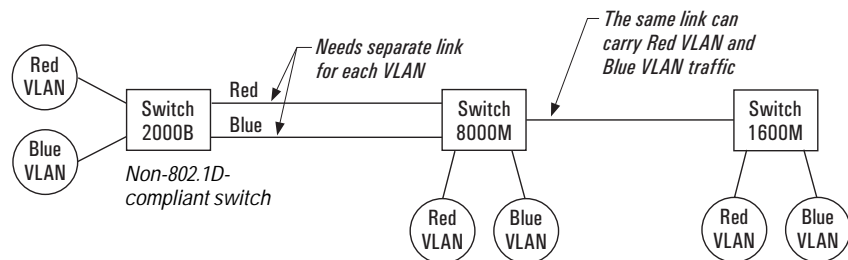


Figure 6-29. Example of Tagged and Untagged VLAN Technology in the Same Network

For more information on VLANs, refer to:

- “Overview of Using VLANs on the Switch 8000M and Switch 1600M”, below.
- “Using the Switch Console To Configure VLAN Parameters” on page 6-49.
- “VLAN Restrictions” on page 6-62.
- “How VLANs Operate” on page 6-56.
- “VLAN Tagging” on page 6-56.
- “Effect of VLANs on Other Switch Features” on page 6-60.

Overview of Using VLANs

VLAN Support and the Default VLAN

In the factory default configuration, VLAN support is de-activated. When you activate VLAN support, all ports are assigned to a physical broadcast domain named **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 8 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 Spanning Tree Protocol, load balancing, IGMP, and Automatic Broadcast Control. (Refer to “Effect of VLANs on Other Switch Features” on page 6-60.)
2. Enable VLANs in the switch. (In the factory default configuration, VLANs are disabled.)
3. Configure at least one VLAN in addition to the default VLAN (**DEFAULT_VLAN**).
4. If you are managing VLANs with SNMP in an IP network, either configure an IP address and subnet mask for each VLAN or use the (default) DHCP/Bootp feature to download an IP configuration from a DHCP or Bootp server. Refer to “Internet (IP) Service” on page 6-6.

Note

Before you delete a VLAN, you must re-assign its ports to another VLAN.

When VLANs are used and are managed from an SNMP workstation, you should configure IP services for each VLAN. (Refer to pages 6-7 and 6-8.)

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.

Further Information

- For further operating information and restrictions, refer to “Further VLAN Operating Information” on page 6-56.
- For further explanation and examples of VLANs operating with other switch features, see HP’s Network City website at the following URL on the World Wide Web:

http://www.hp.com/go/network_city

Using the Switch Console To Configure VLAN Parameters

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 7 additional VLANs by adding new VLAN names, and then assigning one or more ports to each VLAN. (The switch accepts a maximum of 8 VLANs, including the default VLAN.) Note that each port can be assigned to multiple VLANs by using VLAN tagging (described later in this section). DEFAULT_VLAN *can be renamed, but not deleted*. Any ports not specifically assigned to another VLAN will remain assigned to DEFAULT_VLAN.

To Activate or De-Activate VLANs

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

Note

If you activate VLAN support and configure VLANs, then subsequently deactivate 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 Spanning Tree Protocol is enabled.

To Activate VLANs:

1. From the Main Menu select:
 3. Switch Configuration
 5. Advanced Features
 5. VLAN Menu ...
 1. Activate VLAN Support

You will then see the following screen:

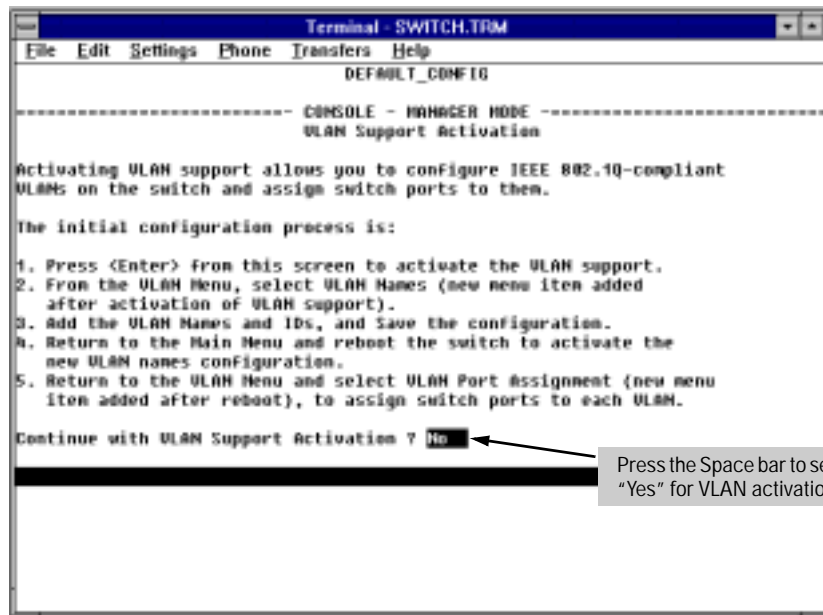


Figure 6-30. VLAN Support Activation Screen

2. Press the Space bar to select **Yes** (for activating VLAN support), then press **Enter**. You will then see the VLAN Menu screen:

The "*" indicates you should reboot the switch to implement the change performed in step 1, above (activate VLAN support).

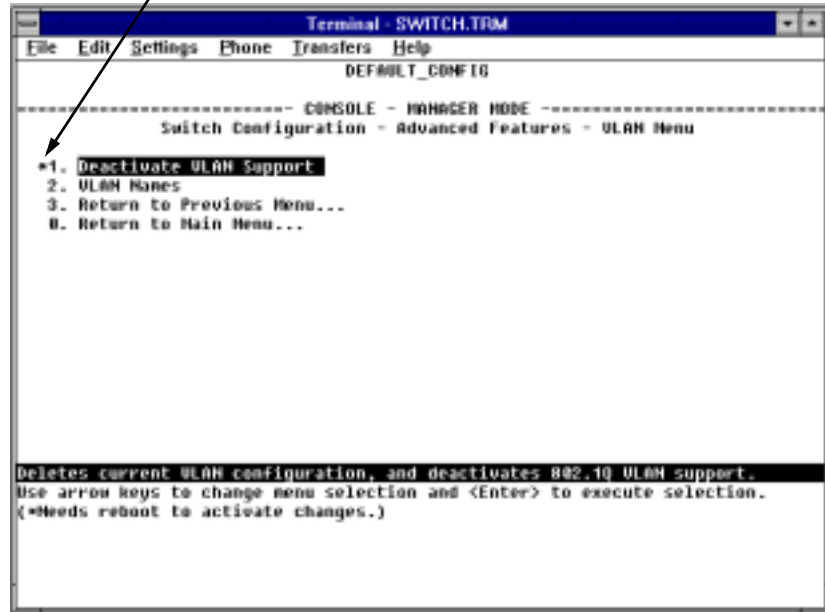


Figure 6-31. The VLAN Menu Screen

3. Do one of the following:
 - If you are not ready to add a specific VLAN at this time, return to the Main Menu and reboot the switch to implement VLAN activation. Once this is done, you can return to the VLAN menu at any time to add specific VLANs.
 - If you want to add one or more specific VLANs now, refer to "How To Create or Edit a VLAN" on page 6-52.

How To Create or Edit a VLAN.

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

Note

If you add a new VLAN or edit the name of an existing VLAN, you should then reboot the switch to activate the new VLAN. (A new VLAN will not appear as an option in the Port VLAN Assignment screen until after the switch is rebooted.) If you create a new VLAN without also rebooting the switch, you will be prompted to choose whether to reboot the switch before entering the Port VLAN Assignment screen. When you move a port to an active VLAN, the new assignment is automatically enabled, and it is not necessary to reboot the switch a second time.

1. From the Main Menu select:

3. Switch Configuration

5. Advanced Features

5. VLAN Menu . . .

2. VLAN Names

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

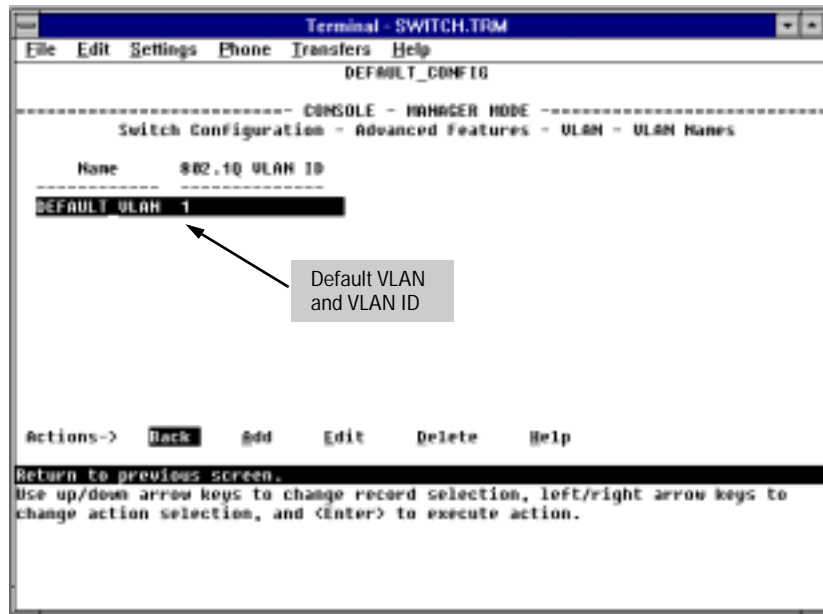


Figure 6-32. The (Default) VLAN Names Screen

2. Press **[A]** (for **A**dd). 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, then press **[Enter]**.
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.)
5. Press **[S]** (for **S**ave). You will then see the VLAN Names screen with the new VLAN listed.

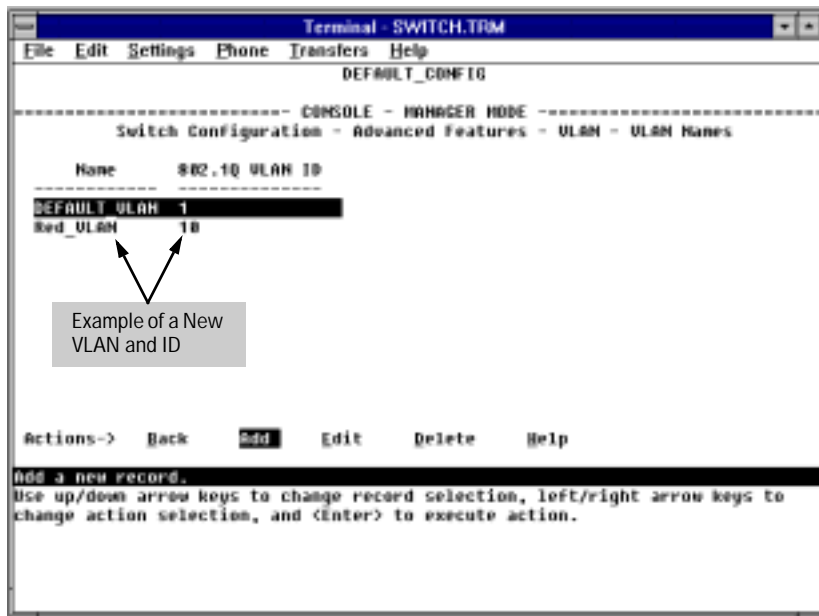


Figure 6-33. Example of the VLAN Names Screen with a New VLAN Added

6. Return to the Main Menu and reboot the switch to activate the new VLAN(s) you have just entered.

Note

After entering a new VLAN, you must reboot the switch before assigning ports to the new VLAN. Also, you can rename "DEFAULT_VLAN", but you cannot delete it from the Switch, regardless of which name you assign to it. When there are no other VLANs configured in the switch, all ports belong to the default VLAN.

To Add or Remove a Port VLAN Assignment

Use this procedure 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
 5. VLAN Menu . . .
 2. VLAN Port Assignment

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

In this example, the "Red_VLAN" has been configured, 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".

```

Terminal - SWITCH.TRM
File Edit Settings Phone Transfers Help
-----
                DEFAULT_CONFIG
-----
Switch Configuration - Advanced Features - VLAN - VLAN Port Assignment
-----
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  No       |  C3   |  Untagged  No
A5   |  Untagged  No       |  C4   |  Untagged  No
A6   |  Untagged  No       |  E1   |  Untagged  No
A7   |  Untagged  No
-----
Actions->  Cancel  Edit  Save  Help
-----
Cancel changes and return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.

```

Figure 6-34. 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 would look like this:

| | | | | | |
|----|----------|----------|----|----------|----|
| 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 6-35. Example of VLAN Assignments for Specific Ports

For information on VLAN tags (“Untagged” and “Tagged”), refer to “Vlan Tagging” on page 6-56.

- 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.)

Further VLAN Operating Information

VLAN Tagging

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 Switch 8000M and 1600M 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 enables you to use the “Untagged” designation for ports connected to non 802.1Q-compliant devices and the “Tagged” designation for ports connected to devices that do comply with the 802.1Q standard.

For example, if port A7 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 A7, then at least one of those VLAN assignments must be “tagged” so that red traffic can be distinguished from green traffic. The following illustration demonstrates this concept:

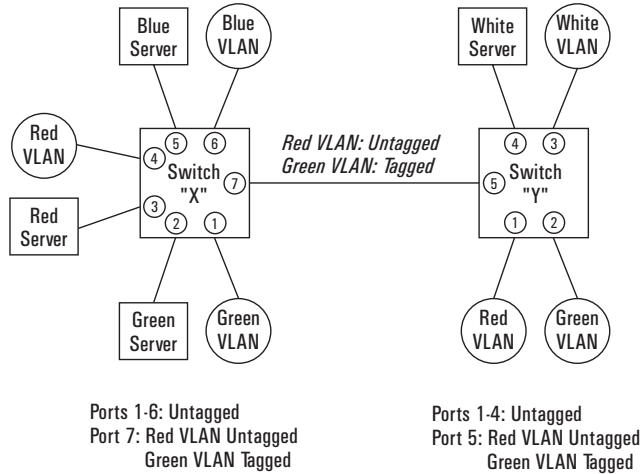


Figure 6-36. Example of Tagged and Untagged VLAN Port Assignments

- In switch X:
 - VLANs assigned to ports X1 - X6 can all be untagged because there is only one VLAN assignment per port. Red traffic will go out only the red ports; green 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.
- 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 Blue 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. That is, a particular VLAN should be given the same VLAN ID in every device. That is, if the “red” VLAN has a VLAN ID of 10 in switch “A”, then 10 should also be used for the red VLAN ID in switch “B”.

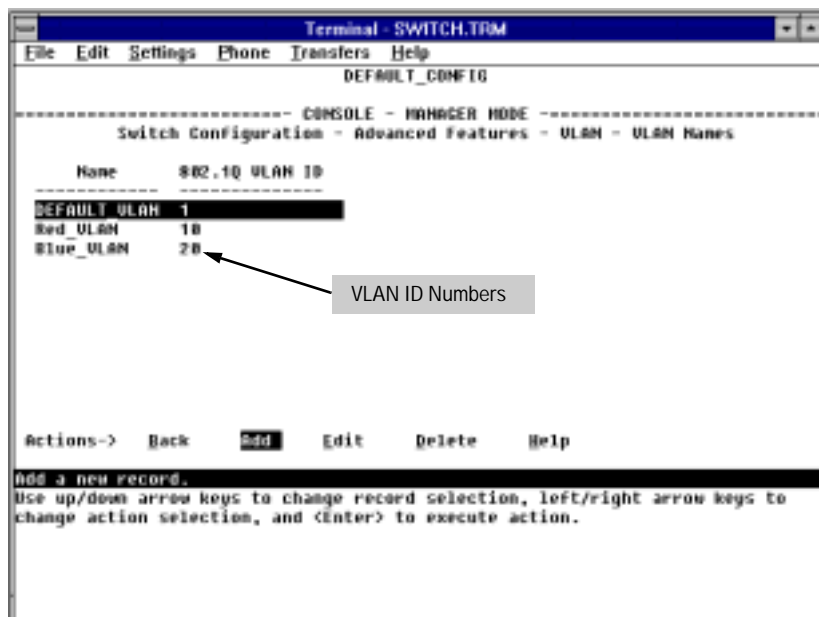


Figure 6-37. Example of VLAN ID Numbers Assigned in the VLAN Names Screen

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.

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.)

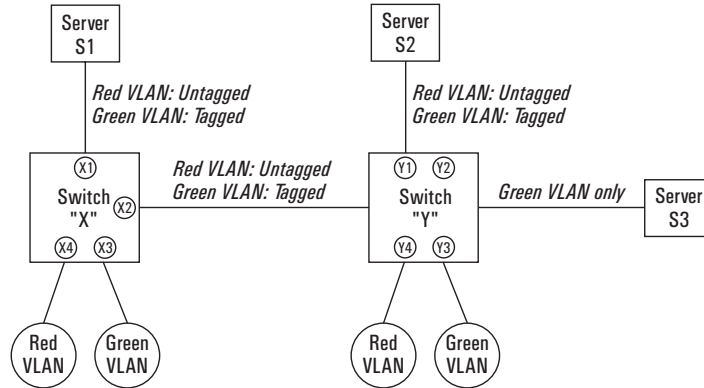


Figure 6-38. Example of Networked 802.1Q-Compliant Devices with Multiple VLANs on Some Ports

The VLANs assigned to ports X-3, X-4, Y-2, Y-3, and Y-4 can all be untagged because there is only one VLAN assigned per port. Port X-1 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 X-2 and Y-1.

| Switch "X" | | | Switch "Y" | | |
|------------|----------|------------|------------|----------|------------|
| Port | Red VLAN | Green VLAN | Port | Red VLAN | Green VLAN |
| X-1 | Untagged | Tagged | Y-1 | Untagged | Tagged |
| X-2 | Untagged | Tagged | Y-2 | No* | Untagged |
| X-3 | No* | Untagged | Y-3 | No* | Untagged |
| X-4 | Untagged | No* | Y-4 | Untagged | No* |
| | | | Y-5 | Untagged | Tagged |

*"No" means the port is not a member of that VLAN. For example, port X-3 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 X-A and Y-E 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 VLAN should have the same VLAN ID on any 802.1Q-compliant device in the network. The ports connecting two 802.1Q devices should have identical VLAN configurations, as shown for ports A1 and B5, above.

Effect of VLANs on Other Switch Features

Spanning Tree Protocol Operation with VLANs

Because the Switch 8000M and the Switch 1600M 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 Switch Meshing to prevent STP from unnecessarily blocking ports (and to improve overall network performance). Refer to “Spanning Tree Operation with Switch Meshing” on page 6-83.

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 8000M or Switch 1600M 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 8 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 8-8.

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 6-85.

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 port per VLAN 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 A09.70 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 remove all of its unmeshed ports from the 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 Services” 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 a duplicate MAC address can appear in the Port Address Table screen to be linked with one port, and then later appear to be linked to another port.

Load Balancing: Port Trunking

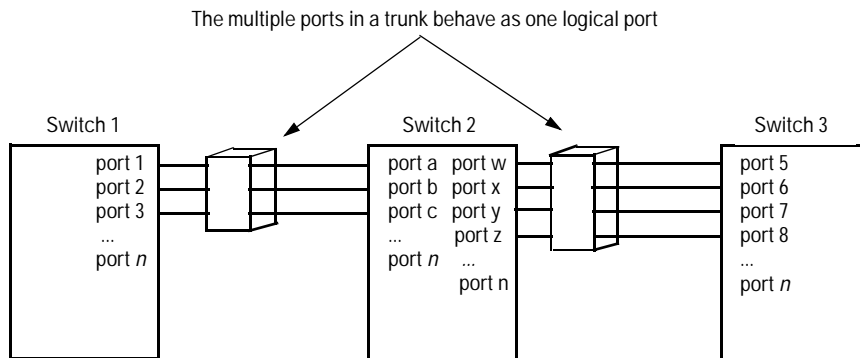


Figure 6-39. Conceptual Illustration of Port Trunking

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:

- 10Base-T links: Up to 80Mbps
- 100Base-T links: Up to 800 Mbps

The Switch 8000M and the Switch 1600M both support up to ten four-port trunks.

Note

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 re-connect 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 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, traffic is again redistributed to utilize the restored link.

Port Connections and Configuration: All port trunk links must be point-to-point connections between the Switch 8000M/1600M 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 blue VLAN.

then port A3 will be a member of the blue VLAN instead of the original red VLAN. However, if filters are in use:

- If, for example, port A3 was configured to *drop* IPX packets *before* it became a member of trunk 1 and . . .
- If trunk 1 was configured to *forward* IPX packets, then port A3 will also forward IPX packets while it is a member of trunk 1. However, if you subsequently remove port A3 from trunk 1, then port A3 resumes dropping IPX packets.

Interoperability

The Switch 8000M and the Switch 1600M both provide a broad set of port trunking capabilities that enable trunking with the HP switch products listed below. These two 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 Switch 8000M and Switch 1600M. (However, note that the Trunk option uses the IEEE 802.3 standards for auto-negotiating half- or full-duplex operation and auto-sensing 10Mbps, 100Mbps, and 1Gps links.) For more information on this topic, refer to the Technology area of HP's network city website at:

www.hp.com/go/network_city

Trunk Configuration Options

There are three trunk configuration types from which to select:

| Type | Distribution Method | Recommended Switch 8000M/1600M Configuration for Trunking to: |
|-------|--|---|
| Trunk | Source Address/Destination Address (SA/DA) | <ul style="list-style-type: none">• Another HP Switch 8000M/1600M• 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 |

| Type | Distribution Method | Recommended Switch 8000M/1600M Configuration for Trunking to: |
|----------|-----------------------------|--|
| 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. |

Using the Console To Configure Port Trunks

Important. 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 6-24—to temporarily disable the ports until the trunk is configured.)

To Access Port Trunking:

1. If you need to connect ports for a trunk before configuring them, refer to “Port Settings” on page 6-24 to temporarily disable the ports until the trunk is configured. Otherwise, just avoid connecting the ports in the trunk until after you configure trunking. (This avoids creating a loop that could result in overloading the network with a broadcast storm.)
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.

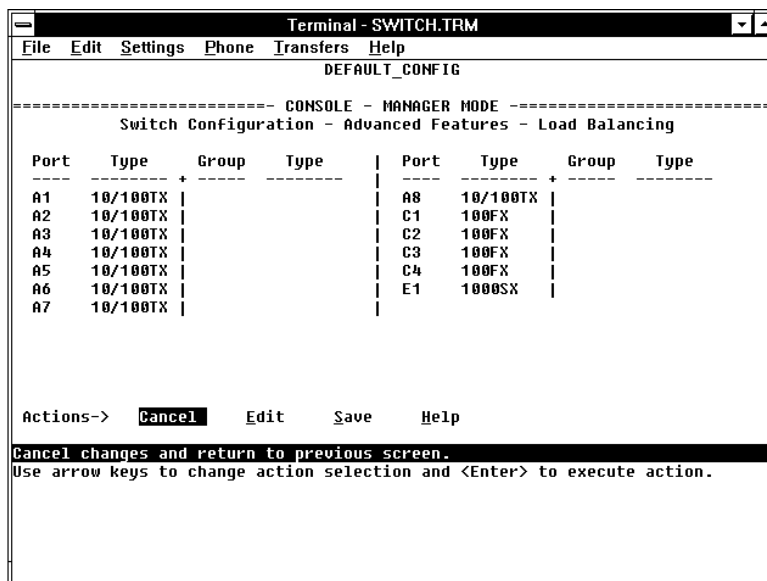


Figure 6-40. Example of the Screen for Configuring Ports for Load Balancing

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 6-24.
 - 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 must belong to the same VLAN or set of VLANs. (With the 802.1Q VLAN capability built into the switch, a port can belong to more than one VLAN. Refer to “Virtual LANs (VLANs)” on page 6-45.)

(To return a port to a non-trunk status, keep pressing the Space bar until a blank appears in the highlighted Group cell for that port.)


```

Terminal - SWITCH.TRM
File Edit Settings Phone Transfers Help
DEFAULT_CONFIG
----- CONSOLE - MANAGER MODE -----
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 6-41. 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 6-71.
 - SA-Trunk (Source-Address trunk)—page 6-72
 - FEC (Fast EtherChannel® trunk)—page 6-72

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

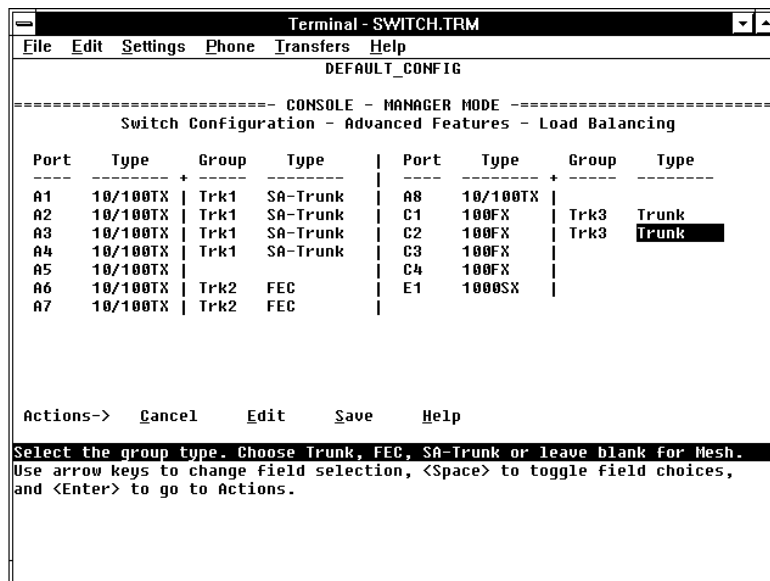


Figure 6-42. Example of trunks with different trunk types

- 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.

- 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 6-24.)
- Check the Event Log and the Switch Mesh Information screen (page) to verify that the meshed 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 (Source Address/ Destination Address, or SA/DA) Option

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

Configuring the Trunk (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 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.

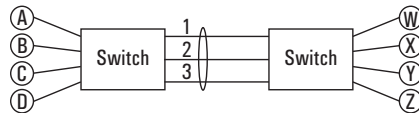


Figure 6-43. Example of Port-Trunked Network

Example of Link Assignments in a Trunk

| 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 (Source-Address Distribution) 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. For example, in figure 6-43 above:

| Source Nodes: | Destination Nodes: | Link: | |
|---------------|--------------------|-------|---|
| Node A | Node W | 1 | |
| Node B | Node X | 2 | |
| Node C | Node Y | 3 | <i>Source Nodes A and D Always Appear on Port 1</i> |
| Node D | Node Z | 1 | |
| Node A | Node Y | 1 | |
| Node B | Node W | 2 | |

Trunk Operation Using the FEC (Fast EtherChannel®) Option

This is the most flexible method for distributing traffic over trunked links when connecting to devices that use the FEC technology. HP FEC trunks offer the following benefits:

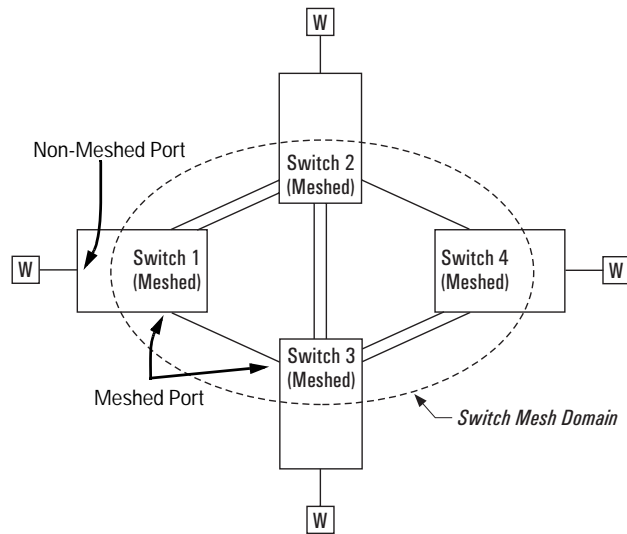
- Provide trunked connectivity to a FEC-compliant server, switch, or router.
- Enable quick convergence to remaining links when a failure is detected on a trunked port link.
- Depending on the capabilities of the device on the other end of the trunk, negotiate the forwarding mechanism on the trunk to 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 6-44. 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 (page 6-23)—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.

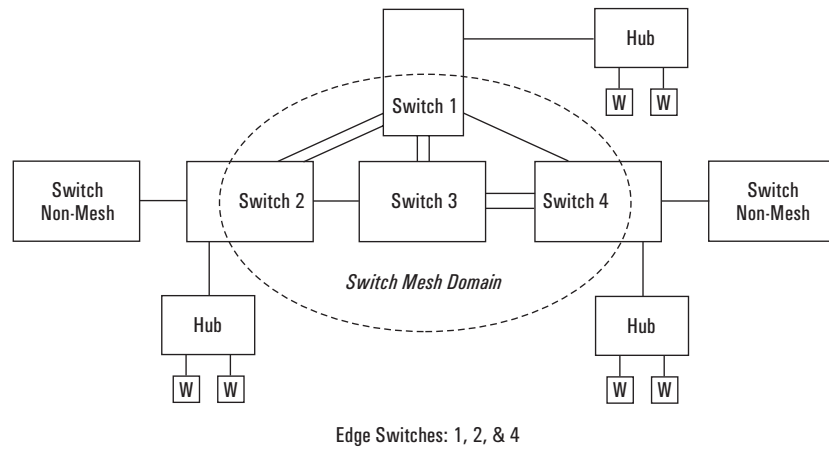


Figure 6-45. Example of a Switch Mesh Domain in a Network

Note

Hubs, switches that are not configured for load balancing, and non load-balanced ports in a switch that has some 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 6-76, above.)

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

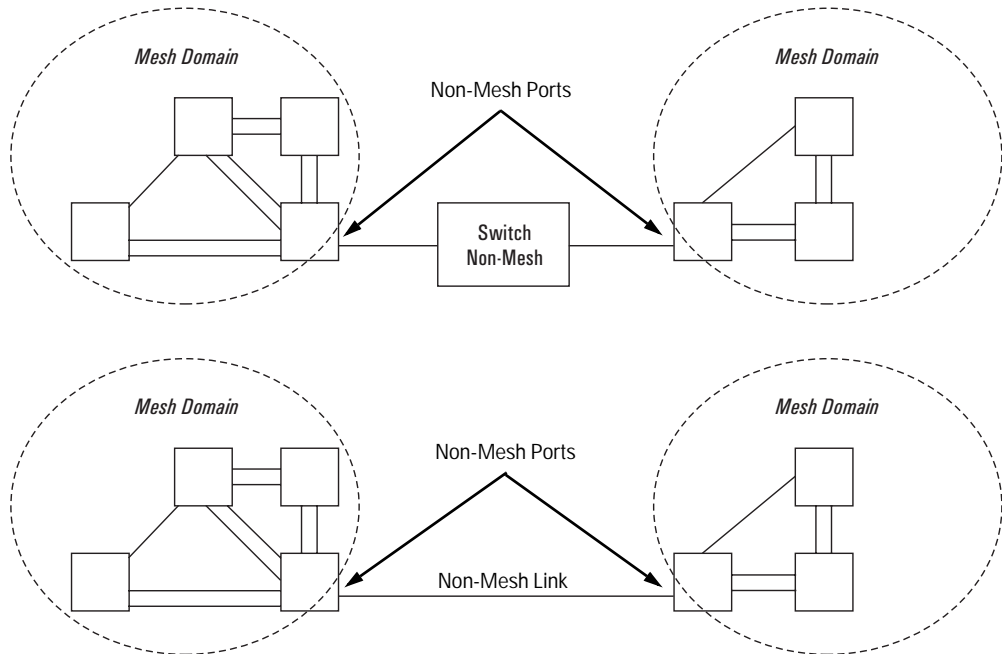


Figure 6-46. Example of Multiple Meshed Switch Domains Separated by a Non-Mesh Switch or a Non-Mesh Link

Configuration Requirements. Before configuring switch meshing on any ports in the Switch 8000M or Switch 1600M, 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 6-78)

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 6-81.

- 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/network_city

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 6-50 to activate VLAN support before continuing here. (VLAN support must be active 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.

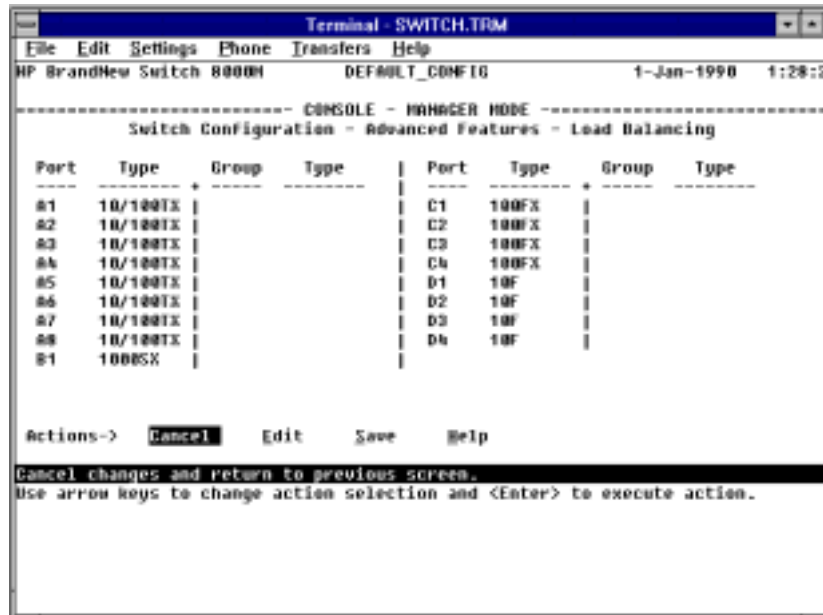


Figure 6-47. Example of the Screen for Configuring Ports for Load Balancing

4. In the Group column, move the cursor to the port you want to assign to the switch mesh.
5. 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 6-45 on page 6-76.)

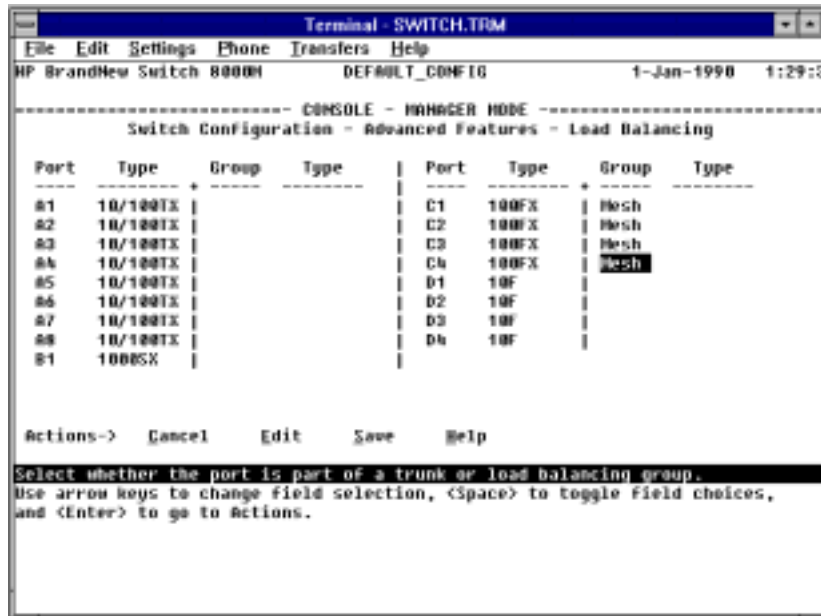


Figure 6-48. Example of Mesh Group Assignments for Several Ports

- 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 7-21.

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.)

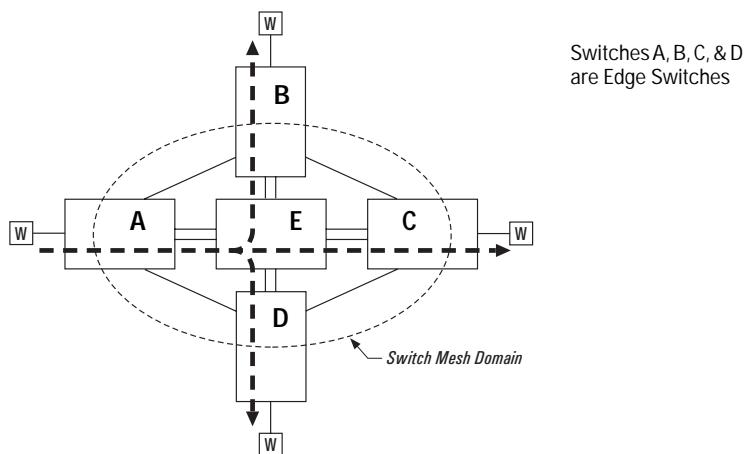


Figure 6-49. Example of a Broadcast Path Through a Switch Mesh Domain

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 6-85.) 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 6-85.
- 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 disrupting traffic within a VLAN. For example:

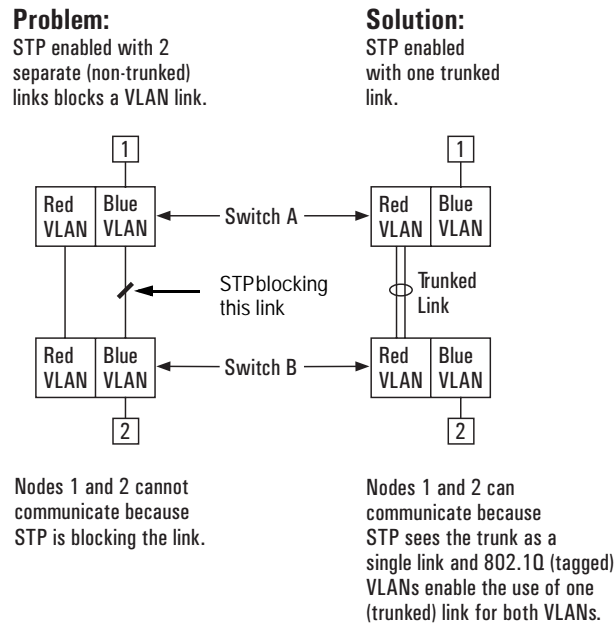


Figure 6-50. Example Using STP Without and With Switch Meshing

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:

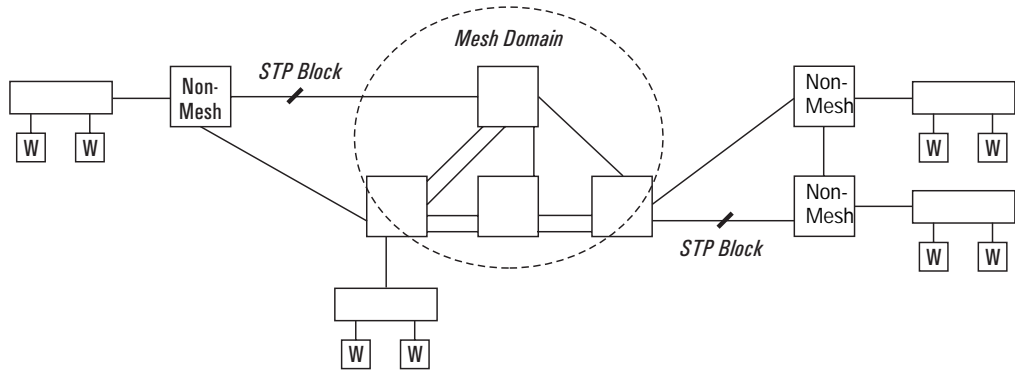


Figure 6-51. Connecting a Switch Mesh Domain to Non-Meshed Devices

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:

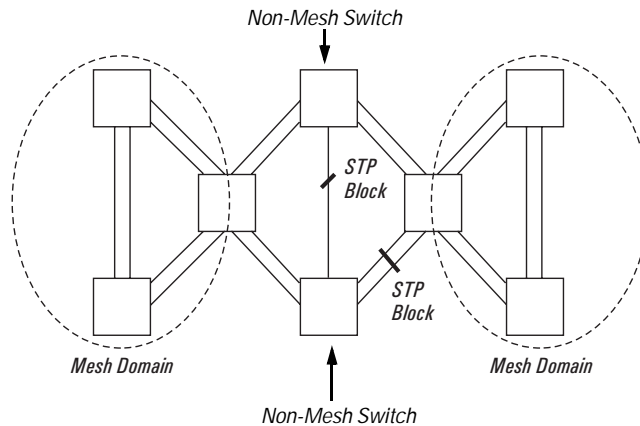


Figure 6-52. Interconnecting Switch Mesh Domains with Redundant Links

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 6-34), 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.

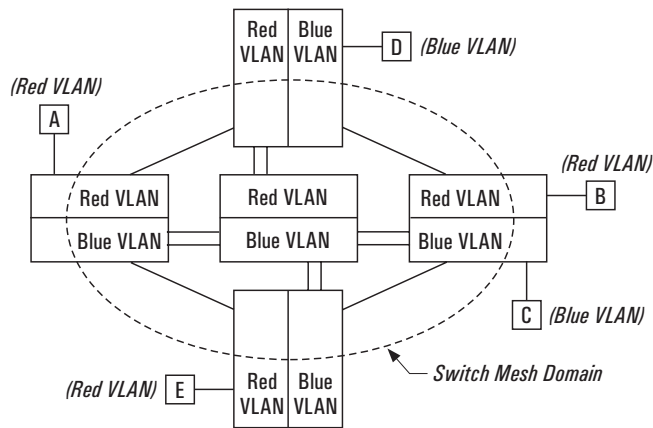
IP Multicast (IGMP) in Meshed Switches

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 6-53. VLAN Operation with a Switch Mesh Domain

Using Automatic Broadcast Control in a Switch Mesh Environment

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 a Switch 8000M or a Switch 1600M.
- **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.

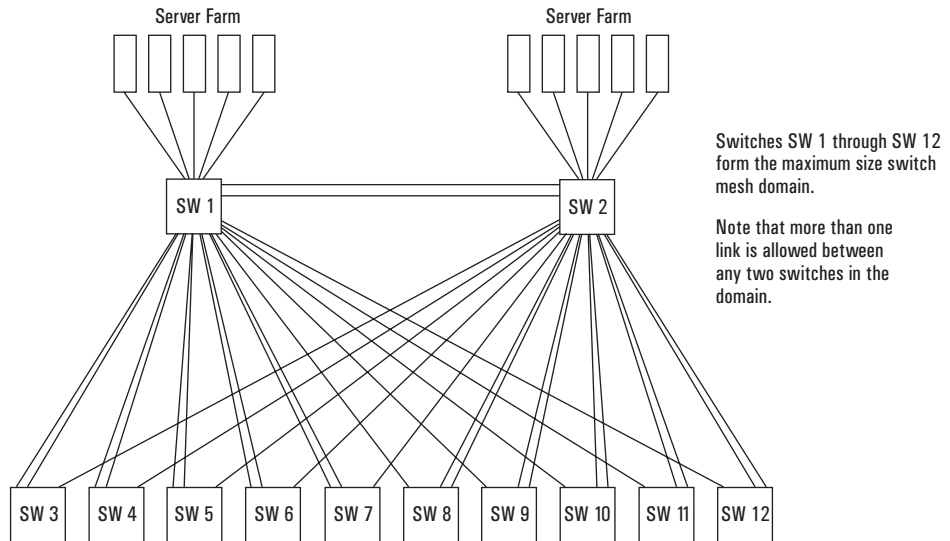


Figure 6-54. Example of a Backbone Using the Maximum Number of Meshed Switches

- **Mesh Support Within the Domain:** All switches in the mesh domain, including edge switches, must support the HP switch meshing protocol. As of Fall, 1998, this includes the HP Switch 8000 and HP Switch 1600 models. For further information, contact your HP-authorized LAN dealer or refer to HP's Network City website at:

http://www.hp.com/go/network_city

- **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.

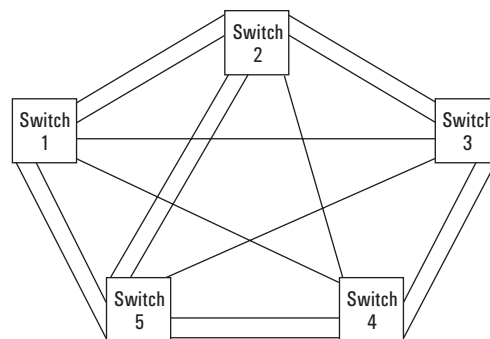


Figure 6-55. Example of the Maximum Meshed Switch Hop Count

- **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 6-46 on page 6-77.
- **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) Service 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. HP switches that support IGMP include:

- HP Switch 1600M ■ HP Switch 2000 (B-version)
- HP Switch 8000M ■ HP Switch 800T

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 6-98.)

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 (Internet) Service on page 6-6.

For more information on IGMP operation, refer to “How IGMP Operates” on page 6-94.

Configuring IGMP from the Web Browser Interface

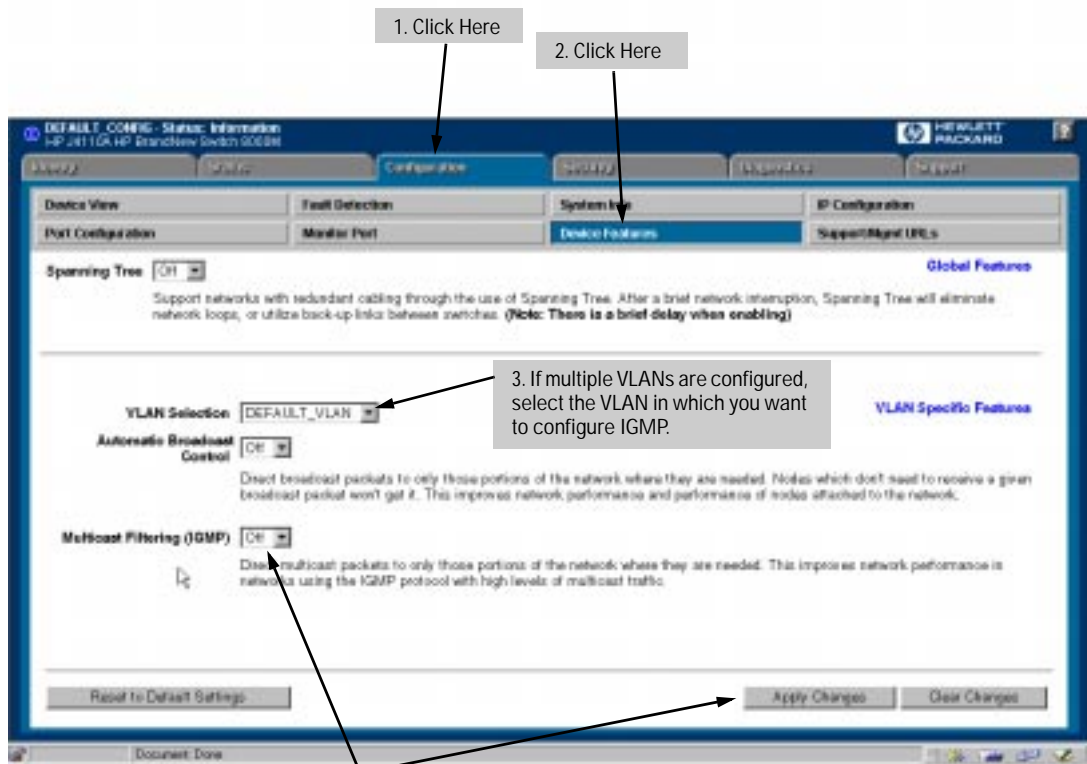


Figure 6-56. Configuring IGMP on the Web Browser Interface

| WBI Parameter | Description |
|---|--|
| Multicast Filtering (IGMP) Default: Off | 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. When Off, all ports on the switch or VLAN simply forward IP multicast traffic. When On, enables each port on the switch or VLAN to detect IGMP queries and report packets, and to manage IP multicast traffic. 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. |
| Further Options Available in the Switch Console | By using the switch console, you can make these further changes to IGMP operation: <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.) For more information, refer to "Using the Switch Console to Configure IGMP" (page 6-92) and "How IGMP Operates" (page 6-94.). |

Using the Switch Console To Configure IGMP

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. If priority forwarding is supported by the network technology you are using, 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 6-94.

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

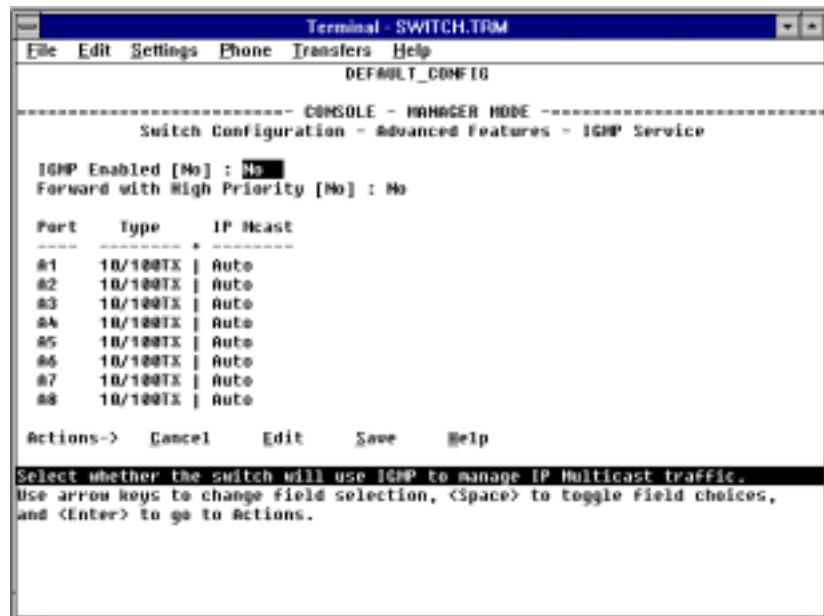


Figure 6-57. Example of the (Default) IGMP Service Screen

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 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 **[Enter]** and **[S]** (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 the "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) are termed a *multicast group*, and have 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 console, using the IGMP configuration MIB. Refer to "Changing the Querier Configuration Setting" on 6-98.)
- **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 7-18.

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 6-59 on page 6-97 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.

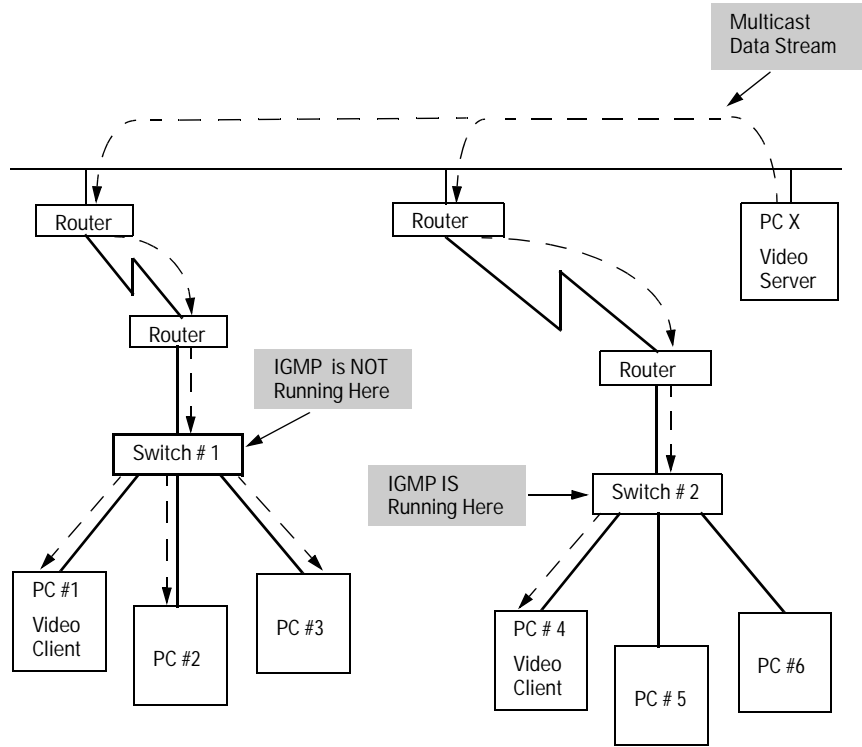


Figure 6-58. The Advantage of Using IGMP

The next figure (6-59) 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.)

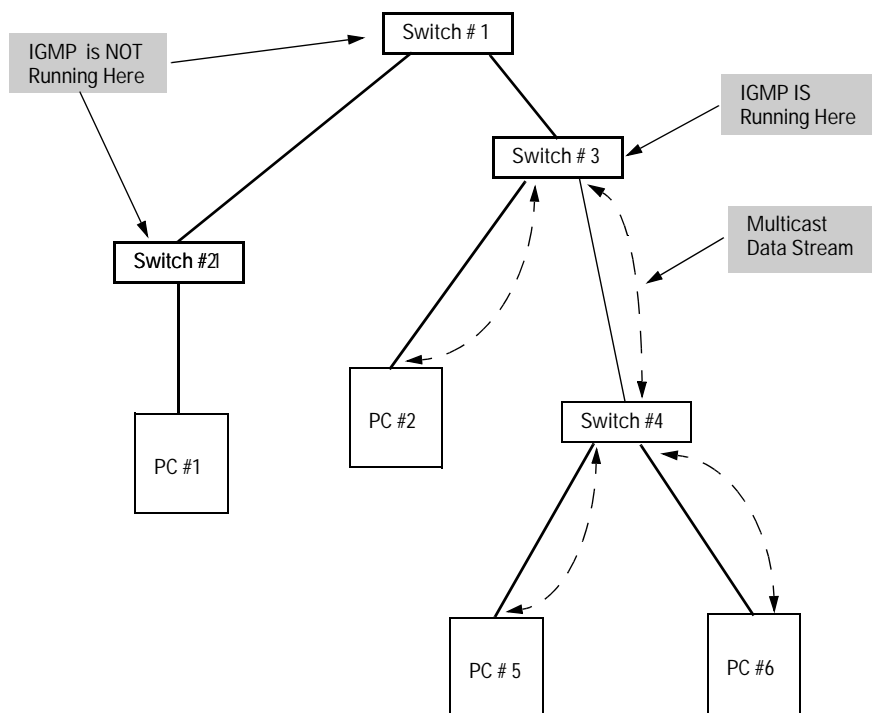


Figure 6-59. Isolating IP Multicast Traffic in a Network

- 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 off of 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.

Note:

IP Multicast Filters

IP multicast addresses occur in the range from 224.0.0.0 through 239.255.255.255. Any static Traffic/Security filters (page 6-40) 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 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 formerly controlled by IGMP.

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 6-40) 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 Advanced Command prompt from the Main Menu and enter this command:

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

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

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

To view the current querier setting, select the Advanced 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

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

Automatic Broadcast Control (ABC) Features—Layer 3 Switching

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 the ultimate destination of broadcast IP ARP and RIP packets, IPX NSQ, and RIP or SAP packets. 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 6-12) for all ports on the switch (or selected VLAN, if VLANs are configured) that have not already been set to a nonzero value.

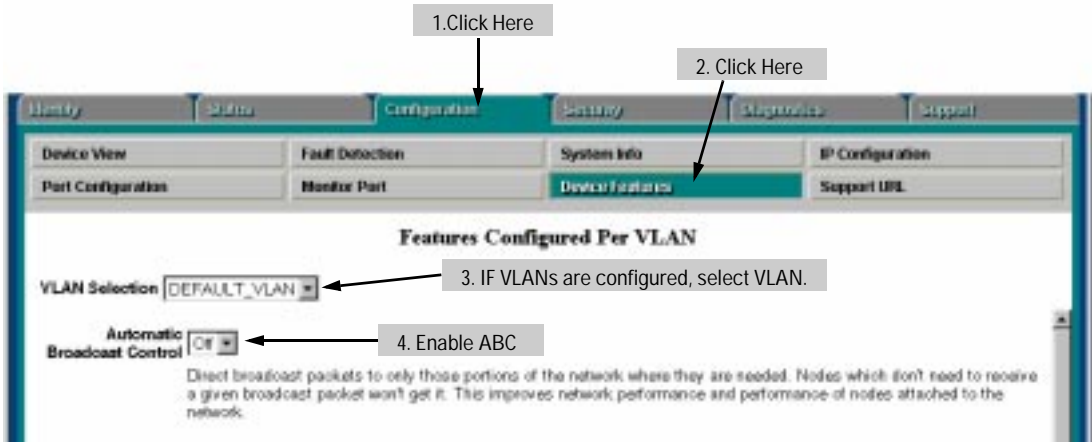
In the factory default state, ABC is disabled.

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 6-40.

For further operating information and restrictions, refer to “How ABC Operates” on page 6-107.

Using the HP Web Browser Interface To Configure ABC Parameters



| HP-WBI 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.) For more on VLANs, refer to “Virtual LAN (VLAN) Features” on page X-YY. |
| 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 “Using the Switch Console To Configure ABC Parameters” (page 6-102) and “How ABC Operates” (page 6-107). |

Using the Switch Console To Configure ABC Parameters

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 ports where 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 RIPs 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 6-27—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 ABC for IPX RIP/SAP control. If enabled, IPX RIP/SAP control causes IPX RIP and SAP broadcasts to be forwarded only to ports where IPX RIPs 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)

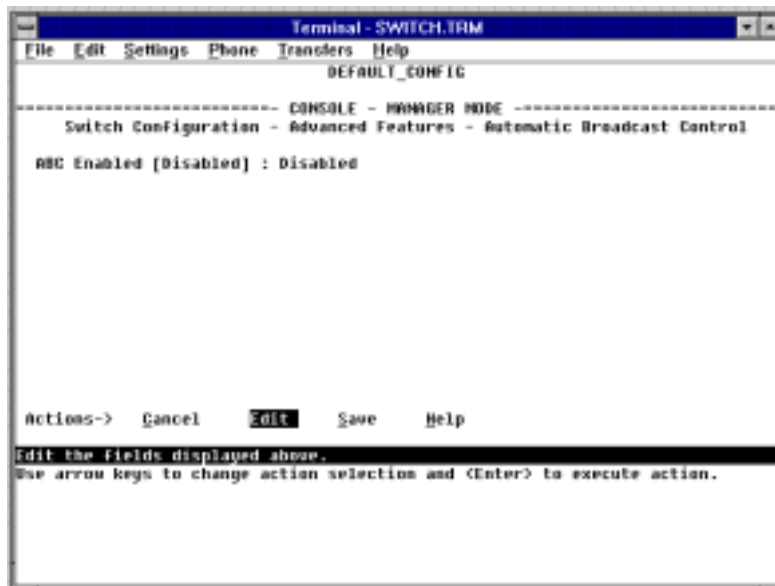


Figure 6-60. The Default ABC Screen (No VLANs Configured)

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.

5. Press the key to display the remaining ABC parameters. Then do *one* of the following:
 - If you enabled ABC for IP_IPX and pressed (figure 6-61, below):

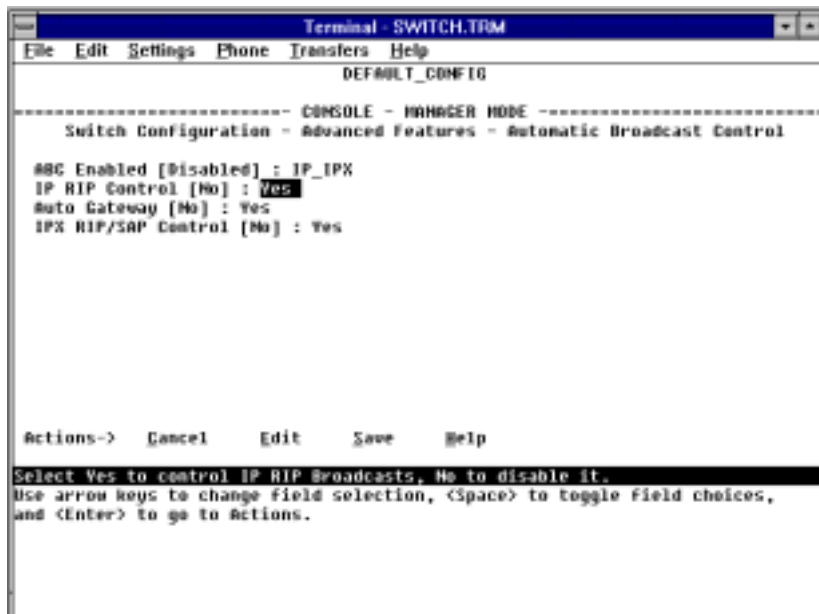


Figure 6-61. ABC Enabled With Default IP_IPX Option (No VLANs Configured)

- 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 6-110.)
- 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 6-107.

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 Configuration screen (page 6-27) and setting the broadcast limit individually for one or more ports.

- If you enabled ABC for IP (figure 6-62, below):

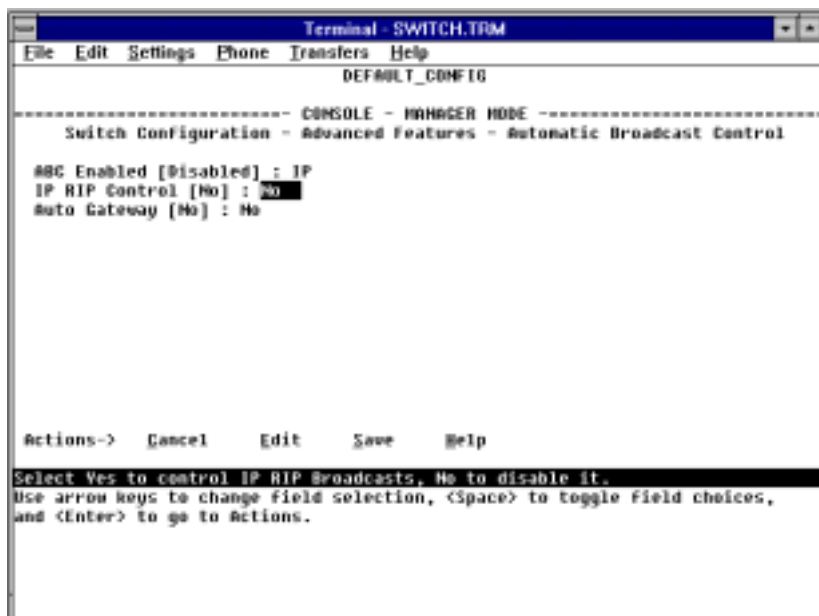


Figure 6-62. ABC Enabled With Default IP Option (No VLANs Configured)

- 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 6-110.)
- iii. Go to step 6 on page 6-107.

- If you enabled ABC for IPX (figure 6-63, below):

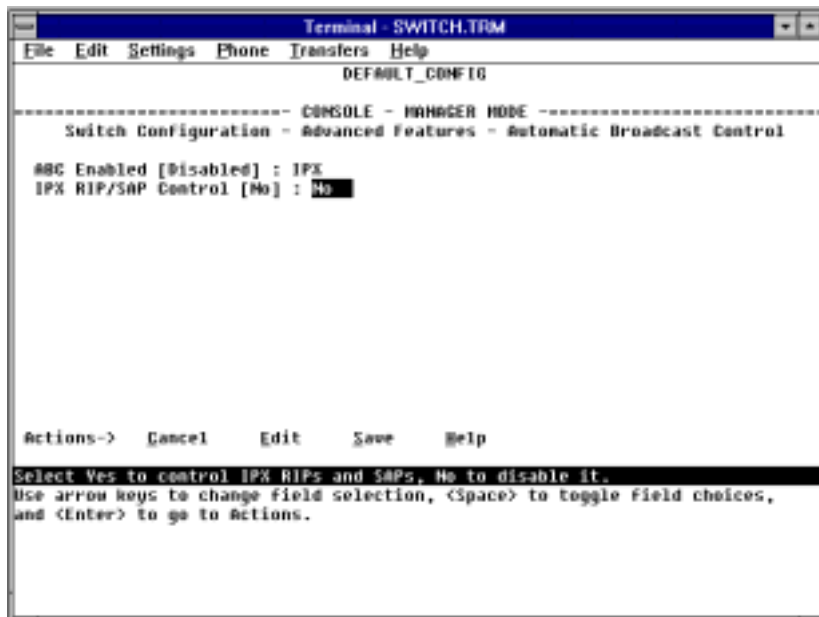


Figure 6-63. ABC Enabled With Default IPX Option (No VLANs Configured)

- If you want IPX RIP/SAP control, then select the **IPX RIP/SAP Control** parameter.
 - Use the Space bar to select **Yes**.
 - Go to step 6, below.
- Press **[Enter]** to return to the **Actions** menu.
 - Press **[S]** (for **Save**) to activate the changes you have made.
 - 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 6.)

How ABC Operates

Level 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-Pack-

ard 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. Learning 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 responding 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.

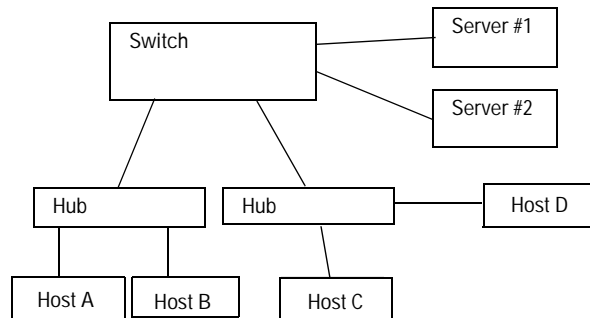


Figure 6-64. Example of a Network Using ABC

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 6-64) 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 produces better performance because the switch is able to provide proxy replies to more nodes.)

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:

- A switch has replaced a router as the gateway to nodes on other subnets.
- DHCP is the automatic configuration protocol used to manage IP addresses on the network

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.

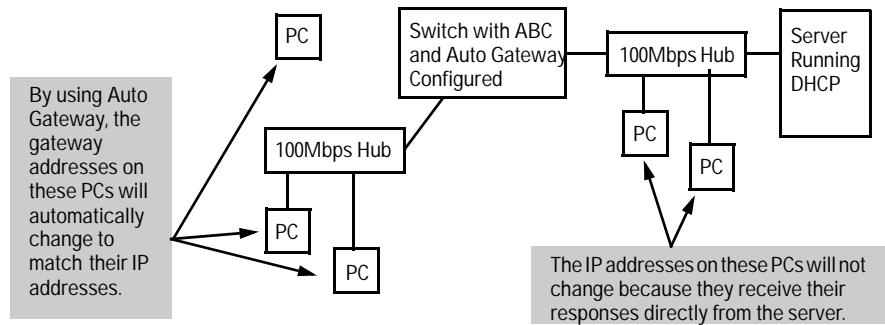


Figure 6-65. DHCP Server Responses Must Come Through the Switch

Restrictions

- **Default Gateway Configuration:** For ABC to operate properly in a multi-subnet structure, 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 6-110. For troubleshooting information, see “Automatic Broadcast Control Problems” on page 8-4.
- **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. Also, proxy replies from the switch are not sent out meshed ports. For more on ABC operation with other switch features, see HP’s Network City site at the following URL on the World Wide Web:

`http://www.hp.com/go/network_city`
- **IPX Networks:**
 - Only four IPX networks (with 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 6-40.

Monitoring and Analyzing Switch Operation

Overview

You can use the console interface (and, in some cases, the web browser interface) to access the switch monitoring and analysis features listed below:

- Read-only status and counter information to help you monitor, analyze, and troubleshoot switch operation (page 7-2)
- Diagnostic and management tools, including:
 - Link test (page 7-23)
 - Ping test (page 7-23)
 - Browse configuration (page 7-27)
 - Command prompt (page 7-28)

Note

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 8-10

Status and Counter 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 “Starting an HP Web Browser Interface Session with the Switch” on page 3-3.

| Status or Counters Type | Interface | Purpose |
|---|--------------------|---|
| General System Information | Console | Lists switch-level operating information (page 7-4). |
| 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 (page 7-5). |
| Module Information | Console | For each slot, lists the module type (such as 10/100TX) and description (page 7-6). |
| Port Status Overview | Browser | Shows port utilization and the Alert Log (page 3-11). |
| Port Status | Console Browser | Displays the operational status of each port (page 7-7). |
| Port Counters | Console Browser | Summarizes port activity (page 7-9). |
| Address Table (Address Forwarding Table) | Console | Lists the MAC addresses of nodes the switch has detected on the network, with the corresponding switch port (page 7-13). |
| Port Address Table | Console | Lists the MAC addresses that the switch has learned from the selected port (page 7-14). |
| 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 (page 7-16). |
| IP Multicast (IGMP) Status | Console | Lists IGMP groups, report, query, and type of device access on ports (page 7-18). |
| Automatic Broadcast Control (ABC) Information | Console | If VLANs are configured, reports on a per-VLAN basis (page 7-20). |
| Switch Mesh Information | Console | For meshed ports, describes operating state, MAC address of adjacent meshed switch, and identity of peer port on adjacent switch (page 7-21). |
| VLAN Information | Console | For each VLAN configured in the switch, lists 802.1Q VLAN ID and up/down status (page 7-22). |

Select **Status and Counters** from the Main Menu to display the Status and Counters menu:

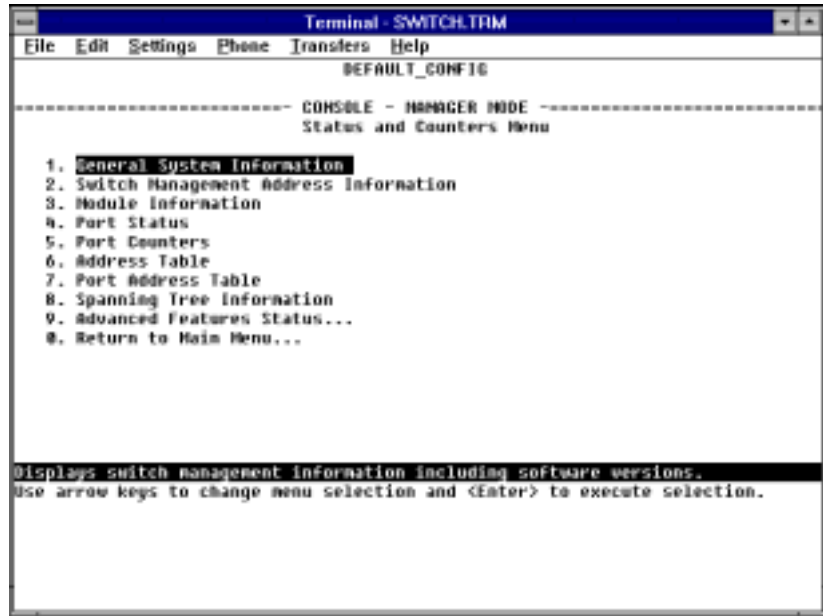


Figure 7-1. The Status and Counters Menu

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 you will be prompted to select a VLAN if multiple VLANs are configured.

General System Information

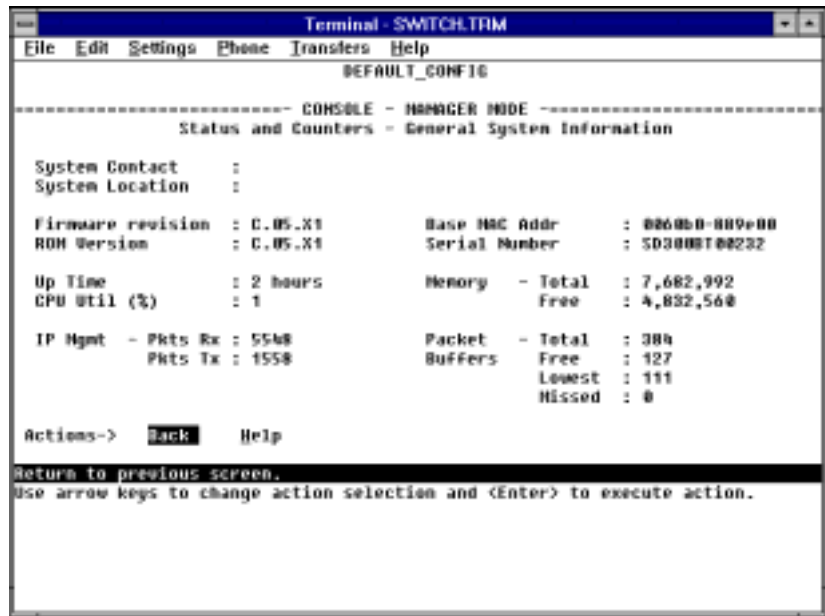


Figure 7-2. Example of General Switch Information

This screen dynamically indicates how individual switch resources are being used. See the online Help for details.

Switch Management Address Information

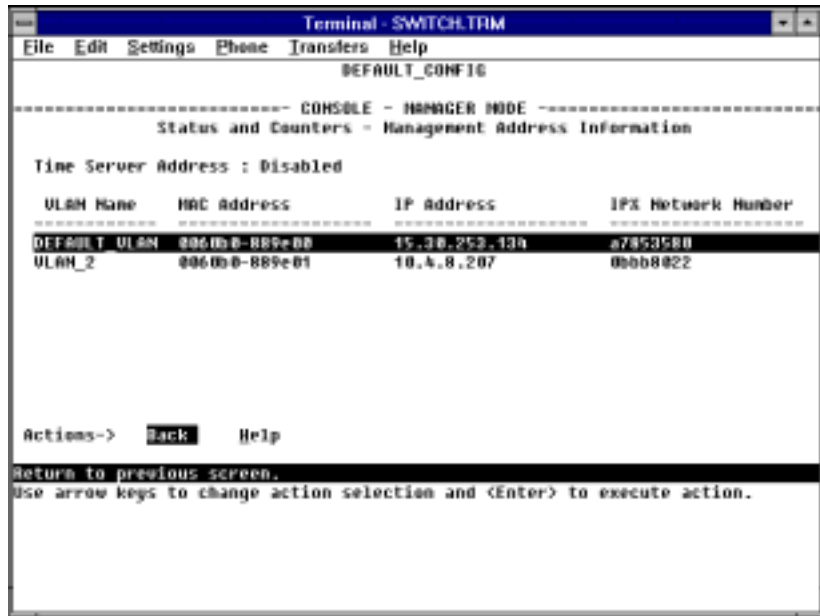


Figure 7-3. Example of Management Address Information with VLANs Configured

If multiple VLANs are not configured, this screen displays data for the entire switch. See the online Help for details.

Module Information

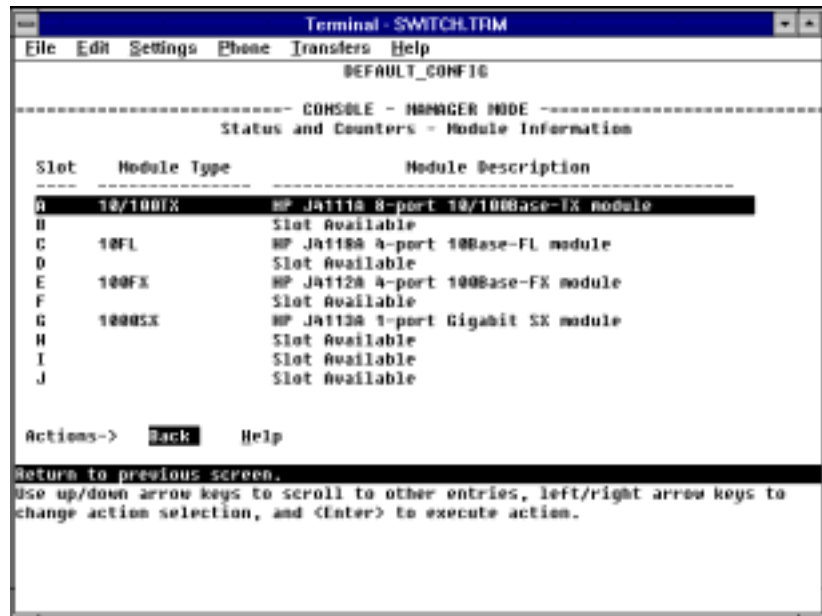


Figure 7-4. Example of the Module Information Screen

Displays data on the current installed modules. See the online Help for details.

Port Status

The web browser interface and the console interface show the same port status data.

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 6-24.)

Displaying Port Status from the Web Browser Interface

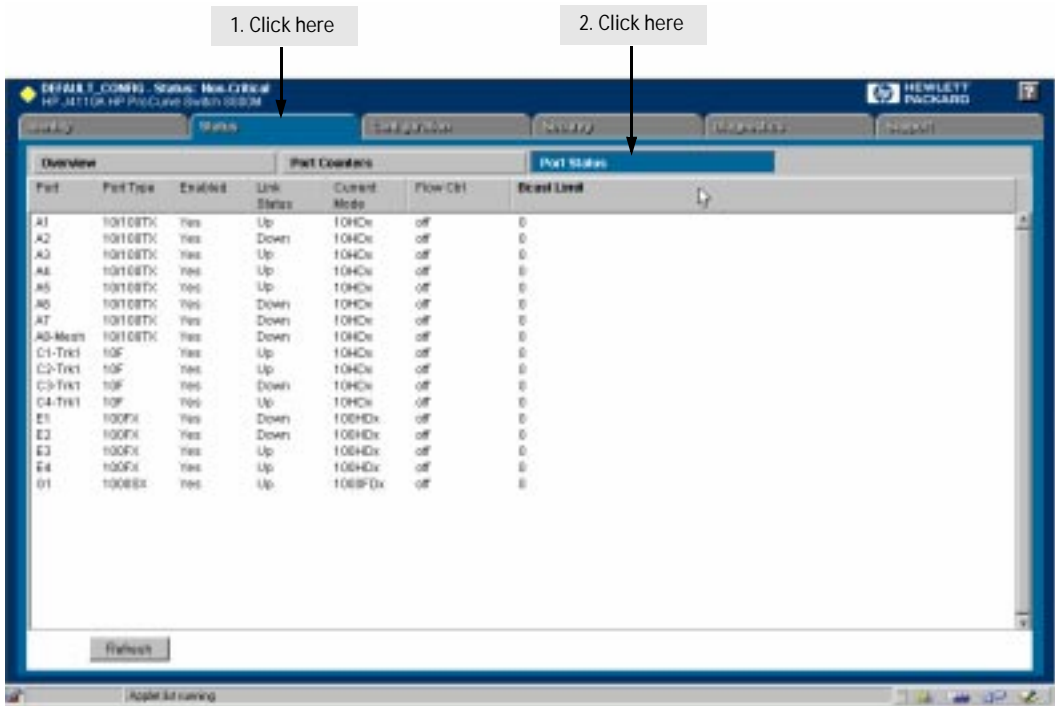


Figure 7-5. Example of Port Status on the Web Browser Interface

Displaying Port Status from the Console Interface

```
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      Down    10Hdx     off        0
A2        10/100Tx  Yes      Down    10Hdx     off        0
A3        10/100Tx  Yes      Down    10Hdx     off        0
A4        10/100Tx  Yes      Down    10Hdx     off        0
A5        10/100Tx  Yes      Down    10Hdx     off        0
A6        10/100Tx  Yes      Down    10Hdx     off        0
A7        10/100Tx  Yes      Up      100Fdx    off        0
A8        10/100Tx  Yes      Up      100Fdx    off        0
G1-Trk1  10F       Yes      Down    10Hdx     off        30
G2-Trk1  10F       Yes      Down    10Hdx     off        30
G3-Trk1  10F       Yes      Down    10Hdx     off        30

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 7-6. Example of Port Status on the Console Interface

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, MAC address, 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

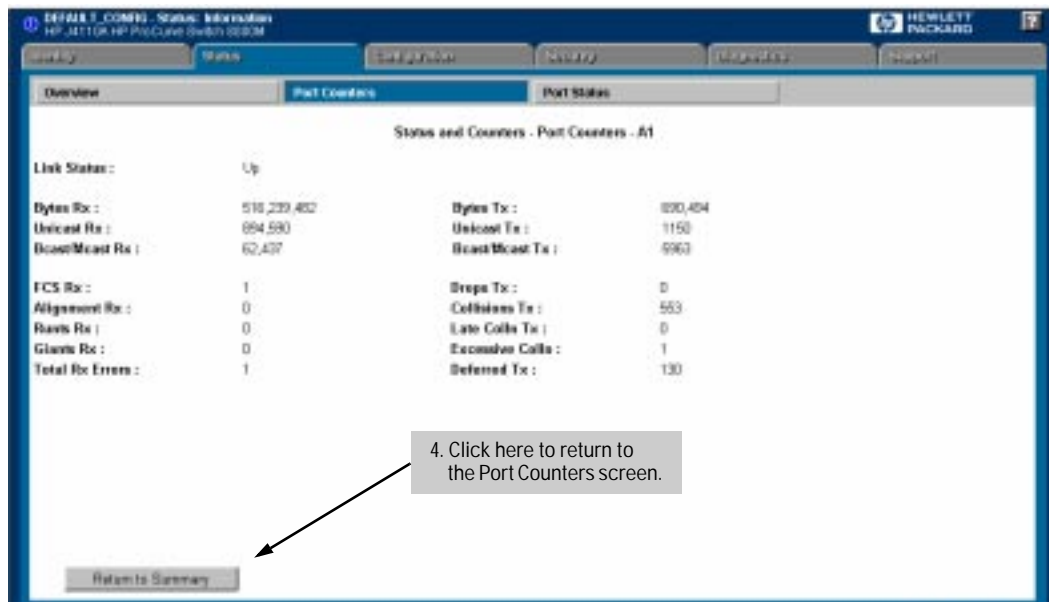
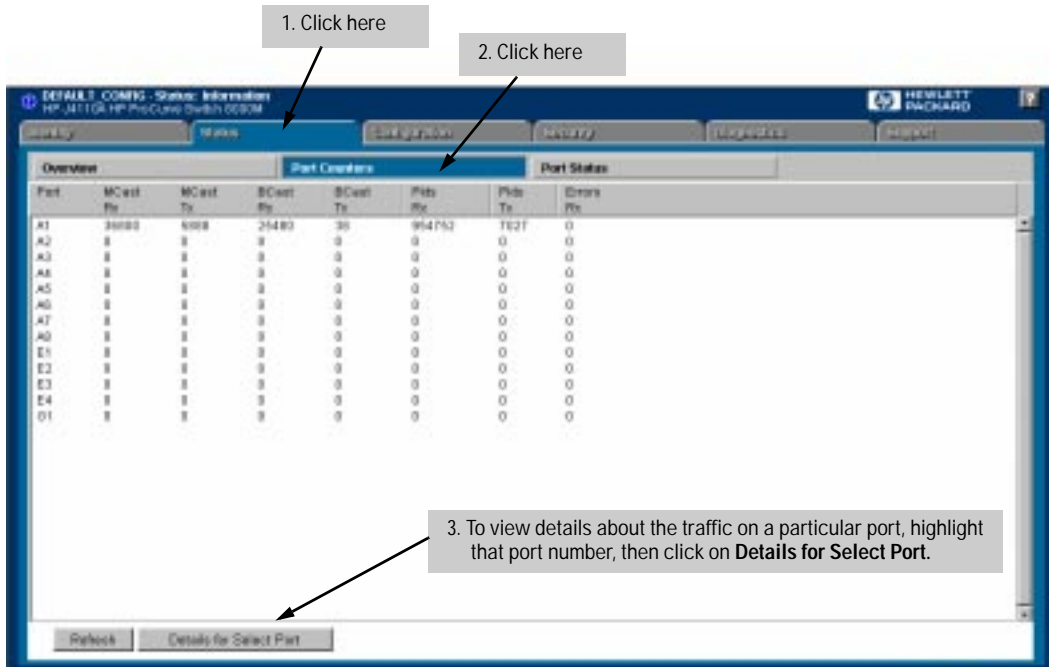
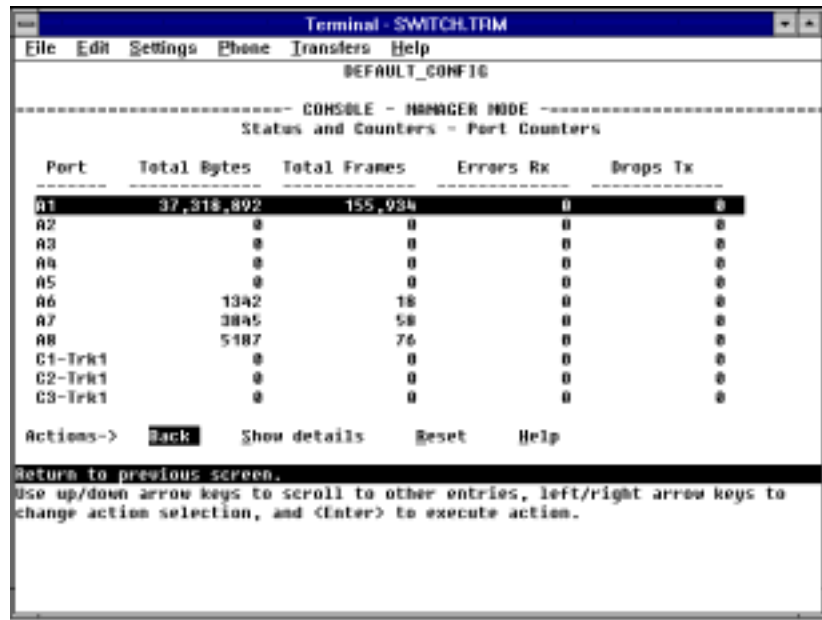


Figure 7-7. Example of Port Counters and Details on the Web Browser Interface

Displaying Port Counters from the Console Interface



| Port | Total Bytes | Total Frames | Errors Rx | Drops Tx |
|---------|-------------|--------------|-----------|----------|
| A1 | 37,218,892 | 155,934 | 0 | 0 |
| A2 | 0 | 0 | 0 | 0 |
| A3 | 0 | 0 | 0 | 0 |
| A4 | 0 | 0 | 0 | 0 |
| A5 | 0 | 0 | 0 | 0 |
| A6 | 1342 | 18 | 0 | 0 |
| A7 | 3845 | 58 | 0 | 0 |
| A8 | 5187 | 76 | 0 | 0 |
| G1-Trk1 | 0 | 0 | 0 | 0 |
| G2-Trk1 | 0 | 0 | 0 | 0 |
| G3-Trk1 | 0 | 0 | 0 | 0 |

Figure 7-8. Example of Port Counters on the Console Interface

To view details about the traffic on a particular port, highlight that port number (figure 7-8), then select **Show Details**. For example, selecting port A1 displays a screen similar to figure 7-9, below.

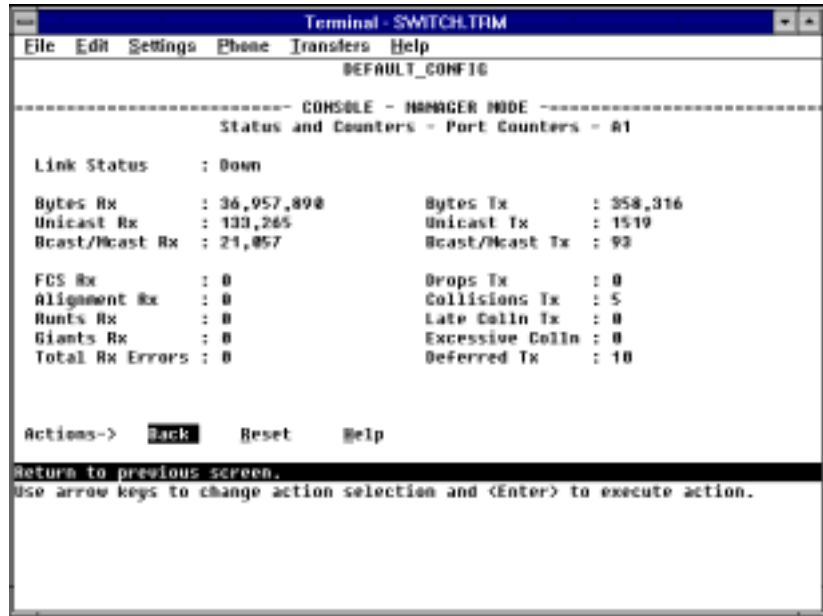


Figure 7-9. Example of the Display for Show details on a Selected Port

This screen also includes the **Reset** action. Refer to the note on page 7-9.

Address Table

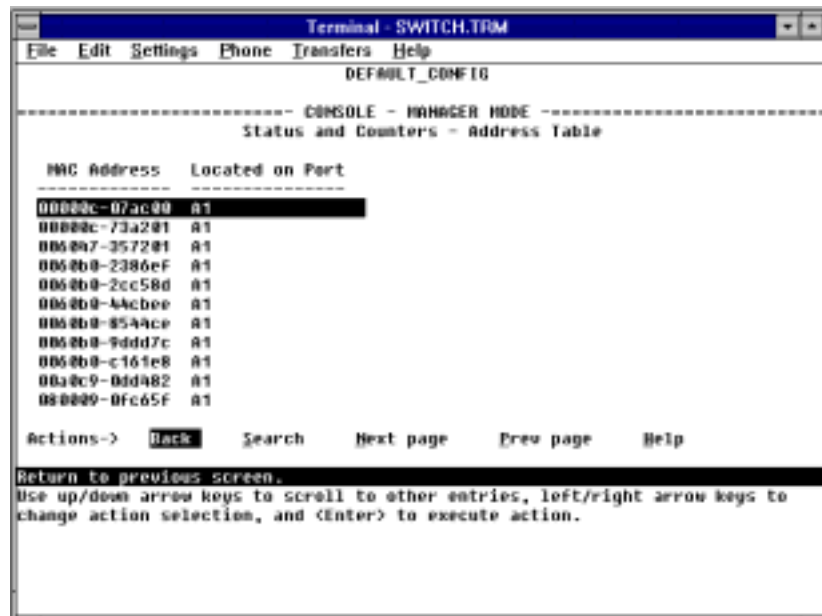


Figure 7-10. Example of the Address Table

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.

Use the **Search** action at the bottom of the screen to determine whether a specific device (MAC address) is connected to the selected port.

To use the port address table:

1. Select **Port Address Table** from the menu in the Status and Counters screen.

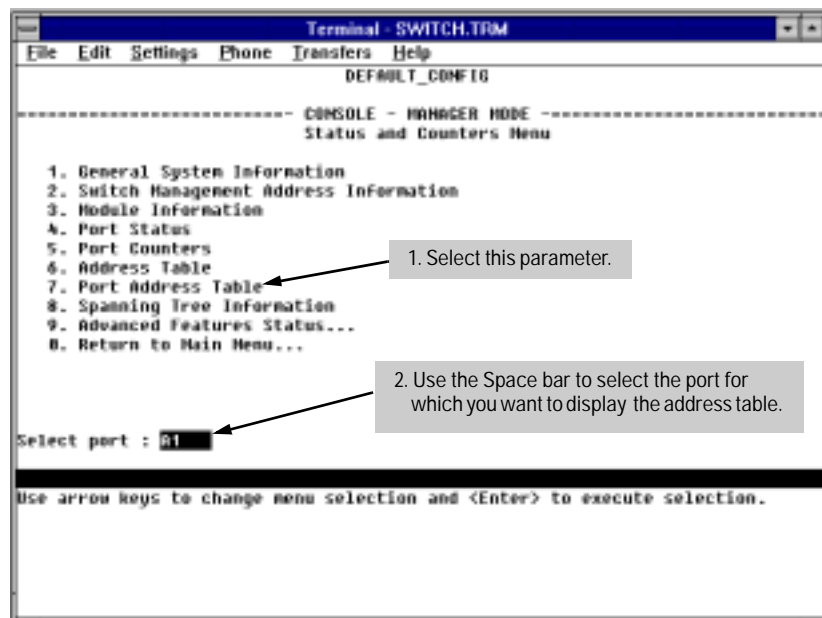


Figure 7-11. Example of How To Access the Port Address Table

2. When the `port` prompt appears, press the Space bar or type the port name to display the port you want to examine, then press `[Enter]`. (See figure 7-11, above.)

Each port is identified by the sequential port numbers on the front of the switch.

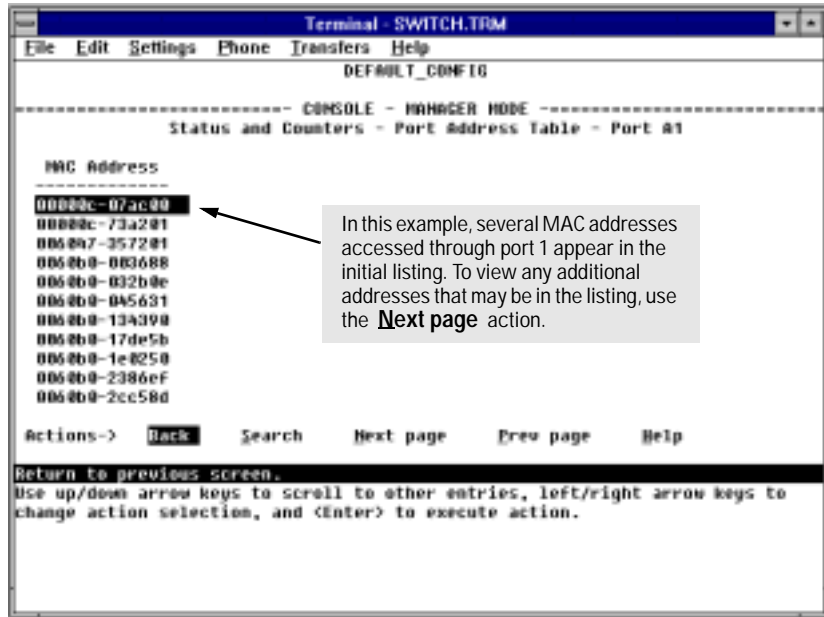
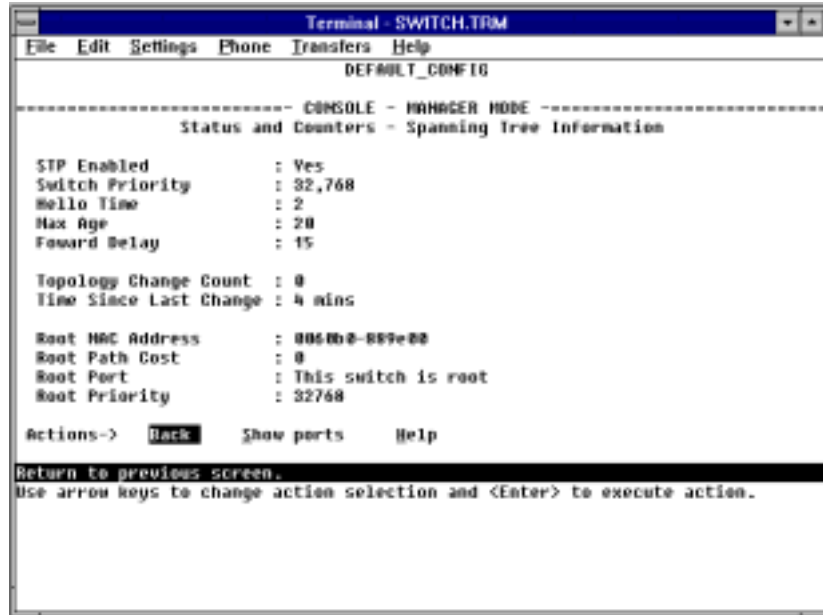


Figure 7-12. Example of a Port Address Table for a Specific Port

Spanning Tree (STP) Information

STP must be enabled on the switch to display the following data:

A terminal window titled "Terminal - SWITCH.TRM" with a menu bar (File, Edit, Settings, Phone, Transfers, Help) and a title bar (DEFAULT_CONFIG). The main content is a screen titled "CONSOLE - MANAGER MODE" with a subtitle "Status and Counters - Spanning Tree Information". It displays STP parameters: STP Enabled (Yes), Switch Priority (32,768), Hello Time (2), Max Age (20), Forward Delay (15), Topology Change Count (0), Time Since Last Change (4 mins), Root MAC Address (0060b0-889e00), Root Path Cost (0), Root Port (This switch is root), and Root Priority (32768). At the bottom, there are actions: Back (highlighted), Show ports, and Help. A footer message says "Return to previous screen. Use arrow keys to change action selection and <Enter> to execute action."

```
Terminal - SWITCH.TRM
File Edit Settings Phone Transfers Help
DEFAULT_CONFIG
----- CONSOLE - MANAGER MODE -----
Status and Counters - Spanning Tree Information

STP Enabled           : Yes
Switch Priority       : 32,768
Hello Time            : 2
Max Age               : 20
Forward Delay         : 15

Topology Change Count : 0
Time Since Last Change : 4 mins

Root MAC Address      : 0060b0-889e00
Root Path Cost        : 0
Root Port             : This switch is root
Root Priority          : 32768

Actions->  Back      Show ports  Help

Return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

Figure 7-13. 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).

| Port | Type | Cost | Priority | State | Designated Bridge |
|------|----------|------|----------|------------|-------------------|
| A1 | 10/100FX | 10 | 128 | Forwarding | 0060b0-809e00 |
| A2 | 10/100FX | 10 | 128 | Disabled | |
| A3 | 10/100FX | 10 | 128 | Disabled | |
| A4 | 10/100FX | 10 | 128 | Disabled | |
| A5 | 10/100FX | 10 | 128 | Disabled | |
| A6 | 10/100FX | 10 | 128 | Disabled | |
| A7 | 10/100FX | 10 | 128 | Forwarding | 0060b0-809e00 |
| A8 | 10/100FX | 10 | 128 | Blocking | 0060b0-809e00 |
| E1 | 100FX | 10 | 128 | Disabled | |
| E2 | 100FX | 10 | 128 | Disabled | |
| E3 | 100FX | 10 | 128 | Disabled | |

Figure 7-14. Example of STP Port Information

Caution

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)” on page 6-34.

IP Multicast (IGMP) Status

To access this screen from the Main Menu, click on:

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.

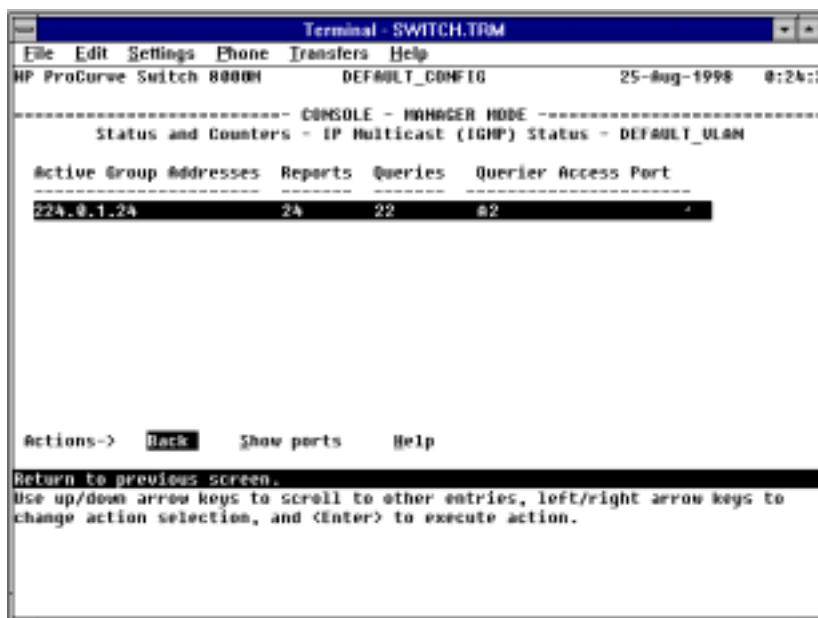


Figure 7-15. Example of IGMP Status Screen

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:

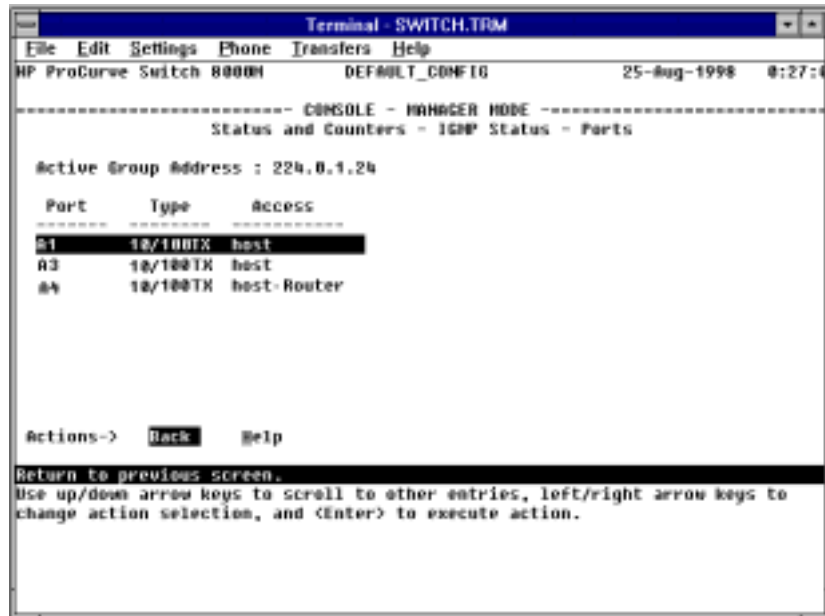


Figure 7-16. Example of an IGMP Status Screen for a Selected Multicast Group

Automatic Broadcast Control (ABC) Information

To access this screen from the Main Menu, click on:

1. Status and Counters

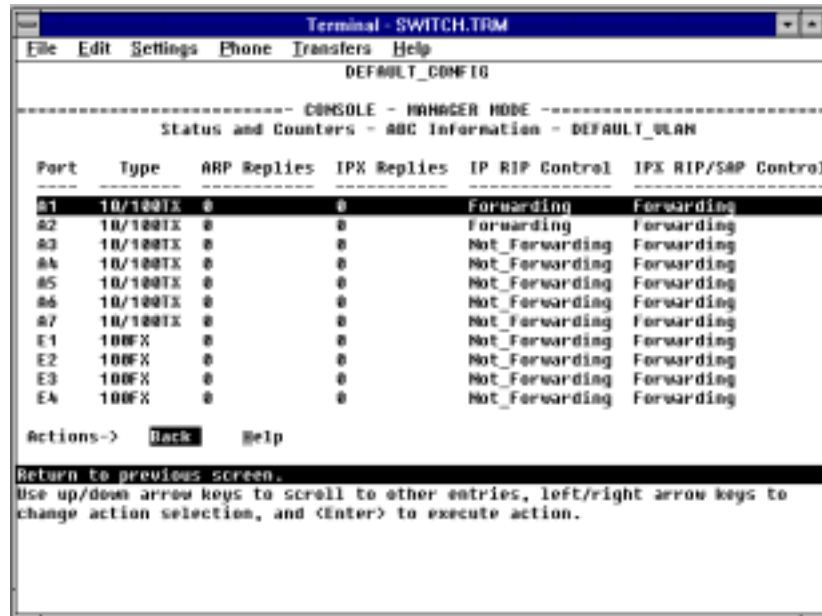
9. Advanced Features Status

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.



```
Terminal - SWITCH.TRM
File Edit Settings Phone Transfers Help
-----
                DEFAULT_CONFIG
-----
----- CONSOLE - MANAGER MODE -----
                Status and Counters - ABC Information - DEFAULT_VLAN
-----
Port  Type  ARP Replies  IPX Replies  IP RIP Control  IPX RIP/SAP Control
-----
A1   10/100TX  0             0             Forwarding      Forwarding
A2   10/100TX  0             0             Forwarding      Forwarding
A3   10/100TX  0             0             Not_Forwarding  Forwarding
A4   10/100TX  0             0             Not_Forwarding  Forwarding
A5   10/100TX  0             0             Not_Forwarding  Forwarding
A6   10/100TX  0             0             Not_Forwarding  Forwarding
A7   10/100TX  0             0             Not_Forwarding  Forwarding
E1   100FX    0             0             Not_Forwarding  Forwarding
E2   100FX    0             0             Not_Forwarding  Forwarding
E3   100FX    0             0             Not_Forwarding  Forwarding
E4   100FX    0             0             Not_Forwarding  Forwarding

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 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

```
Terminal - SWITCH.TRM
File Edit Settings Phone Transfers Help
DEFAULT_CONFIG
----- CONSOLE - MANAGER MODE -----
Status and Counters - Switch Mesh Information
Port      State      Adjacent Switch  Peer Port
-----
1         Established  000000-889e00   000000-889e78

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 7-18. 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, click on:

1. Status and Counters
9. Advanced Features Status
4. VLAN Information

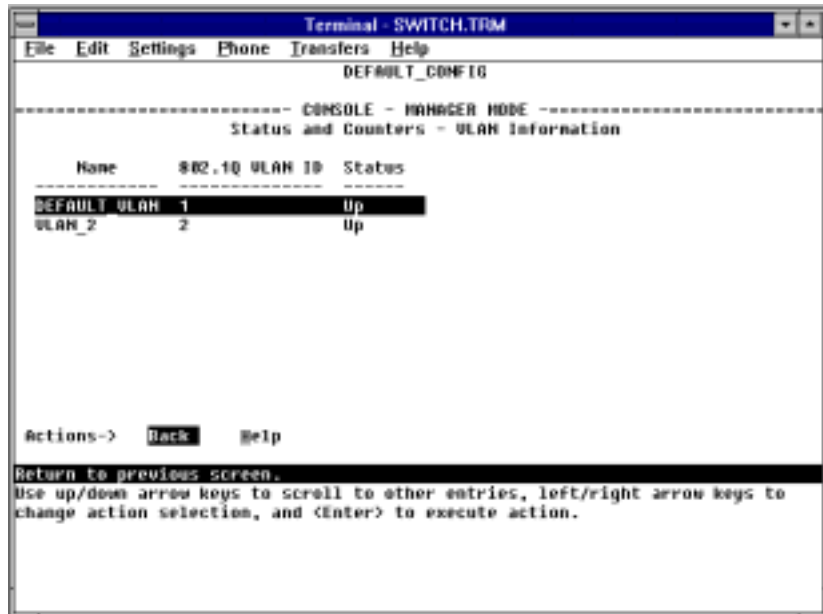


Figure 7-19. Example of VLAN Information Screen

This screen displays the VLAN identification and status for each VLAN configured in the switch.

Diagnostics

The switch's diagnostic tools include the following:

| Feature | Switch Console | Web Browser Interface | Page |
|--------------------|----------------|-----------------------|------|
| Link Test | Yes | Yes | 7-23 |
| Ping Test | Yes | Yes | 7-24 |
| Browse Config File | Yes | Yes | 7-27 |
| Command Prompt | Yes | No | 7-28 |

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.

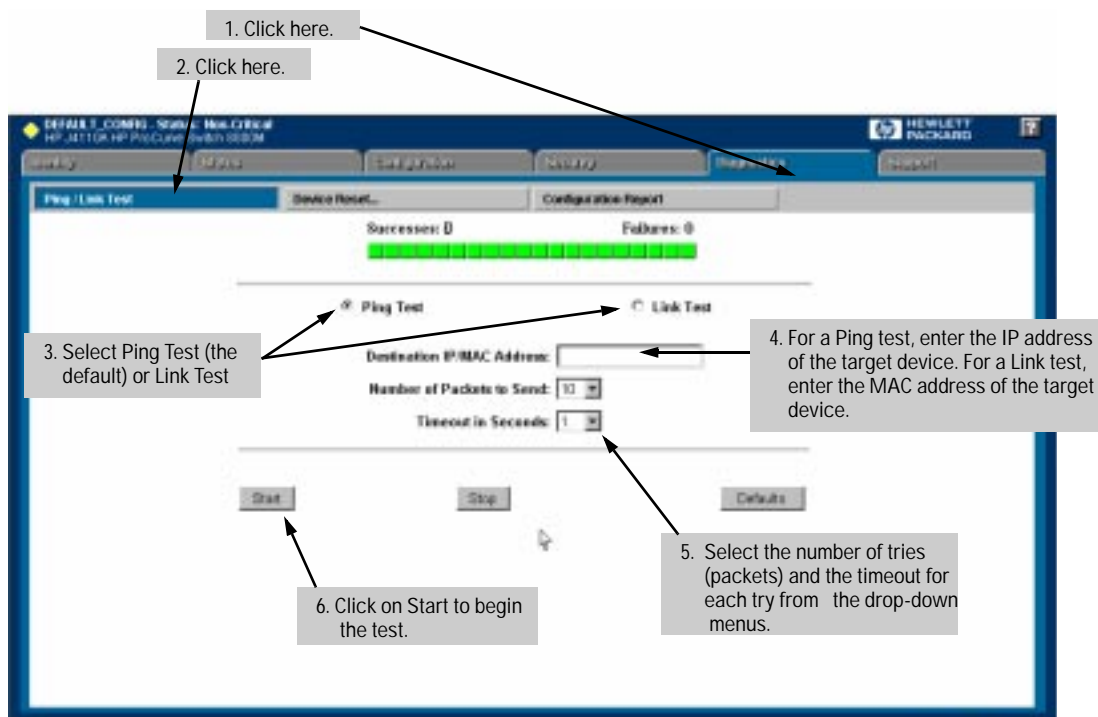
Note

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



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, 08000c-070a00.

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 Console Interface

To cancel a Ping or Link test that is in progress, press **Ctrl** **C**.

- From the Main Menu, select:

5. Diagnostics . . .

1. Link Test

or

2. Ping Test

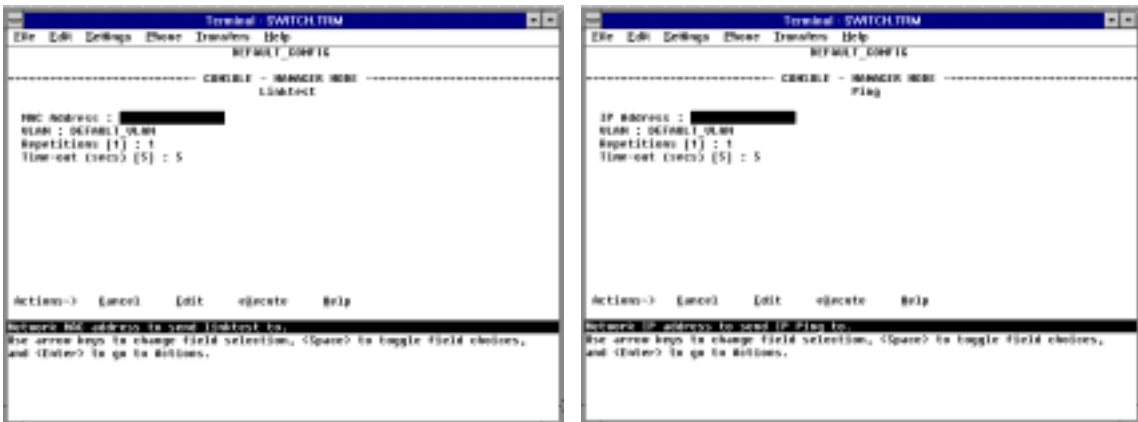


Figure 7-20. Examples of Link Test and Ping Test Screens with VLANs Configured

- Do one of the following:
 - For a Link test, enter the MAC address of the target device. (This is a 12-digit hexadecimal number. For an example, see the screen on page 7-13.)
 - For a Ping test, enter the IP address of the target device.
- 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.
- Select the **Repetitions** parameter and type in the number of times you want the test to be made.
- 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

Browse Configuration File

This command displays the switch configuration that is currently saved.

To display the configuration file:

1. From the Main Menu, select:
 5. Diagnostics
 3. Browse Configuration File

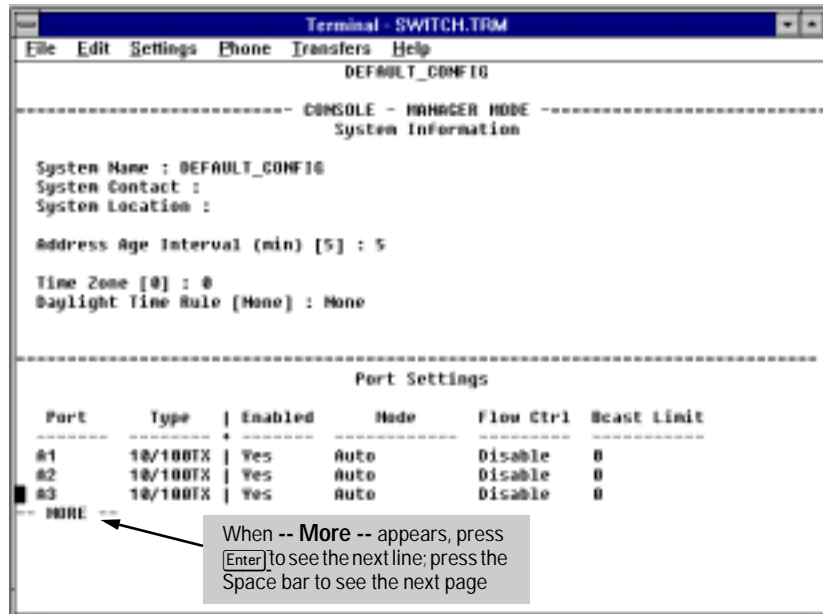


Figure 7-21. Example of the Browse Configuration Display

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:

| | | | |
|--------|----------|--------|------------|
| Browse | Help | Page | Version |
| Config | History | Ping | Vlan |
| Date | Get | Print | WalkMIB |
| Time | Put | Redo | Xget |
| Delete | LinkTest | GetMIB | Xput |
| Kill | Log | SetMIB | romversion |

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**.
- To exit from the command prompt, type **exit** and press **Enter**.

How To Use the Command Prompt:

1. From the Main Menu select:

5. Diagnostics ...

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.

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 8-3)
 - General Problems (page 8-3)
 - Automatic Broadcast Control Problems (page 8-4)
 - IGMP-Related Problems (page 8-5)
 - Switch Mesh Problems (page 8-5)
 - STP-Related Problems (page 8-7)
 - VLAN-Related Problems (page 8-8)
- Using the Event Log To Identify Problem Sources (page 8-10)

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 for flashing fault LEDs. (See the installation guide shipped with the switch.)
- Check the network topology/installation. (See the installation guide shipped with the switch.)
- Check cables for damage, correct type, and proper connections. (See the installation guide shipped with the switch.)
- Use HP TopTools for Hubs and 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.”)
- For help in isolating problems, use the easy-to-access Console RS-232 port built into the switch or Telnet to the switch console. (See chapter 4, “Using the Switch Console Interface” for operating information.)
 - Status and Counters screens
 - Event Log
 - Diagnostics tools (Link test, Ping test, configuration file)

Browser or Console Interface Problems

Cannot access the web browser interface: Access may be disabled by the **Web Agent Enabled** parameter in the switch console. Go to the console serial link screen to check (.

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 “Using the Switch Console To Configure the Console/Serial Link” on page 21.
 - The switch may not have the correct IP address or subnet mask.
-

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 ASCII 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 are occurring in the network. These may be due to redundant links between nodes.

- If you are configuring a switch mesh or a port trunk, finish configuring the ports in the mesh or 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 IP address that 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 on the 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 the 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 6-104.)
- 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:

- **Using the Web Browser Interface:** Click on the Configuration tab, then click on the IP Configuration button.
- **Using the Switch Console Interface:** From the Main Menu, check the Management Address Information screen by clicking on

1. Status and Counters

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 6-61.

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

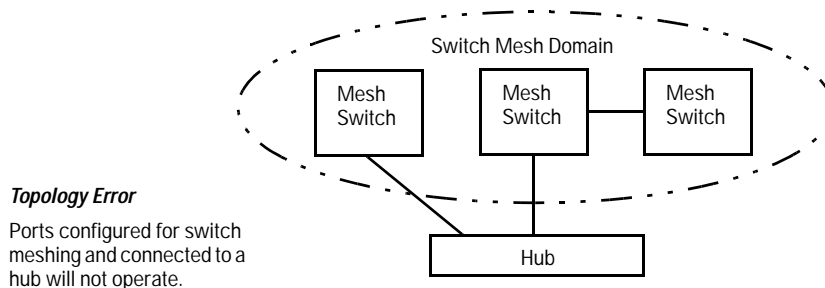


Figure 8-1. Connecting a Hub To Meshed Ports Causes a Topology Error

- A non-meshed switch or port connected to a mesh port

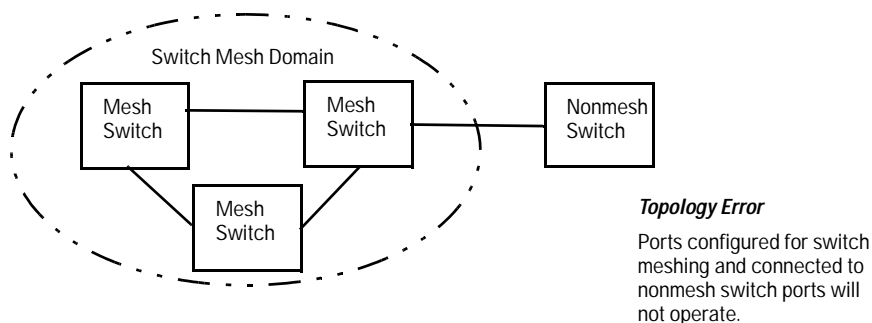


Figure 8-2. Connecting a Non-Meshed Switch Port to a Meshed Port Causes a Topology Error

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

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. This includes all switches in a switch mesh.

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 6-76.)

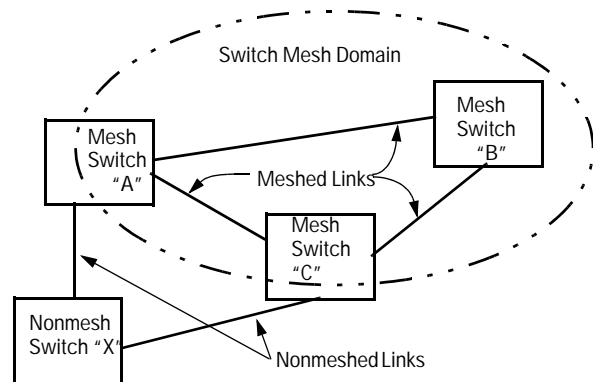


Figure 8-3. Example of Meshed and Nonmeshed Links Forming a Redundant Pair

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 6-38.

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.

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.

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 8000M and Switch 1600M, 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 VLAN” on page 6-38.

VLAN-Related Problems

(Also see “Switch Mesh Problems” on page page 8-5.)

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”.

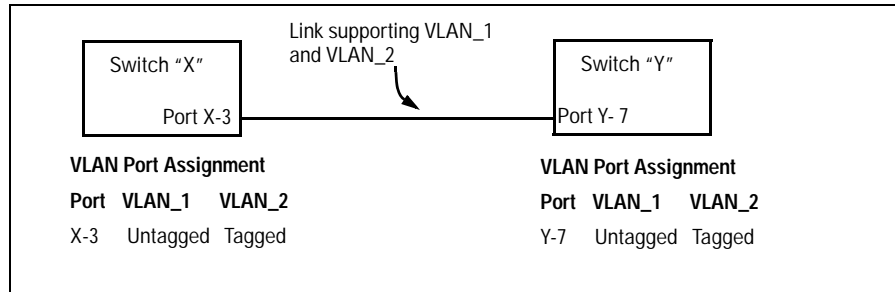


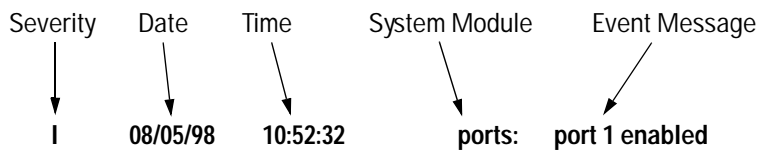
Figure 8-4. Example of Correct VLAN Port Assignments on a Link

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 6-62.

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

| Event Type | Activity | Event Type | Event Description |
|------------|-----------------------------------|-------------|-------------------------------------|
| abc | Automatic Broadcast Control | pagp | Port trunks |
| addrMgr | Address table | ports | Change in port status |
| chassis | switch hardware | snmp | SNMP communications |
| console | Console interface | stp | Spanning Tree |
| dhcp | DHCP addressing | sys, system | Switch management |
| download | file transfer | telnet | Telnet activity |
| fault | Web browser interface faultfinder | tcp | Transmission control |
| igmp | IP Multicast | testmode | HP internal use |
| ip | IP-related | tftp | File transfer for new OS or config. |
| ipx | Novell Netware | timep | Time protocol |
| ldbal | Load-balancing | vlan | VLAN operations |
| mgr | Command line | Xmodem | Xmodem file transfer |

Event Message is a brief description of the operating event.

Entering and Navigating in the Event Log Display. From the Main Menu, select **Event Log**.

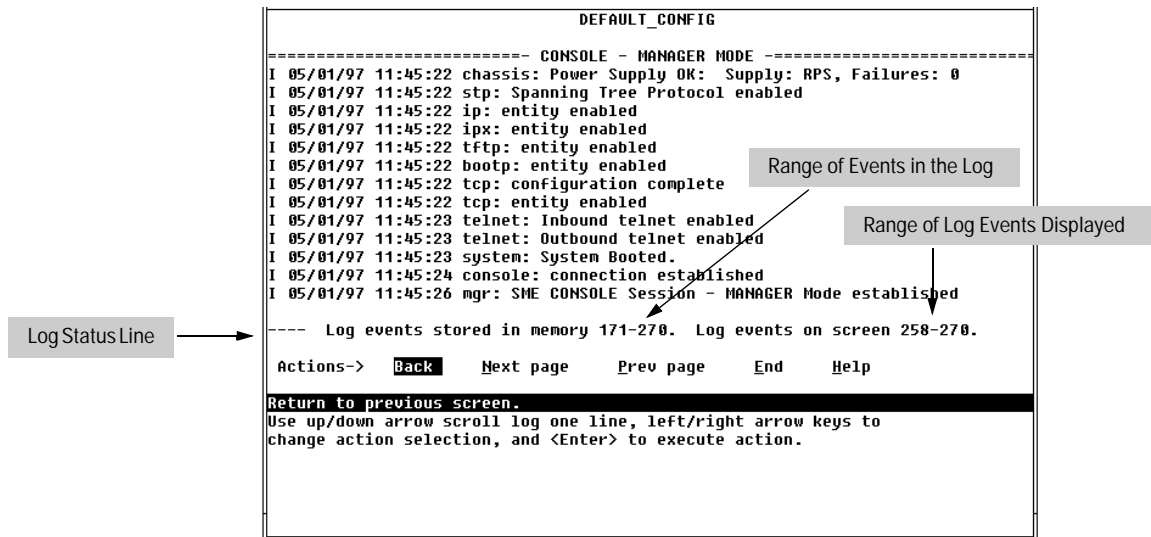


Figure 8-5. Example of an Event Log Display

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 7-1. 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.)

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.

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-9.

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.

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:

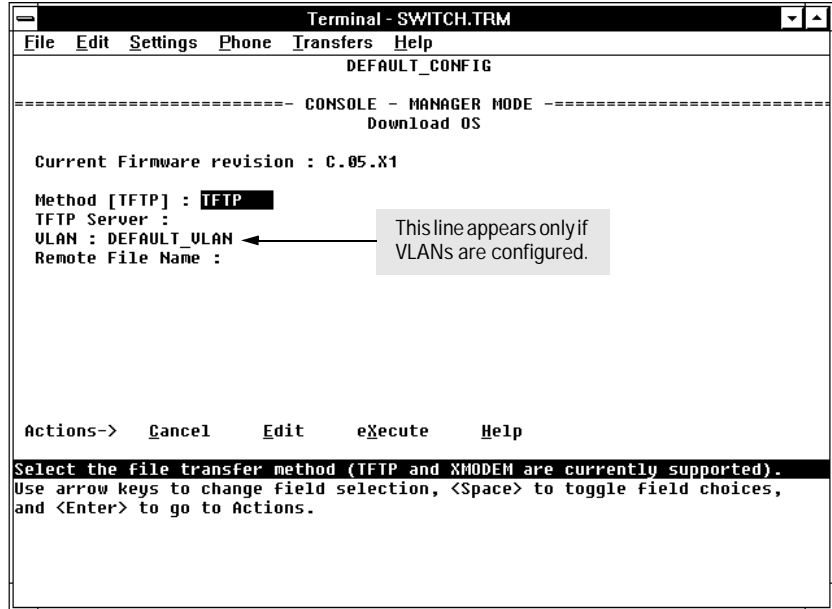


Figure 8-1. Example of the Download OS Screen (Default Values)

2. Press **[E]** (for **Edit**).
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 **eXecute**) to begin the OS download. The following screen then appears:

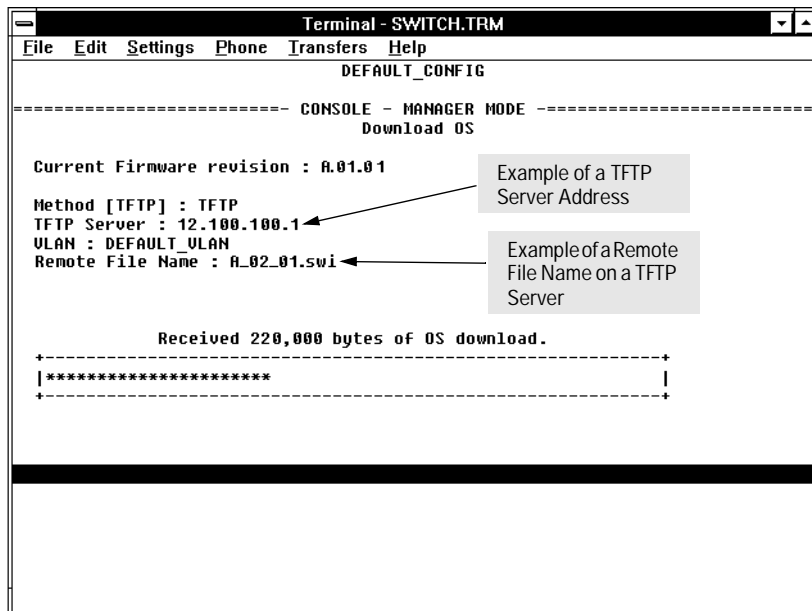


Figure 8-2. Example of the Download OS Screen During a Download

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 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.

9. 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 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 8000Ms and/or Switch 1600Ms 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 8000M and the Switch 1600M use the same OS.) To do so:

1. From the switch console Main Menu in the switch to receive the download, go to the **Download OS** screen.
2. In the **TFTP Server** field, enter the IP address of the remote Switch 8000M or 1600M containing the OS you want to download.
3. Enter "os" for the **Remote File Name**.
4. Press , then (for eXecute) to begin the OS download.
5. 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.

6. 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 a binary transfer feature. (For example, in the Windows 3.1 terminal emulator, you would use the **Send Binary File** option in the **T**ransfers dropdown menu.)

To Perform the OS Download:

1. From the console Main Menu, select
 - 7. Download OS**
2. Press **[E]** (for **E**dit).
3. Use the Space bar to select **XMODEM** in the **M**ethod field.
4. Press **[Enter]**, then **[X]** (for **eX**ecute) 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
 - Status and Counters**
 - General System Information**
 - b. Check the **Firmware revision** line.

Troubleshooting TFTP Downloads

If a TFTP download fails, the Download OS screen indicates the failure.

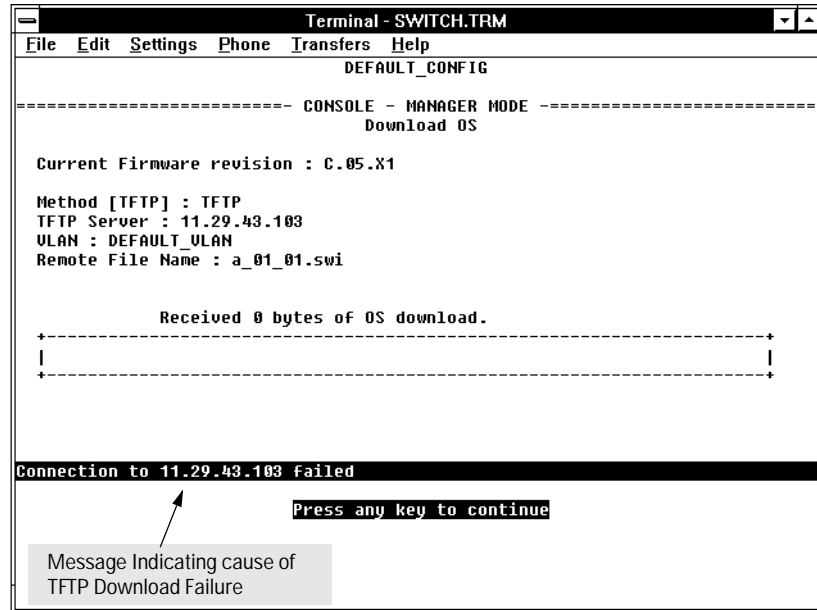


Figure 8-3. Example of Message for Download Failure

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 8-10.)

Some of the causes of download failures include:

- Incorrect or unreachable address specified for the **TFTP Server** parameter. This may include network problems.
- 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 **Advanced Commands** option from the Main Menu and executing the History command.

Transferring Switch Configurations

You can use the following commands to transfer Switch 8000M and Switch 1600M 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

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 to be stored.

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 VT100 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:

Diagnostics...

Command Line

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

`[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 primary 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

The Primary and VLAN MAC Addresses

These addresses appear in the Management Address Information screen. Also, the primary MAC address appears on a label on the front of the switch.

Note

The primary 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 primary 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.

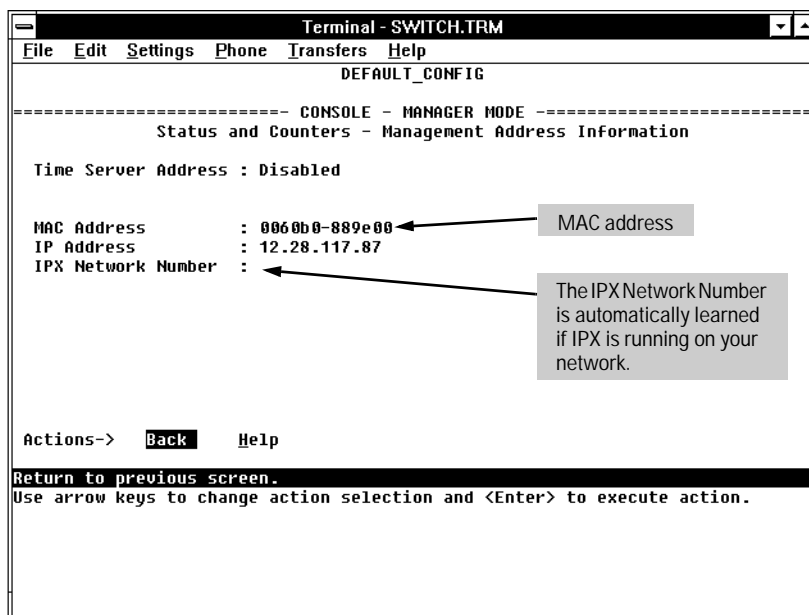


Figure B-1. Example of the Management Address Information Screen

The Port MAC Addresses

These MAC addresses are used internally by such features as Flow Control, Switch Meshing, 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
 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`

MAC addresses are listed for all ports on the switch. Eight consecutive values are reserved for each slot, regardless of how many ports are actually installed in the slot. For example, with the four-port 100FX module installed in a Switch 1600M, the above command gives the following result:

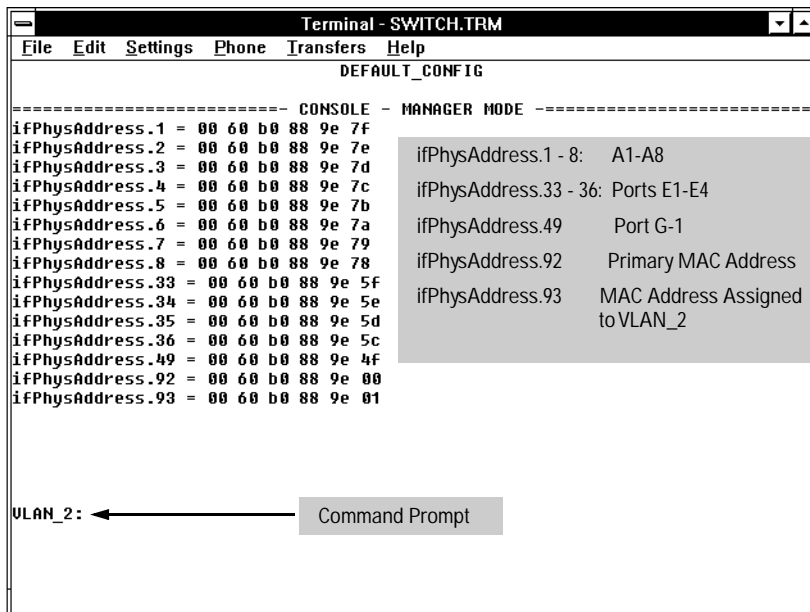


Figure B-2. Example of Port MAC Address Assignments on the Switch 1600M

Index

Numerics

- 802.1q ... 6-3
- 802.1Q VLAN standard ... 6-34
- 802.3u auto negotiation standard ... 6-24

A

- A.09.70 router release ... 6-63
- ABC ... 6-100
 - AppleTalk packets forwarded ... 6-112
 - broadcast limit ... 7-7
 - broadcast limit, automatic ... 6-102, 6-105
 - console configuration ... 6-102
 - DECnet packets forwarded ... 6-112
 - encapsulation type ... 6-109
 - gateway ... 8-4, 6-110
 - IGMP ... 6-48
 - IPX option ... 6-104, 6-41
 - operation ... 6-107–6-108
 - reducing RIP/SAP traffic ... 6-109
 - restrictions ... 6-111
 - router ... 6-107
 - statistics ... 7-3
 - switch meshing ... 6-111
 - VLAN ... 6-48, 6-102, 6-104, 6-108
 - web browser interface ... 6-101
 - with IPX ... 6-111
- Actions line ... 4-6, 4-7, 4-8
- Active button ... 3-12
- active path ... 6-34
- Active tab ... 3-12
- address aging ... 6-22
- address resolution protocol ... 6-108
- address table, port ... 7-13
- address, manager ... 6-15, 6-17
- address, network manager ... 5-3
- AdvanceStack Assistant ... 1-5
- Alert Log ... 3-12
 - alert types ... 3-16
 - Control Bar ... 3-12
 - sorting the entries ... 3-15
- Alert log ... 3-14, 3-15
- Alert Log Header Bar ... 3-12

- alert log
 - See* web browser interface
- analysis, traffic ... 5-1
- ANSI terminal ... A-10
- AppleTalk packets forwarded, ABC ... 6-112
- ARP ... 6-108
- ARP statistics ... 7-20
- ARP, proxy ... 6-109, 8-5
- ARP, proxy response ... 6-108
- ASCII terminal ... 2-2
- asterisk ... 4-7, 6-51
- authentication trap ... 6-18
- Auto Gateway ... 6-110
- Auto Gateway parameter ... 8-4
- auto port setting ... 6-92
- auto-discovery ... 5-4
- automatic broadcast control
 - See* ABC
- automatic gateway configuration ... 6-110
- auto-negotiation ... 6-24

B

- bandwidth display control ... 3-13
- bandwidth savings ... 6-100
- bandwidth usage, filters ... 6-40
- bandwidth, savings ... 6-95
- baud rate ... 4-2
- benefits ... 6-107
- blocked link ... 6-38
- blocked port ... 6-37, 6-92
- blocking state ... 6-34
- Bootp ... 5-1, 6-6, 6-8, 6-10
- Bootp configuration, automatic ... 2-2
- Bootp table file ... 6-12
- Bootp, configuring ... 6-13
- Bootp, no reply ... 8-4
- Bootp, Unix systems ... 6-11
- Bootp/DHCP differences ... 6-11
- Bootp/DHCP router option ... 6-111
- Bootptab file ... 6-12
- bridge ... 2-1
- broadcast ... 6-109
- broadcast domain ... 6-45, 6-100

broadcast limit ... 6-26–6-27, 6-102, 6-105, 7-7
broadcast limit, override ... 6-25
broadcast storm ... 6-3, 6-34, 6-50, 6-64, 6-75, 8-7
broadcast traffic ... 6-109
broadcast, restricting ... 6-24
Browser interface
 access parameters ... 3-6
 Active Tab ... 3-12
 Button bar ... 3-12
 Gauges Area ... 3-12
 online help location ... 6-5
 Status Bar ... 3-12
 where to run ... 3-3
browsers ... 3-2
Button bar ... 3-12

C

Clear button ... 3-8
Clear button, to delete password protection ... 4-12
command prompt ... 4-5, 7-28–7-29
 exit ... 7-29
communities, SNMP ... 6-16
Community field ... 6-19
comparison, features ... 6-2
configuration ... 4-4, 6-37
 activating ... 5-4
 automatic, DHCP/Bootp ... 2-2
 Bootp ... 6-12
 console ... 6-20
 copying ... A-9
 DHCP, gateway ... 6-110
 download ... A-2
 factory default ... 6-3, 6-1, 6-34, 6-49, 7-29
 features ... 6-2
 IGMP, console ... 6-93
 IP ... 2-2, 2-3, 6-6
 network monitoring ... 6-29
 port ... 6-24
 port trunk ... 6-65
 serial link ... 6-20
 SNMP ... 5-3, 6-15
 spanning tree ... 6-34, 6-37
 subnet mask ... 2-2
 switch management access ... 4-4
 system ... 6-22
 traffic/security filter ... 6-40
 transfer ... A-9

transferring ... A-9
trap receivers ... 6-18
VLAN ... 6-45
 subnet mask ... 2-2
connection inactivity time ... 4-9
console ... 8-33
 ending a session ... 4-3
 Main menu ... 4-4
 navigation ... 4-5, 4-7
 operation ... 4-7
 overview ... 4-1
 starting a session ... 4-2
 status and counters access ... 4-4
 switch management access configuration ... 4-4
console configuration screen ... 6-20
console interface features ... 1-4
console RS-232 ... 6-20
console session ... 4-2
console, Telnet access ... 3-4
Control bar
 Alert log ... 3-12
copyright screen ... 4-2
CPU utilization ... 7-4
crash information ... 4-3

D

date format ... 8-10
date parameter ... 6-23
DECnet packets forwarded, ABC ... 6-112
default gateway ... 6-111
DEFAULT_VLAN ... 6-49
Device Passwords window ... 3-6
device, managed ... 2-1
DHCP ... 6-8, 6-10
DHCP configuration, automatic ... 2-2
DHCP gateway configuration ... 6-110
DHCP, address problems ... 8-4
DHCP, no reply ... 8-4
DHCP/Bootp differences ... 6-11
DHCP/Bootp process ... 6-11
diagnostics tab ... 3-21
disable IP address ... 6-6
DNS name ... 3-3
domain ... 6-49
Domain Name Server ... 3-4
domain, broadcast ... 6-100
down time ... 4-3

- download
 - SNMP-based ... A-5
 - switch-to-switch ... A-5
 - troubleshooting ... A-7
 - Xmodem ... A-6
- download configuration ... A-9
- download OS ... 4-5, 8-12, 4-5
- download, TFTP ... A-2–A-3
- duplicate MAC address ... 6-62, 6-63, 8-9
- duplicate MAC addresses ... 6-63

E

- ending a console session ... 4-3
- EtherChannel
 - See* FEC
- Event Log ... 4-3
- event log ... 4-3, 4-5, 6-18, 8-10, 8-12
 - navigation ... 8-11
 - severity code ... 8-10
- exiting from command prompt ... 7-29

F

- factory default configuration ... 6-3
- failure, OS download ... A-7
- fault detection ... 3-6
- Fault Detection Policy
 - setting ... 3-6, 3-23
- fault sensitivity level ... 3-23
- fault-tolerance ... 6-65
- feature comparison ... 6-2
- FEC, benefits ... 6-72
- filter ... 6-40
 - IGMP override ... 6-98
 - maximum allowed ... 6-98
 - multicast ... 6-43
 - protocol ... 6-44
 - source port ... 6-44
 - types ... 6-40

- filter, static ... 6-40
- filter, effect of IGMP ... 6-43, 6-97
- firmware version ... 7-4
- flow control ... 6-26
- flow control, terminal ... 6-20
- format, date ... 8-10
- format, time ... 8-10
- forwarding port, IGMP ... 6-92
- forwarding state ... 6-34

G

- gateway ... 6-8
 - configuration, DHCP ... 6-110
 - DHCP configuration ... 6-110
 - IP ... 6-6, 6-9
 - IP configuration ... 2-4
 - router ... 6-9
- Get ... A-9
- getmib ... 6-99
- Graphs area ... 3-12

H

- Help ... 3-9, 4-8
- Help line
 - about ... 4-6
 - location on screens ... 4-6
- help, online inoperable ... 3-9
- History command ... A-8
- host-only ... 6-62
- HP proprietary MIB ... 5-2
- HP Router 440 ... 6-63
- HP Router 470 ... 6-63
- HP Router 480 ... 6-63
- HP Router 650 ... 6-63
- HP TopTools
 - See* TopTools
- HP web browser interface ... 1-3

I

- IEEE 802.1d ... 6-34, 6-36, 8-8
- IGMP ... 6-89
 - configuring ... 6-92, 6-94
 - console configuration ... 6-93
 - effect on filters ... 6-43, 6-97
 - example ... 6-95–6-96
 - filter override ... 6-98
 - high priority forwarding ... 6-92, 6-93
 - host not receiving ... 8-5
 - IP multicast address range ... 6-43, 6-97
 - leave group ... 6-94
 - maximum address count ... 6-98
 - multicast group ... 6-94, 6-97
 - multimedia ... 6-89
 - not working ... 8-5
 - operation ... 6-94
 - port states ... 6-92
 - querier setting, changing ... 6-98
 - query ... 6-94
 - report ... 6-94
 - statistics ... 7-3, 7-18
 - status ... 6-94
- IGMP traffic ... 6-92
- in-band ... 2-1
- in-band security ... 6-40
- Inbound Telnet Enabled parameter ... 8-3
- interface, console ... 1-4
- interfaces listed ... 1-1
- IP
 - address function ... 2-1
 - broadcast traffic ... 6-100
 - browser interface ... 3-3
 - duplicate address ... 8-33
 - duplicate address, DHCP network ... 8-4
 - gateway ... 2-4
 - gateway (IP) address ... 6-6
 - gateway address ... 6-6
 - host-only ... 6-62
 - subnet mask ... 2-1, 6-6, 6-9

IP address

- browser interface ... 3-3
- configuration ... 6-6
- DHCP/Bootp ... 6-6
- disable ... 6-6
- effect when not used ... 6-10
- gateway ... 6-8
- global assignment ... 6-14
- globally assigned addressing ... 6-14
- SNMP ... 5-1
- VLAN ... 6-6
- web browser interface ... 6-7–6-8

IPX

- 802.2 to SNAP ... 6-111
- broadcast traffic ... 6-100
- encapsulation type ... 6-111
- network number ... 7-5, B-2
- proxy reply ... 6-111
- proxy response ... 6-111

J

- Java ... 3-3–3-4

L

- latency ... 6-100, 6-107
- learning bridge ... 6-1
- leave group
 - See IGMP. ... 6-94
- legacy VLAN ... 6-47
- link failure ... 6-74
- link speed, port trunk ... 6-65
- link status, port ... 7-9
- link test ... 7-23
- link, blocked ... 6-3
- link, redundant ... 6-3
- Link, serial ... 6-20
- LOGOUT command ... 4-5
- loop ... 6-34, 6-37, 6-64
- loop, redundant ... 6-50
- lost password ... 3-8

M

- MAC address ... 6-11, 7-4, B-1
 - duplicate ... 6-62, 8-7, 8-9
 - learned ... 7-13
 - port ... 7-14, B-1, B-2
 - switch ... B-1
 - VLAN ... 6-61, B-1
- Main menu ... 2-3
 - features ... 4-4
- managed device ... 2-1
- management
 - access configuration from console ... 4-4
- management interfaces described ... 1-1
- management server URL ... 6-4–6-5
- management server URL default ... 3-9
- management, console port ... 2-1
- manager access ... 6-15
- manager address ... 6-15, 6-17
- Manager Address field ... 5-3
- manager password ... 3-7, 3-8, 4-9, 4-11
- Manual, IP address ... 6-9
- media type, port trunk ... 6-65
- mesh
 - benefits ... 6-74
 - blocked ports ... 6-77
 - broadcast storm ... 6-75
 - connecting multiple domains ... 6-76
 - domain ... 6-37, 6-74
 - edge switch ... 6-76
 - hub not allowed ... 6-75–6-76
 - port types ... 6-74
 - problems ... 8-5
 - redundant paths ... 6-75
 - spanning tree ... 8-7
 - STP ... 6-37
 - STP operation ... 6-38
 - VLAN ... 6-61
 - VLAN requirement ... 6-77
 - VLAN support required ... 6-76
 - when ABC used ... 6-111
- MIB ... 5-2, 6-98
- MIB listing ... 5-1
- MIB, HP proprietary ... 5-1
- MIB, standard ... 5-1
- Microsoft Internet Explorer ... 3-3
- Monitor parameter ... 6-32
- monitoring a VLAN ... 6-33
- monitoring traffic ... 6-29

- monitoring, traffic ... 5-1
- multicast address, spanning tree ... 6-44
- multicast filter ... 6-40, 6-43
- multicast group
 - See IGMP
- multimedia
 - See IGMP
- multiple VLAN ... 5-1
- multi-port bridge ... 2-1
- multiport bridge ... 6-1

N

- navigation, console ... 4-5, 4-7
- navigation, event log ... 8-12
- Netscape ... 3-3
- network management functions ... 5-4
- network manager address ... 5-3
- network monitoring
 - VLAN monitoring parameter ... 6-33
- network monitoring port
 - traffic overload ... 6-33
- Network Monitoring Port screen ... 6-29
- network slow ... 8-3
- NSQ reply, proxy ... 6-103
- NSQ request ... 6-109
- NSQ statistics ... 7-20

O

- online help ... 3-9
- online help location, specifying ... 6-5
- operator access ... 6-15
- operator mode ... 4-10
- operator password ... 3-7, 3-8, 4-9, 4-11
 - password ... 4-9
- OS
 - download failure ... A-7
 - download, troubleshooting ... A-7
 - switch-to-switch download ... A-5
 - version ... A-4–A-6
- OS download, TFTP ... A-2
- OS, download ... 8-12
- out-of-band ... 1-4
- overview of the switch console ... 4-1
- Overview window
 - Active Button ... 3-12

Overview window

- Active Tab ... 3-12
- Alert Log ... 3-12
- Alert Log Control Bar ... 3-12
- Alert Log Header Bar ... 3-12
- Button Bar ... 3-12
- description ... 3-11
- Graphs area ... 3-12
- Status Bar ... 3-12
- Tab Bar ... 3-12

P

- password ... 3-8, 4-2
 - browser/console access ... 4-9
 - case-sensitive ... 4-11
 - creating ... 3-7
 - delete ... 3-8, 4-11
 - deleting with the Clear button ... 4-12
 - if you lose the password ... 3-8
 - incorrect ... 4-10
 - length ... 4-11
 - lost ... 3-8, 4-12
 - setting ... 3-7, 4-10
 - manager ... 3-7
 - operator ... 3-7
 - using to access browser and console ... 3-8
- path cost ... 6-37
- ping test ... 7-23
- port
 - address table ... 7-13
 - auto, IGMP ... 6-92
 - auto-negotiation ... 6-24
 - blocked ... 6-37
 - blocked in mesh ... 6-77
 - blocked, IGMP ... 6-92
 - cost
 - See* spanning tree
 - counters ... 7-9
 - forwarding, IGMP ... 6-92
 - MAC address ... B-2, B-3
 - monitoring ... 6-61
 - monitoring, VLAN ... 6-30
 - numbering ... 6-24
 - state, IGMP control ... 6-92
 - traffic patterns ... 7-9
- Port Address Table screen ... 6-63

- port trunk ... 6-64
 - configuration ... 6-65
 - FEC ... 6-72
 - interoperation ... 6-66
 - limit ... 6-64
 - media type ... 6-65
 - network management ... 6-65
 - SA/DA ... 6-71
 - SA-trunk ... 6-72
 - spanning tree ... 6-65
 - utilization ... 3-13
 - VLAN ... 6-61, 6-65
- Port Utilization and Status displays
 - Web Browser Interface ... 3-12
- priority
 - See* spanning tree
- proprietary MIB ... 5-2
- protocol filter ... 6-40, 6-44
- proxy ARP ... 6-109, 8-5
- proxy NSQ reply ... 6-103
- proxy reply ... 6-110
- proxy reply, IPX ... 6-111
- proxy response to ARP ... 6-108
- proxy response, IPX ... 6-111
- public SNMP community ... 5-3–5-4
- Put ... A-9

Q

- query
 - See* IGMP

R

- reboot ... 4-5, 4-7, 4-13, 5-4, 6-51
- reconfigure ... 4-7
- redundant link ... 6-3
- redundant links ... 6-75
- redundant path ... 6-34, 6-37
 - spanning tree ... 6-34
- report
 - See* IGMP
- requirements, TopTools ... 1-1
- requirements, web browser interface ... 1-1
- reset ... 4-13, 8-12
- Reset button ... 8-12
- reset port counters ... 7-9
- restricted access ... 6-15

- restricted write access ... 6-15
- RFC 1213 ... 5-2
- RFC 1493 ... 5-1
- RFC 1515 ... 5-2
- RFC 1573 ... 5-2
- RFC 1757 ... 5-2
- RFC 2132 ... 6-111
- RIP ... 6-109
- RIP statistics ... 7-20
- RMON ... 5-1
- router ... 6-63, 6-94, 6-100
 - gateway ... 6-9
- router release A.09.70 ... 6-63
- router, Bootp/DHCP ... 6-111
- router, with ABC enabled ... 6-110
- RS-232 ... 1-4
- RS-232 console ... 6-20
- RS-232 Console port ... 2-1

S

- SAP ... 6-109
- SAP statistics ... 7-20
- SAP table ... 6-111
- security ... 3-8
- security filter ... 6-40
- security, in-band ... 6-40
- send authentication traps ... 6-19
- Serial Link Configuration screen ... 6-20
- serial number ... 7-4
- server not accessible ... 8-4
- server, DHCP/Bootp ... 6-8
- server, TFTP ... A-9
- server, Timep ... 6-7
- setmib ... 6-98
- setting a password ... 4-10
- setting Fault Detection Policy ... 3-23
- severity ... 8-10
- severity code, event log ... 8-10
- slow network ... 8-3
- SNAP ... 6-109

- SNMP ... 5-1, 6-18
 - Communities screen ... 6-15
 - community ... 6-16, 6-17
 - configure ... 5-3
 - IP address ... 5-1
 - manager address ... 6-15, 6-17
 - public community ... 6-15
 - traps ... 5-1
 - v1 agent ... 5-1
- SNMP community ... 5-3
 - restricted access ... 6-15
- SNMP public community ... 5-4
- SNMP-based download ... A-5
- software version ... 7-4
- software, OS ... 4-5
- sorting Alert Log entries ... 3-15
- source port filter ... 6-40, 6-44
- spanning tree ... 6-34
 - blocked link ... 6-38
 - blocked port ... 6-37
 - blocking ... 6-34
 - blocking in VLANs ... 6-3
 - browser interface ... 6-35
 - caution ... 7-17
 - default ... 6-34
 - disabled by VLANs ... 6-34
 - duplicate MAC ... 6-62
 - filter ... 6-44
 - forwarding state ... 6-34
 - global information ... 7-16
 - link priority ... 6-34, 6-85
 - mesh ... 6-38
 - not in menu ... 6-34
 - port cost ... 6-37
 - port trunk ... 6-65
 - priority ... 6-37
 - problems ... 8-7
 - root data ... 7-16
 - statistics ... 7-16
 - switch mesh ... 8-7
 - VLANs ... 6-60
- Spanning Tree Configuration screen ... 6-34
- standard MIB ... 5-1
- starting a console session ... 4-2
- static filter limit ... 6-40
- statistical sampling ... 5-1
- statistics ... 4-4, 7-2
 - clear counters ... 4-13

status and counters
 access from console ... 4-4
status and counters menu ... 7-3
Status Bar ... 3-12
status overview screen ... 3-5
STP
 See spanning tree
subnet ... 6-94
subnet address ... 6-45
subnet mask ... 2-1, 2-4, 6-6, 6-8–6-9
 IP ... 6-6
 See also IP. ... 6-8
subnetting, multiple ... 6-100
Sun workstation ... 6-62
support URL ... 6-4
 changing default ... 6-4
 default ... 6-4
Support URL Window ... 6-4
support/mgmt URLs ... 3-20
switch console
 ending a session ... 4-3
 Main menu ... 4-4
 overview ... 4-1
 starting a session ... 4-2
 status and counters access ... 4-4
 switch management access configuration ... 4-4
switch management
 access configuration ... 4-4
switch mesh
 See mesh
switch-to-switch download ... A-5
system configuration screen ... 6-22
system down ... 4-3
system name
 when none is specified ... 7-29
System Name parameter ... 6-23

T

Tab Bar ... 3-12
Telnet ... 3-4, 4-2, 4-5
Telnet, problem ... 8-3
terminal type ... 6-20
terminal, ANSI ... A-10
terminal, VT100 ... A-10
TFTP server ... A-9
TFTP download ... A-2–A-3
TFTP OS download ... A-2

threshold setting ... 5-4
time command
 how to enter ... 7-29
time format ... 8-10
time parameter ... 6-22
Time Protocol Enabled ... 6-8, 6-23
time server ... 6-6
Timep ... 6-6, 6-7
Timep Poll Interval ... 6-8
Timep server ... 6-8
TopTools ... 1-5
TopTools access ... 3-4
TopTools requirements ... 1-1
TopTools system requirements ... 3-3
TopTools, main screen ... 1-5
traffic analysis ... 5-1
traffic monitoring ... 5-1, 5-4
traffic, monitoring ... 6-29
traffic, port ... 7-9
transparent bridge ... 2-1
Trap ... 6-18
 limit ... 6-18
 Trap Receivers Configuration screen ... 6-18
trap
 authentication trap ... 6-18
trap event levels ... 6-19
trap receiver ... 5-3–5-4
traps
 SNMP ... 6-18
troubleshooting ... 7-1
 approaches ... 8-2
 unusual network activity ... 8-3
troubleshooting, OS download ... A-7
types of Alert Log entries ... 3-16

U

unauthorized access ... 6-18
Universal Resource Locator
 See URL. ... 6-4
Unix, Bootp ... 6-11
unrestricted write access ... 6-15
unusual network activity ... 8-3
up time ... 7-4
upload configuration ... A-9

- URL ... 3-9
 - network city ... 6-4
 - online help ... 6-5
 - support ... 6-4
- URL for Browser Interface
 - changing default ... 6-4
- URL for support
 - default address ... 6-4
- URL, management ... 6-5
- URL, support/Mgmt ... 3-20
- URLs
 - browser interface online help location ... 6-5
 - management server ... 6-5
- user names
 - using for browser and console access ... 3-8
- usernames
 - creating ... 3-7
- using the passwords ... 3-8
- utilization, port ... 3-13

V

- version, OS ... A-4–A-6
- VLAN ... 6-6, 6-32–6-33, 6-45, 6-61, 6-63, 8-9
 - 802.1Q ... 6-38
 - ABC ... 6-102, 6-104, 6-108
 - address ... 5-1
 - Bootp ... 6-12
 - Bootp or DHCP ... 6-10
 - configuring Bootp ... 6-12
 - DEFAULT_VLAN ... 6-48–6-49, 6-54
 - default ... 2-3
 - deleting ... 6-62
 - device not seen ... 8-8
 - event log entries ... 8-10
 - ID ... 6-58
 - IP address ... 2-3, 6-6
 - IPX with ABC configured ... 6-111
 - limit ... 6-49
 - link blocked ... 8-8
 - MAC address ... 6-61
 - management ... 6-48
 - mesh ... 6-61
 - mesh domain ... 6-38
 - monitoring ... 6-30
 - multiple ... 5-1
 - multiple VLANs on port ... 6-58

- network monitoring ... 6-29
- OS download ... A-2–A-3
- port assignment ... 6-54
- port configuration ... 6-60, 8-9
- port monitoring ... 6-61
- port trunk ... 6-61, 6-65
- reboot ... 6-52
- required for mesh ... 6-77
- restrictions ... 6-62
- source port filters ... 6-44
- STP ... 6-60
- STP operation ... 6-38
- Switch 2000 ... 6-60
- Switch 800T ... 6-60
- switch capacity ... 6-45
- switch mesh ... 6-76
- tagged ... 6-46
- tagging ... 6-56, 6-58
- tagging broadcast, multicast, and unicast traffic ... 8-8
- untagged ... 6-47, 6-55
- VLAN ID ... 6-58
- VT-100 terminal ... 2-2
- VT100 terminal ... 6-20, A-10

W

- warranty ... ii
- WBI
 - See* ... 6-7
- Web Agent
 - advantages ... 1-3
- Web Agent Enabled ... 3-1

web browser interface

- active button ... 3-12
- active tab ... 3-12
- features ... 1-3
- alert log ... 3-5, 3-12, 3-14–3-15
- alert log control ... 3-18
- alert log control bar ... 3-12
- alert log details ... 3-17
- alert log header bar ... 3-12
- alert types ... 3-16
- bandwidth adjustment ... 3-14
- bar graph adjustment ... 3-14
- button bar ... 3-12
- configuration tab ... 3-20
- configuration, support URL ... 3-9
- diagnostics tab ... 3-21
- disable access ... 3-1
- enabling ... 3-3
- error packets ... 3-13
- fault detection policy ... 3-6, 3-23
- fault detection window ... 3-23
- first-time install ... 3-6
- first-time tasks ... 3-5
- graphs area ... 3-12
- help via TopTools ... 3-9
- identity tab ... 3-19
- main screen ... 3-11
- management server URL ... 3-9
- online help ... 3-9
- online help, inoperable ... 3-9
- overview window ... 3-11
- password lost ... 3-8
- passwords, setting ... 3-7
- port status ... 3-14
- port utilization ... 3-12
- Port Utilization and Status displays ... 3-12
- requirements ... 1-1
- screen elements ... 3-11
- screen layout ... 3-11
- security ... 3-1, 3-6
- security tab ... 3-21
- standalone ... 3-3
- status bar ... 3-12, 3-22
- status indicators ... 3-22
- status overview screen ... 3-5
- status tab ... 3-19
- support tab ... 3-21
- system requirements ... 3-2–3-3

- tab bar ... 3-12
- Telnet to console ... 3-4
- unicast ... 3-13
- non-unicast ... 3-13
- URL default ... 3-9
- URL, management server ... 3-10
- URL, support ... 3-10

web site, HP ... 5-2

world wide web site ... 5-2

world wide web site, HP ... 6-5

write access ... 6-15

X- Z

- Xmodem OS download ... A-6
- XNS ... 6-62
- XPut ... A-9