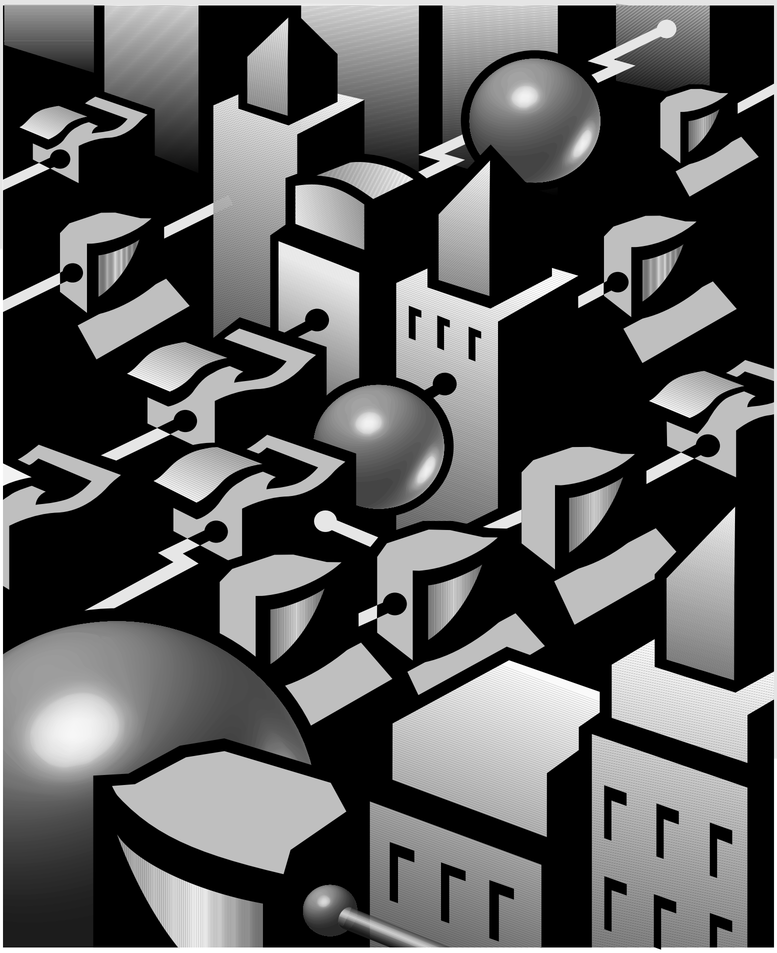
HEWLETT® PACKARD

# Installation and Configuration Guide

HP J3100B



# HP AdvanceStack Switch 2000

# HP Customer Support Services

### How to get the latest software/agent firmware

You can download from the World Wide Web, HP FTP Library Service, CompuServe, and HP BBS a compressed file (j3100b.exe) containing the latest version of the HP Switch 2000 software and proprietary MIB, the HP J3108A FDDI Module software, and a software download utility file (update.exe). After you download the file, **extract** the file by typing *filename* and pressing Enter. For example, j3100b Enter.

### World Wide Web

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

Select the “Support” section.

From this web site, you can also download information on the HP networking products. If you have a growing network, download the *Designing HP AdvanceStack Workgroup Networks Guide* or call 1-800-752-0900 in the U.S. to receive a copy through the mail.

### HP FTP Library Service

1. FTP to Internet IP Address — ftp ftp.hp.com.
2. Log in as anonymous and press Return at the password prompt.
3. Enter bin to set the transfer type.
4. Enter cd /pub/networking/software.
5. Enter get *filename* to transfer the file to your computer, then quit.

### CompuServe

1. Login to CompuServe.
2. Go to the “hp” service.
3. Select “HP Systems, Disks, Tapes, etc.”
4. Select “Networking Products” library.
5. Download *filename* and then quit.

### HP BBS

Set your modem to no parity, eight bits, 1 stop bit, set speed up to 14400 bps, and with your telecommunication program (e.g., Windows Terminal) dial (208) 344-1691 in the U.S. to get the latest software for your HP networking product. For other countries, see http://www.hp.com/cposupport/eschome.html.

*(over for more services)*

HEWLETT® PACKARD

*Obtain the latest console code (j3100b.exe) from*

| | |
|---|---|
| HP FTP Library: | ftp ftp-boi.external.hp.com |
| World Wide Web: | http://www.hp.com/go/network_city |
| HP BBS: | (208) 344-1691 |

*(over)*

HP NETWORK CONNECTIVITY • HP NETWORK CONNECTIVITY •

### HP FIRST Fax Retrieval Service

HP FIRST is an automated fax retrieval service that is available 24 hours a day, seven days a week. HP FIRST provides information on the following topics:

- Product information
- Troubleshooting instructions
- Technical reviews and articles
- Configuration information

To access HP FIRST, dial one of the following phone numbers:

| Location | Phone Number |
|---|---|
| U.S. and Canada Only | Dial 1 (800) 333-1917 with your fax machine or touch-tone phone and press 1. |
| Outside the U.S. and Canada | Dial 1 (208) 344-4809 from your fax machine and press 9. |

To receive a list of currently available documents, enter document number 19941. The information you requested will be sent to you by return fax. For other countries, see http://www.hp.com/cposupport/eschome.html.

### Additional HP Support Services

In addition to the above services, you can purchase various HP telephone support services which provide you expert HP technical assistance:

- Network Phone-In Support provides you support at an hourly rate. In the U.S., call 1-800-790-5544. In other countries, please contact your local HP Response Center to see if this service is available in your country.
- HP SupportPack Comprehensive Network Support provides complete problem resolution for medium to large interconnected local and wide area networks. Contact your HP Authorized Reseller or the nearest HP Sales and Support Office for more information.

HP offers other hardware support services. Please contact your reseller for more information.

✂

|  |  |
|---|---|
| CompuServe: | Go hpsys<br>Lib 7.<br>Download j3100b.exe |
| Network Phone-In Support (hourly): | 1-800-790-5544 |

# HP AdvanceStack Switch 2000

# Installation and Configuration Guide

HP J3100B

## Publication Number

5966-5212
March 1997

## Applicable Product

HP J3100B

## 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.

Hewlett-Packard Company
8000 Foothills Boulevard, m/s 5551
Roseville, California  95747-5551
*http://www.hp.com/go/network_city*

# Preface

## Use of This Guide and Other Switch 2000 Documentation

This guide describes how to install the B-version of the Switch 2000 (HP J3100B) in your network and use the console interface for the HP AdvanceStack Switch 2000 (hereafter referred to as the “Switch 2000”).

### Operating Differences

This manual describes features of the B-version of the Hewlett-Packard Switch 2000 (HP J3100B). In some cases, such as the Spanning Tree Protocol (operating within VLANs) and port trunking capabilities, there are significant operating differences between the A-version of the Switch 2000 (HP J3100A) and the B-version. For information on the features available in the A-version, refer to the manuals shipped with that product.

**Important!** Before installing or removing an interface module (or installing or removing a transceiver used with a module), refer to the specific module documentation describing these procedures.

- If you need information on specific parameters in the console interface, refer to the online help provided in the interface.
- If you need further information on Hewlett-Packard switch technology, refer to the *HP AdvanceStack Products CD* shipped with your Switch 2000.

# Overview of Console Applications

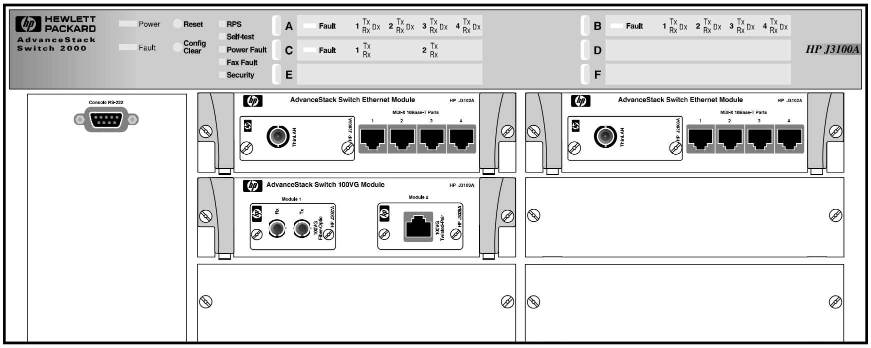


**Figure 1. Example of the HP AdvanceStack Switch 2000 with Optional Modules and Transceivers installed**

When powered-up in the factory default configuration, the Switch 2000 automatically operates as a multiport learning bridge with the following configuration:

- All installed ports are enabled and are members of a single broadcast domain
- Spanning tree protocol (STP) is disabled

The console interface provides the following capabilities for use when you want to move beyond this basic level of operation:

- Monitoring system performance and status
- Customizing the system configuration for improved performance and unique system requirements
- Enabling network management (SNMP) access
- Setting passwords to help protect system security
- Downloading system software updates
- Troubleshooting

# Contents

## 1 Installing the Switch

## 2 Using the Console Interface

## 3 Configuring the Switch

## 4 Monitoring and Analyzing Switch Operation from the Console

## 5 Using SNMP To Monitor and Manage the Switch

## 6 Using the Advanced Commands

## 7 Advanced Concepts

# Installing the Switch

## Installation Summary

This chapter describes the installation procedures for the HP J3100B AdvanceStack Switch 2000 (hereafter referred to as the Switch 2000). The following is a summary of those procedures:

1. **Install interface modules and transceivers (optional).** The best time to install Switch 2000 interface modules and their related transceivers is prior to powering up the switch or during scheduled down times. Note that, because the Switch 2000 allows module changes ("hot swaps") while operating, you can make hardware changes once the switch is in use. That is, you can replace one module with another module of the same type without needing to reboot the switch. Similarly, you can install a module in an unused slot without needing to reboot the switch. (An "unused slot" is one that has not been used since the last time the switch was rebooted.) However, it is necessary to remove a particular interface module from the Switch 2000 before adding, removing, or changing a transceiver in that module. In cases where one module is exchanged for another of a different type, it is necessary to reboot or reset the switch. This procedure is described later in this chapter and also in the installation guides for the various interface modules that are compatible with the Switch 2000.
2. **Install the optional redundant power supply (RPS).** This optional power supply (HP J3136A AdvanceStack Switch 2000 Redundant Power Supply) shares the power requirement load with the switch's main power supply, and will keep the switch operating in the unlikely event that the main power supply fails.
3. **Verify the switch's operation.** This is a simple process of applying power to the Switch 2000 and ensuring that the LEDs on the switch's front panel respond properly.
4. **Mount the switch in a rack or place it on a tabletop.** Hewlett-Packard sells 19-inch free-standing equipment racks. To order a rack, contact your HP-authorized LAN dealer.

**Warning**

**Install the Switch 2000 only on a tabletop or in an equipment rack or cabinet designed for this product. The Switch 2000 weighs a minimum of 17.3 lbs (7.86 kilos) with no interface modules or redundant power supply installed. Rack or cabinet mounting should be done by two people. If the rack or cabinet is empty, install the Switch 2000 at the bottom; if not, install the switch as close to the bottom as possible. (If a lightweight device is already installed at the bottom, you may want to remove it, install the Switch 2000 at the bottom, then reinstall the lightweight device above the Switch 2000.) If the Switch 2000 is mounted high, the rack or cabinet may become unstable and possibly fall over.**

5. **Connect the Switch 2000 to a network and connect computers and/ or other devices to the switch's ports.**

6. **Configure the Switch 2000**. The Switch 2000, in its factory default configuration, operates as a multiport transparent bridge. You will need to use the console interface to configure the switch for additional functionality. Initially, this requires one of the following:

   - A PC with a terminal emulator connected to the Console RS-232 port on the switch either directly or via a modem
   - An actual terminal directly connected to the Console RS-232 port on the switch

   (For examples of terminal emulator configurations, refer to appendix C, "Sample Console Configurations".)

7. After receiving a minimal IP or IPX configuration through one of the above options, you can also access the console interface via Telnet or use a network management tool for some configuration and monitoring functions.

# 1. Install Add-In Modules *(Optional)*

To begin operating in your network, the Switch 2000 needs at least one interface module. If you need to install a module, refer to the instructions you received with the module(s) you plan to use. Note that you must install any optional transceivers in a module before installing the module in the Switch 2000, or remove the module from the switch before installing an optional transceiver. (Refer to the documentation for the specific module.) For example, the HP J3102A AdvanceStack Switch 2000 4-Port 10Base-T module illustrated below is shown with the optional HP J2608A ThinLAN transceiver installed. (Transceivers must be purchased separately.)

**Caution**

If you will be installing or removing a module while the switch is operating, refer to the documentation you received with the module for important information, including any "readme" file on the disk shipped with the module. Also, refer to the module documentation if you will be installing or removing a transceiver from a module in an operating Switch 2000.

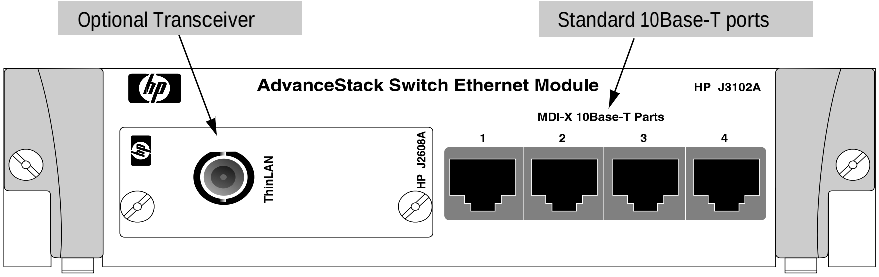


**Figure 1-1. HP J3102A Interface Module With Optional Transceiver Installed**

It may be more convenient to install a module before installing the Switch 2000 into a rack or other location. Inspect your installation site and identify whether the switch's module slots will be accessible.

For a description of currently available modules, contact your HP-authorized LAN dealer.

# 2. Install the Redundant Power Supply *(Optional)*

**Caution**

Disconnect the power supply from the Switch 2000 before installing the redundant power supply (RPS). Otherwise, damage to the switch's components could occur.

**Note**

*For important information on how to install the HP J3136A AdvanceStack Switch 2000 Redundant Power Supply (RPS) in the Switch 2000, refer to the documentation provided with the RPS.*

The optional HP J3136A AdvanceStack Switch 2000 Redundant Power Supply (RPS) shares the power load with the Switch 2000's main power supply. It is recommended that, if possible, you install the RPS before beginning to use the switch in your network. Otherwise, you must schedule downtime to install the RPS. (RPS installation requires removal of the Switch 2000's back panel, which interrupts power to the switch.) When the RPS is installed in a Switch 2000 and power is applied to the RPS, the RPS LED on the Switch 2000's front panel is lit.

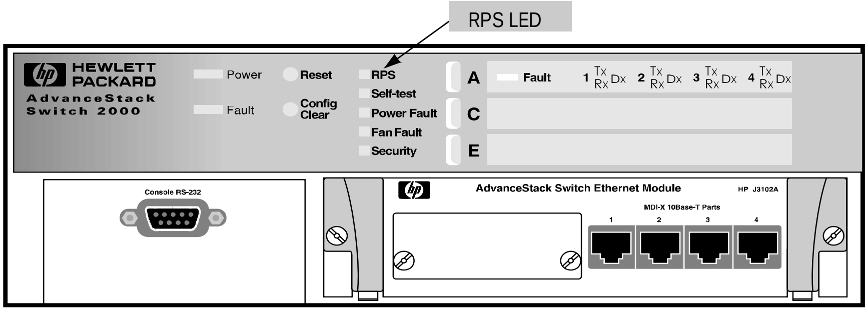


**Figure 1-2. RPS LED on the Switch 2000's Front Panel**

The RPS connects to the back of the Switch 2000. Thus, if you are going to install an RPS, it may be more convenient to install it before installing the Switch 2000 into a rack or other location. Inspect your installation site and identify whether the switch's back panel will be accessible.

# 3. Verify the Switch's Operation

This process verifies that the Switch 2000 is operating properly.

## Verify the Switch Hardware

1. Connect the supplied power cord to the switch's power receptacle.

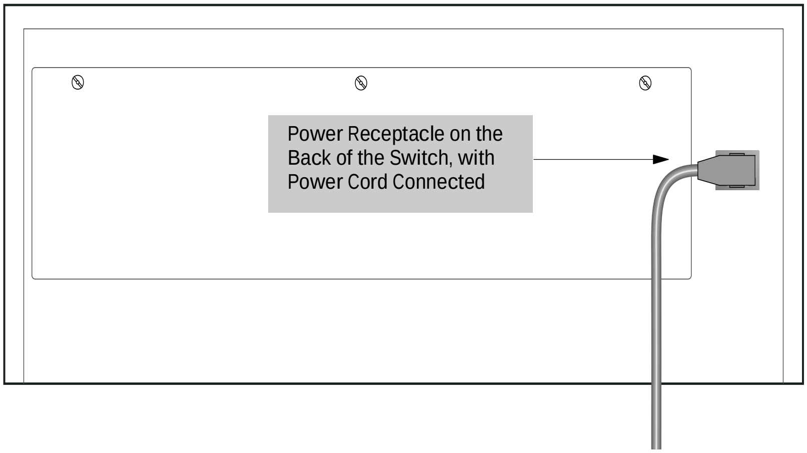

Power Receptacle on the Back of the Switch, with Power Cord Connected

**Figure 1-3. Back Panel of the Switch 2000**

2. Plug the power cord into a properly grounded electrical outlet.

**Note**

Neither the Switch 2000 nor the RPS has a power switch. The Switch 2000 is powered on when the power cord for either the switch itself or an installed RPS is plugged into a power source.

If your installation requires a different power cord than the one supplied with the switch, be sure to use a power cord displaying the mark of the safety agency that defines the regulations for power cords in your country. The mark is your assurance that the power cord can be used safely with the switch.

3. Check the LEDs on the switch's front panel.

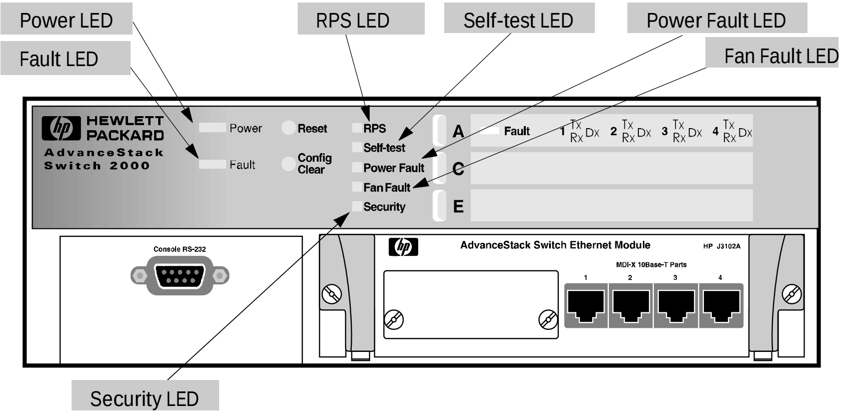


**Figure 1-4. The Switch 2000 System LEDs**

When the switch is powered on, it performs a self-diagnostic test. During the test, the following occurs:

- All LEDs turn on momentarily.
- The Power LED remains on; the Fault LED turns on.
- The RPS LED turns on if an RPS is connected and supplying power.
- The Self-test and Fault LEDs remain on for less than one minute.

When the self-test completes successfully, the following events occur:

- The power LED and, if an RPS is connected, the RPS LED, remain on.
- The self-test and Fault LEDs turn off.

**Note**

If any Fault LED is flashing, the Switch 2000 has encountered a problem. Refer to chapter 9, "Troubleshooting".

4. After the switch has passed its self-test, disconnect the power cord from the switch and proceed with the mounting instructions.

**Note**

If the switch's permanent location makes it difficult to access the Console RS-232 port from a terminal or PC running a terminal emulator, you may want to temporarily connect a terminal device now and configure the switch minimally for Telnet access. If you want to do this, refer to "Connect a Console Device" on page 1-14 before continuing here.

# 4. Mount the Switch

A Switch 2000 can be mounted in two ways:

- In a rack or cabinet
- On a table

The hardware for mounting the switch is included in the accessory kit (5063-8544) packed with the switch.

Hewlett-Packard sells 19-inch free-standing equipment racks. For more information, contact your HP authorized LAN dealer.

## Mounting Precautions

Before mounting the switch, read and follow these mounting precautions:

- Plan the switch's location and orientation relative to other devices and equipment. Also consider the cabling that will be attached to the switch and ports that will be used. In the front of the switch, leave 3 inches (7.6 cm) of space for twisted-pair cables. In the back of the switch, leave 1-1/2 inches (3.8 cm) of space for the power cord.
- Ensure that any installation of Switch 2000s, together with any other devices, does not overload the power circuits, wiring, and over-current protection. To determine the possibility of overloading the supply circuits, add together the ampere ratings from the nameplates of all devices installed on the same circuits and compare the total with the rating limits for the supply circuits.
- Make sure that the power source circuits are properly grounded, then use the supplied power cord to connect the Switch 2000 to the circuit. Refer to the Safety and Regulatory Statements that follow the appendixes at the back of this manual.
- Do not install the Switch 2000 in an environment where the operating ambient temperature might exceed 55°C (131°F).
- Make sure the air flow around the sides and back of the switch is not restricted.
- If an HP J3136A AdvanceStack Switch 2000 Redundant Power Supply is installed, make sure the air flow around the fan area of the RPS is not restricted.

## Rack or Cabinet Mounting

**Warning**

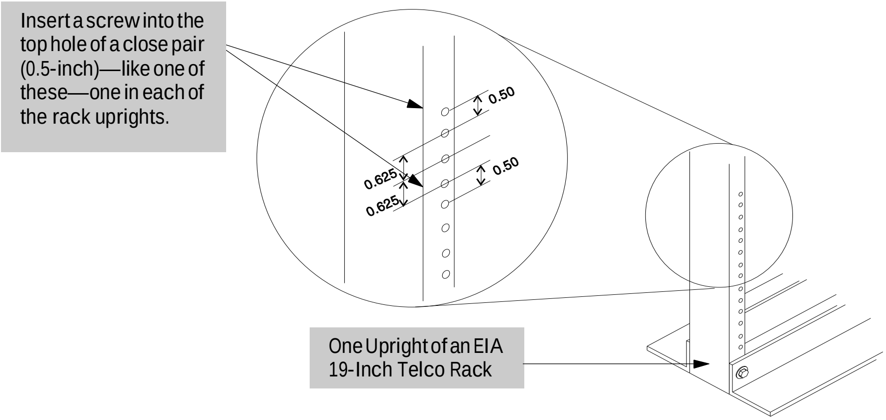
**The rack or cabinet should be adequately secured to prevent it from becoming unstable and/or falling over.**

**Install the Switch 2000 only on a tabletop or in an equipment rack or cabinet designed for this product. The Switch 2000 weighs a minimum of 17.3 lbs (7.86 kilos) with no interface modules or redundant power supply installed. Rack or cabinet mounting should be done by two people. If the rack or cabinet is empty, install the Switch 2000 at the bottom; if not, install the switch as close to the bottom as possible. If a lightweight device is already installed at the bottom, you may want to remove it, install the Switch 2000 at the bottom, then reinstall the lightweight device above the Switch 2000. If the Switch 2000 is mounted high, the rack or cabinet may become unstable and possibly fall over.**

1. As shown below, partially install one of the 5/8-inch number 12-24 screws in each rack upright. Install the screw in the upper hole of a close pair. (Some cabinets require number 10-32 screws instead, which are not included in the accessory kit.)

**Caution**

Make sure you have screws that fit your cabinet or rack before mounting the switch.



Insert a screw into the top hole of a close pair (0.5-inch)—like one of these—one in each of the rack uprights.

One Upright of an EIA 19-Inch Telco Rack

**Figure 1-5. Installing the Mounting Screws**

2. Using a Phillips cross-head screwdriver, attach the L-shaped mounting brackets to each side of the switch with four 10-mm M4 screws (included in the accessory kit).

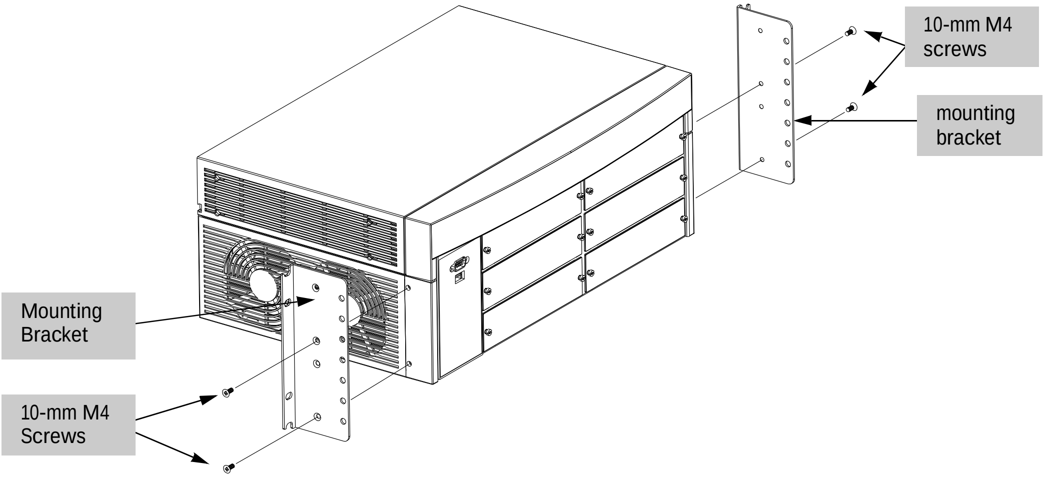


**Figure 1-6. Attach the Mounting Brackets**

3. Place the switch in the rack and lower it so the notches in the bottom of the bracket slide onto the screws you installed in step 1. Tighten these screws—be careful not to overtighten.

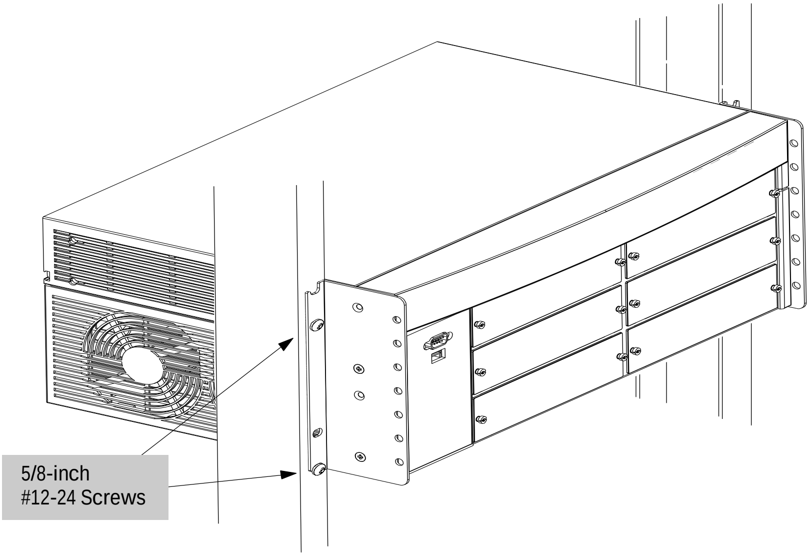


**Figure 1-7. Install the Switch in the Rack**

4. Install the other two 5/8-inch 12-24 screws into the upper hole in each bracket. Tighten these screws—be careful not to overtighten.

## Table Mounting

Place the switch on a table or other horizontal surface. (No special tools are necessary.) Attach the self-adhesive feet (included in the accessory kit) to the recessed areas on the bottom front area of the switch. Be certain to pick a sturdy table in an uncluttered area. You may want to secure the switch's cables to the leg of the table to help prevent people from tripping over them.

**Caution**

Make sure the air flow around the sides and back of the switch is not restricted. Also, if an HP J3136A AdvanceStack Switch 2000 Redundant Power Supply is installed, make sure the air flow around the fan area of the RPS is not restricted.

Route the power cord(s) and data cables so that they will not create a tripping hazard for people walking in the area of the switch installation.

# 5. Complete the Network Connections to the Switch

Reconnect the switch to the power source. With the switch mounted, you are now ready to connect it to your network. Typical switch connections are:

- Switch-to-networked devices (i.e. computers, servers, and printers).
- Switch-to-hub
- Switch-to-switch
- Switch-to-router
- Switch-to-network backbones

**Note**

*For important information on connecting the Switch 2000 to other devices, refer to the Connectivity Quick Reference that is shipped with the optional HP AdvanceStack Switch 2000 modules and is also available on the "HP AdvanceStack Product CD" shipped with your switch.*

For other network design guidelines, refer to *An Introduction to Ethernet LAN Switches* and *Designing Switched Networks*, both of which are included on the *HP AdvanceStack Product CD* shipped with the Switch 2000. For physical topology guidelines, refer to *Designing HP AdvanceStack Workgroup Networks*, available from HP authorized LAN dealers and also on the product CD shipped with your Switch 2000.

Network connections to the Switch 2000 are through ports on the optional modules and transceivers installed in the switch. For connections to these ports, see the documentation you received with the specific module or transceiver, and to the *Quick Reference* mentioned in the above note.

## Twisted-Pair Cascade Connections

The 10Base-T ports on the optional HP J3102A AdvanceStack Switch Ethernet Module are designed for MDI-X operation. This enables you to use a "straight-through" twisted-pair cable to connect to transceivers on computers and other devices having MDI (Media-Dependent Interface) requirements. For connecting cascaded hubs or switches having 10Base-T ports configured for MDI-X operation, use a crossover cable unless the cascaded hub or switch offers a port that you can switch between MDI and MDI-X operation (such as the HP AdvanceStack J2610B 10Base-T Hub-8U). In this case, you can either set the port on the cascaded device to MDI operation and use a straight-through cable or set it to MDI-X operation and use a crossover cable. (For more information on cables and connectors, refer to appendix A.)

**Cable Management.** The mounting brackets designed for the Switch 2000 provide help for the problem of managing your network cables. Each bracket has a series of holes for attaching a cable tie to bundle network cables away from the switch.

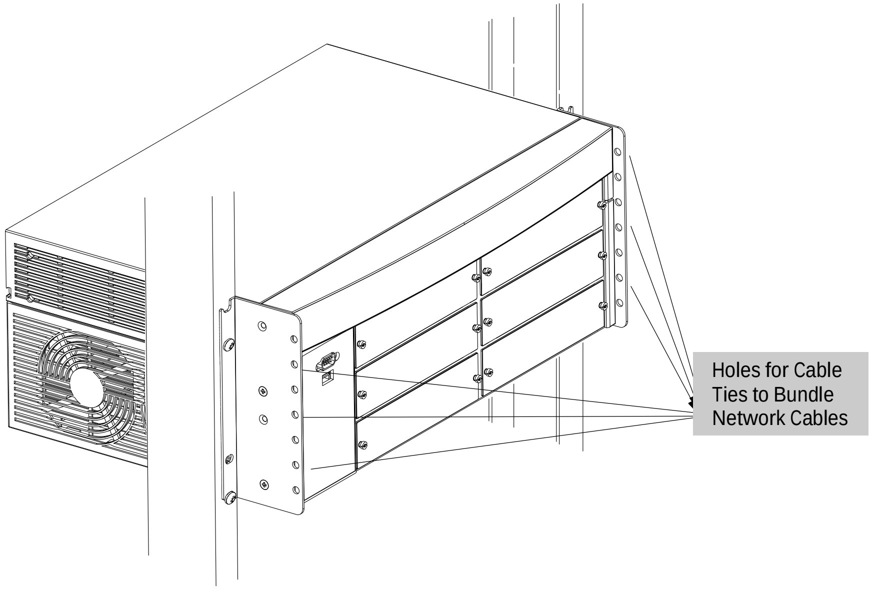


**Figure 1-8. Cable Management**

# 6. Connect a Console Device *(Optional)*

The Switch 2000 console interface enables you to use a PC or a terminal to do the following:

- Control password security
- Monitor switch and port statistics
- Modify the switch's configuration
- Use the switch's event log and command line to help in troubleshooting
- Download new software

**Note**

The Switch 2000 is shipped with a factory default configuration that enables operation as a multiport transparent bridge when installed in a network. For this operation, connecting a console device is unnecessary. However, for some of the other uses listed above, you will probably want to have console access.

You can use either of the following methods for console access:

- **Console RS-232** using either a direct or modem connection to a PC terminal emulator program, or a direct connection to an actual terminal
- **In-Band** using Telnet from a network management workstation. (To enable Telnet—or network management access—it is necessary to first use a direct-connect or modem-connect console device to configure an IP address and subnet mask for the switch.)

The Switch 2000 can simultaneously support one console session via the Console RS-232 port and one console session via Telnet.

## Direct Console Management, Using A Serial Cable and a Terminal or PC Terminal Emulator

You can use either a PC emulating an ASCII terminal (such as the terminal application included with Microsoft Windows 3.1 or HyperTerminal with Windows 95) or an ASCII terminal.

To directly connect a PC or terminal to a Switch 2000, follow these steps:

1. Connect the PC or terminal to the switch's Console RS-232 port using an RS-232-C console cable (included). (If you need information on pin-outs and recommended cables, see appendix A, "Cables and Connectors")

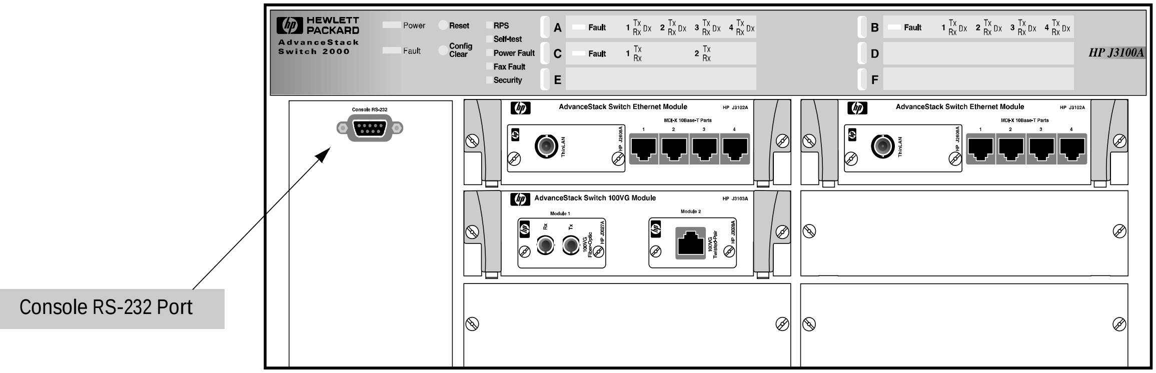


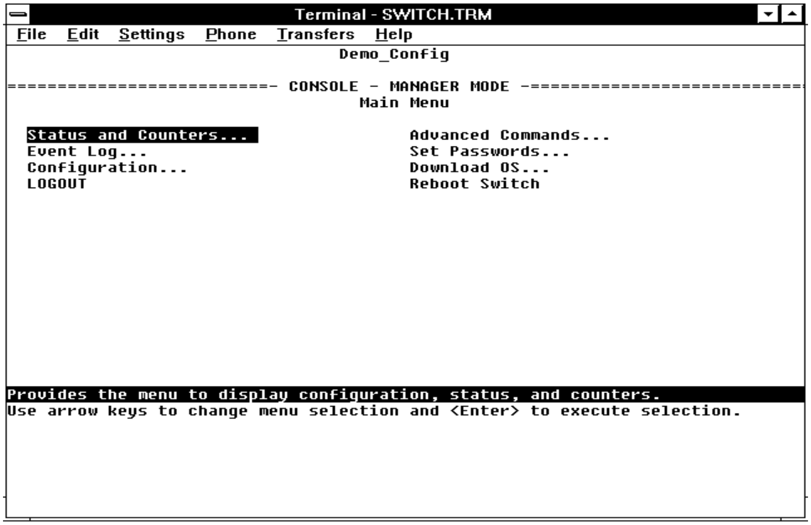
**Figure 1-9. Connecting a PC or Terminal to the Console RS-232 Port**

2. Turn on the terminal or PC's power (and, if using a PC, start the PC terminal emulation program). For recommended parameter settings, refer to appendix C, "Sample Console Configurations".

3. When you see this message:

```
Waiting for speed sense. Press enter to continue.
```

Press Enter. You will then see the Switch 2000's Main Menu.



```
                                Demo_Config

=========================- CONSOLE - MANAGER MODE -===========================
                                 Main Menu

  Status and Counters...                    Advanced Commands...
  Event Log...                              Set Passwords...
  Configuration...                          Download OS...
  LOGOUT                                    Reboot Switch

Provides the menu to display configuration, status, and counters.
Use arrow keys to change menu selection and <Enter> to execute selection.
```

**Figure 1-10. The Main Menu**

4. If you want to continue with direct console management at this time, refer to chapter 2, “Using the Console Interface”.

## Remote Console Management Using a Modem and a Terminal or PC Terminal Emulator

**Note**

For remote, console management, use a full-duplex, asynchronous (character-mode) modem.

1. At the Switch 2000 site:
   a. Connect the modem to the Switch 2000’s console port using an RS-232-C modem cable. (For pin-outs and recommended cables refer to appendix A, “Cables and Connectors”.)
   b. If necessary, configure the modem to operate with the current configuration of the Switch 2000. (The modem’s default configuration may be sufficient.)
2. At the remote site, connect the terminal (or PC emulating a terminal) to the remote modem using a modem cable. Make sure the terminal and modems are functioning properly, then establish the link between the terminal’s modem and the Switch 2000’s modem according to the modem instructions.

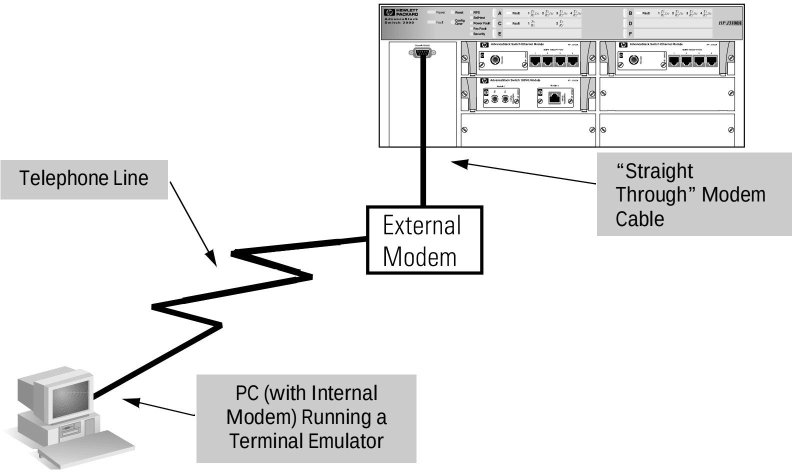

Telephone Line
External Modem
"Straight Through" Modem Cable
PC (with Internal Modem) Running a Terminal Emulator

**Figure 1-11. Example of Remote Access via a Modem**

3. When you see this message:

   ```
   Waiting for speed sense. Press enter to continue.
   ```

   Press [Enter]. You will then see the Switch 2000's Main Menu.

4. If you want to continue with direct console management at this time, refer to chapter 2, "Using the Console Interface".

# Where To Go from Here

| **Chapter** | **Topics** |
|---|---|
| 2 and 3 | To use the console, to configure the switch features, and to monitor and manage switch operation |
| 4 | To monitor and analyze switch operation from the console |
| 5 | To prepare the switch for SNMP management and to learn which MIBs are supported by the switch |
| 6 | To use the "Advanced Commands" functions |
| 7 | To find further information on the following features and to configure them:<br>• Spanning Tree Protocol<br>• Port Trunking<br>• Filters and Security<br>• Virtual LANs<br>• Internet Group Management Protocol (IGMP)<br>• Automatic Broadcast Control (ABC) |
| 8 | To download a new operating system or transfer a switch configuration |
| 9 | Troubleshooting information |
| Appendixes | To access the following:<br>• A: Cable and connector information<br>• B: Switch specifications<br>• C: Sample console configurations<br>• D: LED reference<br>• E: Bootp information<br>• F: MAC address management<br>• Safety and Regulatory information |

# Using the Console Interface

## Overview

This chapter describes the following features:

- Starting and ending a console session (page 2-2)
- The Main Menu (page 2-4)
- Screen structure and navigation (page 2-5)
- Using password security (page 2-7)
- Rebooting the switch (page 2-10)
- Resetting the switch (page 2-12)

**About the Console Interface.** The console interface enables you to reconfigure the switch and to monitor the switch status and performance. It consists of a series of management screens accessed through a menu-driven screen structure that begins at the Main Menu, and is organized as described in this section.

The Switch 2000 offers two methods of access to the console interface:

- Console RS-232 (out-of-band) access:
  - Directly connected to the Console RS-232 port, using a serial cable and a PC running a terminal emulator or an actual terminal
  - Remotely connected to the Console RS-232 port, using modems and a PC running a terminal emulator or an actual terminal

  Refer to chapter 1, “Installation”, for information on making RS-232 hardware connections.
- In-Band access using Telnet from a PC or UNIX station on the network. This method requires that you first configure an IP address and subnet mask by using either out-of-band console access or Bootp. The Switch 2000 allows one outbound and one inbound Telnet session to be running simultaneously.

Console access can be limited by setting Manager-level and Operator-level passwords.

# Starting and Ending a Console Session

**Note**

This manual assumes that either a terminal device is already configured and connected to your Switch 2000 (as described in chapter 1, “Installation”) or that you have already enabled Telnet access to the switch. (To enable Telnet access, refer to “Console Features” on page 3-16.)

### How To Start a Console Session:

1. Start your PC terminal emulator, terminal, or Telnet session on a remote terminal device.
2. Do one of the following:
   - If you are using Telnet, go to the next step.
   - If you are using a PC terminal emulator or a terminal, you should then see the following prompt:

   ```
   Waiting for speed sense. Press <enter> to continue.
   ```

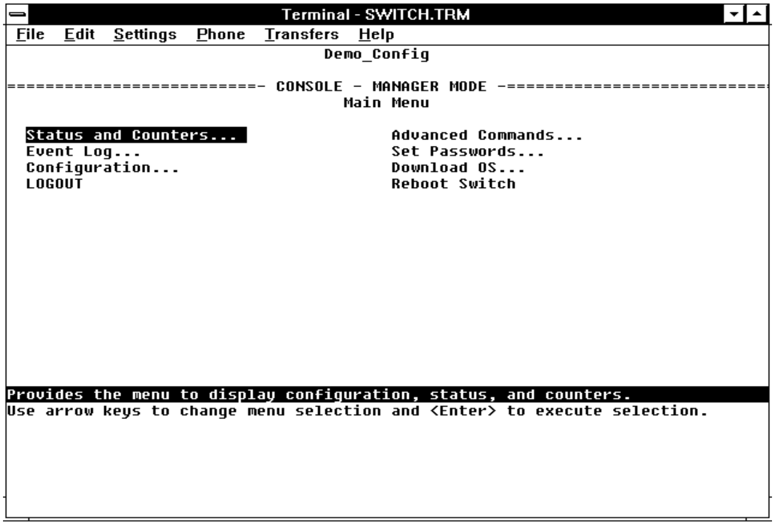
   ***Note:*** *If the console displays a series of random and/or unreadable characters instead of the above prompt, the Baud Rate setting for the terminal may be different from that of the console interface. The switch's autosensing feature remedies this problem when you press a key.*

   Press Enter and go to the next step.
3. The display then briefly displays a message indicating the baud rate at which the serial interface (Console RS-232 port) 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 Enter to display the Main Menu (figure 2-1).
   - If no password has been set, you will see this prompt:

   ```
   Press any key to continue.
   ```

   Press Enter to display the Main Menu (figure 2-1).

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



```
                              Demo_Config

==========================- CONSOLE - MANAGER MODE -============================
                               Main Menu

  Status and Counters...                    Advanced Commands...
  Event Log...                              Set Passwords...
  Configuration...                          Download OS...
  LOGOUT                                    Reboot Switch

Provides the menu to display configuration, status, and counters.
Use arrow keys to change menu selection and <Enter> to execute selection.
```

**Figure 2-1. The Main Menu**

For a description of Main Menu features, refer to “Main Menu Features” on page 2-4.

### How To End a Console Session:

1. If you have not made configuration changes in the current session, go to step 3.

2. Configuration changes requiring a reboot of the switch are indicated by an asterisk (*) next to the configured item in the Configuration menu. (See “Rebooting To Activate Configuration Changes” on page 2-11) If you have made configuration changes that require a reboot of the switch in order to take effect:

   a. Return to the Main Menu.

   b. Use the arrow keys ( [←], [→], [↓], and [↑] ) to highlight `Reboot Switch` in the Main Menu and press [Enter] to reboot.

3. Do one of the following:

   - If you have accessed the switch through a direct connection from a terminal device, exit from the terminal application.
   - If you have accessed the switch through Telnet or a modem connection:
     i. Return to the Main Menu.
     ii. Highlight LOGOUT in the Main Menu and press [Enter].

# Main Menu Features

The Main Menu (figure 2-1 on page 2-3) gives you access to these console interface features:

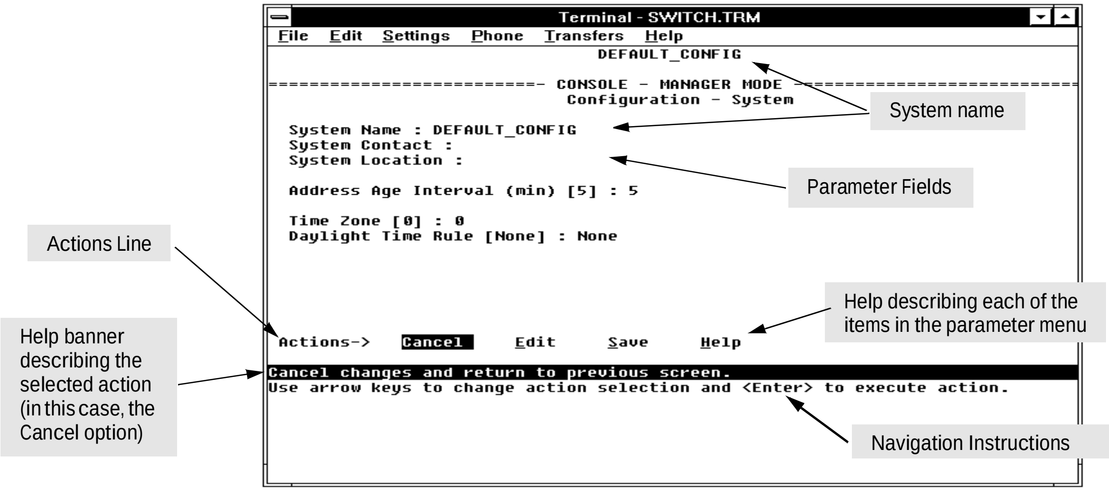
- **`Status and Counters:`** Displays information on the switch, individual ports, the address tables, protocols and spanning tree. (Refer to chapter 4, “Monitoring and Analyzing Switch Operation from the Console”.)
- **`Event Log:`** Enables you to read progress and error messages that are useful for checking and troubleshooting switch operation. A listing of Event Log messages is included on the CD shipped with your switch. (Refer to “Event Log” on page 4-16.)
- **`Configuration:`** Enables you to display the current configuration settings and to reconfigure individual parameters. (Refer to chapter 3, “Configuring the Switch”.)
- **`LOGOUT:`** Disconnects Telnet or modem access to the switch. (Refer to “How To End a Console Session” on page 2-3.)
- **`Advanced Commands:`** Provides access to a set of system management, monitoring, and troubleshooting commands. (Refer to chapter 6, “Using the Advanced Commands”.)
- **`Set Passwords`**: Enables you to set Operator and Manager passwords to help restrict who has access to the console interface. (Refer to “Using Password Security” on page 2-7.)
- **`Download OS:`** Enables you to download a new software version to theswitch.(Refer to chapter 8,“FileTransfers”.)
- **`Reboot Switch:`** Performs a software reboot, which is required (in some cases) to activate configuration changes that have been made. (Refer to “Rebooting To Activate Configuration Changes” on page 2-11.)

# 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 banner to describe navigation options, and individual parameters

For example, in the System configuration screen:



```
Terminal - SWITCH.TRM
File   Edit   Settings   Phone   Transfers   Help
                                 DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -==========================
                              Configuration - System

  System Name : DEFAULT_CONFIG
  System Contact :
  System Location :

  Address Age Interval (min) [5] : 5

  Time Zone [0] : 0
  Daylight Time Rule [None] : None




 Actions->   Cancel     Edit     Save     Help

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

System name
Parameter Fields
Actions Line
Help describing each of the items in the parameter menu
Help banner describing the selected action (in this case, the Cancel option)
Navigation Instructions

**Figure 2-2. Elements of Screen Structure**

**Table 2-1. How To Navigate in the Console**

| Task: | Actions: |
|---|---|
| Execute an action from an "Actions"-→ menu: | Use either of the following methods:<br>■ Use the arrow keys ( ← , → , ↓ , or ↑ ) to highlight the action you want to execute, then press Enter.<br>■ Press the key corresponding to the capital letter in the action name. For example, in a configuration menu, press E to begin editing parameter values. |
| Reconfigure (edit) a parameter setting or a field: | 1. Select a configuration area, such as `System`. (See figure 2-2.)<br>2. Press E (for `Edit` on the Actions line).<br>3. Use Tab or the arrow keys (←, →, ↑, or ↓) to highlight the item or field.<br>4. Do one of the following:<br>• If the parameter has preconfigured values, use the Space bar to select a new option<br>• If there are no preconfigured values, type in a value.<br>5. If you want to change another parameter value, return to step 3.<br>6. If you're finished editing parameters in the displayed screen, press Enter and do one of the following:<br>• To save any configuration changes you have made (or if you have made no changes), press S (for the `Save` action).<br>• To exit from the screen without saving any changes that you have made, press C (for `Cancel`).<br>***Note:*** Some 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.<br>7. When you are finished editing parameters, return to the Main Menu.<br>8. If necessary, reboot the switch by highlighting Reboot Switch and pressing Enter. (Refer to the ***Note***, above.) |
| Exit from a read-only screen. | Press B (for the `Back` action). |

# 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. This is the default level. (That is, if a Manager password has *not* 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 areas (System, Console, and Ports) for display only.<br>Use of the LOGOUT command.<br>On the Operator level, the Advanced Commands, 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).
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 Serial Link configuration screen (page 3-15). This causes the console session to end after the specified period of inactivity, thus giving you added security against unauthorized console access. (Once a Manager password is set and the console session is ended, access to the full console interface for any subsequent sessions requires the Manager password to be entered.)

**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.*

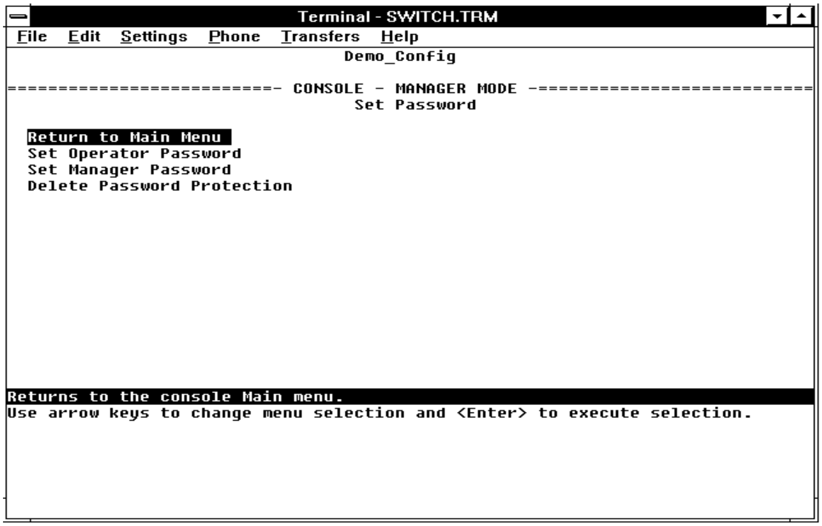
Passwords are case-sensitive.

The rest of this section covers how to:

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

**To set Manager and Operator passwords:.**

1. From the Main menu select Set Passwords. This screen appears:



```
                                 Demo_Config

=========================- CONSOLE - MANAGER MODE -==========================
                                 Set Password

  Return to Main Menu
  Set Operator Password
  Set Manager Password
  Delete Password Protection

Returns to the console Main menu.
Use arrow keys to change menu selection and <Enter> to execute selection.
```

**Figure 2-3. 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 characters and press [Enter]. (Remember that passwords are case-sensitive.)

   c. When prompted with `Enter new password again`, retype the new password and press [Enter].

   d. To set another password, return to step 2a. Otherwise, go to step 3.

3. Select `Return to Main Menu` to exit from the Set Password screen.

After a password is set, if you use LOGOUT or reboot or reset the Switch 2000, you will be prompted to enter the password to start a new console session.

**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 Config Clear button 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. From the Main menu select Set Passwords. You will then see the screen shown in figure 2-3.
3. Select Delete Password Protection. You will then see the following prompt:

```
Continue Deletion of password protection? No
```

4. Press the Space bar or press [Y] to select Yes, then press [Enter].
5. Press [Enter] to clear the Password protection message.
6. Select `Return to Main Menu` to exit from the Set Password screen.

**To Recover from a Lost Manager Password:**

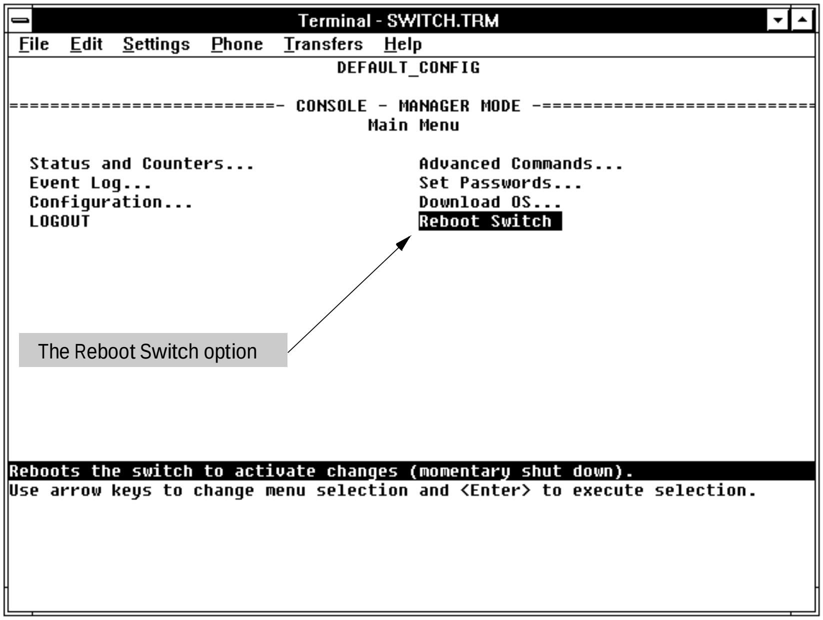
If you cannot start a console session at the manager level because of a lost Manager password, you can clear the password by getting physical access to the switch and pressing and holding the Config Clear button for at least one second.

# Rebooting the Switch

Rebooting the switch terminates the current console session and performs a reset of the operating system. Some of the reasons for performing a reboot include:

- Activating certain configuration changes that require a reboot
- Activating port modules that have been changed since the last reboot. (That is, where a port module has been replaced with a different type of port module.)
- Resetting statistical counters to zero

To Reboot the switch, use the `Reboot Switch` option in the Main menu. (If a Manager password has been previously set, `Reboot Switch` appears only if this password is entered at the beginning of the console session.)



```
                                  DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -==========================
                                     Main Menu

  Status and Counters...                        Advanced Commands...
  Event Log...                                  Set Passwords...
  Configuration...                              Download OS...
  LOGOUT                                        Reboot Switch







Reboots the switch to activate changes (momentary shut down).
Use arrow keys to change menu selection and <Enter> to execute selection.
```

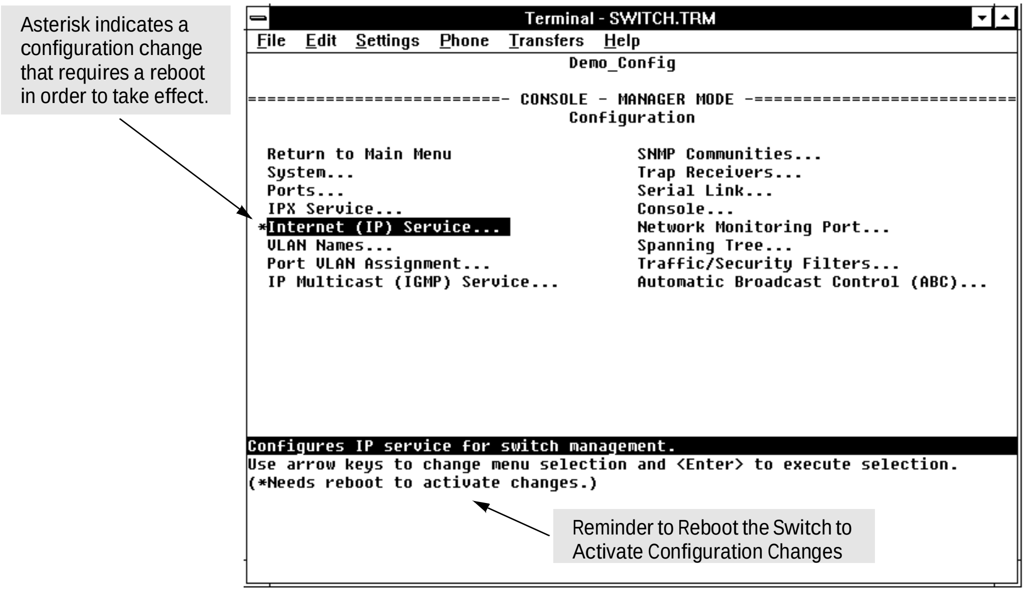
The Reboot Switch option

**Figure 2-4. 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:

- IPX Service
- Internet (IP) Service
- Serial Link
- Console Parameters
- New VLAN Names
- System Parameters

If configuration changes requiring a reboot have been made, the switch displays an asterisk next to the configuration menu item in which the change has been made. For example, if you change and save parameter values for the switch's IP configuration, the need for rebooting the switch would be indicated by an asterisk appearing in the following screen:


Asterisk indicates a configuration change that requires a reboot in order to take effect.

```
                                 Demo_Config

==========================- CONSOLE - MANAGER MODE -==========================
                                 Configuration

  Return to Main Menu                          SNMP Communities...
  System...                                    Trap Receivers...
  Ports...                                     Serial Link...
  IPX Service...                               Console...
 *Internet (IP) Service...                     Network Monitoring Port...
  VLAN Names...                                Spanning Tree...
  Port VLAN Assignment...                      Traffic/Security Filters...
  IP Multicast (IGMP) Service...               Automatic Broadcast Control (ABC)...





Configures IP service for switch management.
Use arrow keys to change menu selection and <Enter> to execute selection.
(*Needs reboot to activate changes.)
```

Reminder to Reboot the Switch to Activate Configuration Changes

**Figure 2-5. Example of a Configuration Change Requiring a Reboot**

# Resetting the Switch

Resetting requires physical access to the front of the Switch 2000. There are two levels of reset:

- **Hardware reset:** Momentarily interrupts switch operation and performs a complete hardware self-test. This also clears the Event Log.
- **Configuration reset:** This is a drastic action that interrupts switch operation, clears any passwords, clears the event log, performs a complete self-test, and reboots the switch in its factory default configuration. You should consider performing a configuration reset only if you want all configurable parameters reset to the factory default values.

**To perform a hardware or configuration reset:** Refer to appendix D, “Switch Reference”. Refer to the table on page D-5.

# Advanced Commands Features

The Advanced Commands prompt enables you to perform advanced management, monitoring, and troubleshooting activities. Below is a command listing.

| **Listing of Advanced Commands Available at the Commands Prompt** | | | |
|---|---|---|---|
| ! | Get (TFTP) | Ping | Time |
| ClearLED | Help | Print | Version |
| Config | History | Put (TFTP) | VLAN |
| Date | IPXPing | Redo | WalkMIB |
| Delete | LinkTest | Repeat | Zget |
| Exit | Log | SetMIB | Zput |
| GetMIB | Page | Telnet | |

Refer to chapter 6, “Using the Advanced Commands” for more on the command prompt and on individual commands.

# 3

# Configuring the Switch

## Overview

This chapter provides an overview of the Switch 2000 configuration features.

In its factory default configuration, the Switch 2000 automatically operates as a multiport learning bridge with network connectivity provided by the particular modules that you have installed. However, to “fine-tune” your switch for the specific performance and security needs in your network, you may choose to reconfigure certain switch parameters.

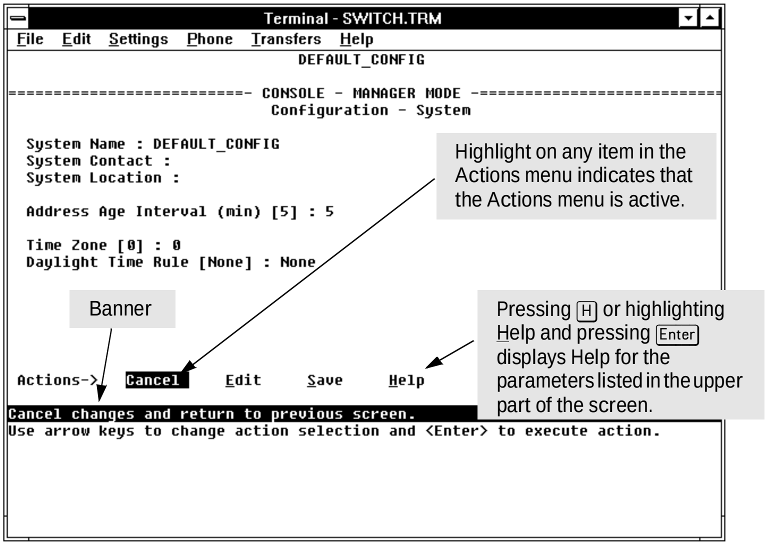
**Configuration Features.** The Switch 2000 enables you to configure the following switch features. For information on individual configuration parameters, use the online Help provided with each configuration screen in the console user interface.

- System (page 3-5)
- Ports (page 3-6)
- IPX Service (page 3-7)
- Internet (IP) Service (page 3-9)
- Virtual LANs (VLANs) (page 3-19)
- IP Multicast (IGMP) Service (page 3-14)
- SNMP Communities (page 3-11)
- Trap Receivers (page 3-13)
- Serial Link (page 3-15)
- Console (page 3-16)
- Network Monitoring Port (page 3-20)
- Spanning Tree (page 3-17)
- Traffic/Security Filters (page 3-18)
- Automatic Broadcast Control (ABC) (page 3-23)

**Note**

In the factory default configuration, the Spanning Tree Protocol (STP) is off. However, if the topology of your network includes any redundant loops between switches or bridges, you should enable STP. See “Spanning Tree” (page 3-17).

**To get Help on individual parameter descriptions.** In all screens except the Advanced Commands screen there is a `Help` option in the `Actions` menu. Whenever the `Actions` menu is active, you can display Help for that screen’s parameters by pressing H. (The Actions menu is active whenever any of the choices in the Action menu is highlighted.) For example:



```
                                DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -===========================
                              Configuration - System

  System Name : DEFAULT_CONFIG
  System Contact :
  System Location :

  Address Age Interval (min) [5] : 5

  Time Zone [0] : 0
  Daylight Time Rule [None] : None



 Actions->  Cancel     Edit     Save     Help

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

Highlight on any item in the Actions menu indicates that the Actions menu is active.

Banner

Pressing H or highlighting Help and pressing Enter displays Help for the parameters listed in the upper part of the screen.

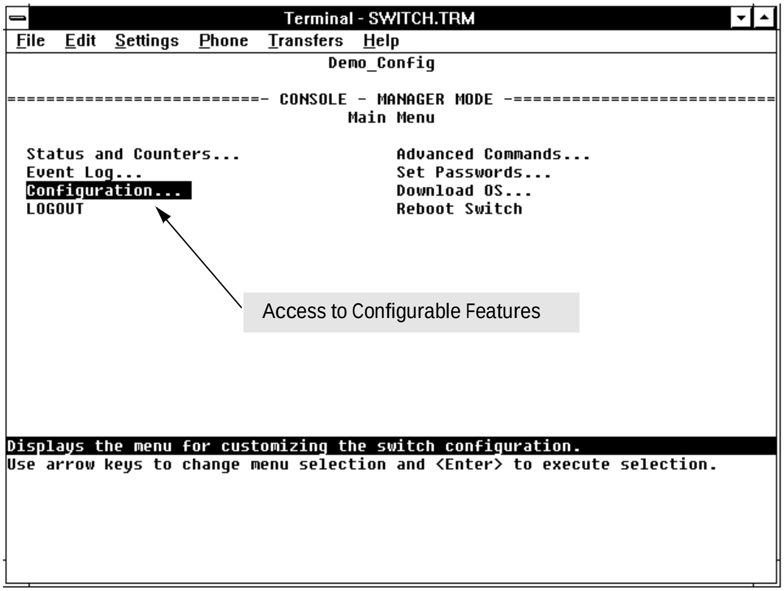
Figure 3-1. Example Showing How To Display Help

**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 banner under the action items will describe the currently selected action or data field. (For guidance in 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 2-5.)

# Configurable Features

**How To Access the Switch 2000 Configuration:** Use this procedure to access the switch's configurable features.

1. Begin at the Main Menu and select `Configuration` (figure 3-2):

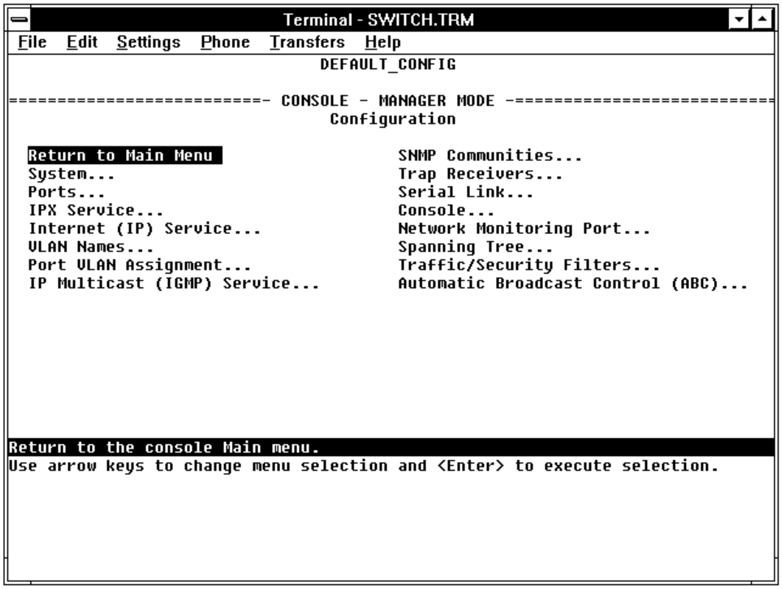

Terminal - SWITCH.TRM
File Edit Settings Phone Transfers Help

```
                                Demo_Config

==========================- CONSOLE - MANAGER MODE -===========================
                                 Main Menu

  Status and Counters...                      Advanced Commands...
  Event Log...                                Set Passwords...
  Configuration...                            Download OS...
  LOGOUT                                      Reboot Switch

Displays the menu for customizing the switch configuration.
Use arrow keys to change menu selection and <Enter> to execute selection.
```

Access to Configurable Features

**Figure 3-2. Select "Configuration" in the Main Menu**

After you select `Configuration`, the Configuration menu appears as shown in (figure 3-3).



```
                              DEFAULT_CONFIG

=========================- CONSOLE - MANAGER MODE -=========================
                               Configuration

  Return to Main Menu                    SNMP Communities...
  System...                              Trap Receivers...
  Ports...                               Serial Link...
  IPX Service...                         Console...
  Internet (IP) Service...               Network Monitoring Port...
  VLAN Names...                          Spanning Tree...
  Port VLAN Assignment...                Traffic/Security Filters...
  IP Multicast (IGMP) Service...         Automatic Broadcast Control (ABC)...

Return to the console Main menu.
Use arrow keys to change menu selection and <Enter> to execute selection.
```

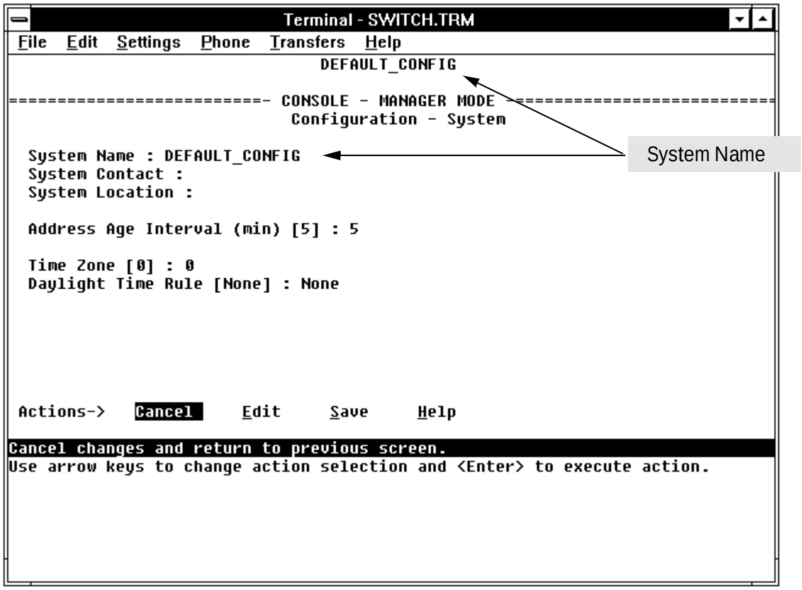
**Figure 3-3. The Configuration Menu**

2. Use the arrow keys ( [←], [→], [↑], and [↓] ) to highlight the configuration topic you want, then press [Enter].

3. Refer to the appropriate sections in the remainder of this chapter for information on configuring specific features.

## System Features

Configures basic switch management information, including system data, address aging, and time zone parameters:



```
                                  DEFAULT_CONFIG

========================- CONSOLE - MANAGER MODE -=========================
                               Configuration - System

  System Name : DEFAULT_CONFIG
  System Contact :
  System Location :

  Address Age Interval (min) [5] : 5

  Time Zone [0] : 0
  Daylight Time Rule [None] : None




 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 3-4. The System Configuration Screen (Default Values)**

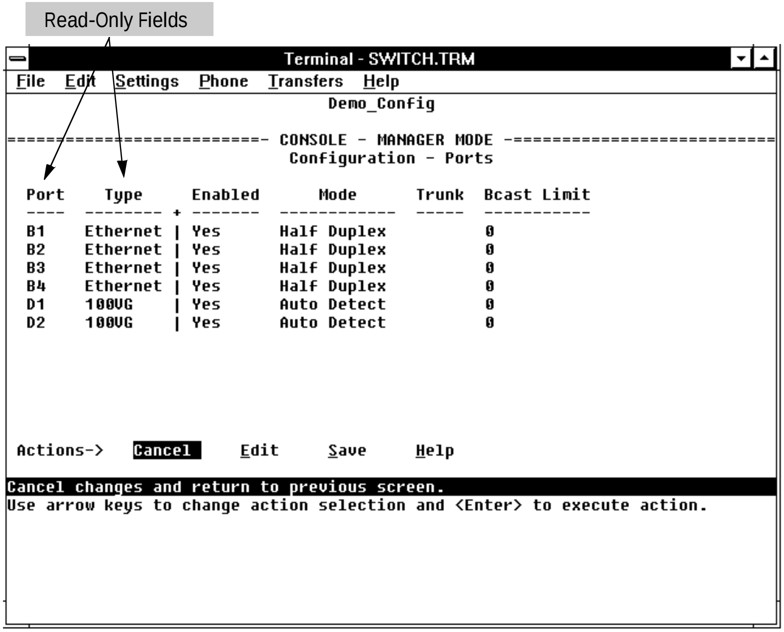
**Note**

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 "Internet (IP) Service Features" (page 3-9) for your time server or use the time and date commands described in chapter 6.

## Port Features

Configures the operating state for each port and optionally assigns selected ports to a port trunk. (For more on port trunking, refer to chapter 7.) 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.



```
                            Demo_Config

=========================== CONSOLE - MANAGER MODE ===========================
                       Configuration - Ports

  Port     Type      Enabled       Mode       Trunk   Bcast Limit
  ----   --------- + -------   ------------   -----   -----------
  B1     Ethernet  | Yes       Half Duplex            0
  B2     Ethernet  | Yes       Half Duplex            0
  B3     Ethernet  | Yes       Half Duplex            0
  B4     Ethernet  | Yes       Half Duplex            0
  D1     100VG     | Yes       Auto Detect            0
  D2     100VG     | Yes       Auto Detect            0




 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 3-5. Example of the Port Configuration Screen with 100VG and Ethernet Modules Installed in the Switch**

Port names are assigned by slot letter and port number. For example, if an HP J3102A AdvanceStack Switch Ethernet Module is installed in slot B, then the four ports in this module are identified as ports B1, B2, B3, and B4. Similarly, if an HP J3103A AdvanceStack Switch 100VG Module is installed in slot A, then the two ports in this module are identified as ports A1 and A2.

**Note**

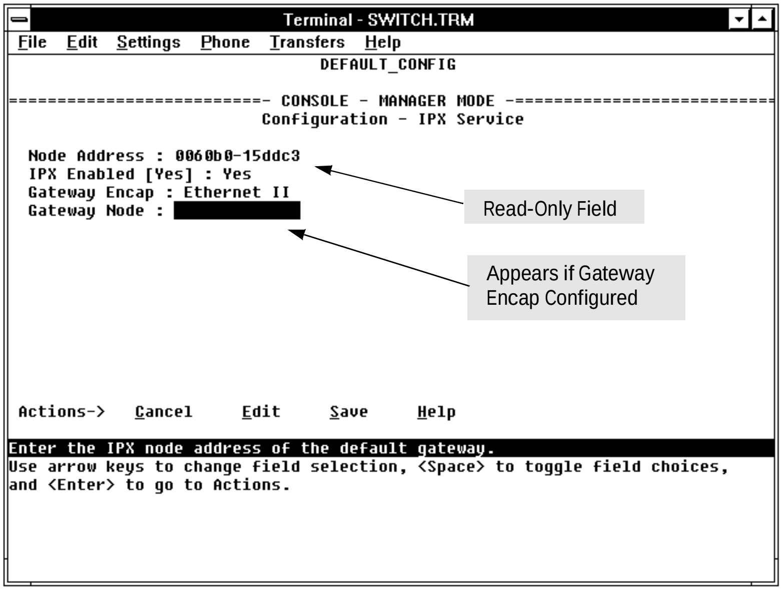
Broadcast limit (the Bcast Limit parameter) can be set for all ports in the switch (or VLAN, if VLANs are configured) from the Automatic Broadcast Control (ABC) screen (page 7-30 and following) if ABC is enabled. Setting the broadcast limit (Bcast Limit) in the above screen is on a per-port basis and overrides any settings done in Automatic Broadcast Control.

# IPX Service Features

Enables the switch to be managed in an IPX network. The Switch 2000 automatically enables IPX, configures the IPX node address, and learns the IPX network number. Thus, in the factory default configuration, IPX is automatically enabled for the switch.

**Note**

In this case, the factory-assigned node address is displayed as shown below. (The switch automatically detects the IPX network number.)



Terminal - SWITCH.TRM
File Edit Settings Phone Transfers Help

```
                              DEFAULT_CONFIG

=========================- CONSOLE - MANAGER MODE -==========================
                        Configuration - IPX Service

  Node Address : 0060b0-15ddc3
  IPX Enabled [Yes] : Yes
  Gateway Encap : Ethernet II
  Gateway Node :

 Actions->   Cancel     Edit     Save     Help

Enter the IPX node address of the default gateway.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

Read-Only Field
Appears if Gateway Encap Configured

**Figure 3-6. The IPX Service Configuration Screen**

**Note**

If VLANs are configured, the above parameters appear in a horizontally formatted screen.

You can also configure an IPX gateway frame encapsulation type and gateway node so that the switch can be managed from a remote IPX network.

If VLANs are configured, the switch can automatically learn the IPX network number of each attached VLAN. For more on VLANs, refer to chapter 7, “Advanced Concepts”.

**(Optional) How To Configure IPX for Management from a Remote IPX Network.** In the factory default, IPX is already enabled. If you want to enable management from a remote IPX network, you must configure the gateway encapsulation type and gateway node.

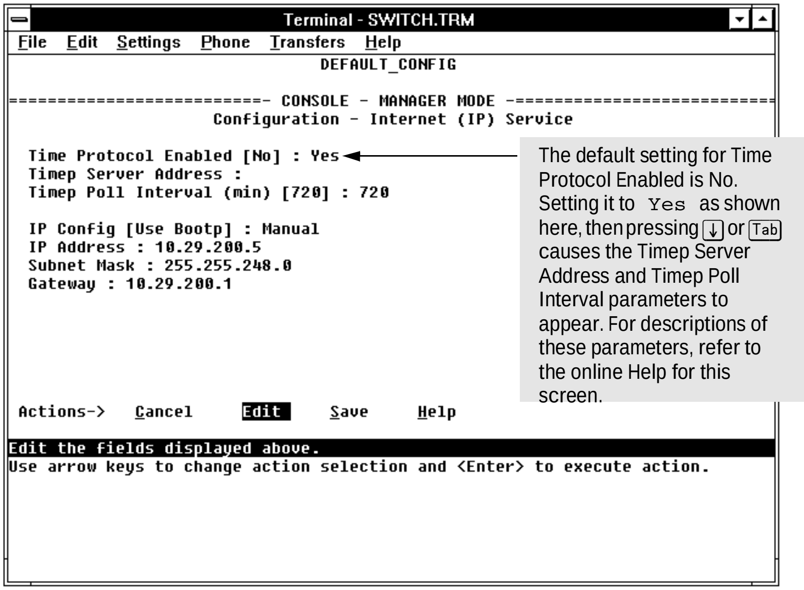
1. From the Configuration screen, select IPX Service to display the above screen.
2. If the `IPX Enabled` parameter is not already set to "`Yes`" (the factory default), then select this parameter and press the Space bar to select `Yes`.
3. Select the Gateway Encap field and use the Space bar to select the appropriate gateway encapsulation for the gateway device.
4. Press [↓] to display and select the Gateway Node field.
5. Type the IPX node address (MAC address) of the gateway device that is using the encapsulation defined in step 3.
6. Press [Enter], then [S] (for `Save`).
7. Return to the Main Menu and reboot the switch.

## Internet (IP) Service Features

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)

You can manually configure an IP address, subnet mask, and a Gateway IP address by setting the `IP Config` parameter to `Manual`. Or, you can use Bootp to configure IP for the switch from a Bootp server. In this case you must also configure your Bootp server accordingly. If you plan to use Bootp, refer to appendix E, “Bootp Operation”. Otherwise, set the `IP Config` parameter to `Manual` and then manually enter the IP address and subnet mask you want for the Switch 2000.



```
                                DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -===========================
                     Configuration - Internet (IP) Service

  Time Protocol Enabled [No] : Yes
  Timep Server Address :
  Timep Poll Interval (min) [720] : 720

  IP Config [Use Bootp] : Manual
  IP Address : 10.29.200.5
  Subnet Mask : 255.255.248.0
  Gateway : 10.29.200.1


 Actions->   Cancel     Edit     Save     Help

Edit the fields displayed above.
Use arrow keys to change action selection and <Enter> to execute action.
```

The default setting for Time Protocol Enabled is No. Setting it to `Yes` as shown here, then pressing ↓ or Tab causes the Timep Server Address and Timep Poll Interval parameters to appear. For descriptions of these parameters, refer to the online Help for this screen.

**Figure 3-7. Example of the IP Service Configuration Screen**

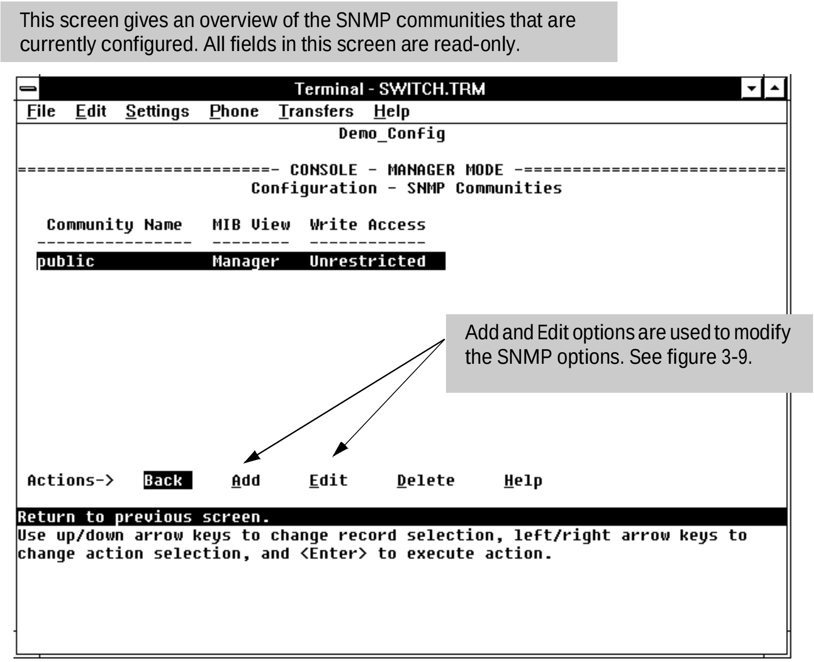
If VLANs are configured, then enable IP on a “per VLAN” basis. This is because each VLAN is a separate network and requires a unique IP address, plus a subnet mask. A gateway (IP) address is optional. For more on VLANs, refer to “Virtual LANs (VLANs)” on page 3-19 and in chapter 7, “Advanced Concepts”.

### How To Manually Configure for IP.

1. From the Configuration screen, select `Internet (IP) Service` to display the above screen.
2. Press [E] (for `Edit`).
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 you want to assign to 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 `Save`).
8. Return to the Main Menu and reboot the switch.

# SNMP Communities Features

Enables you to add, edit, or delete SNMP communities. Use this feature if you expect to manage the switch from an SNMP management station. 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. (For more on this topic, refer to chapter 5, “Using SNMP To Monitor and Manage the Switch”, and to the online Help.)



This screen gives an overview of the SNMP communities that are currently configured. All fields in this screen are read-only.

```
                              Demo_Config

==========================- CONSOLE - MANAGER MODE -===========================
                      Configuration - SNMP Communities

  Community Name   MIB View   Write Access
 ---------------- --------   ------------
 public            Manager    Unrestricted





 Actions->  Back    Add     Edit     Delete     Help

Return to previous screen.
Use up/down arrow keys to change record selection, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

Add and Edit options are used to modify the SNMP options. See figure 3-9.

**Figure 3-8. The SNMP Communities Screen (Default Values)**

**Caution**

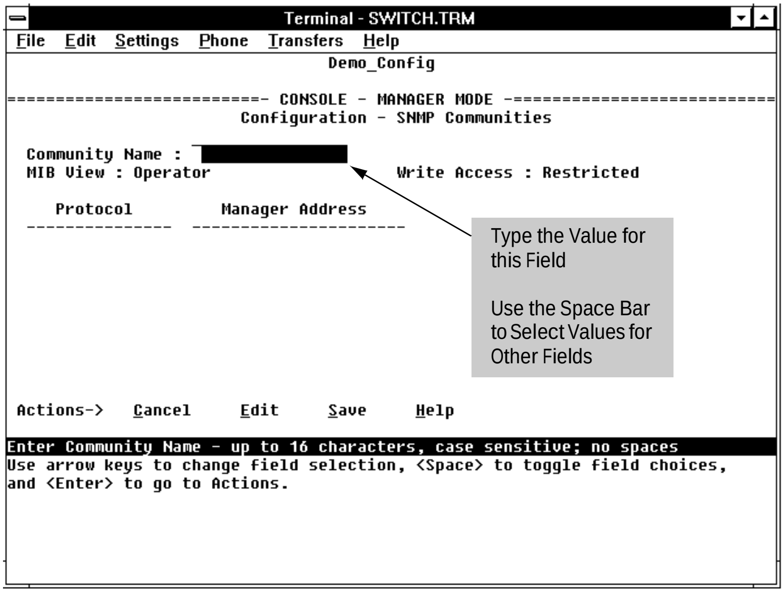
Deleting the community named “public” disables many network management functions (such as auto-discovery, traffic monitoring, and threshold setting). If security for network management is a concern, it is recommended that you change the write access for the “public” community to “Restricted”.

### How To Configure for SNMP Communities.

Ensure that the switch has been configured for IP and/or IPX.

1. From the Configuration screen, select SNMP Communities to display a screen similar to the one above.

2. Press [A] (for `Add`) to display the following screen:



```
                                Demo_Config

==========================- CONSOLE - MANAGER MODE -==========================
                      Configuration - SNMP Communities

  Community Name : 
  MIB View : Operator                    Write Access : Restricted

     Protocol         Manager Address
  ---------------  ----------------------









 Actions->   Cancel     Edit     Save     Help

Enter Community Name - up to 16 characters, case sensitive; no spaces
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

Type the Value for this Field

Use the Space Bar to Select Values for Other Fields

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 3-9. The SNMP Add or Edit Screen**

**Note**

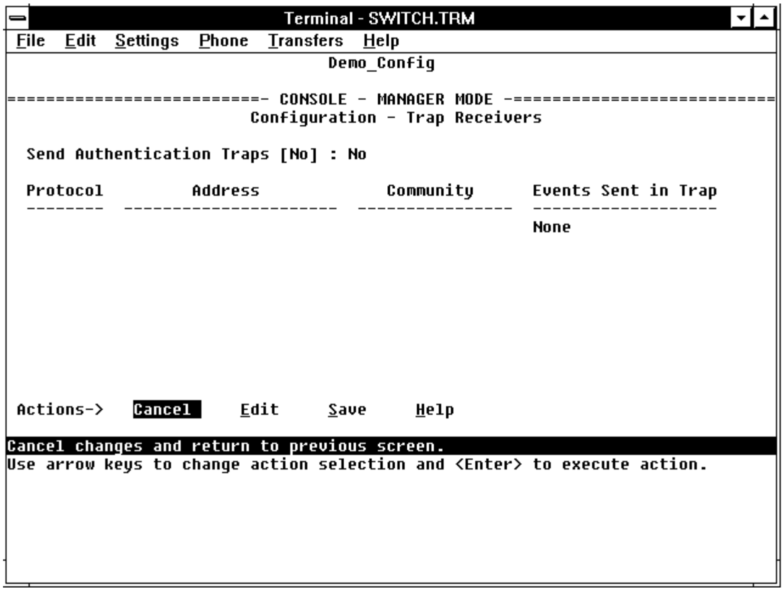
In the default configuration, no manager addresses are configured. In this case, all management stations using the correct community name may access the switch with the corresponding View and Access levels. If you want to restrict access to one or more specific nodes, you can enter up to ten IP and/or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

3. Enter the appropriate value in each of the above fields (use the [Tab] key to move from one field to the next).

4. Press [Enter], then [S] (for `Save`).

## Trap Receivers Features

Enables you to configure up to ten IP and/or IPX 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 protocol, address, and community define which management stations receive the traps. An authentication trap is sent and the Security LED on the front panel of the switch begins flashing if a management station attempts an unauthorized access. (The ClearLED command turns off the Security LED—page 6-6.) Check the event log to help determine why the authentication trap was sent. (Refer to chapter 4 for information on the event log.)



```
                              Demo_Config

==========================- CONSOLE - MANAGER MODE -==========================
                     Configuration - Trap Receivers

  Send Authentication Traps [No] : No

  Protocol         Address              Community       Events Sent in Trap
  --------  ----------------------  ----------------  -------------------
                                                      None

 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 3-10. The Trap Receivers Configuration Screen (Default Values)**

## IP Multicast (IGMP) Service Features—Multimedia Traffic Control

The IGMP (Internet Group Management Protocol) feature helps to reduce network congestion and improve security by reducing unnecessary multicast traffic on a per-port basis. This 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 (such as the Switch 800T or the B-version of the Switch 2000) can then be configured to direct the multicast traffic to only the ports where needed.

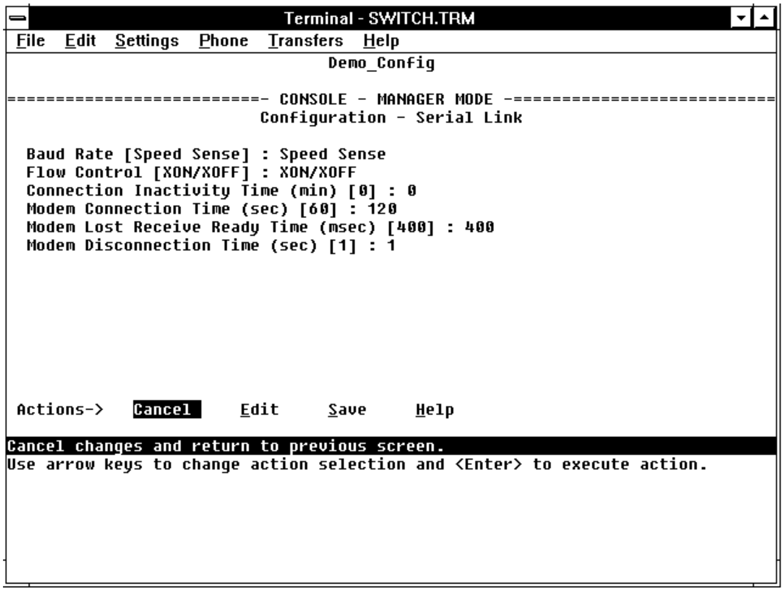
In the factory default state (IGMP disabled), the switch forwards all IGMP traffic. When IGMP is enabled, you can configure the switch to any of the following states on a per-port basis:

- Automatic (the default): Causes the switch to interpret IGMP packets and to filter IP multicast traffic based on the IGMP packet information for that port.
- Blocking: Causes the switch to drop all IGMP transmissions received and block all outgoing IP Multicast packets for that port.
- Forwarding: Causes the switch to forward all IGMP and IP multicast transmissions through the port.

For more information on IGMP and how to configure it, refer to “IP Multicast (IGMP)” on 7-23.

## Serial Link Features

Enables you to adjust the Console RS-232 configuration to customize the connection with the PC, terminal, or modem you are using for console access. Refer to the online Help for information on modem settings. Refer also to "Console Features" on page 3-16.



```
                                 Demo_Config

=========================- CONSOLE - MANAGER MODE -==========================
                          Configuration - Serial Link

  Baud Rate [Speed Sense] : Speed Sense
  Flow Control [XON/XOFF] : XON/XOFF
  Connection Inactivity Time (min) [0] : 0
  Modem Connection Time (sec) [60] : 120
  Modem Lost Receive Ready Time (msec) [400] : 400
  Modem Disconnection Time (sec) [1] : 1






 Actions->   Cancel     Edit     Save     Help

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

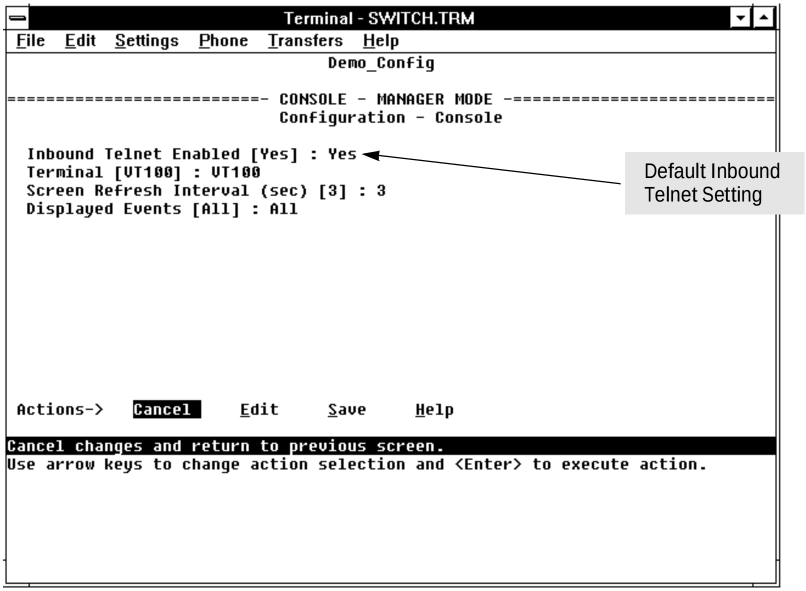
**Figure 3-11. The Serial Link Configuration Screen (Default Values)**

## Console Features

Lets you enable or disable inbound Telnet access and control the types of events displayed in the event log. Also specifies the terminal type and the console screen refresh interval used by the statistics screens (that is, the frequency with which statistics are updated on the statistics screens).

**Note**

"Inbound" Telnet is Telnet access to the switch console from another device. "Outbound" Telnet, which is using Telnet through the switch console to access another device, is always enabled as long as the switch has been configured with a valid IP address. (To configure an IP address for the switch, refer to "Internet (IP) Service Features" on page 3-9.) The switch supports one inbound and one outbound Telnet session simultaneously.


Terminal - SWITCH.TRM
File Edit Settings Phone Transfers Help
Default Inbound Telnet Setting

```
                                 Demo_Config

========================- CONSOLE - MANAGER MODE -========================
                             Configuration - Console

  Inbound Telnet Enabled [Yes] : Yes
  Terminal [VT100] : VT100
  Screen Refresh Interval (sec) [3] : 3
  Displayed Events [All] : All

 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 3-12. The Console Configuration Screen (Default Values)**

## Spanning Tree Features

Enables you to activate the IEEE 802.1d Spanning Tree Protocol (STP) and to adjust spanning tree parameters. In the factory default, STP is off. Thus, if there are any redundant paths (loops) 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.

If VLANs are configured, then you can configure STP separately for each VLAN.

**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 chapter 7, “Advanced Concepts”, and examine the IEEE 802.1d standard.

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

To configure STP, refer to “Spanning Tree Protocol (STP)” on page 7-2.

## Traffic/Security Filter Features

Enables you to control traffic and increase network security by creating filters based on any of the following criteria:

- Multicast address
- Source port only
- Source MAC address and source port
- Protocol frame type
  - IP (Ethernet or 802.3 SAP)
  - ARP
  - DEC LAT
  - AppleTalk
  - SNA
  - NetBIOS
  - IPX (Ethernet or 802.3 SAP)
  - VINES IP or ECHO

If you are using VLANs, they will affect source port and source MAC filter configuration. For more information on filtering, using filters with VLANs, and configuring filters, refer to “Filters and Security” on page 7-8.

## Virtual LAN (VLAN) Features

Enables you to create up to eight port-based VLANs. A VLAN is a group of ports designated by the Switch 2000 as belonging to the same broadcast domain. This feature enables you to configure port-based virtual LANs to help isolate broadcast traffic and increase security. Typically, if VLANs are used, all ports carrying traffic for a particular subnet address should be configured to the same VLAN. For more on when, why, and how to use VLANs, refer to "Virtual LANS (VLANs)" on page 7-14.

In the factory default state, VLANs are not configured. All ports belong to the same broadcast/multicast domain. This domain is called "DEFAULT_VLAN" and appears in the "VLAN Names" screen. You can create up to seven additional VLANs by adding new VLAN names, and then assigning one or more ports to each VLAN. (The switch accepts a maximum of eight VLANs, including the default VLAN.) Note that each port can be assigned to only one VLAN. DEFAULT_VLAN *can be renamed, but not deleted*. Any ports not specifically assigned to another VLAN will remain assigned to DEFAULT_VLAN.

**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 the IPX and/or IP services for each VLAN. (Refer to pages 3-7 and 3-9.)

Spanning Tree protocol (STP), 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.

For more information on VLANs and how to configure them, refer to "Virtual LANs (VLANs)" on page 7-14.

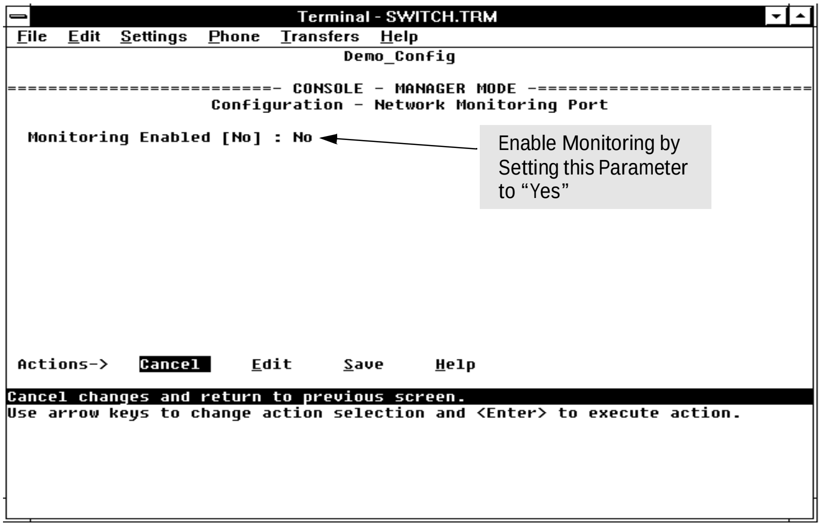
## Network Monitoring Port Features

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** If Automatic Broadcast Control (ABC) is configured and more than one port is being monitored, then broadcast packets may be duplicated on the monitor port.

**How To Configure for 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. Select `Network Monitoring Port` from the 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`.

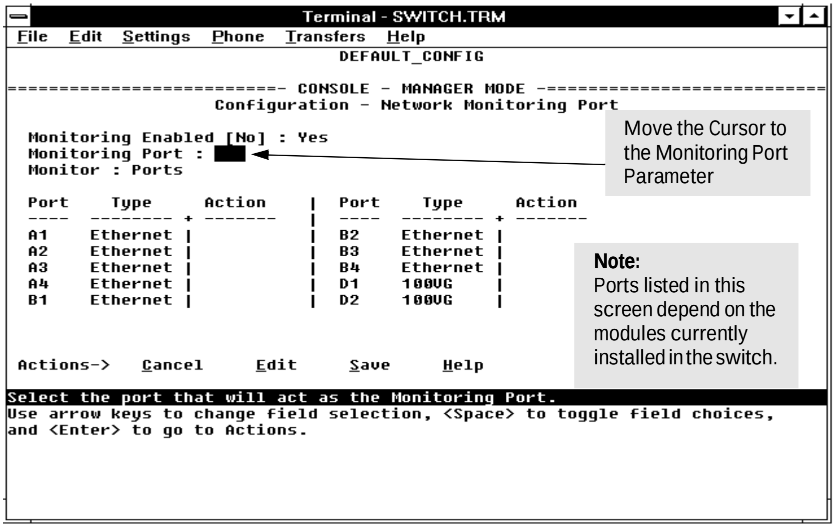


```
                              Demo_Config

==========================- CONSOLE - MANAGER MODE -==========================
                  Configuration - Network Monitoring Port

  Monitoring Enabled [No] : 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.
```

Enable Monitoring by Setting this Parameter to “Yes”

**Figure 3-13. The Default Network Monitoring Configuration Screen**

4. Press [↓] to display a screen similar to the following and move the cursor to the `Monitoring Port` parameter.



```
                              DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -===========================
                    Configuration - Network Monitoring Port

  Monitoring Enabled [No] : Yes
  Monitoring Port :
  Monitor : Ports

  Port    Type     Action    |  Port    Type     Action
  ----  -------- + -------   |  ----  -------- + -------
  A1    Ethernet |           |  B2    Ethernet |
  A2    Ethernet |           |  B3    Ethernet |
  A3    Ethernet |           |  B4    Ethernet |
  A4    Ethernet |           |  D1    100VG    |
  B1    Ethernet |           |  D2    100VG    |


 Actions->   Cancel     Edit     Save     Help

Select the port that will act as the Monitoring Port.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

Move the Cursor to the Monitoring Port Parameter

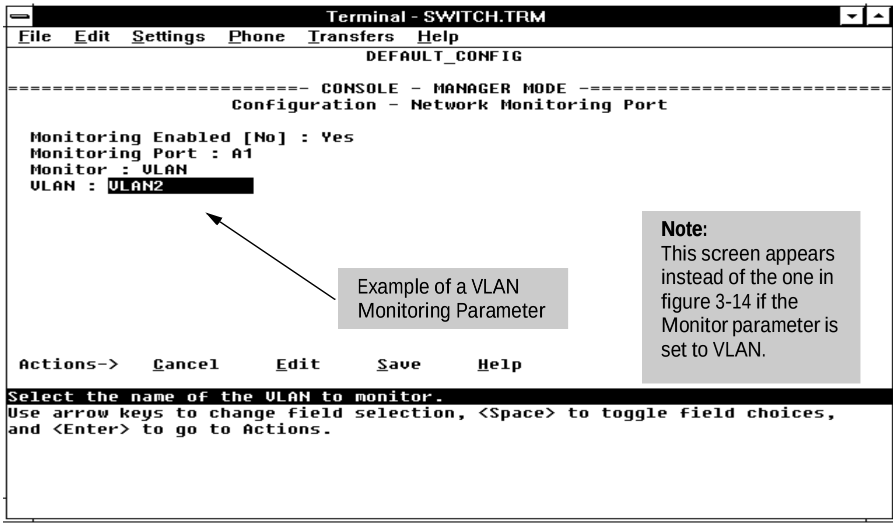
**Note:**
Ports listed in this screen depend on the modules currently installed in the switch.

**Figure 3-14. Example of Selecting a Monitoring Port**

5. Press 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 3-15). 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.



```
                         DEFAULT_CONFIG

========================== CONSOLE - MANAGER MODE ===========================
                 Configuration - Network Monitoring Port

  Monitoring Enabled [No] : Yes
  Monitoring Port : A1
  Monitor  : VLAN
  VLAN : VLAN2

 Actions->   Cancel     Edit     Save     Help

Select the name of the VLAN to monitor.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

Example of a VLAN Monitoring Parameter

**Note:**
This screen appears instead of the one in figure 3-14 if the Monitor parameter is set to VLAN.

**Figure 3-15. 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.

## Automatic Broadcast Control (ABC) Features—Layer 3 Switching

ABC reduces the amount of IP and/or IPX broadcast traffic on a network by enabling the switch to serve as a proxy for the ultimate destination of broadcast IP ARP and RIP packets, and 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 (multi-netting), can reduce or eliminate the need for routers within the VLAN.)

When enabled, ABC also allows you to set the broadcast limit parameter (`Bcast Limit`) in the Port Configuration screen (figure 3-5) for all ports on the switch (or all ports on the VLAN, if VLANs are configured and ABC is enabled for the VLAN).

In the factory default state, ABC is disabled. For more information on ABC and how to configure it, refer to “Automatic Broadcast Control (ABC)” on page 7-30.

# Monitoring and Analyzing Switch Operation from the Console

## Overview

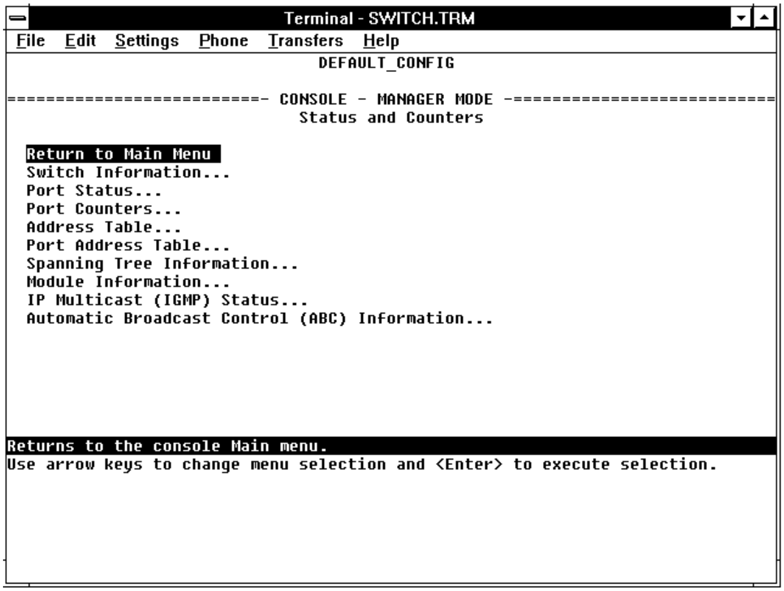
The Main Menu in the switch's console interface gives you access to the following sources of read-only data for helping you to monitor, analyze, and troubleshoot switch operation:

**Table 4-1. Read-Only Monitoring and Analyzing Features**

| Main Menu Item | Data Type | Purpose |
|---|---|---|
| Status and Counters Menus | Switch Information | Lists switch-level operating information. |
| | Port Status | Displays the operational status of each port. |
| | Port Counters | Summarizes port activity. |
| | Address (forwarding) Table | Lists the MAC addresses of nodes the switch has detected on the network, along with the corresponding switch port. |
| | Port Address Table | Lists the MAC addresses that the switch has learned from the selected port. |
| | Spanning Tree Information | Lists Spanning Tree data for the switch and for individual ports. If VLANs are configured, reports on a per-VLAN basis. |
| | Module Information | Lists the modules currently installed and detected by the switch. |
| | IP Multicast (IGMP) Status | Lists IGMP groups, report, query, and type of device access on ports. If VLANs are configured, reports on a per-VLAN basis. |
| | Automatic Broadcast Control (ABC) Information | If VLANs are configured, reports on a per-VLAN basis. |
| Event Log | | Lists event messages generated by the switch. |

# Status and Counters Menu

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



```
                                DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -===========================
                             Status and Counters

  Return to Main Menu
  Switch Information...
  Port Status...
  Port Counters...
  Address Table...
  Port Address Table...
  Spanning Tree Information...
  Module Information...
  IP Multicast (IGMP) Status...
  Automatic Broadcast Control (ABC) Information...




Returns to the console Main menu.
Use arrow keys to change menu selection and <Enter> to execute selection.
```

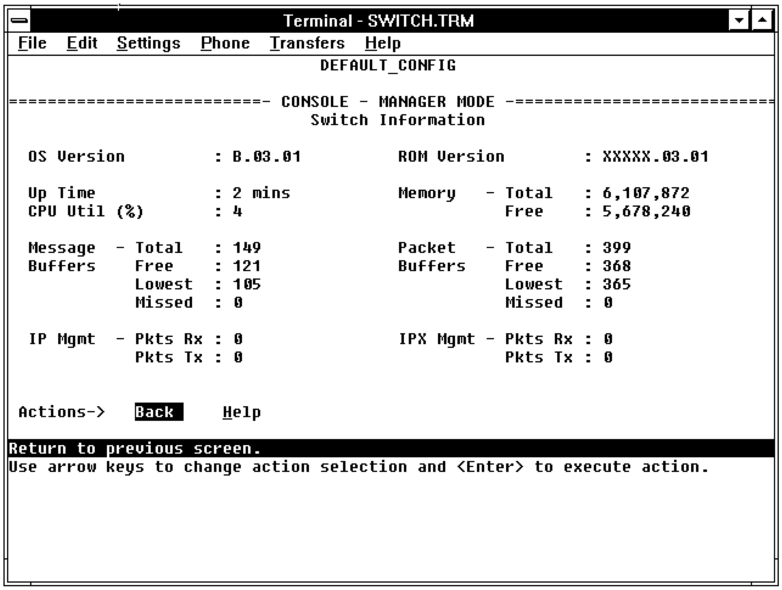
**Figure 4-1. The Status and Counters Menu**

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**

Spanning Tree, 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.

# Switch Information

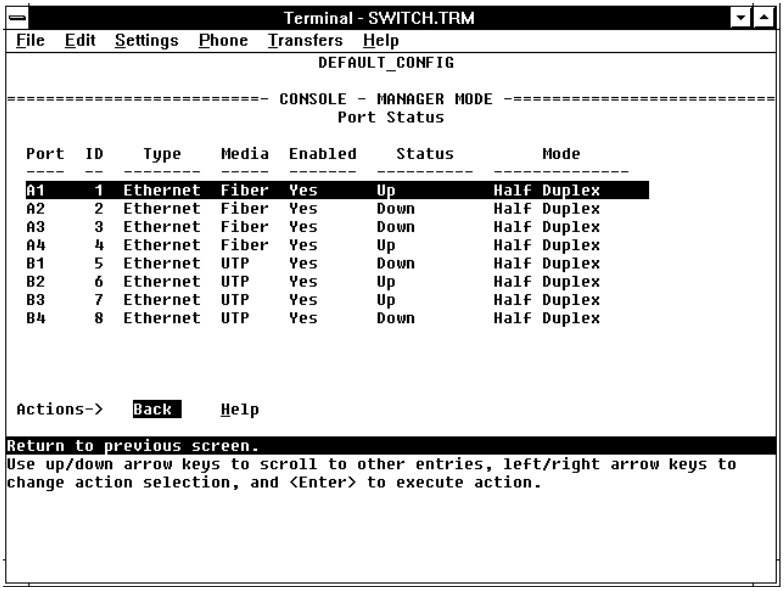


```
                              DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -==========================
                             Switch Information

  OS Version         : B.03.01          ROM Version        : XXXXX.03.01

  Up Time            : 2 mins           Memory   - Total   : 6,107,872
  CPU Util (%)       : 4                           Free    : 5,678,240

  Message  - Total   : 149              Packet   - Total   : 399
  Buffers    Free    : 121              Buffers    Free    : 368
             Lowest  : 105                         Lowest  : 365
             Missed  : 0                           Missed  : 0

  IP Mgmt  - Pkts Rx : 0                IPX Mgmt - Pkts Rx : 0
             Pkts Tx : 0                           Pkts Tx : 0


 Actions->   Back     Help

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

**Figure 4-2. Example of Switch Information**

This screen tells you which version of the OS (operating system) and ROM (low-level startup code located in read-only memory) the switch is using, and dynamically indicates how individual switch resources are being used.

# Port Status

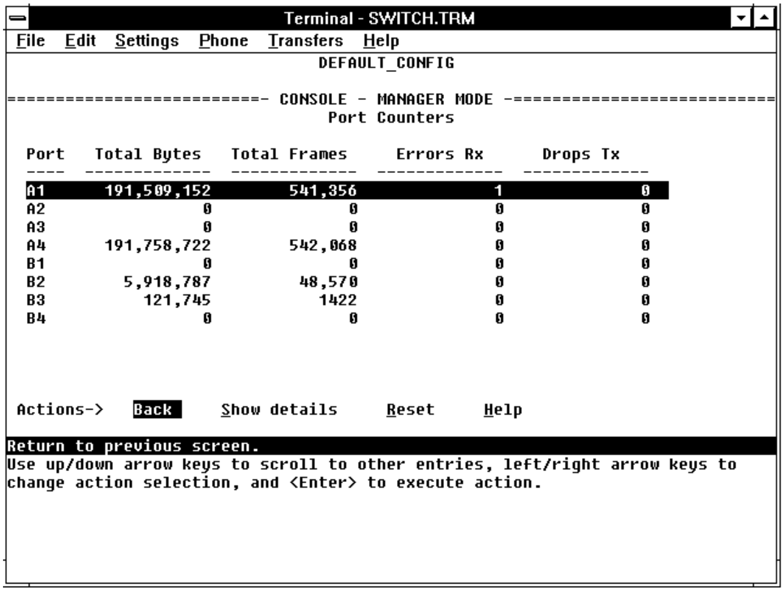


```
                                  DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -===========================
                                    Port Status

  Port  ID    Type    Media  Enabled    Status        Mode
  ----  --  --------  -----  -------  ----------  --------------
  A1     1  Ethernet  Fiber  Yes      Up          Half Duplex
  A2     2  Ethernet  Fiber  Yes      Down        Half Duplex
  A3     3  Ethernet  Fiber  Yes      Down        Half Duplex
  A4     4  Ethernet  Fiber  Yes      Up          Half Duplex
  B1     5  Ethernet  UTP    Yes      Down        Half Duplex
  B2     6  Ethernet  UTP    Yes      Up          Half Duplex
  B3     7  Ethernet  UTP    Yes      Up          Half Duplex
  B4     8  Ethernet  UTP    Yes      Down        Half Duplex



 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 4-3. Example of Port Status**

For each port, this screen tells you the type of port and media, whether the port is enabled and up or down, and the port's operating mode. (Included is the port ID number to use for SNMP MIB access.)

## Port Counters



```
                                DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -===========================
                                 Port Counters

  Port   Total Bytes   Total Frames     Errors Rx      Drops Tx
  ----  -------------  -------------  -------------  -------------
  A1      191,509,152        541,356              1              0
  A2                0              0              0              0
  A3                0              0              0              0
  A4      191,758,722        542,068              0              0
  B1                0              0              0              0
  B2        5,918,787         48,570              0              0
  B3          121,745           1422              0              0
  B4                0              0              0              0



 Actions->   Back     Show details     Reset     Help

Return to previous screen.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

**Figure 4-4. Example of Port Counters**

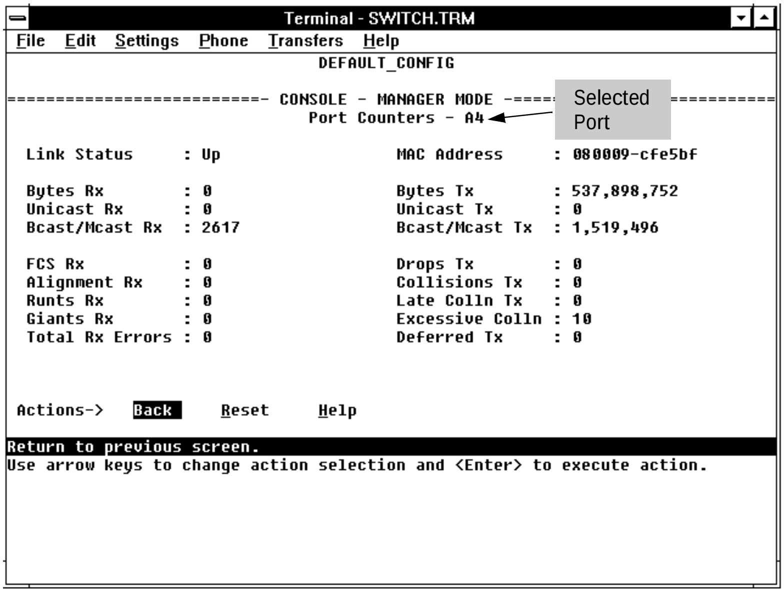
This screen enables you to determine the traffic patterns for each port. Port Counter features include:

- 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 ( `Show details` ).

**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.

To view the elements that comprise the traffic on a particular port, highlight that port number (figure 4-5), then select `Show details`. For example, selecting port A4 displays a screen similar to figure 4-5, below.

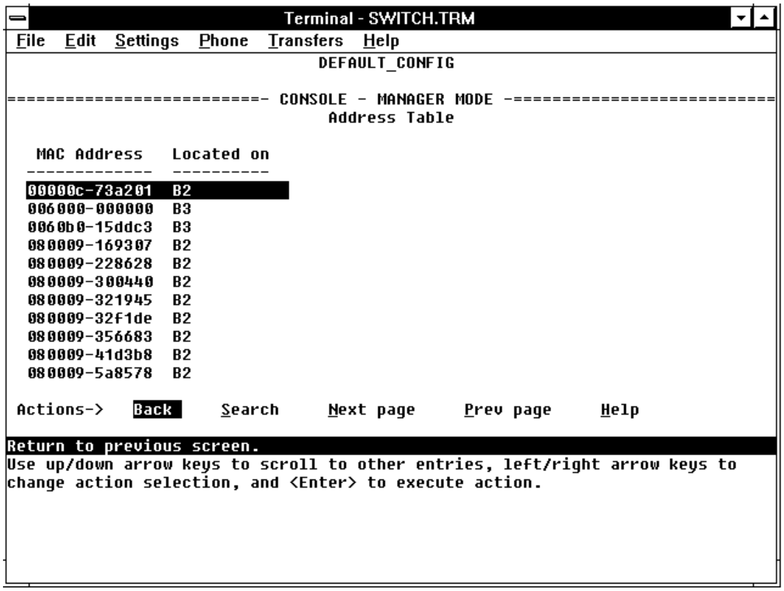


```
                              DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -=========================
                             Port Counters - A4

  Link Status     : Up                  MAC Address     : 080009-cfe5bf

  Bytes Rx        : 0                   Bytes Tx        : 537,898,752
  Unicast Rx      : 0                   Unicast Tx      : 0
  Bcast/Mcast Rx  : 2617                Bcast/Mcast Tx  : 1,519,496

  FCS Rx          : 0                   Drops Tx        : 0
  Alignment Rx    : 0                   Collisions Tx   : 0
  Runts Rx        : 0                   Late Colln Tx   : 0
  Giants Rx       : 0                   Excessive Colln : 10
  Total Rx Errors : 0                   Deferred Tx     : 0


 Actions->   Back     Reset     Help

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

**Figure 4-5. Example of the Display for Show details on a Selected Port**

This screen also includes the `Reset` action. Refer to the note on page 4-5.

# Address Table



```
                                 DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -===========================
                                  Address Table

   MAC Address   Located on
  -------------  ----------
  00000c-73a201  B2
  006000-000000  B3
  0060b0-15ddc3  B3
  080009-169307  B2
  080009-228628  B2
  080009-300440  B2
  080009-321945  B2
  080009-32f1de  B2
  080009-356683  B2
  080009-41d3b8  B2
  080009-5a8578  B2

 Actions->   Back     Search     Next page     Prev page     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 4-6. Example of the Address Table**

This screen lets you easily determine which switch port is being used to access 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

You can use the `Search` action at the bottom of the screen to locate a specific device (MAC address).

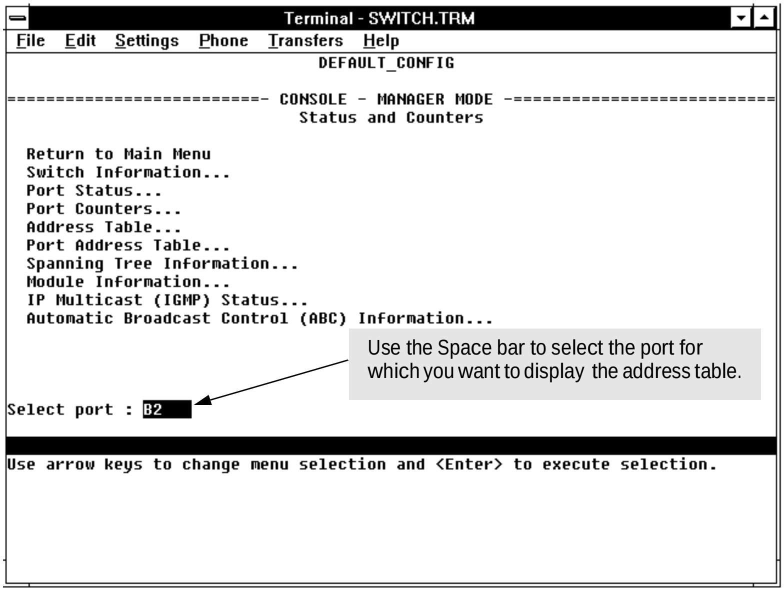
## Port Address Table

This screen lets you easily determine which devices are attached to the selected switch port by listing all of the MAC addresses detected on that port.

You can 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.



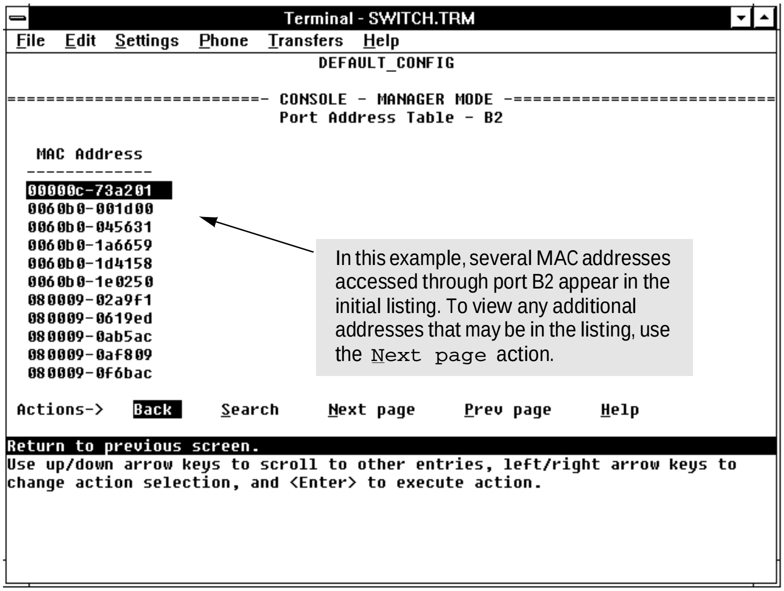
```
                                DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -===========================
                              Status and Counters

  Return to Main Menu
  Switch Information...
  Port Status...
  Port Counters...
  Address Table...
  Port Address Table...
  Spanning Tree Information...
  Module Information...
  IP Multicast (IGMP) Status...
  Automatic Broadcast Control (ABC) Information...


Select port : B2

Use arrow keys to change menu selection and <Enter> to execute selection.
```

Use the Space bar to select the port for which you want to display the address table.

**Figure 4-7. Example of How To Access the Port Address Table**

2. When the `Select Port` prompt appears, press the Space bar to display the port you want to examine, then press [Enter]. (See figure 4-7, above.)

   Each port is identified by its slot letter and sequential port number in the slot. For example, port A1 is the first port in slot A, while port D4 is the fourth port in slot D.



```
                              DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -==========================
                          Port Address Table - B2

   MAC Address
  -------------
  00000c-73a201
  0060b0-001d00
  0060b0-045631
  0060b0-1a6659
  0060b0-1d4158
  0060b0-1e0250
  080009-02a9f1
  080009-0619ed
  080009-0ab5ac
  080009-0af809
  080009-0f6bac

 Actions->  Back     Search     Next page     Prev page     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.
```

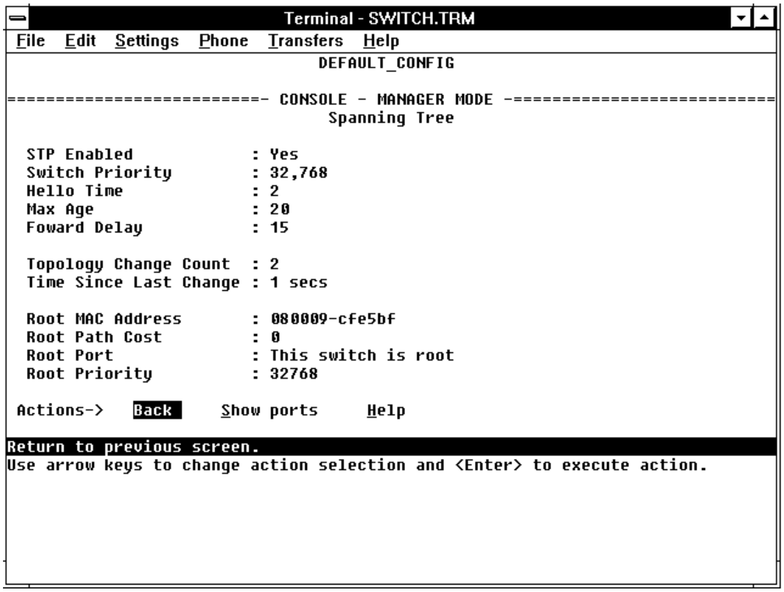
In this example, several MAC addresses accessed through port B2 appear in the initial listing. To view any additional addresses that may be in the listing, use the `Next page` action.

**Figure 4-8. Example of a Port Address Table for a Specific Port**

## Spanning Tree (STP) 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.

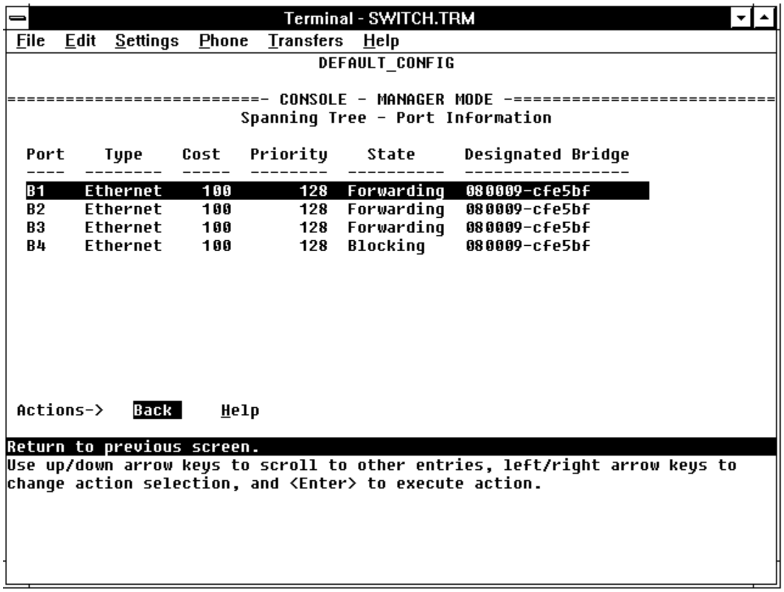


```
                         DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -==========================
                          Spanning Tree

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

  Topology Change Count  : 2
  Time Since Last Change : 1 secs

  Root MAC Address       : 080009-cfe5bf
  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 4-9. 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).



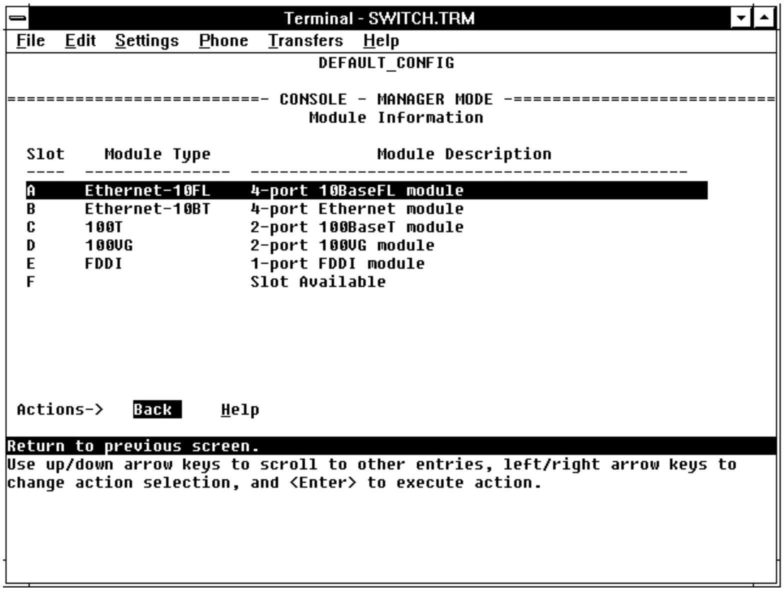
```
                          DEFAULT_CONFIG

=========================- CONSOLE - MANAGER MODE -==========================
                   Spanning Tree - Port Information

  Port    Type     Cost   Priority    State      Designated Bridge
  ----  --------  -----  --------  ----------  -----------------
  B1    Ethernet    100       128  Forwarding  080009-cfe5bf
  B2    Ethernet    100       128  Forwarding  080009-cfe5bf
  B3    Ethernet    100       128  Forwarding  080009-cfe5bf
  B4    Ethernet    100       128  Blocking    080009-cfe5bf




 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 4-10. 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 7-2.

## Module Information



```
                              DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -===========================
                             Module Information

  Slot    Module Type                Module Description
  ----  ---------------  ---------------------------------------------
  A     Ethernet-10FL    4-port 10BaseFL module
  B     Ethernet-10BT    4-port Ethernet module
  C     100T             2-port 100BaseT module
  D     100VG            2-port 100VG module
  E     FDDI             1-port FDDI module
  F                      Slot Available




 Actions->   Back    Help

Return to previous screen.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

**Figure 4-11. Example of Module Information**

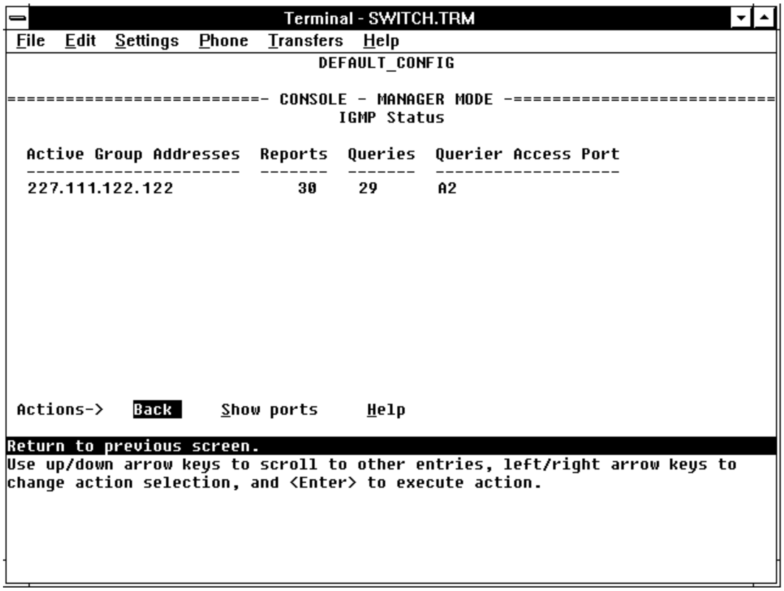
This screen tells you which type of module the switch detects in each slot.

## 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.

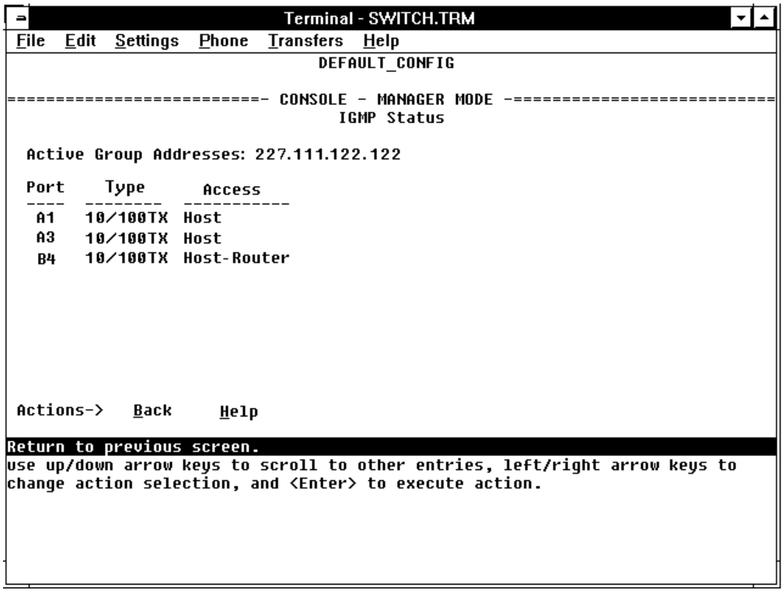
This screen identifies the active IP multicast groups the switch has detected, along with the number of report packets and query packets seen for each group. It also indicates which port is used for connecting to the querier.



```
                               DEFAULT_CONFIG

=========================- CONSOLE - MANAGER MODE -==========================
                                 IGMP Status

  Active Group Addresses  Reports  Queries  Querier Access Port
  ----------------------  -------  -------  -------------------
  227.111.122.122              30     29      A2







 Actions->   Back     Show ports     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 4-12. 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 227.111.122.122 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:



```
                                DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -===========================
                                  IGMP Status

  Active Group Addresses: 227.111.122.122

  Port    Type      Access
  ----  ---------  -----------
   A1   10/100TX  Host
   A3   10/100TX  Host
   B4   10/100TX  Host-Router




 Actions->   Back     Help

Return to previous screen.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

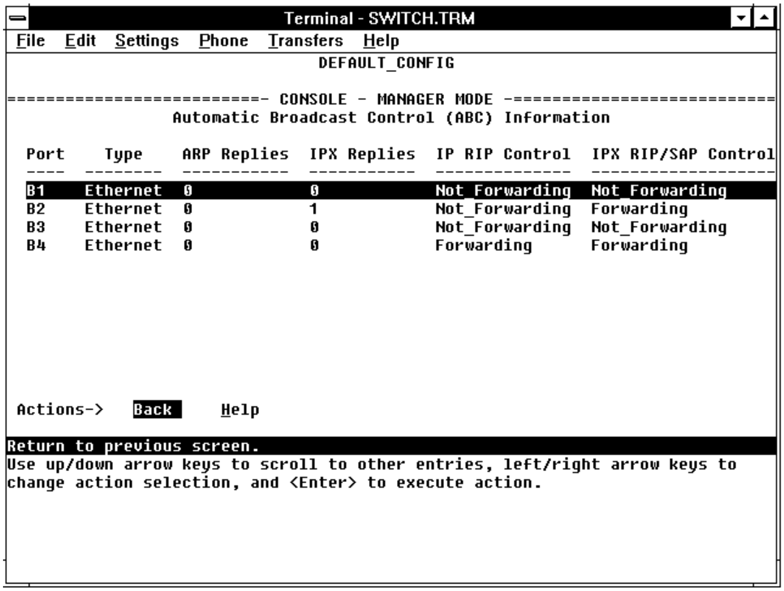
**Figure 4-13. Example of an IGMP Status Screen for a Selected Multicast Group**

## 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.

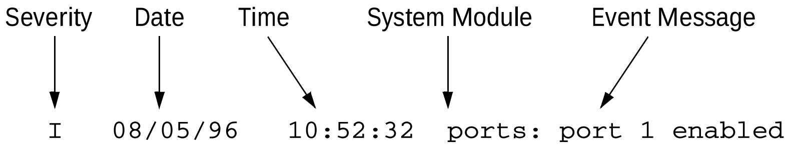


```
                                DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -==========================
                Automatic Broadcast Control (ABC) Information

  Port    Type     ARP Replies  IPX Replies  IP RIP Control   IPX RIP/SAP Control
  ----  --------   -----------  -----------  --------------   -------------------
  B1    Ethernet   0            0            Not_Forwarding   Not_Forwarding
  B2    Ethernet   0            1            Not_Forwarding   Forwarding
  B3    Ethernet   0            0            Not_Forwarding   Not_Forwarding
  B4    Ethernet   0            0            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 4-14. Example of Automatic Broadcast Control (ABC) Screen**

# Event Log

The Event Log records operating events as single-line entries listed in chronological order. Each entry is composed of five fields:



```
I   08/05/96   10:52:32  ports: port 1 enabled
```

***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.

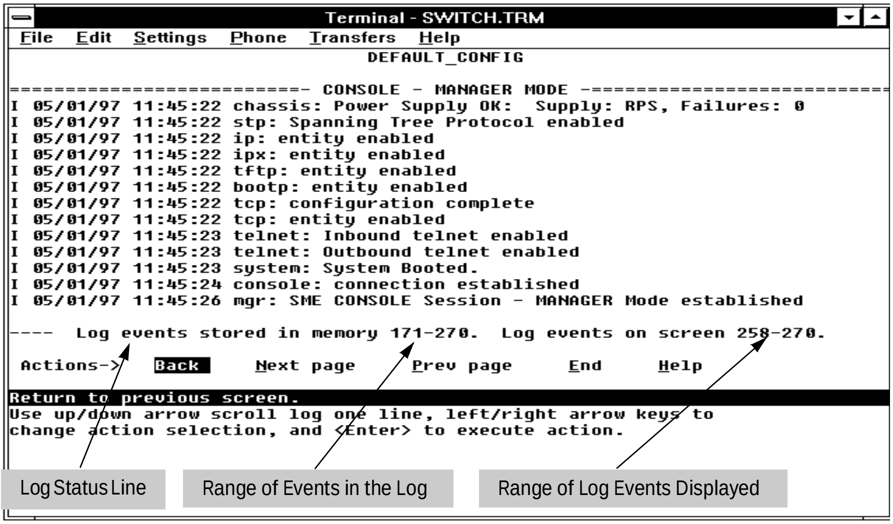
***Date*** is the date in *mm/dd/yy* format that the entry was placed in the log.

***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 Message*** is a brief description of the operating event.

**Entering and Navigating in the Event Log Display.** To enter the event log, select Event Log from the Main menu.



```
                              DEFAULT_CONFIG

=========================- CONSOLE - MANAGER MODE -===========================
I 05/01/97 11:45:22 chassis: Power Supply OK:  Supply: RPS, Failures: 0
I 05/01/97 11:45:22 stp: Spanning Tree Protocol enabled
I 05/01/97 11:45:22 ip: entity enabled
I 05/01/97 11:45:22 ipx: entity enabled
I 05/01/97 11:45:22 tftp: entity enabled
I 05/01/97 11:45:22 bootp: entity enabled
I 05/01/97 11:45:22 tcp: configuration complete
I 05/01/97 11:45:22 tcp: entity enabled
I 05/01/97 11:45:23 telnet: Inbound telnet enabled
I 05/01/97 11:45:23 telnet: Outbound telnet enabled
I 05/01/97 11:45:23 system: System Booted.
I 05/01/97 11:45:24 console: connection established
I 05/01/97 11:45:26 mgr: SME CONSOLE Session - MANAGER Mode established

----  Log events stored in memory 171-270.  Log events on screen 258-270.

 Actions->   Back     Next page     Prev page     End     Help

Return to previous screen.
Use up/down arrow scroll log one line, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

**Figure 4-15. 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 4-2. Event Log Control Keys**

| Key | Action |
|---|---|
| [N] | Advance the display by one page (next page). |
| [P] | Roll back the display by one page (previous page). |
| [↓] | Advance display by one event (down one line). |
| [↑] | Roll back display by one event (up one line). |
| [E] | Advance to the end of the log. |
| [H] | Display Help for the event log. |

The event log holds up to 100 lines in chronological order, from the oldest to the newest. Each line consists of one complete event message. Once the log has received 100 entries, it discards the current oldest line each time a new line is received. The event log window contains 20 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.)

# Using SNMP To Monitor and Manage the Switch

You can manage the switch via SNMP from a network management station. (The switch supports SNMP v1 and SNMP v2c, except as noted below for SNMP v2 Notifications.) If you are using IP, you must either configure the switch with the appropriate IP address or, if you are using Bootp to configure the switch, ensure that the Bootp process provides the IP address. (The IPX address is automatically configured.) 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

SNMP management features on the switch include:

- Security via configuration of SNMP communities
- Event reporting via SNMP traps and RMON (SNMP v2 Notifications are not supported at this time.)
- Managing the switch with a network management tool such as HP AdvanceStack Assistant
- Monitoring data normally associated with the SNMP agent ("Get" _operations). Supported *Standard* MIBs include:
  - Bridge MIB (RFC 1493)
  - Etherlike MIB (RFC 1650)
  - Ethernet MAU MIB (RFC 1515)
  - Interfaces Evolution MIB (RFC 1573)
  - Novell Standard IPX MIB (ipx.mib)
  - RMON MIB (RFC 1757)—etherstats, events, alarms, and history
  - SNMP MIB-II (RFC 1213)

*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)
- 802.12 (100VG) information (vg.mib)
- Integrated Communications Facility Authentication Manager and SNMP communities (icf.mib)
- HP AdvanceStack Switch 2000 configuration (config.mib)
- HP VLAN configuration information (vlan.mib) supporting hpVlanGeneralGroup
- HP EASE MIB version 4 to allow EASE sampling
- HP Linktest MIB for basic device management (linktest.mib)
- HP ICF Linktest MIB for link test features (icfbasic.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 compact disk (CD) shipped with the switch, or from following World Wide Web site:

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

For more information, refer to the card at the front of this manual.

# SNMP Configuration Process

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

1. From the Main menu, select `Configuration`.
2. Enable and configure an IP address for the switch, including any necessary gateways. An IPX address is automatically configured. (For more on configuring IPX and IP, refer to page 3-7 and page 3-9.)
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 page 3-11.)
4. Configure the appropriate trap receivers. (For more on configuring trap receivers, refer to page 3-13.)

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 10 IP and/or IPX addresses of such nodes into the Manager Address field. *Configuring one or more IP or IPX 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 2-10.)

# Using the Advanced Commands

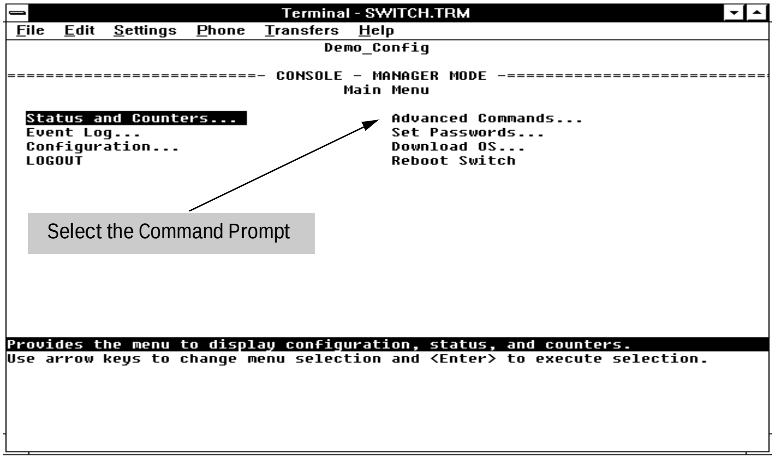
## Overview

The Advanced Commands , which are accessed from the Main Menu, gives you access to the following system management commands:

- Help
- Date
- Time
- History
- Ping
- IpxPing
- LinkTest
- Telnet
- VLAN
- ClearLED
- Config
- Delete
- GetMIB
- SetMIB
- WalkMIB
- Exit
- Get/Put (TFTP)
- ZGet/ZPut (ZMODEM)
- Version
- Log
- !
- Repeat
- Page
- Print
- Redo

### How To Use the Command Prompt:

1. To access the command prompt, use the arrow keys to highlight Advanced Commands in the Main Menu and press Enter.



```
                          Demo_Config

=========================== CONSOLE - MANAGER MODE ============================
                             Main Menu

  Status and Counters...                    Advanced Commands...
  Event Log...                              Set Passwords...
  Configuration...                          Download OS...
  LOGOUT                                    Reboot Switch

Provides the menu to display configuration, status, and counters.
Use arrow keys to change menu selection and <Enter> to execute selection.
```

Select the Command Prompt

**Figure 6-1. Selecting the Command Prompt**

2. Do the following:
   - If there are no VLANs (virtual LANs) configured, go to step 3.
   - If VLANs are configured, the prompt displays the name of the default, or first VLAN, then asks you to select the VLAN in which to operate. Use the Space bar to select the VLAN in which you want to operate, then press Enter.

3. The command prompt appears near the bottom of the screen. The text in the prompt matches the System Name parameter. (If there are multiple VLANs configured, then the text in the prompt matches the name of the VLAN in which the command prompt is operating.) For example, in the factory default configuration (no system name or VLANs configured), the command prompt looks like this:

```
DEFAULT_CONFIG:
```

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

```
DEFAULT_CONFIG: time 9:55 Enter
```

### How To Exit from the command prompt:

Type `exit` and press Enter to return to the Main Menu.

### How To List Available Commands:

At the command prompt, type h and press Enter.

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.

**How To Stop the Help Listing:** Press Q.

# Commands

To execute any of these commands, select Advanced Commands from the Main Menu, type the command, and press [Enter].

## Conventions:

- Commands are shown in the normal typeface.
- Required parameters are shown in italics.
- Optional parameters are shown in italics, with brackets ( *[…]* ).

  For example:

| Command | Required Parameters | Optional Parameters |
|---|---|---|
| ping | *ip-addr* | *[repetitions] [timeout]* |

| Command Syntax | Description |
|---|---|
| H (help) | Lists the commands available at the command prompt. |
| date *[mm/dd/yy]* | Without parameters, displays the date and time currently held by the switch. With parameters in the month/date/year format, resets the date. |
| time *[hh:mm:ss]* | Without parameters, displays the date and time currently held by the switch. With parameters in the hours:minutes:seconds format, resets the time. |
| history | displays the times and reasons for the last four occasions on which the switch was rebooted or restarted. |
| ping *ip-addr [repetitions] [timeout]*<br>where:<br>*ip-addr* is the IP address of the target node in dotted decimal notation.<br>*repetitions* is the number of times to repeat the echo request. Default: send packet once.<br>*timeout* is how many seconds to wait for a response. Default: 5 seconds. | Sends an Internet Control Message Protocol (ICMP) echo request message to a specific IP address, as a network-layer test of the reachability of the node. Ping does not support loopback (pinging this switch) or broadcast addresses. The switch must have IP configured. After transmitting the request message to the node, the switch waits for a response. If it is received within the specified or default timeout interval, the console displays a message indicating that the target is “alive”. If an echo response is not received within the specified or default timeout interval, the console displays a message indicating that the target did not respond.<br>**VLANs:** If multiple VLANs are configured, the Ping command sends requests to the ports in the VLAN environment specified when the command prompt was selected. |

| Command Syntax | Description |
|---|---|
| ipxping *ipx-addr [repetitions] [timeout] [size]*<br>where:<br>*ipx-addr* is the IPX address of the target node in this format:<br>*network number :mac address*<br>*repetitions* is the number of times to repeat the echo request.<br>Default: send packet once.<br>*timeout* is how many seconds to wait for a response.<br>Default: 5 seconds.<br>*size* is the size in bytes of the data to be sent.<br>Default: 40 bytes. | Sends an IPX echo request message to a specific IPX address, as a network-layer test of the reachability of the node. The switch must have IPX enabled. After transmitting the request message to the node, the switch waits for a response. If it is received within the specified or default timeout interval, the console displays a message indicating that the target is "alive". If an echo response is not received within the specified or default timeout interval, the console displays a message indicating that the target did not respond.<br>**VLANs:** If multiple VLANs are configured, ipxping sends requests to the ports in the VLAN environment specified when the command prompt was selected. |
| linktest *mac_addr [count] [delay]*<br>where:<br>*mac_addr* is the MAC address of the target node in 12-character hexadecimal format.<br>*count* is the number of test packets to send.<br>Default: 1 packet<br>*delay* is how many seconds to wait for a response to each packet.<br>Default: 2 seconds. | Verifies communication to a MAC address on the LAN. Sends an 802.2 Test Packet to a specific target node on a network in the VLAN environment specified in the command prompt. The target node must be able to respond to an 802.2 Test Packet with an 802.2 Test Response packet in order for the test to work. (HP managed hubs, bridges, routers, and switches automatically respond to 802.2 Test Packets. Most HP LAN adapters can be configured to operate as a responder.<br>**VLANs:** If multiple VLANs are configured, the linktest command sends requests to the nodes in the VLAN environment specified when the command prompt was selected. |
| telnet *ip-addr*<br>*where:*<br>*ip-addr is the IP address of the target node in dotted decimal notation.* | Used to establish a Transmission Control Protocol (TCP) virtual terminal connection to a remote node, allowing you to interact with the remote node's interface. IP must be configured, and the remote node must have Telnet service enabled. The Switch 2000 supports one inbound and one outbound Telnet session. In the factory default configuration, the `Inbound Telnet Enabled` parameter is set to `Yes`. (To change the Inbound Telnet Enabled parameter, use the Console configuration screen, which is accessed from the Configuration screen selected from the Main menu.) Outbound Telnet is always enabled. To exit from an inbound Telnet session, select `LOGOUT` from the Main menu and answer the confirmation prompt by typing y. To exit from an HP router, another Switch 2000, or a UNIX login, press Ctrl D. To force a disconnection from any device, use Ctrl R. To interrupt command processing without halting an outbound Telnet session, use Ctrl C. |

| Command Syntax | Description |
|---|---|
| vlan *vlan_name*<br>where:<br>*vlan_name* is the name of the virtual LAN you want to access. | Used where VLANs are configured. Used to select a different VLAN environment in which to execute Command Prompt commands. The command prompt will change to show the VLAN name specified by the *vlan_name* parameter. |
| clearled | Turns off the Security LED on the front panel of the Switch 2000. |
| config | Displays the configuration currently saved in flash memory. When — `MORE` — is displayed, pressing [Enter] displays the next line of the configuration, and pressing the Space bar displays the next screen of the configuration. To halt a config listing and return to the command line prompt, press [Q]. |
| delete | Deletes the configuration file currently in use, returns the switch to its factory default configuration, and reboots the switch. |
| getmib *objectname.index*<br>where:<br>*objectname* identifies the MIB object by name or number format.<br>*index* identifies the instance of each object name. | Retrieves the value of an individual MIB object in the switch.<br>Example: The following command returns the enable/disable status for a port having a port ID of 1. (For an example of port ID numbering, see the example of the Port Status screen on page 4-4.)<br>getmib ifAdminStatus.1 |
| setmib *objectname.index type value*<br>where:<br>*objectname* identifies the MIB object by name or number format.<br>*index* identifies the instance of each object name.<br>*type*<br>value identifies the numeric value for the MIB object. | Sets a MIB object to a specific value. Valid types are:<br>-i (integer) -g (gauge)<br>-o (octet) -t (time_ticks)<br>-d (object identifier) -u (unsigned integer 32)<br>-a (ip_addr) -D (Display String)<br>-c (counter) -N (NULL)<br>Example: This command sets port 1 to disabled status.<br>setmib ifAdminStatus.1 -i 2 |

| **Command Syntax** | **Description** |
|---|---|
| walkmib *objectname* | Retrieves the MIB subtree for the specified MIB object. When — `MORE` — is displayed, pressing [Enter] displays the next line of the configuration, and pressing the Space bar displays the next screen of the configuration. To halt a walkmib listing and return to the command line prompt, press [Q].<br>Examples:<br>walkmib ifSpeed displays the speed for each port installed in the switch.<br>walkmib ifPhysAddress displays the MAC address of each port installed in the switch. |
| exit | Returns you to the Main Menu. |
| get *ip-addr* config *filename*<br>get *ipx-addr* config *filename*<br>where:<br>*ip_addr* or *ipx-addr* is the IP or IPX address of the file server.<br>*filename* is the directory path and name of the file containing the configuration. | Uses TFTP to transfer a configuration from a TFTP server on an attached network. The switch must have IP or IPX configured, and the configuration must have been previously transferred from a switch to the file server. TFTP must be enabled on the server.<br>Progress of the transfer, plus successful or unsuccessful completion of the transfer are indicated in the Event Log.<br>**Note:** After transferring a configuration to the switch, the switch automatically reboots to invoke the new configuration. |
| put *ip-addr object filename*<br>put *ipx-addr object filename*<br>where:<br>*ip_addr* or *ipx-addr* is the IP or IPX address of the remote host.<br>*object* is config, crashrec, or a command that generates an output that can be stored in a file.<br>*filename* is the directory path and name of the configuration file on the remote host. | Uses TFTP to transfer a configuration, a "crash record", or the output of a command from the switch to a file on a remote host. The switch must have IP or IPX configured. TFTP must be enabled on the remote host. The target file on the remote host must also exist and have write permissions. A command used as an *object* must have an output that can be stored in a file.<br>Progress of the transfer, plus successful or unsuccessful completion of the transfer are indicated in the Event Log.<br>**Note:** When the switch reboots itself due to an internal error, a "crash record" (crashrec) is generated. This is a binary file holding internal data needed to troubleshoot the cause of the internal error. |
| zget CONFIG *[remote-file] [dos/unix]*<br>where:<br>*remote-file* is a file name on the console PC.<br>*dos* = 0 (specifies DOS format)<br>*unix* = 1 (specifies unix format) | Copies a switch configuration from a file on the console PC to the switch. The PC must be emulating a VT100 or ANSI terminal. Also, the PC must be running a Zmodem-compatible terminal emulation program such as PROCOMM PLUS. |

| **Command Syntax** | **Description** |
|---|---|
| zput *file remote-file overwrite dos/unix*<br>where:<br>*file* is CONFIG or a command.<br>*remote-file* is a file name on the console PC.<br>*overwrite* is:<br>0 (don’t overwrite a file of the same name).<br>1 (create or overwrite a file of the same name).<br>*dos* = 0 (specifies DOS format)<br>*unix* = 1 (specifies unix format) | Copies a switch configuration from the switch to the console PC. The PC must be emulating a VT100 or ANSI terminal. Also, the PC must be running a Zmodem-compatible terminal emulation program such as PROCOMM PLUS. |
| Version | Displays the version of operating system (OS) software currently running in the switch. If an FDDI Module is installed, also displays the current version of the FDDI Module OS. |
| log *[-a]* ‘*[keywrd]* | Displays the event log.<br>(Press the Space bar when prompted by the `-- MORE --` message.)<br>Examples:<br>log Displays100 lines of the current event log, since the last reboot.<br>log -a Displays the entire event log.<br>log -a ‘telnet Displays all event log lines containing the keyword “telnet”<br>log ‘telnet Displays any event log lines, since the last reboot, of the current log that contain the keyword “telnet”. |
| ! *[repetitions]* | Repeat the last command.<br>Examples:<br>! Repeats the last command once.<br>! 3 Repeats the last command three times. |
| Repeat | Continuously repeats the last command until a key is pressed on the console. |
| Page | Toggles paging mode for display commands. |
| Print | Send the output of a Command Prompt command to a printer or to a file. |
| Redo [?] / [number] / [string] | Display or redo a command from the command history.<br>Examples:<br>Redo Re-executes the most recent command.<br>Redo ? Causes the last ten commands to be listed.<br>Redo *n* Re-executes the previous *n*th command (1-10).<br>Redo *string* Re-executes a previous command that begins with the text *string*. |

7

# Advanced Concepts

## Overview

The switch provides support for these advanced features:

- Spanning Tree Protocol—STP (page 7-2)
- Port trunking (page 7-5)
- Filtering for enhanced bandwidth usage and in-band security (page 7-8)
- Virtual LANs—VLANs (page 7-14)
- IP Multicast—IGMP (page 7-23)
- Automatic Broadcast Control—ABC (page 7-30)

# Spanning Tree Protocol (STP)

The switch uses the IEEE 802.1d Spanning Tree Protocol (STP) to ensure that only one path at a time is active between any two nodes on the network. 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. 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**

The default STP setting in the Switch 2000 is “Off”. If you are using the switch to provide redundant links, you should reconfigure the Spanning Tree Protocol to “On”.  Also, when multiple VLANs are configured, you must enable STP separately for each VLAN in which you want spanning tree to operate.

While allowing only one active path through a network at any time, STP retains any redundant physical path to serve as a backup (blocked) path in case the existing active path fails. Thus, if a 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

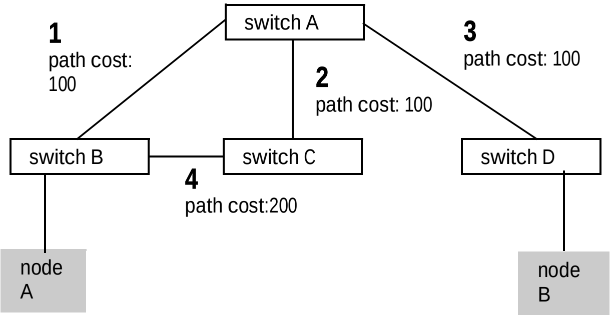


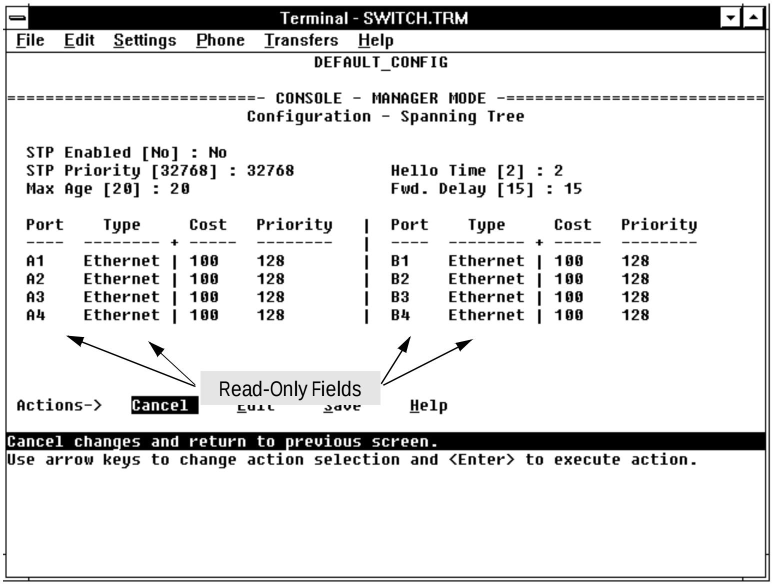
**Figure 7-1. Example of Logical and Redundant Paths Between Two Nodes**

**How To Configure Spanning Tree:** 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 (step 5), 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.

1. From the Main menu, select `Configuration`.
2. In the Configuration screen, select `Spanning Tree` .
3. If multiple VLANs are configured, select the VLAN in which you want to configure STP. If multiple VLANs are not configured, skip this step.
4. Select Edit to highlight the `STP Enabled` parameter.
5. Press the Space bar to select `Yes` . (This enables STP.)



```
                              DEFAULT_CONFIG

=========================- CONSOLE - MANAGER MODE -===========================
                     Configuration - Spanning Tree

  STP Enabled [No] : No
  STP Priority [32768] : 32768          Hello Time [2] : 2
  Max Age [20] : 20                     Fwd. Delay [15] : 15

  Port    Type     Cost    Priority   |  Port    Type     Cost    Priority
  ----  -------- + -----   --------   |  ----  -------- + -----   --------
  A1    Ethernet | 100     128        |  B1    Ethernet | 100     128
  A2    Ethernet | 100     128        |  B2    Ethernet | 100     128
  A3    Ethernet | 100     128        |  B3    Ethernet | 100     128
  A4    Ethernet | 100     128        |  B4    Ethernet | 100     128



 Actions->   Cancel      Edit      Save       Help

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

Read-Only Fields

**Figure 7-2. Example of the STP Configuration Screen with Ethernet Modules Installed in the Switch**

6. If the remaining STP parameter settings are adequate for your network, go to step 9.
7. 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.)
8. Repeat step 7 for each additional parameter you want to change.
9. When you are finished editing parameters, press Enter to return to the `Actions` line.
10. Press S to save the currently displayed STP parameter settings and return to the Configuration menu.
11. When you are finished configuring the switch, return to the Main Menu.

# Port Trunking

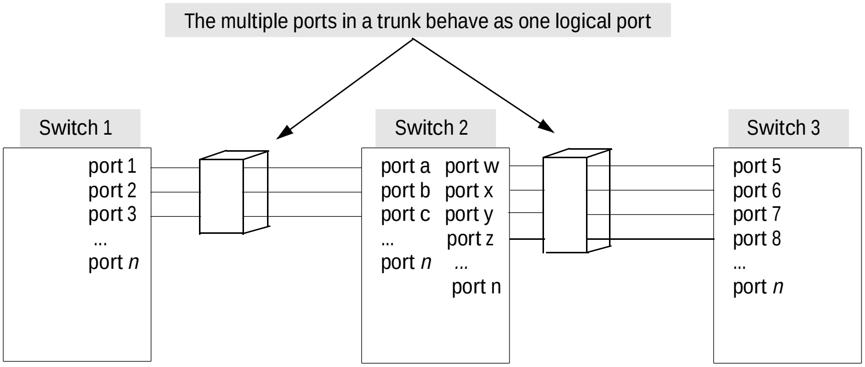


**Figure 7-3. Conceptual Illustration of Port Trunking**

Port trunking is used to allow up to four ports to be connected together to function as a single, higher-speed port to connect to another Hewlett-Packard switch designed for port trunking. This enables speeds of up to 400 Mbit/s in a 100Base-T or 100VG trunk, 200 Mbit/s in an FDDI trunk, and up to 40 Mbit/s in a 10Base-T or 10Base-FL trunk. (The one-port FDDI Module is a "high power" module. The switch supports up to two such modules. Refer to the manual provided with the FDDI Module.) On the B-version of the Switch 2000 (J3100B) and on the Switch 800T, you can implement up to six port trunks in a switch, which enables the switch to function as a high-speed backbone. (The A-version of the Switch 2000—J3100A—allows only one port trunk, but can be trunked to other Hewlett-Packard switches that support port trunking.)

Traffic distribution over the trunk ports is determined when packets arrive with new source MAC addresses. Each new address is assigned to a trunk port in a sequential way that distributes the source addresses evenly over the trunk.

The switch sends broadcast, multicast, and flooded traffic over only one port within the trunk in order to prevent a broadcast loop. (The switch automatically determines which port to use.)

**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.

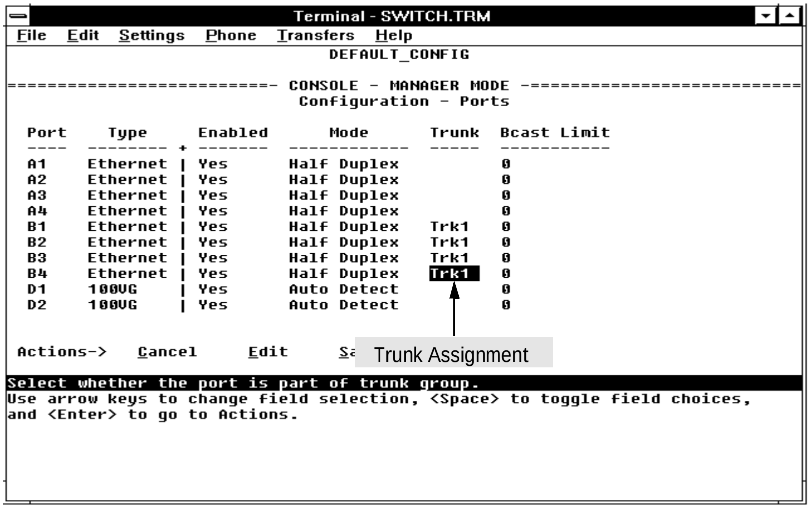
A configured trunk appears as a single port (labeled `Trk1, Trk2...Trk6`) on other configuration screens, such as the Spanning Tree and Port VLAN Assignment screens. Also, when assigning a port trunk to a VLAN, all ports in that trunk must be assigned to that same VLAN.

When trunks are used in conjunction with filters and port monitoring, if a port is removed from the trunk, the filters and port monitoring for that port are returned to their default configuration settings.

**How To Configure the Port Trunk:** Use the Port Configuration screen to configure trunks.

1. From the Main menu, select `Configuration`.
2. In the Configuration menu, select `Ports`.
3. To assign a port to the trunk:
   a. Select `Edit`.
   b. Move the cursor to the Trunk column.
   c. Select the row for a port you want in the trunk.
   d. Press the Space bar to select the trunk you want. (To remove a port from a trunk, repeat the space bar until the trunk assignment is `blank`.)

   For example, in the following screen, ports B1, B2, B3, and B4 have been assigned to trunk Trk1:



```
                               DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -===========================
                            Configuration - Ports

  Port    Type      Enabled      Mode       Trunk  Bcast Limit
  ----  --------- + -------  ------------  -----  -----------
  A1    Ethernet  | Yes      Half Duplex          0
  A2    Ethernet  | Yes      Half Duplex          0
  A3    Ethernet  | Yes      Half Duplex          0
  A4    Ethernet  | Yes      Half Duplex          0
  B1    Ethernet  | Yes      Half Duplex   Trk1   0
  B2    Ethernet  | Yes      Half Duplex   Trk1   0
  B3    Ethernet  | Yes      Half Duplex   Trk1   0
  B4    Ethernet  | Yes      Half Duplex   Trk1   0
  D1    100VG     | Yes      Auto Detect          0
  D2    100VG     | Yes      Auto Detect          0


 Actions->   Cancel     Edit     Sa

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

Trunk Assignment

**Figure 7-4. Example of Configuring a Port Trunk**

4. To assign another port to the trunk, repeat steps 3c, and 3d.

5. When you are finished assigning ports to the trunk, press [Enter], then [S] (for Save) to save the new port trunk configuration and return to the Configuration menu.

6. When you are finished configuring the switch, return to the Main Menu.

**To Remove a Port from the Trunk:** In step 3c, above, select the port you want to remove from the trunk. In step 3d, continue pressing the Space bar until the trunk assignment is blank.

# Filters and Security

To enhance the switch's bandwidth usage and in-band security, configure per-port filters to forward desired traffic or drop unwanted traffic, as described below. The switch can support up to 50 filters.

**Table 7-1. Filter Types and Criteria**

| 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. |
| Source MAC | Traffic from a specified source MAC address and coming through a particular source port will be forwarded or dropped on a per-port (destination) basis within the same VLAN. |

**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.

**Note**

IP multicast addresses occur in the range from 224.0.0.0 through 239.255.255.255. When IGMP is enabled, any Traffic/Security filters configured with a "Multicast" filter type and a "Multicast Address" within the above range are disabled and an event log message indicating this action is logged . That is, IGMP will control the IP multicast traffic flow and the Traffic/Security filter will control any multicast traffic that is not IP multicast. (Multicast addresses are entered in the "Traffic/Security Filters" screen as Ethernet addresses in the range of 01005e-000000 through 01995e-7fffff.)

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 (Ethernet)
- IP (802.3 SAP)
- ARP
- DEC LAT
- AppleTalk
- SNA
- NetBIOS
- IPX (Ethernet)
- IPX (802.3 SAP)
- VINES IP
- VINES Echo

**Note** The switch provides filtering only for Ethernet and 802.3 format packets.

**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.

**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.

**Source MAC Filters.** This filter type enables the switch to specify the port through which a node having a specified (source) MAC address can send traffic. Only ports that are selected are allowed to send and receive traffic for the specified node. For additional security, if traffic from the source MAC address appears on any port other than the selected one, the traffic from that source will be dropped and the Security LED on the front of the switch begins flashing. (To clear the Security LED, use the Advanced Command `ClearLED` command.)

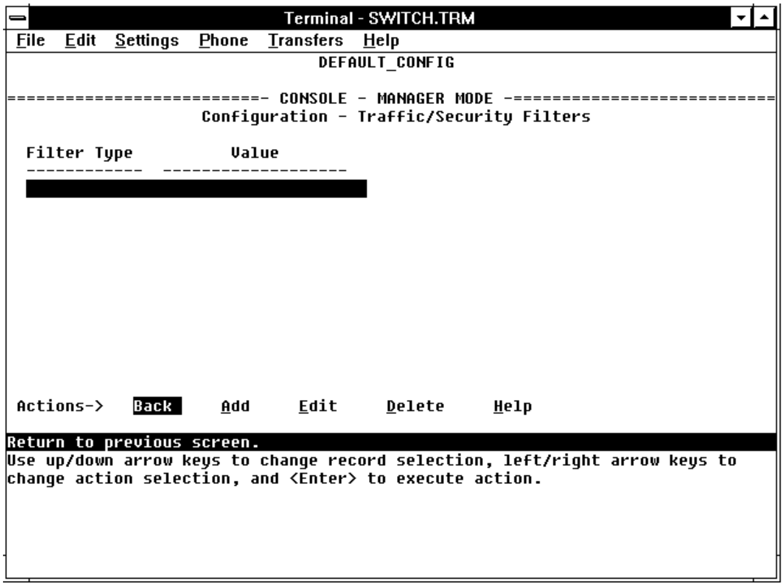
**Note**

If a node designated by the Source MAC parameter is moved to a different port than its original source port, any traffic to or from that node will not be forwarded by the switch. Forwarding will resume if the node is moved back to the original source port.

Traffic between ports *not* designated as a “Source Port” is not affected by the filter.

**How To Configure Traffic/Security Filters:** 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. You can create up to fifty filters.

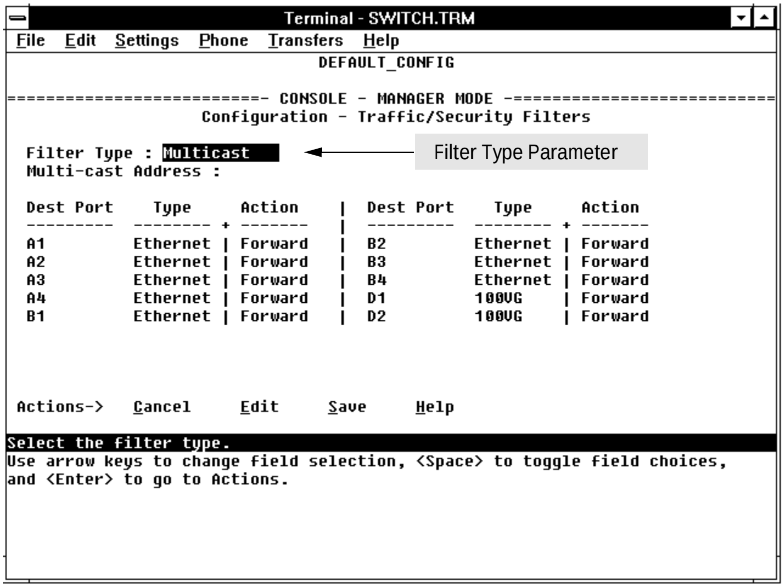
1. From the Main menu, select `Configuration`.
2. In the Configuration menu, select `Traffic/Security Filters` to display the following screen.



```
                               DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -===========================
                  Configuration - Traffic/Security Filters

  Filter Type          Value
  ------------   --------------------



 Actions->   Back     Add     Edit     Delete     Help

Return to previous screen.
Use up/down arrow keys to change record selection, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

Figure 7-5. The Traffic/Security Filters List Screen (Default Values)

3. In the Actions line, press [A] (for `Add`) to display the Traffic/Security Filters Configuration screen shown in figure 7-6.



```
                                DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -===========================
                    Configuration - Traffic/Security Filters

  Filter Type : Multicast
  Multi-cast Address :

  Dest Port    Type     Action    |  Dest Port    Type     Action
  ---------  -------- + -------   |  ---------  -------- + -------
  A1         Ethernet | Forward   |  B2         Ethernet | Forward
  A2         Ethernet | Forward   |  B3         Ethernet | Forward
  A3         Ethernet | Forward   |  B4         Ethernet | Forward
  A4         Ethernet | Forward   |  D1         100VG    | Forward
  B1         Ethernet | Forward   |  D2         100VG    | Forward



 Actions->   Cancel     Edit     Save     Help

Select the filter type.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

Filter Type Parameter

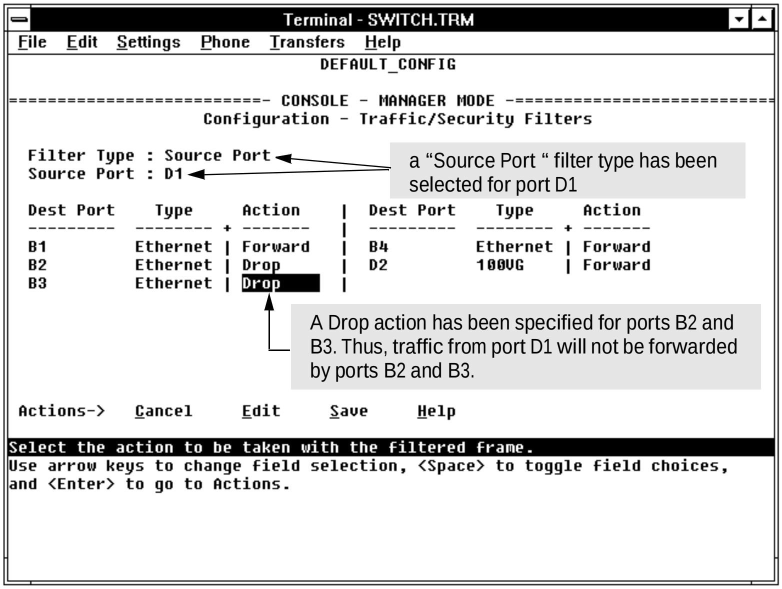
**Figure 7-6. Example of the Traffic/Security Filters Configuration Screen**

4. Press the Space bar to select the type of filter you want to configure. The options are:
   - Multicast (the default)
   - Protocol
   - Source Port
   - Source MAC

5. Press ↓ once to highlight the next line. Depending on the type of filter you selected in step 4, select one of the options listed in the following table:

| **Filter Type Option Selected in Step 4** | **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. |
| Source MAC | Source Port and Source MAC (address) | a. Use the Space bar to select the source port.<br>b. Press → to highlight the Source MAC parameter.<br>c. Type the MAC address of the source device whose packets you want to filter. |

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



```
                              DEFAULT_CONFIG

=========================- CONSOLE - MANAGER MODE -==========================
                  Configuration - Traffic/Security Filters

  Filter Type : Source Port
  Source Port : D1

  Dest Port    Type     Action     |  Dest Port    Type     Action
  ---------  -------- + -------    |  ---------  -------- + -------
  B1         Ethernet | Forward    |  B4         Ethernet | Forward
  B2         Ethernet | Drop       |  D2         100VG    | Forward
  B3         Ethernet | Drop       |


 Actions->   Cancel     Edit     Save     Help

Select the action to be taken with the filtered frame.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

a “Source Port “ filter type has been selected for port D1

A Drop action has been specified for ports B2 and B3. Thus, traffic from port D1 will not be forwarded by ports B2 and B3.

**Figure 7-7. 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 6a.
      – If you are finished configuring actions for the current filter, go to step 7.

7. Press [Enter] to return to the Actions line, then press [S] (for `Save`) to save the current filter configuration.

8. 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.

9. When you are finished configuring the switch, return to the Main Menu.

# Virtual LANs (VLANs)

The switch supports port-based virtual LANs (VLANs). A VLAN is a collection of ports that belong to a single broadcast domain. (That is, all ports carrying traffic for a particular subnet address would belong to the same VLAN.) This allows workgroups to be defined on the basis of their logical function instead of their physical location, and does not require recabling.

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. Cross-domain broadcast traffic is eliminated and bandwidth is saved by not allowing packets to flood throughout the network.

For example, if ports 1 through 5 belong to VLAN_1 and ports 6 through 10 belong to VLAN_2, traffic from end-node stations on ports 2 through 5 is restricted to only VLAN 1, while traffic from ports 6 through 9 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 10.

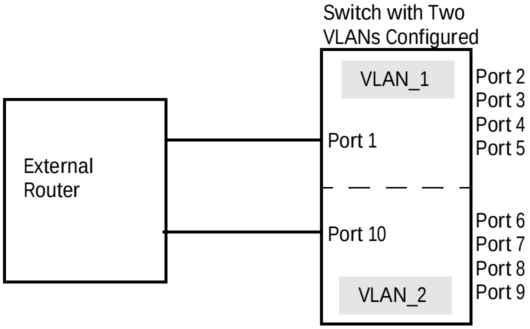


**Figure 7-8. Example of Routing Between VLANs via an External Router**

## Effect of VLANs on Other Switch Features

**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 eight VLAN MAC addresses (one per possible VLAN). If STP is enabled for a VLAN, the Spanning Tree source MAC address in the STP configuration BPDU packets for the VLAN will be the VLAN MAC address itself.

**Note**

If multiple VLANs are configured on the switch, you will need to configure a separate instance of  Spanning Tree for each VLAN in which you want Spanning Tree to operate.

**Port Trunks.** When assigning a port trunk to a VLAN, all ports in the trunk must be assigned to the same VLAN. You cannot split trunk members across multiple VLANs.

**Port Monitoring.** If you designate a port on the switch for network monitoring, this port will not appear in the Port VLAN Assignment screen and cannot be configured as a member of any VLAN.

**VLANs Spanning Multiple Switches.** It is possible to have ports on more than one switch that are members of the same VLAN. Switches having VLANs that cross multiple switches must be interconnected by one link per VLAN. For example, if VLAN A and VLAN B span two switches, the switches must be interconnected by two independent links; one for VLAN A and one for VLAN B. This concept is illustrated in figure 7-9 on the next page.

**Adding a Switch 2000 Module.** If you install a Switch 2000 module in a previously unoccupied slot, the ports in the module will be automatically added to the default VLAN. (To properly install a Switch 2000 module, refer to the documentation you received with the module.)

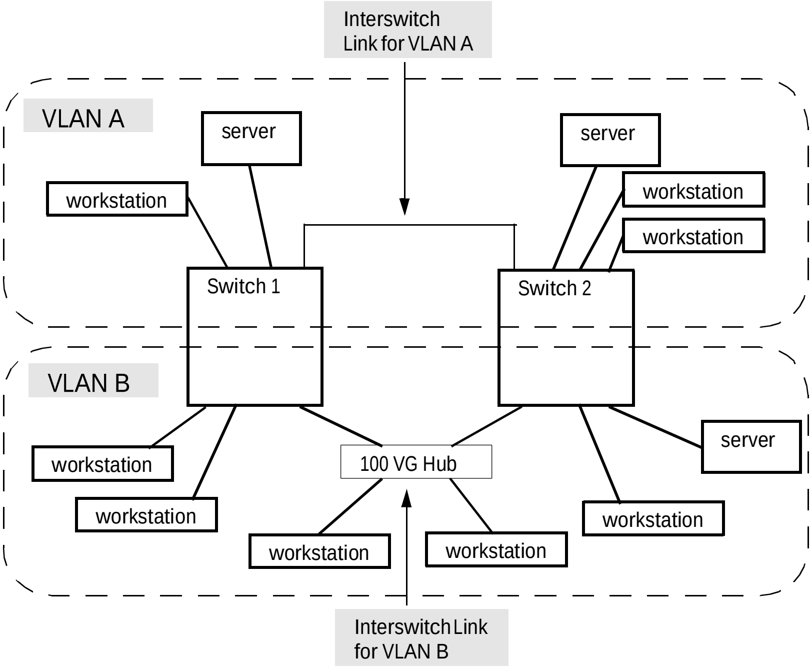


**Figure 7-9. Example of VLANs Spanning Multiple Switches**

## Overview of Using VLANs

To use VLANs, you will need to follow these general steps:

- Configure at least one VLAN in addition to the default VLAN (DEFAULT_VLAN). Refer to “How To Configure a VLAN” on the next page.
- 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) Bootp feature to download an IP configuration from a Bootp server. Refer to “Internet (IP) Service Features” on page 3-9 or to appendix E, “Bootp Operation”.

- If you are managing VLANs with SNMP in an IPX network, configure the IPX gateway encapsulation and gateway node. (An IPX node address is automatically assigned to each VLAN interface.) Refer to “IPX Service Features'' on page 3-7.

## How To Configure a VLAN

In the factory default configuration, all ports on the Switch 2000 belong to a physical broadcast domain named `“DEFAULT_VLAN”`. You can divide the switch ports into multiple virtual broadcast domains by adding one or more 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.

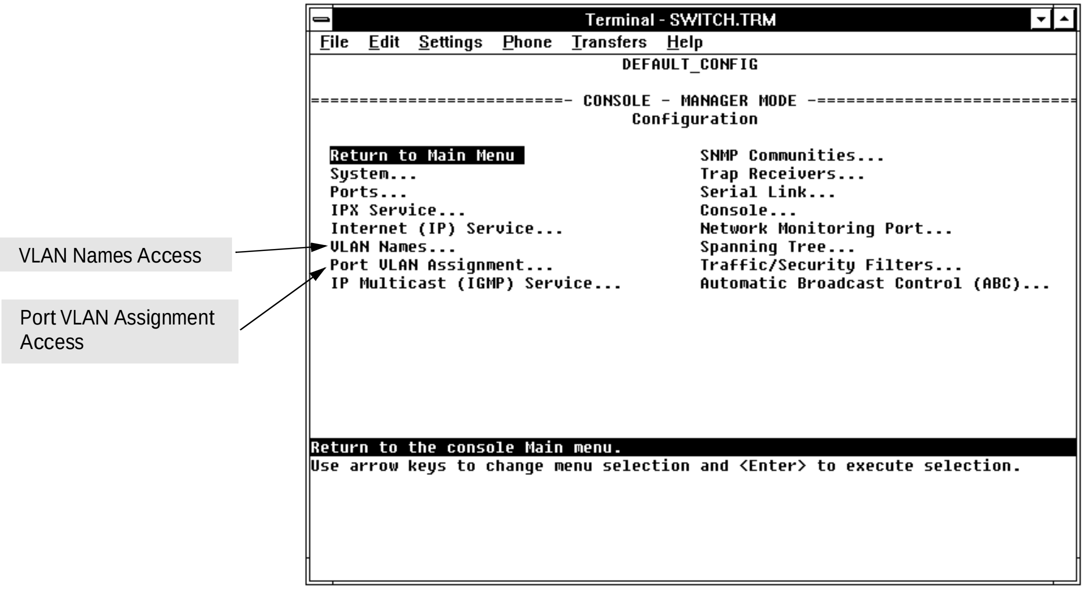
**Note**

If you add one or more new VLAN(s), you should then reboot the switch. (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 a VLAN, the new assignment is automatically enabled, and it is not necessary to reboot the switch a second time.

To create a new VLAN and/or move ports into a VLAN, use the following two procedures.

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

1. Beginning at the Main Menu, select `Configuration` to display the configuration menu.

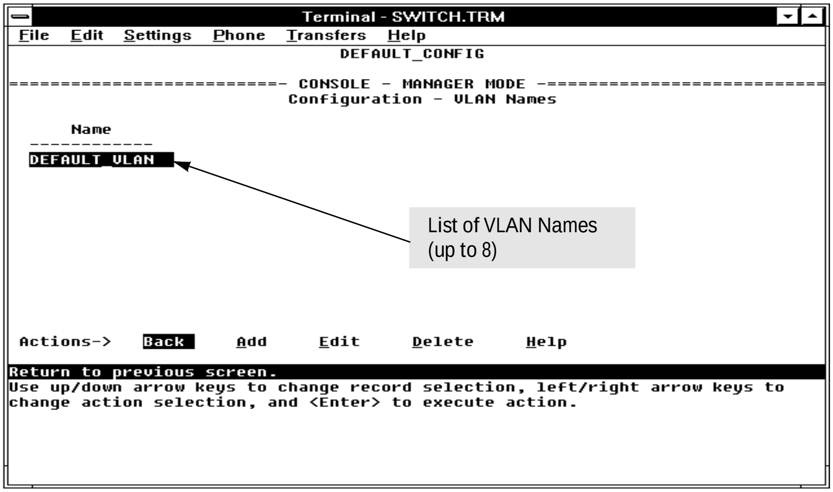


Terminal - SWITCH.TRM
File Edit Settings Phone Transfers Help
VLAN Names Access
Port VLAN Assignment Access

```
                               DEFAULT_CONFIG

=========================- CONSOLE - MANAGER MODE -==========================
                                Configuration

  Return to Main Menu                    SNMP Communities...
  System...                              Trap Receivers...
  Ports...                               Serial Link...
  IPX Service...                         Console...
  Internet (IP) Service...               Network Monitoring Port...
  VLAN Names...                          Spanning Tree...
  Port VLAN Assignment...                Traffic/Security Filters...
  IP Multicast (IGMP) Service...         Automatic Broadcast Control (ABC)...

Return to the console Main menu.
Use arrow keys to change menu selection and <Enter> to execute selection.
```

**Figure 7-10. The VLAN Options in the Configuration Menu**

2. From the Configuration menu, select `VLAN Names`. You will then see a screen similar to the following:



Terminal - SWITCH.TRM
File Edit Settings Phone Transfers Help
List of VLAN Names (up to 8)

```
                               DEFAULT_CONFIG

=========================- CONSOLE - MANAGER MODE -==========================
                         Configuration - VLAN Names

      Name
  ------------
  DEFAULT_VLAN

 Actions->   Back     Add     Edit     Delete     Help

Return to previous screen.
Use up/down arrow keys to change record selection, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

**Figure 7-11. The (Default) VLAN Names Screen**

3. Press [A] (for `Add`). You will then be prompted for a new VLAN name:

```
Name : _
```

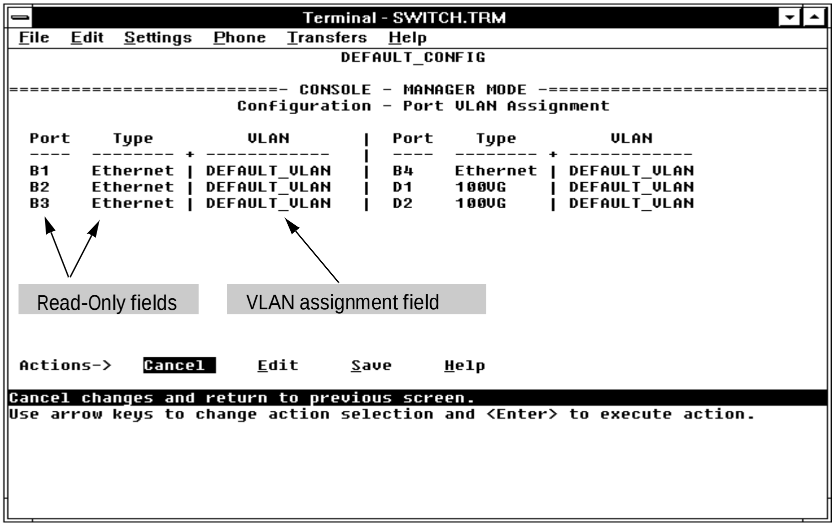
4. Type the name (up to 12 characters, with no spaces) of a new VLAN that you want to add, then press [Enter].
5. Press [S] (for `Save`).
6. Do one of the following:
   - If you want to add another VLAN name, return to step 3.
   - If you are finished entering VLAN names, press [B] (for `Back)` to return to the Configuration menu.
7. Return to the Main Menu and reboot the switch to activate the new VLAN(s) you have just entered.

**Note**

You can rename "`DEFAULT_VLAN`", but you cannot delete it from the Switch, regardless of which name you assign to it.

**To Move a Port to a VLAN.** Use this procedure to move a port into a VLAN. (Ports you do not specifically assign to a VLAN are automatically placed in the default VLAN.)

1. If you have just added a new VLAN name and have not yet rebooted the switch, do so now (step 7 in the previous procedure).
2. Return to the Main Menu and select Configuration to display the Configuration menu.
3. Select `Port VLAN Assignment` . You will then see a Port VLAN Assignment screen similar to the following:



```
                              DEFAULT_CONFIG

=========================- CONSOLE - MANAGER MODE -==========================
                   Configuration - Port VLAN Assignment

  Port     Type         VLAN        |  Port     Type         VLAN
  ----   -------- + ------------    |  ----   -------- + ------------
  B1     Ethernet | DEFAULT_VLAN    |  B4     Ethernet | DEFAULT_VLAN
  B2     Ethernet | DEFAULT_VLAN    |  D1     100VG    | DEFAULT_VLAN
  B3     Ethernet | DEFAULT_VLAN    |  D2     100VG    | DEFAULT_VLAN

 Actions->    Cancel     Edit     Save     Help

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

Read-Only fields

VLAN assignment field

**Figure 7-12. Example of the Port VLAN Assignment Screen**

4. The VLAN column shows the VLAN to which each port on the switch is assigned. (Ports that you do not specifically assign are automatically assigned to the default VLAN.) To assign a port on the switch to a different VLAN than the current selection:

   a. Press E (for `Edit`) to move the highlight to  the VLAN column.

   b. Use ↓ to highlight the VLAN name for the port you want to re-assign to a different VLAN.

   c. Press the Space bar to select a different VLAN name.

   d. Do one of the following:
      – To re-assign another port to a different VLAN, return to step 8b.
      – If you are finished assigning ports to VLANs, press Enter and S (for `Save`) to activate the changes you've made and to return to the Configuration menu.

5. Return to the Main Menu. (It is not necessary to reboot the switch; the new port assignments are implemented when you do the “save” in the preceding step.)

## VLAN Restrictions

- Each port can be assigned to only one VLAN.
- An external router must be used to communicate between two 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 on the Switch 2000.

- If you assign a port to be the  Network Monitoring Port, that port cannot be configured as a member of any VLAN. If the port was previously assigned to a VLAN (including the default VLAN), it will be automatically removed from the VLAN when the Monitoring Port assignment is made. When you subsequently disable the monitoring port assignment, the port will be returned to the default VLAN.
- Before you can delete a VLAN, you must move all of its ports to another VLAN.

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

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

Release A.09.70 (or later) is available electronically through the HP BBS service and the World Wide Web. Refer to the “Customer Support Services” card at the beginning of this manual.

## 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.

# IP Multicast (IGMP)

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.

## 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 the 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.
- **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.

**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 7-13 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.

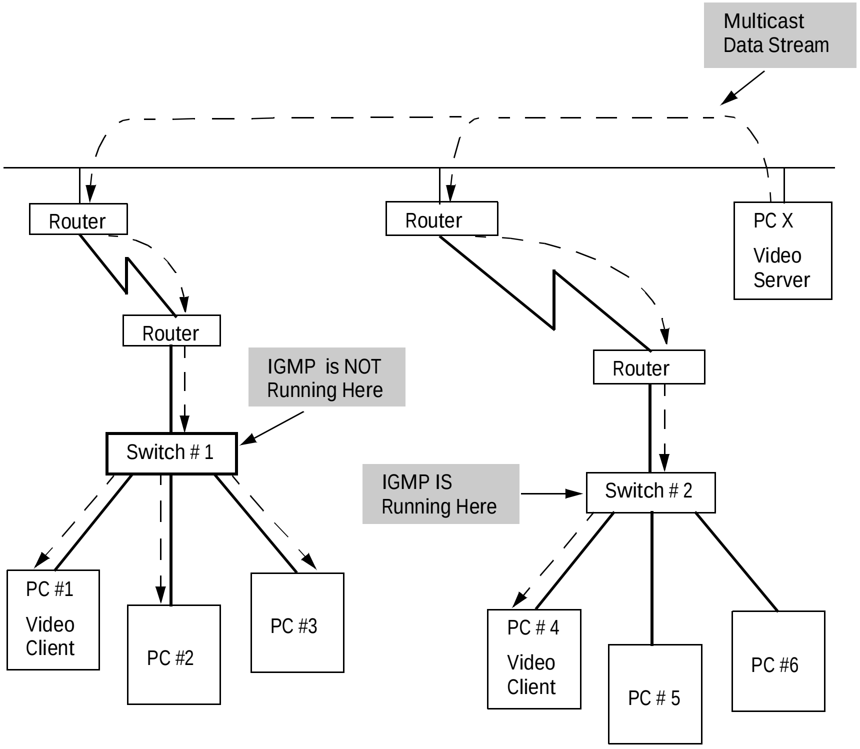


**Figure 7-13. The Advantage of Using IGMP**

The next figure (7-14) 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.)

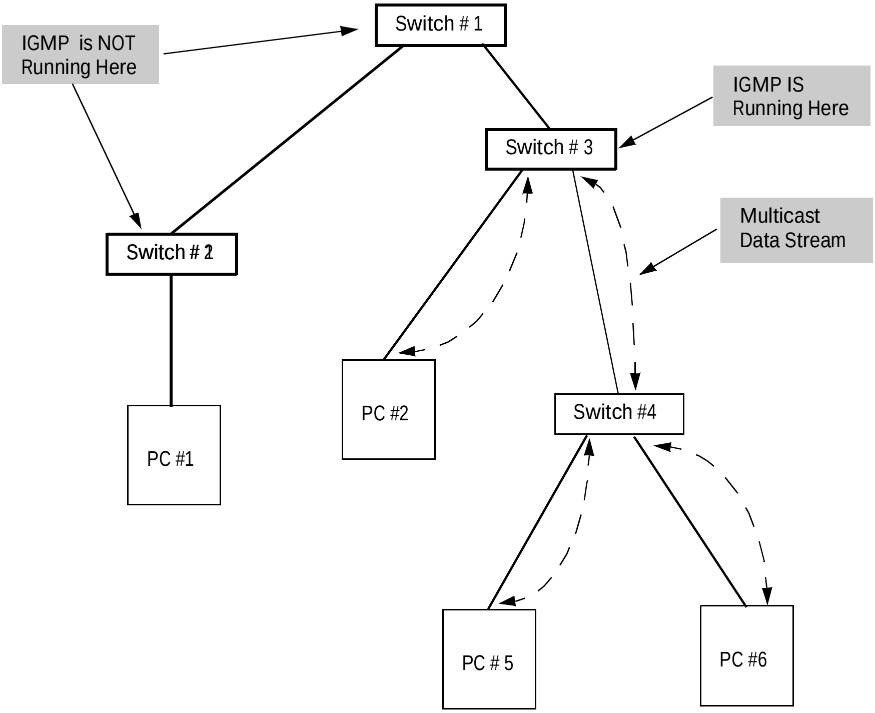


**Figure 7-14. Isolating IP Multicast Traffic in a Network**

- 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 addresses occur in the range from 224.0.0.0 through 239.255.255.255. When IGMP is enabled, any Traffic/Security filters (page 7-8) configured with a “Multicast” filter type and a “Multicast Address” within the above range are disabled and an event log message indicating this action is logged . That is, IGMP will control the IP multicast traffic flow and the Traffic/ Security filter will control any multicast traffic that is not IP multicast traffic.

## How 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. The configuration options include:

- **Enabling or disabling IGMP.** Disabling IGMP (the default) causes all ports on the switch or VLAN to simply forward IP multicast traffic. 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 7-29.)
- **High-priority forwarding.** 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 (such as Hewlett-Packard’s implementation of 100Base-TX), enabling this parameter causes the switch or VLAN to give a higher priority to IP multicast traffic than to other traffic.

**Per-Port handling of IP multicast traffic**. In the factory default state (IGMP disabled), the switch forwards all IGMP traffic. When IGMP is enabled, you can configure the switch to do any of the following on a per-port basis:

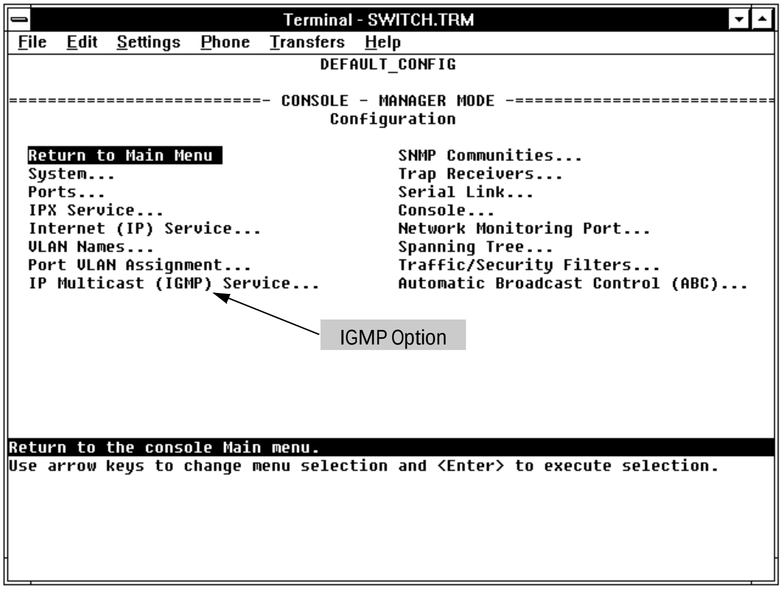
- Automatic (the default): Causes the switch to interpret IGMP packets and to filter IP multicast traffic based on the IGMP packet information for that port.
- Blocking: Causes the switch to drop all IGMP transmissions received and block all outgoing IP Multicast packets for that port.
- Forwarding: Causes the switch to forward all IGMP and IP multicast transmissions through the port.

**Note**

If you move a port from one VLAN to another, that port will retain its IP multicast (`IP Mcast`) parameter setting. For example, suppose port A1 is in DEFAULT_VLAN with an IP Mcast setting of "Blocked". If you create another VLAN named VLAN2 and then move port A1 to VLAN2, the IP Mcast setting will remain the same (Blocked).

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

1. Beginning at the Main Menu, select `Configuration` to display the Configuration menu.

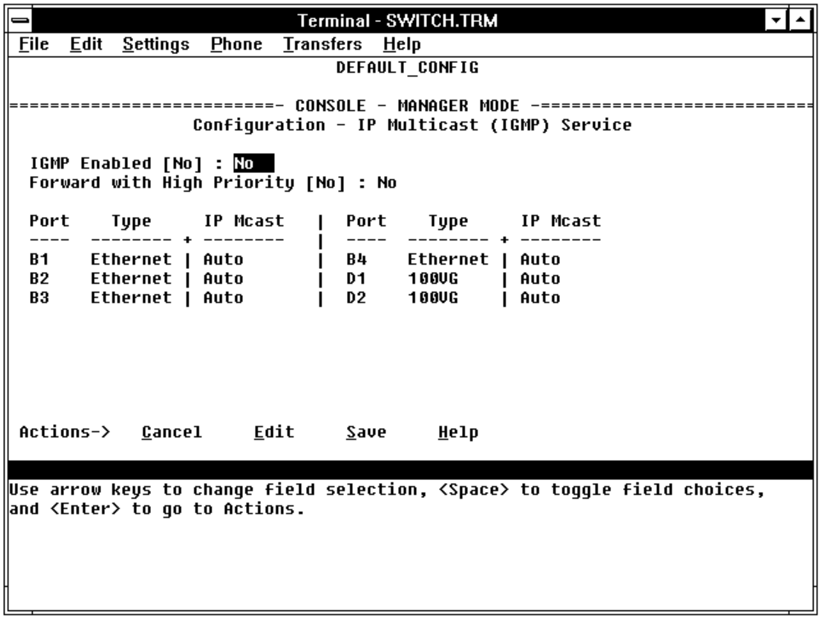


```
                                DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -===========================
                                 Configuration

  Return to Main Menu                    SNMP Communities...
  System...                              Trap Receivers...
  Ports...                               Serial Link...
  IPX Service...                         Console...
  Internet (IP) Service...               Network Monitoring Port...
  VLAN Names...                          Spanning Tree...
  Port VLAN Assignment...                Traffic/Security Filters...
  IP Multicast (IGMP) Service...         Automatic Broadcast Control (ABC)...

Return to the console Main menu.
Use arrow keys to change menu selection and <Enter> to execute selection.
```

**Figure 7-15. The IGMP Option in the Configuration Menu**

2. Select `IP Multicast (IGMP) Service`.

3. If VLANs are configured, select the VLAN in which you want to configure IGMP and press [E] (for `Edit`). You will then see a screen similar to the following:



```
                              DEFAULT_CONFIG

=========================- CONSOLE - MANAGER MODE -==========================
                  Configuration - IP Multicast (IGMP) Service

  IGMP Enabled [No] : No
  Forward with High Priority [No] : No

  Port    Type     IP Mcast   |  Port    Type      IP Mcast
  ----   -------- + --------  |  ----   -------- + --------
  B1     Ethernet | Auto      |  B4     Ethernet | Auto
  B2     Ethernet | Auto      |  D1     100VG    | Auto
  B3     Ethernet | Auto      |  D2     100VG    | Auto




 Actions->   Cancel     Edit     Save     Help

Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

**Figure 7-16. Example of the (Default) IP Multicast (IGMP) Service Screen**

4. Press the Space bar to select `Yes` (to enable IGMP).
5. Use [↓] to highlight the `Forward with High Priority` parameter.
6. 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`.
7. 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 and/or page 7-26 for further informtion on these choices.)
8. Repeat step 7 for each port you want to configure.
9. 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.
10. 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 9.)

**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 hpSwitchIgmpQuerierState.<vlan number>
```

*where:*

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

```
getmib hpSwitchIgmpQuerierState.1
```

# Automatic Broadcast Control (ABC)

ABC helps to conserve bandwidth and processing power for IP and/or IPX traffic within a broadcast domain without adding the levels of cost and latency normally associated with routers. ABC achieves this by using the switch to reduce IP ARP and RIP broadcast traffic and IPX NSQ, RIP, and SAP broadcast traffic normally found on a network. Also, when enabled, ABC allows you to set the broadcast limit (`Bcast Limit` parameter) for all ports on the switch (or, if VLANs are configured, for all ports in the specified VLAN).

## How ABC Operates

**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.

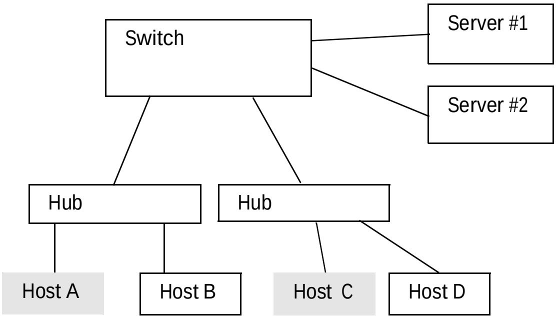


**Figure 7-17. Example of a Network Using ABC**

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 conected 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 7-17) 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.

If Automatic Broadcast Control (ABC) is configured and more than one port is monitored, then broadcast packets may be duplicated on the monitor port.

**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 will forward 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.

## How To Configure ABC

In the factory default configuration, ABC is disabled. If multiple VLANs are configured, you can configure ABC on a per-VLAN basis. Otherwise, the configuration is on the switch level. You can enable ABC for IP only, IPX only, or for both. When ABC is disabled (the default), all broadcasts are sent out either all ports in the switch or, if VLANs are configured, out all ports in VLANs where ABC is disabled. ABC can be enabled with the options described below.

### Enabling IP Only

Enabling ABC for IP 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.
- Activates a broadcast limit for either all ports in the switch or, if VLANs are configured, for all ports in the selected VLAN. (You can accept the default broadcast limit setting, change it, or turn it off.)

### Enabling IPX Only

Enabling ABC for IPX 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.

- Activates a broadcast limit for either all ports in the switch or, if VLANs are configured, for all ports in the selected VLAN. (You can accept the default broadcast limit setting, change it, or turn it off.)

## Enabling Both IP and IPX (IP_IPX)

Enabling ABC for IP and IPX causes the switch to:

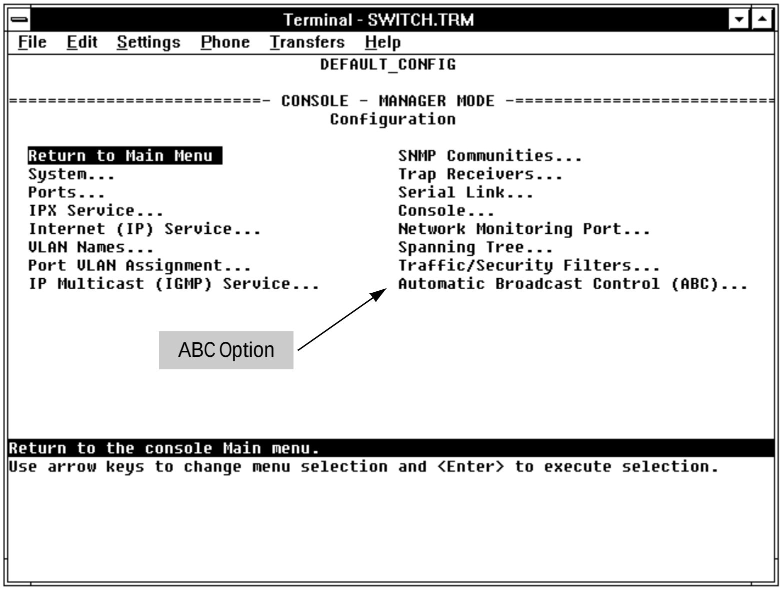
- Send a proxy IP ARP reply for hosts whose addresses the switch has learned.
- Send a proxy NSQ (nearest server query) reply for services the switch has learned.

Enabling for both IP and IPX also allows you to choose whether to:

- Enable ABC for IP RIP Control and/or IPX RIP/SAP control, as described in the preceeding subsections.
- Set a broadcast limit for either all ports in the switch or, if VLANs are configured, for all ports in the selected VLAN.

**To Configure ABC.** Use this procedure to configure or edit the ABC settings for a switch or VLAN.

1. Beginning at the Main Menu, select `Configuration` to display the Configuration menu.



```
                                DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -==========================
                                 Configuration

  Return to Main Menu                     SNMP Communities...
  System...                               Trap Receivers...
  Ports...                                Serial Link...
  IPX Service...                          Console...
  Internet (IP) Service...                Network Monitoring Port...
  VLAN Names...                           Spanning Tree...
  Port VLAN Assignment...                 Traffic/Security Filters...
  IP Multicast (IGMP) Service...          Automatic Broadcast Control (ABC)...

Return to the console Main menu.
Use arrow keys to change menu selection and <Enter> to execute selection.
```

ABC Option

**Figure 7-18. The Configuration Menu**

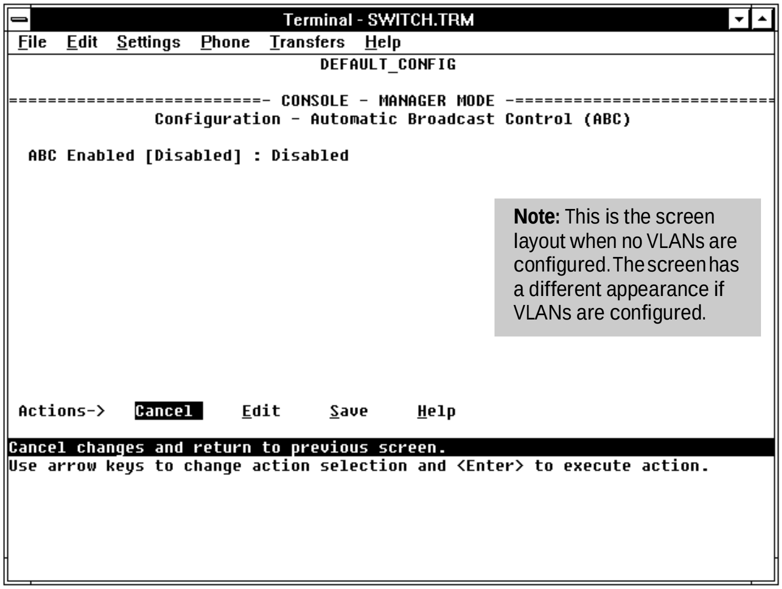
2. Select Automatic Broadcast Control (ABC) and press Enter.

3. If no VLANs are configured, go to step 4 . 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.

4. Press E (for `Edit`).



```
                              DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -===========================
                Configuration - Automatic Broadcast Control (ABC)

  ABC Enabled [Disabled] : Disabled




 Actions->   Cancel     Edit     Save     Help

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

**Note:** This is the screen layout when no VLANs are configured. The screen has a different appearance if VLANs are configured.

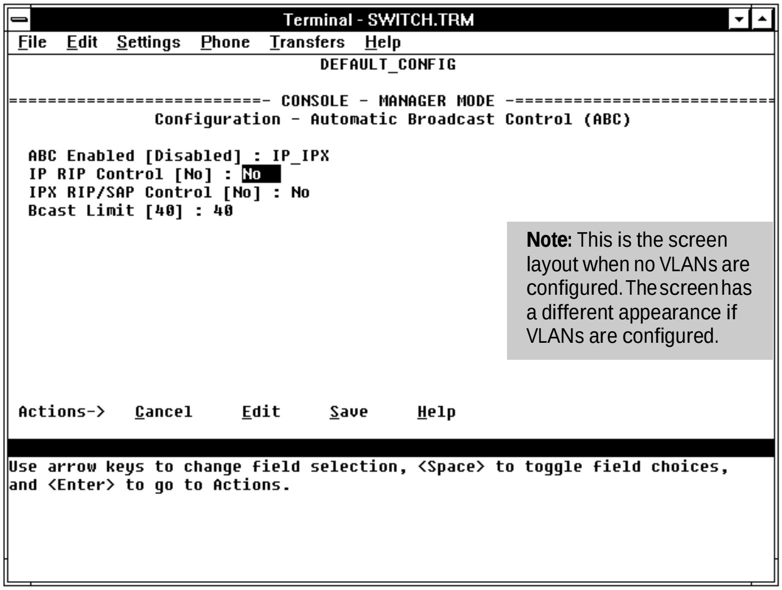
**Figure 7-19. The Default ABC Screen (No VLANs Configured)**

5. 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 only for the IP protocol.
   - `IPX`: Enables ABC only for the IPX protocol.
   - Disabled

6. If you want broadcast control disabled for IP RIP and/or IPX RIP and SAP broadcasts, leave the remaining parameters set to `No` and go to step 7.

   If you *do* want broadcast control for RIP or SAP broadcasts, press an arrow key to display the remaining ABC parameters. (If VLANs are configured, these parameters already appear.) Then do *one* of the following:

- If you enabled ABC for IP_IPX and pressed an arrow key (figure 7-20), below):



```
                              DEFAULT_CONFIG

=========================- CONSOLE - MANAGER MODE -==========================
               Configuration - Automatic Broadcast Control (ABC)

  ABC Enabled [Disabled] : IP_IPX
  IP RIP Control [No] : No
  IPX RIP/SAP Control [No] : No
  Bcast Limit [40] : 40



 Actions->   Cancel     Edit     Save     Help

Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

**Note:** This is the screen layout when no VLANs are configured. The screen has a different appearance if VLANs are configured.

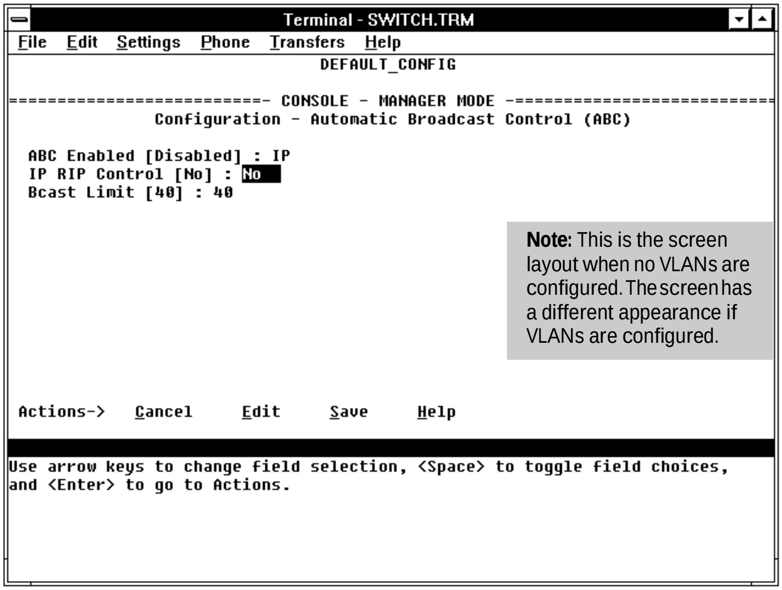
**Figure 7-20. ABC Enabled With IP_IPX Option (No VLANs Configured)**

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 you want IPX RIP/SAP broadcast control, select the `IPX RIP/SAP Control` parameter and use the Space bar to select `Yes`.
iii. If you want to specify a different global broadcast limit for the switch or selected VLAN (if VLANs are configured), select the `Bcast Limit` parameter and type a value from 0 to 99. (A “0” disables broadcast limits; 40 is the default setting.)
iv. Go to step 7.

**Note**

The broadcast limit (`Bcast Limit`) parameter in the ABC screen sets a global broadcast limit value for all ports in the switch or selected VLAN (if VLANs are configured). If you want to set broadcast limits on a per-port basis, you can override the setting in this screen by going to the Port Configuration screen (page 3-6) and setting the broadcast limit value individually for one or more specific ports.

- If you enabled ABC for IP (figure 7-21, below):



```
                              DEFAULT_CONFIG

=========================- CONSOLE - MANAGER MODE -==========================
               Configuration - Automatic Broadcast Control (ABC)

  ABC Enabled [Disabled] : IP
  IP RIP Control [No] : No
  Bcast Limit [40] : 40



 Actions->   Cancel     Edit     Save     Help

Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

**Note:** This is the screen layout when no VLANs are configured. The screen has a different appearance if VLANs are configured.

**Figure 7-21. ABC Enabled With IP Option (No VLANs Configured)**

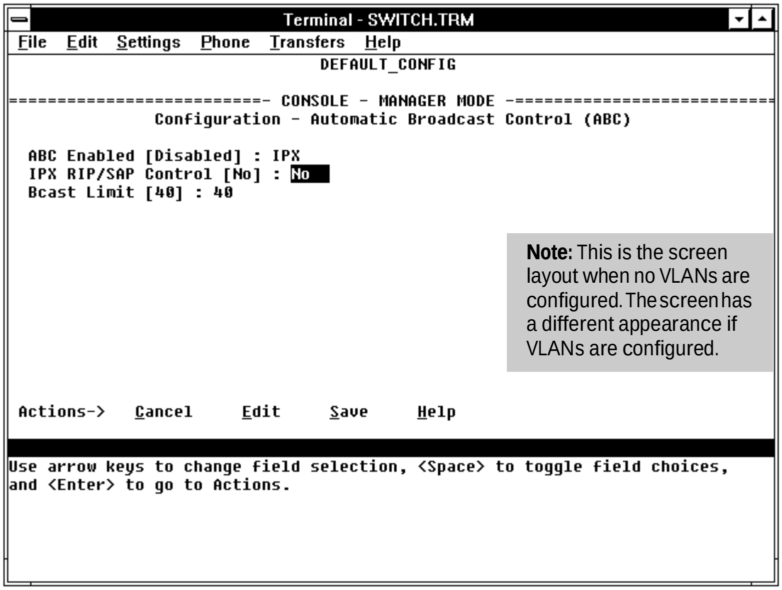
i. Select `IP RIP Control`.

ii. Use the Space bar to select `Yes`.

iii. If you want to specify a different global broadcast limit for the switch or selected VLAN (if VLANs are configured), select the `Bcast Limit` parameter and type a value from 0 to 99. (A “0” disables broadcast limits; 40 is the default setting.) Refer to the Note on page 7-36.

iv. Go to step 7.

- If you enabled ABC for IPX (figure 7-22, below):



```
                              DEFAULT_CONFIG

=========================- CONSOLE - MANAGER MODE -=========================
               Configuration - Automatic Broadcast Control (ABC)

  ABC Enabled [Disabled] : IPX
  IPX RIP/SAP Control [No] : No
  Bcast Limit [40] : 40

 Actions->   Cancel     Edit     Save     Help

Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

**Note:** This is the screen layout when no VLANs are configured. The screen has a different appearance if VLANs are configured.

**Figure 7-22. ABC Enabled With IPX Option (No VLANs Configured)**

i. Select `IPX RIP/SAP Control.`
ii. Use the Space bar to select `Yes`.
iii. If you want to specify a different global broadcast limit for the switch or selected VLAN (if VLANs are configured), select the `Bcast Limit` parameter and type a value from 0 to 99. (A "0" disables broadcast limits; 40 is the default setting.) Refer to the Note on page 7-36.
iv. Go to step 7.

7. Press [Enter] to return to the `Actions` menu.

8. Press [S] (for `Save`) to activate the changes you have made to the ABC parameters.

9. Return to the Main Menu. (It is not necessary to reboot the switch. The new ABC configuration is implemented when you select the "save" in step 8.)

# 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

You can use the switch console's TFTP feature (`Download OS`), HP's SNMP Download Manager, or the HP Update Utility (update.exe) to download a new operating system (OS) to the switch. Downloading a new OS does not change the current switch configuration.

Using the `Download OS` option from the switch Main Menu (described on the following pages):

- The switch must be configured for either IP or IPX service.
- The OS software to download must be stored in a file on a TFTP server in your network or VLAN (if configured).
- The switch must be properly connected to the network.

Using the HP Download Manager:

- At a minimum, use a 386 8-megabyte IBM-compatible PC with a network interface.
- Obtain software and instructions from HP's BBS or World Wide Web site. (Refer to the "Customer Support Services" section in appendix G, "Troubleshooting".)

You can access Download Manager in the HP AdvanceStack Assistant network management application by clicking the right-side mouse button on the background topology view.

Using the HP Update Utility:

- Use a PC with a direct-connect RS-232 serial cable.
- Obtain the update utility and refer to the instructions in the readme.txt file included with the utility. The utility is on disks shipped with some Switch 2000 modules and in a compressed, self-extracting file available from World Wide Web site and BBS. (Refer to the "Customer Support Services" card at the front of this manual.) Updates are routinely supplied free from HP's BBS and WWW services.

## Using TFTP To Download the OS File

This procedure assumes that an OS file for the switch has previously been stored on a TFTP server accessible to the switch. (The OS file is typically available from HP's electronic services—refer to the card at the front of this manual.) Before you use the procedure, do the following:

- Determine the IP or IPX 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, B_03_01.swi).

**Note**

Software versions A.02.01 and later include two OS files; one for the Switch 2000 and one for the optional FDDI Module that you can install in the switch. These two files are named as follows:

*filename*.swi
*filename*.fdd

where *filename* (version number) will be the same for both files. For example:

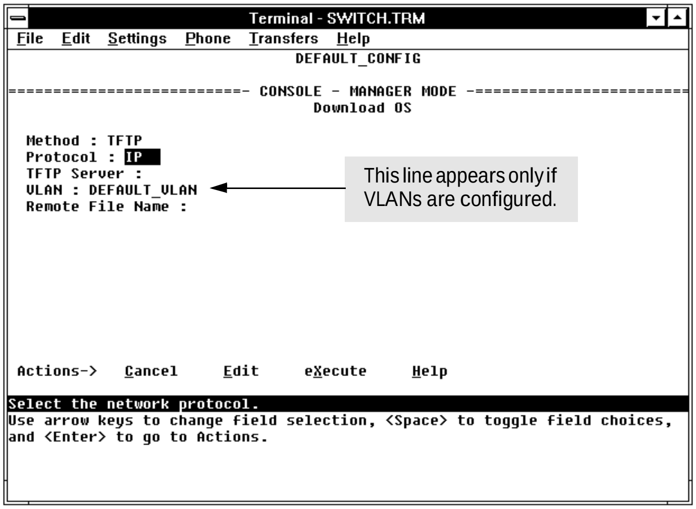
`B_03_01.swi` OS for the B-version of the Switch 2000 chassis and all Switch 2000 modules that operate with version A_03_01 or earlier software.

`B_03_01.fdd` OS for the FDDI module. (Necessary if an FDDI Module is installed.)

**Important:** If you are using the FDDI module in the switch, the version numbers of the FDDI OS and the Switch 2000 OS *must* match. *Otherwise, the FDDI Module may not operate properly even though it is recognized by the switch.* If the FDDI module is installed in the switch, you can compare the version numbers of the FDDI OS and the switch OS by executing the `Version` command. To execute `Version`, select `Advanced Commands` from the Main Menu, then type `Version` and press [Enter]. (If VLANs are configured, select the VLAN to which the FDDI port is assigned before you execute `Version`.

Ensure that both OS files (*filename*.swi and *filename*.fdd) are in the same TFTP server directory when using this procedure to download an OS to the Switch 2000. *If your TFTP server is a Unix workstation, ensure that the case* *(upper or lower) that you specify for the filename in the Switch 2000 Download OS screen is the same case as the characters in the OS filenames in the TFTP server.*

1. In the Main Menu, select `Download OS`. You will then see this screen:



```
                          DEFAULT_CONFIG

=========================- CONSOLE - MANAGER MODE -========================
                            Download OS

 Method : TFTP
 Protocol : IP
 TFTP Server :
 VLAN : DEFAULT_VLAN
 Remote File Name :

Actions->  Cancel    Edit    eXecute    Help

Select the network protocol.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

This line appears only if VLANs are configured.

**Figure 8-1. The Download OS Screen (Default Values)**

2. Press [E] (for `Edit`).

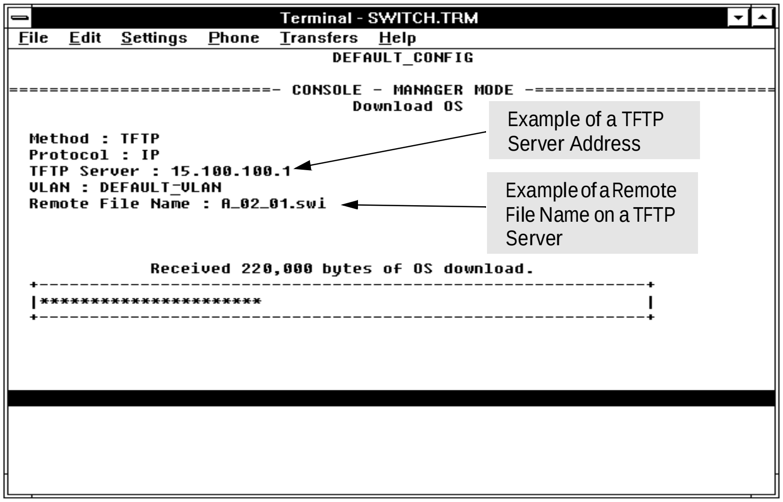
3. With the `Protocol` field highlighted, use the Space bar to select either IP or IPX, depending on the protocol in use in your network.

4. Highlight the `TFTP Server` field and type in the IP or IPX address of the TFTP server in which the OS file has been stored.

5. If VLANs are configured, highlight the `VLAN` field. Then use the Space bar to select the VLAN in which the TFTP Server is operating.

6. Highlight 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:



```
                              DEFAULT_CONFIG

========================== CONSOLE - MANAGER MODE ==========================
                                Download OS

 Method : TFTP
 Protocol : IP
 TFTP Server : 15.100.100.1
 VLAN : DEFAULT_VLAN
 Remote File Name : A_02_01.swi


            Received 220,000 bytes of OS download.
 +-------------------------------------------------------------+
 |**********************                                       |
 +-------------------------------------------------------------+
```

Example of a TFTP Server Address

Example of a Remote File Name on a TFTP Server

**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 message appears:

   ```
   WRITING SYSTEM SOFTWARE TO FLASH, BACK SOON
   ```

   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. Select `Status and Counters` from the Main Menu

   b. Select Switch Information from the `Status and Counters` screen.

   c. Check the `OS Version` line.

## Switch-to-Switch Download

If you have two or more Switch 800Ts and/or the B-version of the Switch 2000 (HP J3100B) 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 800T and the B-version of the Switch 2000 use the same OS.) To do so:

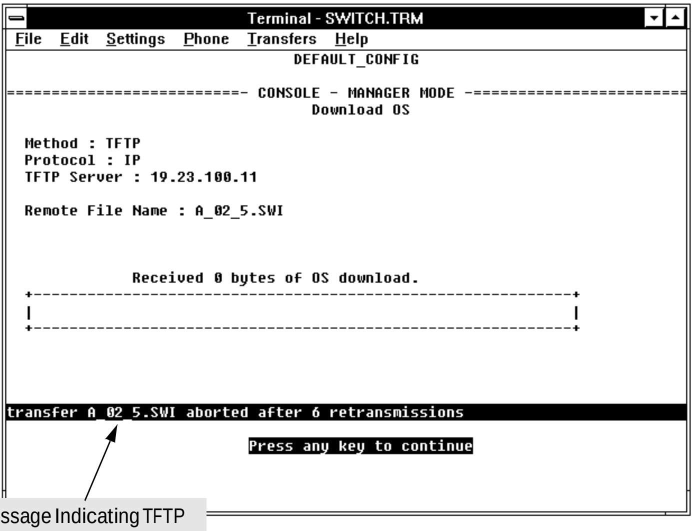
1. Go to the Download OS screen in the switch to receive the download.
2. Enter the IP or IPX address of the remote switch containing the OS you want to download.
3. Enter "OS" for the Remote File Name.
4. Execute the download.

**Note**

The "A" version of the Switch 2000 uses OS software that is different from the OS software used by the "B" version of the Switch 2000 and the Switch 800T. For this reason, transferring OS software between an "A" version of the Switch 2000 and either a Switch 800T or a "B" version of the Switch 2000 is not supported.

# Troubleshooting TFTP Downloads

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



```
                                DEFAULT_CONFIG

=========================- CONSOLE - MANAGER MODE -========================
                                  Download OS

  Method : TFTP
  Protocol : IP
  TFTP Server : 19.23.100.11

  Remote File Name : A_02_5.SWI



              Received 0 bytes of OS download.
  +-------------------------------------------------------------+
  |                                                             |
  +-------------------------------------------------------------+




transfer A_02_5.SWI aborted after 6 retransmissions

                           Press any key to continue
```

Message Indicating TFTP Download 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 4-16.)

Some of the causes of download failures include:

- Wrong protocol specified for the Protocol parameter
- 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 or IPX 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 2000 Configurations

You can use the following commands to transfer Switch 2000 configurations between the switch and a PC or Unix workstation.

| Command | Function |
|---|---|
| Get | Download a Switch 2000 configuration file from a networked PC or Unix workstation using TFTP. |
| Put* | Upload a Switch 2000 configuration to a file in a networked PC or Unix workstation using TFTP. |
| ZGet | Uses a Zmodem-compatible terminal emulation program to download a Switch 2000 configuration file from a PC or Unix workstation connected to the switch's console port (either directly or via a modem). |
| ZPut* | Uses a Zmodem-compatible terminal emulation program to upload a Switch 2000 configuration to a file in a PC or Unix workstation connected to the switch's console port (either directly or via a modem). |
| *Can also be used to send the output of certain commands to a file on another device. Refer to chapter 6, "Using the Advanced Commands". | |

## 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 or IPX 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 Zget overwrites the switch's current configuration with the downloaded configuration. The switch then automatically reboots itself.

1. From the Main Menu select Advanced `Commands line`.
2. At the command prompt, execute one of the following commands:

   To upload a configuration to a file on a PC or Unix workstation:

   ```
   put IP_address CONFIG remote_file
   put IPX_address CONFIG remote_file
   ```

To download a configuration from a file on a PC or Unix workstation:

get *IP_address* CONFIG *remote_file*

get *IPX_address* CONFIG *remote_file*

where: *IP address* or *IPX 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 ZGet and ZPut 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 can be connected either directly or via a modem to the switch's console port. Also, the PC or workstation must be running a Zmodem-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 Zget or Zput commands.

**Note** ZGet overwrites the switch's current configuration with the downloaded configuration. The switch then reboots itself.

To use ZGet or ZPut, you need the name assigned to the configuration file on the PC or workstation.

1. On the PC or workstation, start the Zmodem-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 `Advanced Commands` 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:

```
zput config remote_file [overwrite] [dos/unix]
```

To download a configuration from a file on a PC or Unix workstation:

```
zget config remote_file [dos/unix]
```

where: *remote_file* is the name of the file in which the configuration is stored

*[overwrite]* is one of the following optional values:

`0` (the default) allows a new file to be created, but does not allow an existing file to be overwritten.

`1` creates a new file or overwrites an existing file.

*`[dos/unix]`* is one of the following optional values:

`0` (the default) specifies the DOS file format.

`1` specifies the Unix file format.

If the PC or workstation does not respond to a ZPut or ZGet command within approximately 70 seconds, the command times out and control returns to the `Advanced Command` line.

# Troubleshooting

- Troubleshooting Approaches
- Diagnosing with the LEDs
- Installation Problems
- Unusual Network Activity
- Diagnostic Tests
- Customer Support Services
- Replacement Instructions

## Troubleshooting Approaches

There are four primary ways to diagnose switch problems:

- Checking the LEDs
- Checking the installation
- Checking the cables
- Checking the Console RS-232 interface

# Diagnosing with the LEDs

Most problems with the switch can be diagnosed using the LEDs on its front panel. This section describes:

- The normal LED pattern when the switch is being self-tested
- The LED patterns that indicate error conditions on the switch

## LED Pattern During Self-Test

Whenever the switch is powered on or reset, it performs a self-diagnostic test. During the self-test:

1. All LEDs turn on momentarily, then all but the Power, Self-test, and Fault LEDs turn off.
2. The Power LED remains on; the Self Test and Fault LEDs remain on for less than one minute.

When a module is installed while the switch is operating, the Fault LED for the particular slot turns on momentarily while the switch executes a self-test of that slot.

When the self-test completes successfully, the LEDs go into their normal operational states. If a switch hardware fault exists, the switch will not complete self-test. This will be indicated by the Fault LED.

The tables on the following pages list the switch's LEDs, their possible states, and diagnostic tips to resolve any error conditions.

## LED Error Indications

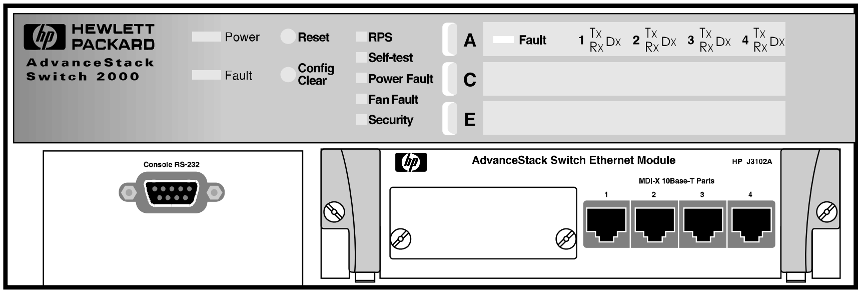


**Figure 9-1. System and Port LEDs with a 4-Port 10Base-T Module Installed**

## LED Error Indications

| LED | State | Diagnostic Tip |
|---|---|---|
| **Power**<br>(green) | Off | If the Power LED is off and the fans are not running, verify that the power cord is plugged into an active power source and to the switch. Make sure these connections are snug. Try power cycling the switch by unplugging and plugging the switch back in.<br>If the Power LED is still not on, verify that the AC power source works by plugging another device into the outlet. Or try plugging the switch into a different outlet or try a different power cord.<br>If this condition persists, the switch may have failed. Call your HP-authorized LAN dealer or HP representative for assistance. |
|  | On then turns off | Make sure the power cord connection is snug into the switch and into the power outlet.<br>Verify that the fans are running and that the chassis intake vents and exhaust ports are clear, and that the area around them is unobstructed.<br>Check the power outlet for power losses or surges.<br>If this condition persists, the switch may have failed. Call your HP-authorized LAN dealer or HP representative for assistance. |
| **Fault**<br>(orange) | Remains On | The Fault LED should remain off during normal operation. If it is on, a self-test failure or a software error has occurred. Power cycle the Switch 2000. If this condition persists, the switch may have failed. Call your HP-authorized LAN dealer or HP representative for assistance. |
|  | Flashing | The switch is operable, but a fault condition has occurred in the switch or an installed module, a fan, or a connected redundant power supply (RPS). The corresponding fault LED for the affected component will flash simultaneously. Check the event log for an indication of the problem source. |
| **RPS**<br>(green) | Off | Should be on if an RPS is installed and operating properly.<br>If there is an RPS problem, this LED is off and the Fault and Power Fault LEDs flash simultaneously. (Check the Event Log in the console user interface for further information on the failure.) Check the connection between the RPS and the power outlet. Verify that power is being supplied to the power outlet. Remove and then reinstall the RPS according to the documentation shipped with the RPS. If the fault condition continues, schedule down time and replace the RPS. |
| **Self-Test**<br>(green) | On | The Self-test LED should be steadily on (for up to 40 seconds) only during the power-on, module installation, and reset self-tests. |
|  | Flashing | The Self-test LED flashes simultaneously with the Fault LED and a slot Fault LED if the slot has failed its self-test. Check the Event Log. (It also flashes during a reset if the Config Clear button is pressed.)<br>If the self-test LED remains on at other times, especially in conjunction with the Fault LED, the switch may have failed. Call your HP authorized LAN representative for assistance. |

## LED Error Indications *(continued)*

| LED | State | Diagnostic Tip |
|---|---|---|
| **Power Fault**<br>(orange) | Flashing | Should be off if the main power supply and optional RPS (if installed) are operating properly. If there is a power problem with either the main power supply or the optional RPS, flashes simultaneously with the Fault LED (above). (Check the RPS LED and the Event Log in the console user interface for further information on the failure.)<br>If an RPS is installed but the RPS LED is off, the RPS has failed. Schedule down time and replace the RPS.<br>If the RPS LED is on, then the main power supply has failed. Contact your HP authorized LAN representative for assistance. |
| **Fan Fault**<br>(orange) | Flashing | Should be off if both fans are operating properly.<br>If there is a fan problem, flashes simultaneously with the Fault LED. One or both fans in the Switch 2000 have failed. (Visually inspect the fans. Also check the Event Log in the console user interface for further information on the failure.) Contact your authorized HP LAN representative for assistance. |
| **Security**<br>(orange) | Flashing | Should remain off during normal operation.<br>Flashes if an SNMP authentication failure has occurred or if a traffic filter violation has occurred. Use the ClearLED command in the console interface to clear this condition. (ClearLED turns off the Security LED if the condition causing the LED to flash has been corrected.) |
| **Fault (slot)**<br>(orange) | Flashing rapidly | A module is only partially installed in a slot. Causes the switch to suspend operation. Either remove the module or firmly install it in the slot.<br>If a module is not installed properly, and the module slot Fault LED continues rapid flashing, other modules in the switch will continue to forward packets normally, but other switch functions will be suspended until the module is removed or properly installed. |
| | Flashing | If this LED is flashing simultaneously with the Fault and Self-test LEDs, then there is a either a failure in the slot, module, or transceiver hardware, or an incorrect transceiver is installed in the module (if a J3191A 100Base-T Module or a J3103A 100VG Module is installed in the slot) . Remove the original module and install a different module in the slot. If the slot Fault LED remains flashing, then the problem is likely to be in the slot hardware and you should contact your HP authorized LAN representative. If the slot Fault LED remains off, then the problem is likely to be in the original module or a transceiver installed in that module. Attempt to isolate the problem to either the module or a transceiver, then contact your HP authorized LAN representative.<br>**Note:** The Slot (fault) LED is steadily on during slot self-test. |

## LED Error Indications *(continued)*

| LED | State | Diagnostic Tip |
|---|---|---|
| **1**, **2**, **3**, **4**<br>(Port Enabled)<br>(green) | Off | The port is not enabled or the link is not operational.<br>If the Switch 2000 port is either a 10Base-T port on an HP J3102A Ethernet Module or 100Base-TX port (HP J3192A or B transceiver) on an HP J3191A 100Base-T Module connected to a hub or another switch, then the port is preconfigured to operate as MDI-X. In this case, ensure that the port on the connected hub or other switch is either an MDI port connected by a straight-through cable, or (if the port on the other device is an MDI-X port) that a crossover cable is used to connect them.<br>**Note:** If an Ethernet port is using an AUI or 10Base2 transceiver, the port is enabled regardless of whether a connection is present. |
| **Rx** and **Tx**<br>Port Receive and Transmit<br>(green) | Off | The Rx and Tx LEDs should be on or flashing as packets are forwarded from or to other ports. If the LEDs do not flash, check the Port Enabled (1, 2, 3, 4) LED. If it is off, the port is not enabled. If the Port Enabled LED is on, then verify that the physical network configuration is correct. Check the console interface for proper configuration and operation. |
| **Dx**<br>(Full Duplex) | Off | If the Port Enabled LED (above) is on, then the Full Duplex (Dx) LED should be on for Ethernet 10Base-T ports that have been configured for full-duplex mode. The Dx LED should be off for Ethernet 10Base-T ports that are disabled or have been configured for half-duplex operation (the default). Check the port configuration in the console interface to ensure that the Mode parameter for the port has been set to Full Duplex.<br>**Note:** Full-duplex should be used only if it is also configured and supported on the media and in the device to which the port is connected. |

# Installation Problems

By carefully following the installation procedures described in chapter 1, “Installing the Switch”, you can avoid most problems caused by improper installation of the switch or one of its components.

## Incorrect Hardware Installation

Incorrectly installing the switch or power cord can result in one or both of these components malfunctioning or not functioning at all. If one or both of these components appear not to be functioning, recheck the installation procedure and, if necessary, reinstall the component correctly.

If the switch will not power on or intermittently resets itself, the switch’s processor may be faulty or the hardware/software setup may be wrong.

## Console RS-232 Problems

If the switch powers on but the console interface will not start up, follow these steps:

- Check the external Console RS-232 connection. If you are not using a modem connection, ensure that the cable is a null modem cable.
- Check the console device settings against the settings listed in appendix C, Sample Console Configurations.
- Try a different baud rate setting in your console device. The Switch 2000’s default setting, “Speed Sense”, automatically matches the Console RS-232 baud rate to the rate used by your PC, terminal, or modem. (However, if the Baud Rate parameter in the switch’s Serial Link screen has been configured to a specific value, the Speed Sense operation is disabled.) The Switch 2000 operates at 300, 600, 1200, 2400, 4800, 9600, 19200, or 38400 bps.
- If you are using a terminal emulation program, try exiting the program and then restarting it.

If the diagnostic information does not appear, or is unintelligible, try changing the baud rate on your terminal or PC terminal emulator. Try 9600 first. If the problem continues, try each of the other rates listed above.

## Cabling Problems

A high percentage of network problems are due to faulty cabling. Cabling problems usually result in the failure of a switch to connect to a network, a hub, or the end nodes.

### Connections

All cables attached to the switch should be checked to see that they are properly connected.

If a PC or network device cannot communicate through the switch, check the following:

- The cable and its connection
- The LED that corresponds to the network device

If the PC or network device establishes a connection with the switch (the port LED is on), but does not communicate reliably through the switch, check the cable and the connection.

### Non-standard Cables

Miswired cables may cause numerous network collisions, and can seriously impair network performance. Before connecting cables into your network, you should verify that they comply with the applicable standards. For a list of compatible cables and a description of the pin-outs for each port on the switch (which can be used to confirm the compatibility of unlisted cables), see appendix A, “Cables and Connectors”. Note that the optional 100VG operation requires that all four pairs in a cable function properly.

### Topology

It is important to make sure you have a valid network topology. Common topology faults include excessive cable length and excessive repeater delays between nodes. Refer to the following sources for further topology information:

- **For connecting the Switch 2000 to other switches and hubs:** *HP AdvanceStack Switch 2000 Connectivity Quick Reference* (shipped with all Switch 2000 modules)
- **For network design guidelines:** *An Introduction to Ethernet LAN Switches* and *Designing Switched Networks,* both of which are included on the CD shipped with your switch.

- **For physical layer topology guidelines:**
  *Designing HP AdvanceStack Workgroup Networks* available on the CD shipped with your switch.

## 100VG Connection Problems

If you are having trouble with a connection between a 100VG end node and a two-port 100VG module installed in the Switch 2000, try the following:

1. Configure the 100VG port in the module to Master (MAC).
2. If the connection still does not operate, use HPVGSET on the end node to set the 10/100 NIC on the end node to 100 mode.

# 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 AdvanceStack Assistant. Refer to “Diagnosing with LEDs” earlier in this chapter for information on using LEDs to identify unusual network activity.

**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 7-21.)

# Diagnostic Tests

If you believe that the switch is not operating correctly, you can test the switch's circuitry by removing, then reinstalling the switch's power cord.

This procedure power-cycles the switch and executes the switch self-test. If the Fault LED stays on, the switch may have failed its self-test. See "Diagnosing with the LEDs" earlier in this chapter to interpret the LED display.

## Testing Twisted-Pair Cabling

The twisted-pair cable attached to 10Base-T ports on the switch must be compatible with the IEEE 802.3 10Base-T standard for Cat. 3 cable. Similarly, the twisted-pair cable attached to 100Base-T ports on the switch must be compatible with the IEEE 802.3u 100Base-TX standard for Cat. 5 cable. To verify that your cable is compatible with this standard, use a qualified cable test device. HP also offers a wire testing service. Contact your HP-authorized LAN dealer or your local HP sales office for more information. Refer also to "Recommended Cables" on page A-2.

Note that the optional 100VG operation requires that all four pairs in a cable function properly.

## Testing End-to-End Network Communications

Both the switch and the cabling can be tested by running an end-to-end communications test — a test that sends known data from one network device to another through the switch — such that you can verify that the data was correctly transmitted between the devices. For example, if you have two PCs on the network that have HP LAN adapter cards, you can use the "Link Test" option from the card's test program to verify the entire communication path between the two PCs.

See your LAN adapter card's manual for information on running an end-to-end communication test.

## Testing Switch-to-Device Network Communications

You can do the following communication tests to verify that the network is operating correctly between the switch and any connected device that can respond correctly to the test.

- Link Test —a physical layer test that sends IEEE 802.2 test packets to any device identified by its MAC address
- Ping Test—a network layer test used on IP networks that sends test packets to any device identified by its IP address
- IPX Ping Test—a network layer test used on IPX networks that sends test packets to any device identified by its IPX address

These tests can also be done from an SNMP network management station running a program that can manage the switch; for example, HP AdvanceStack Assistant.

# Customer Support Services

Hewlett-Packard offers switch support 24 hours a day, seven days a week through the use of automated electronic services including:

- World Wide Web
- Hewlett-Packard FTP Library Service on the Internet
- CompuServ
- Hewlett-Packard BBS
- HP FIRST FAX Retrieval Service
- HP Network Phone-In Support (NPS)

These services are described on the card at the front of this manual.

Your reseller can also provide you with assistance, both with services that they offer and with services offered by Hewlett-Packard.

# Cables and Connectors

- Recommended Cables
- Twisted-Pair Cable/Connector Pin-Outs
- Twisted-Pair Cable Pin Assignments
- RS-232 Connector and Cable Pin-Out

This appendix lists cables that have been tested and verified for use with the Switch 2000. It also includes minimum pin-out information so, if you wish to use an unlisted cable, you can verify that the cables used in your installation are correctly wired. Note that each pin-out diagram does not necessarily match the pin-out for the corresponding HP cable, but cables manufactured to follow the minimum pin-out will function correctly.

**Note**

Incorrectly wired cabling is the most common cause of problems for LAN communications. HP recommends that you work with a qualified LAN cable installer for assistance with your cabling requirements.

# Recommended Cables

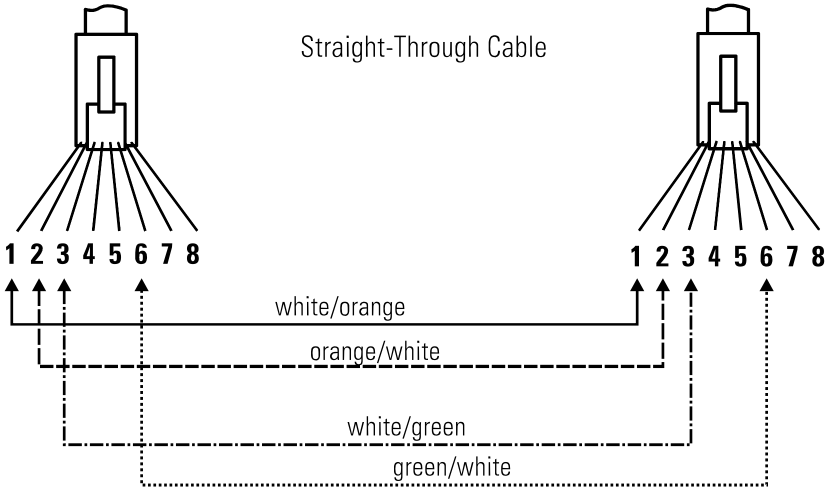
| Cable Function | Port Type on PC, or Modem | Cable Type | Specification or HP Product Number |
|---|---|---|---|
| **Network connections to the switch:** | | | |
| module-based or transceiver-based RJ-45 connection from switch to networked device | — | Twisted-pair "straight-through" cable | Hewlett-Packard recommends category 5 or better, four-pair, 100 ohm unshielded twisted-pair (UTP) cable. (Category 5 cable is required for 100Base-T Twisted-Pair connections.) |
| Transceiver-based SC fiber-optic connection from switch to networked devices | — | Multimode Fiber-Optic cable | 1300nm wavelength cable conforming to the ISO/IEC 793-2 type B1 and ITU-T G.652 standards |
| **Console PC connection to the switch's Console RS-232 port:** | | | |
| Connecting the PC directly to the switch's Console RS-232 port | 9-pin male | RS-232-C 9-pin female to 9-pin female null modem or "crossover" cable | RS-232-C cable provided with the switch (HP p/n 5182-4794) |
| | 25-pin male | RS-232-C 9-pin female to 25-pin female null modem or "crossover" cable | HP 24542H |
| Connecting a modem to the switch's Console RS-232 port | 25-pin female | RS-232-C 9-pin female to 25-pin male standard modem or "straight-through" cable | HP 24542M |

You can contact your HP-authorized dealer or (in the U.S.A.) call HP at 1-800-538-8787 to order these parts.

# Twisted-Pair Cable/Connector Pin-Outs

## Twisted-Pair Cable from Switch-Based MDI-X Module or Transceiver to an MDI Networked Device

To connect PCs or other MDI network devices to an MDI-X port on the switch, use a "straight-through" cable. The twisted-pair wires must be twisted through the entire length of the cable. The wiring sequence must conform to AT&T 258A (not USOC). See "Twisted-Pair Cable Pin Assignments" on page A-6 for a listing of the signals used on each pin.



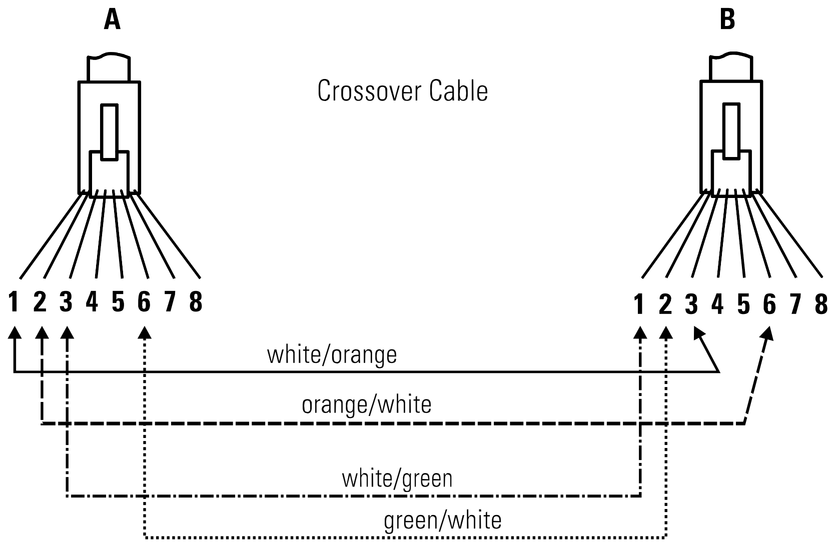
**Note**

Pins 1 and 2 *must* be wired to a twisted pair.
Pins 3 and 6 *must* be wired to a twisted pair.

Pins 4, 5, 7, and 8 are not used in this application, although they may be wired in the cable.

## Twisted-Pair Cable from Switch-Based MDI-X Module to an MDI-X Hub Port

To connect an MDI-X port on a hub to an MDI-X port on the switch, use a "crossover" cable. The twisted-pair wires must be twisted through the entire length of the cable. The wiring sequence must conform to AT&T 258A (not USOC). See "Twisted-Pair Cable Pin Assignments" on page A-6 for a listing of the signals used on each pin.



**Note**

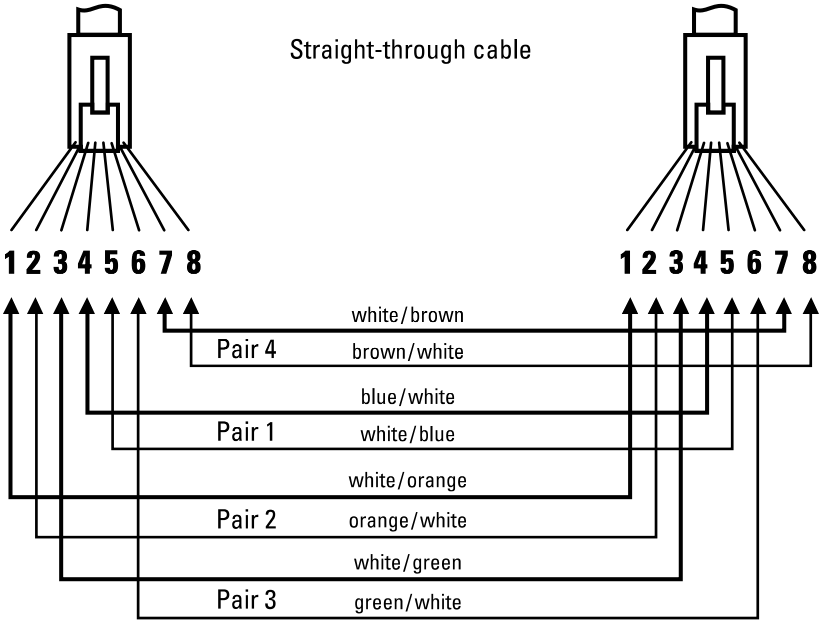
Pins 1 and 2 on connector "A" *must* be wired as a twisted pair to pins 3 and 6 on connector "B".
Pins 3 and 6 on connector "A" *must* be wired as a twisted pair to pins 1 and 2 on connector "B".

Pins 4, 5, 7, and 8 are not used in this application, although they may be wired in the cable.

## Twisted-Pair Cable for HP 100VG LAN Ports

To connect a server or other devices to the 100VG LAN ports, use a “straight-through” 4-pair twisted-pair cable. The twisted-pair wires must be twisted through the entire length of the cable.

The illustration below shows the RJ-45 pin connections, color code, and pair configuration for an HP 100VG LAN cable (unbundled) that conforms to the EIA/TIA 568B wiring standard for a straight-through cable.



**Note**

Pins 1 and 2 *must* be wired to a twisted pair.
Pins 3 and 6 *must* be wired to a twisted pair.
Pins 4 and 5 *must* be wired to a twisted pair
Pins 7 and 8 *must* be wired to a twisted pair.

# Twisted-Pair Cable Pin Assignments

## Twisted-Pair Straight-Through Cable for a 10/100Base-T Connection From the Switch to a Networked Device

| **Switch End (MDI-X)** | | | **End Node (NIC or Transceiver) or Other MDI Port** | |
|---|---|---|---|---|
| **Signal** | **Pins** | | **Pins** | **Signal** |
| (receive +) | 1 | ← | 1 | (transmit +) |
| (receive –) | 2 | ← | 2 | (transmit –) |
| (transmit +) | 3 | → | 3 | (receive +) |
| (transmit –) | 6 | → | 6 | (receive –) |

## Twisted-Pair Crossover Cable for Module-Based 10/100Base-T Connection from the Switch to an MDI-X Port

| **Switch End (MDI-X)** | | | **Switch Port or Other MDI-X Port** | |
|---|---|---|---|---|
| **Signal** | **Pins** | | **Pins** | **Signal** |
| (receive +) | 1 | ← | 3 | (transmit +) |
| (receive –) | 2 | ← | 6 | (transmit –) |
| (transmit +) | 3 | → | 1 | (receive +) |
| (transmit –) | 6 | → | 2 | (receive –) |

# RS-232 Connector and Cable Pin-Outs

The switch's Console RS-232 connector is wired as if it is a terminal (DTE), ready to be connected to a modem (DCE). The switch includes a null modem cable that can be used to directly connect a PC to be used as the console. To connect a modem to the switch, use a standard RS-232-C modem cable.

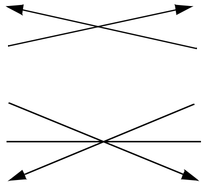
This section provides pin assignment information for the cables you can use on the RS-232 port.

## Pin-Out for Switch's RS-232 Port Connector

| PIN | US | CCITT | DIN |
|---|---|---|---|
| 1 | DCD | 109 | M5 |
| 2 | Rx | 104 | D2 |
| 3 | Tx | 103 | D1 |
| 4 | DTR | 108 | S1 |
| 5 | GND | 102 | – |
| 6 | DSR | 107 | M1 |
| 7 | RTS | 105 | S2 |
| 8 | CTS | 106 | M2 |
| 9 | RI | 125 | M3 |

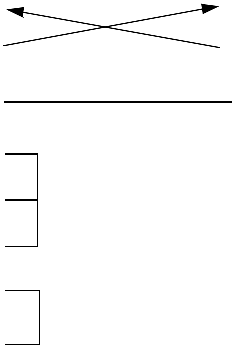
## RS-232-C “Null Modem” Cable

This cable type is supplied with the switch for connection to a PC having a 9-pin connector.



| **PC End**<br>**9-pin male** | **Switch End**<br>**9-pin male** | |
|---|---|---|
| 1 | 1 | DCD |
| 2 | 2 | Rx |
| 3 | 3 | Tx |
| 4 | 4 | DTR |
| 5 | 5 | GND |
| 6 | 6 | DSR |
| 7 | 7 | RTS |
| 8 | 8 | CTS |
| 9 | 9 | RI |

## Minimum Cable Pin-out for Direct Console Connection



| **PC End**<br>**9-pin male** | **Switch End**<br>**9-pin male** | |
|---|---|---|
| 2 | 2 | Rx |
| 3 | 3 | Tx |
| 5 | 5 | GND |
| 1 | | |
| 4 | | |
| 6 | | |
| 7 | | |
| 8 | | |

## RS-232 Modem Cable

| **Modem** | | | |
|---|---|---|---|
| **(DCE) End** | | **Switch End** | |
| **25-pin male** | | **9-pin male** | **Signal** |
| 2 | ← | 3 | Tx |
| 3 | → | 2 | Rx |
| 4 | ← | 7 | RTS |
| 5 | → | 8 | CTS |
| 6 | → | 6 | DSR |
| 7 | — | 5 | GND |
| 8 | → | 1 | CD OR DCD |
| 20 | ← | 4 | DTR |
| 22 | → | 9 | RI |
| 23 | ← | | DRS—typically on V.24 (European) modems (not connected) |

# Specifications

## Physical

| | |
|---|---|
| **Width:** | 44 cm (17.3 in) |
| **Depth:** | 30 cm (11.8 in) |
| **Height:** | 18 cm (7.0 in) |
| **Weight (without Modules or RPS:** | 7.86 kg (17.3 lbs) |

## Electrical

| | | |
|---|---|---|
| **AC voltage:** | 100 - 127 volts | 200-240 volts |
| **Maximum current:** | 2.5A max | 1.5A max |
| **Frequency range:** | 50/60 Hz | 50/60 Hz |

## Environmental

| | **Operating** | **Non-Operating** |
|---|---|---|
| **Temperature:** | 0°C to 55°C (32°F to 131°F) | -40°C to 70°C (-40°F to 158°F) |
| **Relative humidity: (non-condensing)** | 15% to 95% at 40°C (104°F) | 15% to 90% at 65°C (149°F) |
| **Maximum altitude:** | 4.6 km (15,000 ft) | 4.6 km (15,000 ft) |

## Connectors

The RS-232-C console port conforms to V.22 bis.

## Electromagnetic

**Emissions:** FCC part 15 Class A
EN 55022 / CISPR-22 Class A
VCCI Level I

Complies with Canadian EMC Class A requirements.

**Immunity:** See the Declaration of Conformity for details at the end of the Regulatory Statements in this guide.

## Safety

EN60950 (1992) + A1, A2 / IEC950: 1991 + A1, A2
UL 1950
CSA 950
NOM-019-SCFI-1993

# Sample Console Configurations

## Windows 3.1 Terminal Application

You can use a PC with the Windows 3.1 Terminal Application for console management access to the switch. This section provides an example of the configuration settings to use with the Windows 3.1 Terminal Application.

### Option Settings:

- Terminal Emulation: DEC VT-100 (ANSI)
- Terminal Preferences:
  - Terminal Modes:
    - Line-Wrap: On
    - Sound: On
  - CR > CR/LF: No
  - Use Function, Arrow, Ctrl keys for Windows:  NO

### Communications:

- 9600 Baud or 19.2 baud recommended
- No Parity
- 8 bits
- 1 stop bit
- Xon/Xoff
- Carrier Detect

# Procomm Plus V2.01

## Terminal Options

- Terminal Emulation: VT-100
- Duplex: FULL
- Software Flow Control: Xon/Xoff
- Hardware Flow Control: Off
- Screen Scroll: ON
- CR Translation: CR
- BS Translation: NON-DESTRUCTIVE
- Break Length: 350
- Enquiry: CIS B
- ANSI 7 or 8 bit command: 7 bit
- ASCII Protocol Options
- Echo Locally: NO
- Expand Blank Lines: NO
- Expand Tabs: YES
- Clear pacing: 1 ms
- Line pacing: 1
- Pace character: 0
- Strip 8 bit: NO
- ASCII download timeout: 10
- CR translation (upload): NONE
- LF translation (upload): NONE
- CR translation (download): NONE
- LF translation (download): NONE

# Other Terminal Emulators

For other communication programs, use the following table as a configuration guide:

| Option | Setting |
|---|---|
| Baud rate | 300, 600, 1200, 2400, 9600, 19200, or 38400.<br>(9600 or 19200 recommended) |
| Parity | None |
| Data bits and stop bits | 8, 1 |
| Autobaud upon break | On |
| Handshaking | None |
| Terminal emulation | VT100. For Windows, disable the “Use Function, Arrow, and Ctrl Keys for Windows” option, located in the Terminal Preference menu. |
| Duplex | Full |
| Soft flow control (XON/XOFF) | On (input and output) |
| Hard flow control (RTS/CTS) | Off |
| Line wrap | On |
| Screen scroll | On |
| CR translation | CR |
| Backspace (BS) translation | Destructive |
| Break length (milliseconds) | 350 |
| Enquiry (ENQ) | Off |
| EGA/VGA true underline | Off |
| Terminal width | 80 |
| ANSI 7 or 8 bit commands | 7 |

# Switch Reference

## Front of Switch

All LEDs used by the Switch 2000 are on the front panel. During the power-on or reset cycles, all LEDs are on.

### Switch Status LEDs

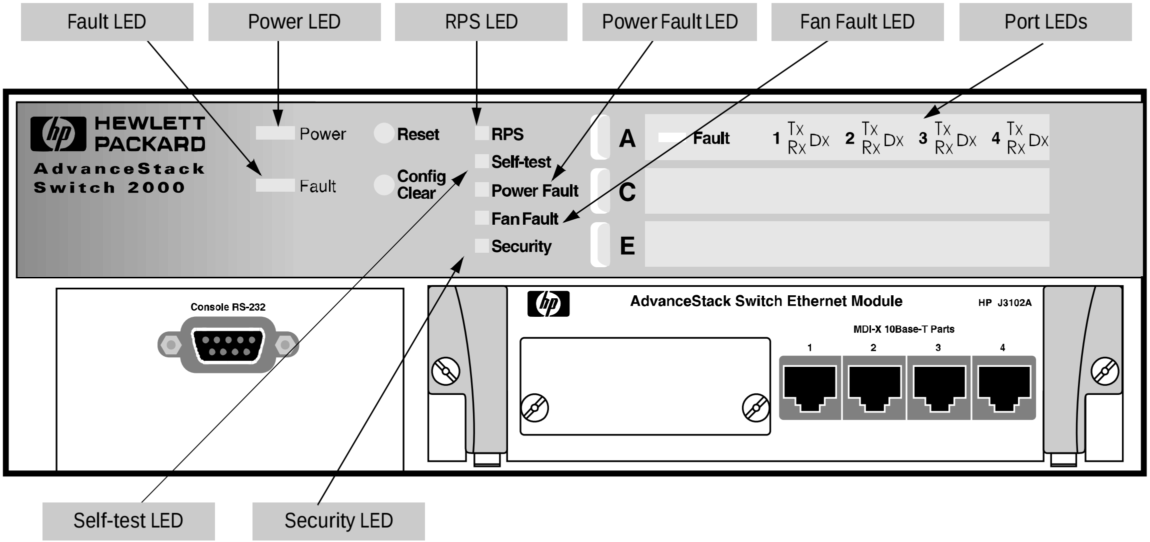


**Figure D-1. Example of Status LEDs for the Switch 2000**

| LED | State | Meaning of LED |
|---|---|---|
| **Power** (green) | on | The switch is receiving power from the main power supply and/or from the optional RPS (redundant power supply). |
| | off | The switch is not receiving power. See chapter 9, “Troubleshooting”. |
| **Fault** (orange) | on (steady) | Either the switch hardware has failed the self-test or a software error has occurred and auto-reboot is off. In this case, push the Reset button. See chapter 9, “Troubleshooting”. |
| | flashing | The switch is operable, but a fault condition has occurred in the switch, an installed module, a fan, or a redundant power supply (RPS—if installed). The corresponding fault LED for the affected component will flash simultaneously. Refer to chapter 9, “Troubleshooting”. |
| **RPS** (green) | on | An (optional) Redundant Power Supply (RPS) is connected and functioning properly. |
| | off | No RPS is connected to the switch, or the RPS has failed. See chapter 9, “Troubleshooting”. |
| **Self-test** (green) | off | Normal operation, except as described below. |
| | on (steady) | Power-on or reset self-test. During this time the Fault LED is also on and the switch is inoperable. |
| | flashing | Indicates one of the following:<br>• A self-test failure has occurred, but the switch remains partially operable.<br>• The Config Clear button is being pressed during a reset. Release the button. (Refer to “Reset and Config Clear Buttons” on page D-4.) |
| **Power Fault** (orange) | flashing | An RPS (redundant power supply) is present and either the RPS or the main power supply is not operating properly. Flashes simultaneously with the switch's Fault LED. Refer to chapter 9, “Troubleshooting”. |
| **Fan Fault** (orange) | flashing | One or both ventilation fans are not operating properly. Flashes simultaneously with the switch's Fault LED. Refer to chapter 9, “Troubleshooting”. |
| **Security** (orange) | flashing | Either an SNMP Authentication failure or a traffic filter violation has occurred. Refer to chapter 9, “Troubleshooting”. |

## Slot and Port Status LEDs

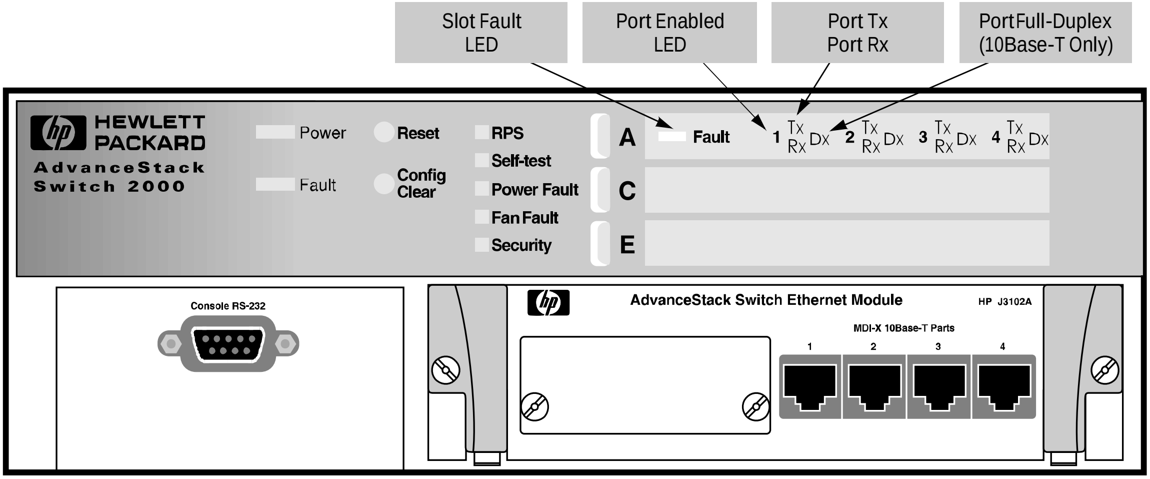


**Figure D-2. Example of Slot and Port Status LEDs for a 10Base-T Module in the Switch 2000**

| LED | State | Meaning of LED |
|---|---|---|
| **Fault (slot)**<br>(orange) | rapid flash | A module hot-swap condition is occurring. |
| | slow flashing | Either the indicated slot has failed self-test or an incorrect transceiver (for a J3191A 100Base-T Module or a J3103A 100VG Module) has been installed. For this condition, flashes simultaneously with the switch's Fault and Self-test LEDs. Refer to chapter 9, "Troubleshooting". |
| **1, 2, 3, 4 (port enabled LED)**<br>(green) | on | The indicated port on the indicated module is enabled and the link is operational. |
| **Tx**<br>(green) | on or flashing | The indicated port is transmitting packets. |
| **Rx**<br>(green) | on or flashing | The indicated port is receiving packets. |
| **Dx**<br>(green) | on | The indicated port is enabled and configured for full-duplex operation. |

Reset and Config Clear Buttons

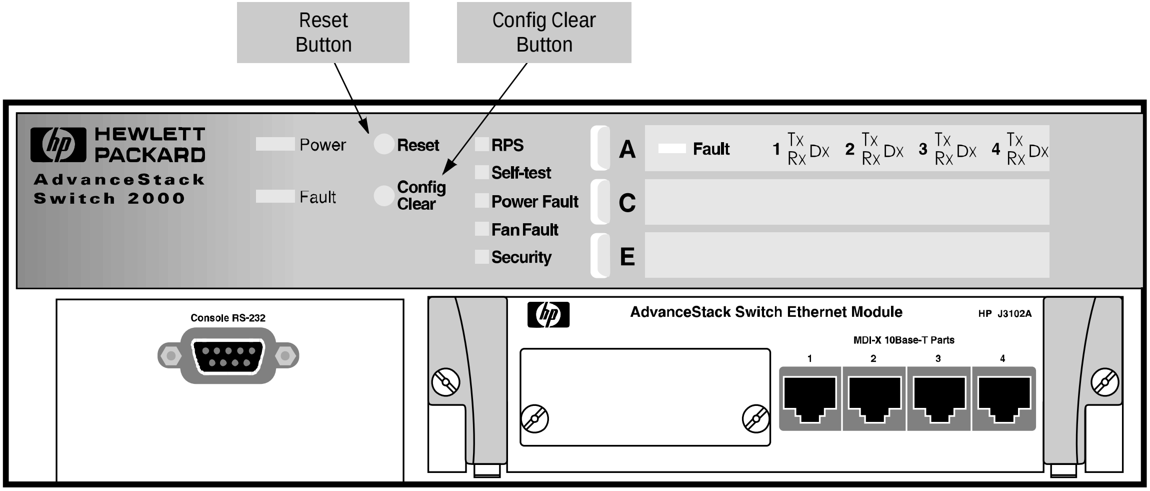


**Figure D-3. Reset and Config Clear Buttons on the Switch 2000**

| Button | Action |
|---|---|
| **Reset** | Performs a software and hardware reset, including a hardware self-test. (This achieves the same result as disconnecting the power from the switch, then reconnecting it.) |
| **Config Clear** | When used as described below, causes the switch to delete the current configuration, and to reboot to a default configuration based on the installed modules and transceivers. This resets the switch to the factory default and is a drastic action that interrupts switch operation and can seriously diminish or even halt network operation. Depending on the current network operating condition, it may be best to avoid a reset until you can schedule system downtime. Some reasons for a reset include:<br>• The switch appears to be malfunctioning, and pressing just the Reset button does not clear the problem.<br>• Several elements in the configuration may be inconsistent with each other and it is more efficient to start with the defaults than to try to adjust individual parameters.<br>Effects of a reset to the factory default:<br>• Clears all passwords.<br>• Configures the switch as a multiport transparent bridge with Bootp enabled. The switch then transmits Bootp requests until either a Bootp reply is received or the retransmission timeout of approximately 1 minute is reached. (If the switch receives a reply from a Bootp server, the switch restarts itself for operation according to the configuration received from the Bootp server. Refer to appendix E, “Bootp Operation”.)<br>• Returns all configuration parameters to their factory default settings. (Turns off the Spanning Tree Protocol.)<br>• Clears the event log.<br>• Runs the system self-test. |
| **To clear the current configuration and reboot the switch:** | |
| 1. | Press and release the Reset button. All LEDs turn on momentarily. |
| 2. | While all LEDs are turned on, press and hold the Config Clear button until the Self-test LED begins flashing, then immediately release the Config Clear button. If a console is connected, you will see the following message when the switch has reset itself to the factory default configuration and rebooted.<br>`Waiting for speed sense. Press enter to continue.` |
| 3. | Press [Enter] to restart the console. |
| **To clear the password(s)** | |
| | Press and release the Config Clear button. |

## Console RS-232 Port

The switch's Console RS-232 port is a standard RS-232 serial link used to connect a Windows-based PC, a terminal, or a modem. (For pinouts, refer to appendix A, Cables and Connectors.)

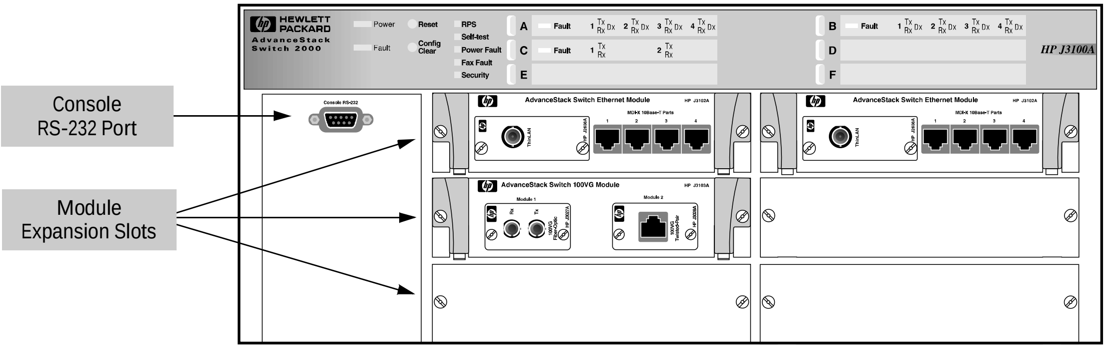


**Figure D-4. Front Panel of the Switch 2000**

## Interface Module Expansion Slots

The Switch 2000 offers six universal port expansion slots, each of which can accept any Hewlett-Packard module designed for the Switch 2000.

# Back of the Switch

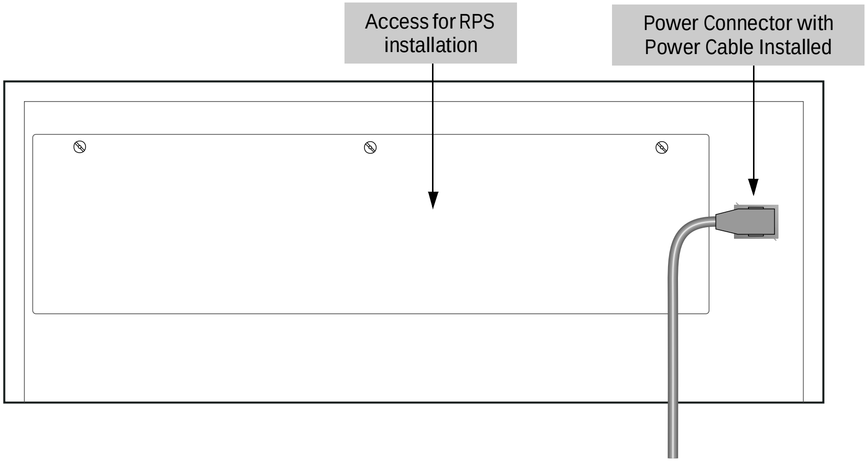

Access for RPS installation
Power Connector with Power Cable Installed

**Figure D-5. Back Panel of the Switch 2000**

## Power Connector

The Switch 2000 does not have a power switch; it is powered on when the power cord is plugged into the power connector. The switch's power supply automatically adjusts to any AC power source between 90 and 240 volts. There are no voltage or frequency range settings needed.

## HP J3136 AdvanceStack Switch 2000 Redundant Power Supply (RPS—Optional)

The RPS is an optional power supply you can connect to your Switch 2000 for backup power in case the main power supply fails. Also, adding an RPS to your switch helps to extend the life of the main power supply because the two power units work together to share the power load. For more on the RPS, refer to “Install the Redundant Power Supply (Optional)” on page 1-5, and to the documentation provided with the RPS.

**Caution**

Power to the Switch 2000 should be off before you install the RPS. For this reason, you should perform an RPS installation only during a scheduled down time, when you can remove power from the switch.

Refer to the documentation provided with the RPS before connecting it to the Switch 2000.

# BOOTP Operation

## Overview

Bootp is used to download configuration data from a Bootp server 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 Bootp server.

**Note**

The Switch 2000 supports only the DHCP (Dynamic Host Configuration Protocol) implementations that are backwards compatible with Bootp.

## The Bootp Process

Whenever the switch reboots with the IP Config parameter set to Use Bootp (the default), Bootp requests are broadcast on all local networks. When the Bootp server receives the 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.

# 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:

```
j3100switch:\
   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:

```
j3100switch:\
   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:*

| | |
|---|---|
| j3100switch | 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 HP AdvanceStack Switch 2000, set this to **ether** (for Ethernet). *This tag must precede the* ha *tag*. |
| 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 HP AdvanceStack Switch 2000, set this parameter to **rfc1048**. |

# Configuring Bootp

In its default configuration, the switch is configured for 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 Bootp operation.

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

**To configure the switch or a VLAN for Bootp:**

1. In the Main Menu, select `Configuration` .
2. In the Configuration screen select `Internet (IP) Service`.
3. Press [E] (for Edit mode), then use [↓] to move the cursor to the `IP Config` parameter field.
4. Use the Space bar to select the `Use Bootp` option for the `IP Config` parameter. (This disables access to the IP Address, Subnet Mask, and Gateway parameters.)
5. Press [Enter] to exit from edit mode, then press [S] to save the configuration change.

When you reboot the switch with Bootp enabled, it will do one of the following:

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

# MAC Address Management

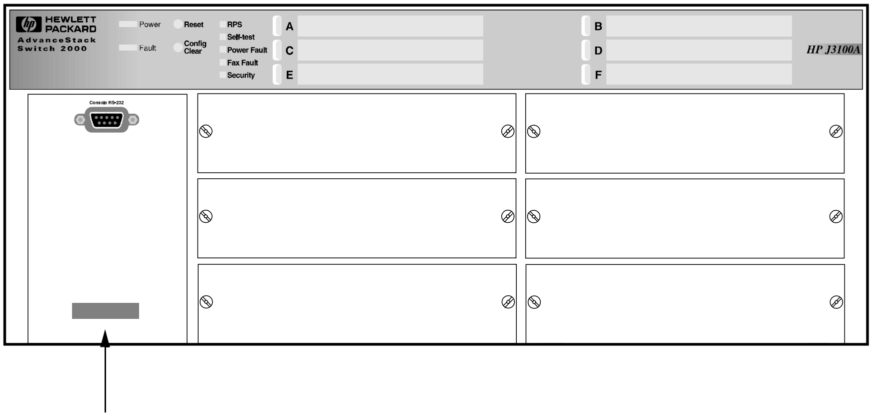
## Overview

The Switch 2000 assigns MAC addresses in the following three areas:

- Default MAC address assigned at the factory
- Automatically assigned MAC address(es) corresponding to any VLANs you configure in the switch
- The Spanning Tree Protocol (STP) uses either the default MAC address for the switch or, if VLANs are configured, the MAC addresses automatically assigned to the VLANs.

# Switch (Default) MAC Address

A default MAC address is assigned to each Switch 2000 at the factory. This address is on the label below the Console RS-232 port (shown below):



Label Showing
Default MAC Address

**Figure F-1. Location of the Default MAC Address Assigned to the Switch**

If there are no VLANs configured on the Switch 2000, then the factory-assigned MAC address is the same for all ports on the switch.

### To display the MAC address assigned to a port:

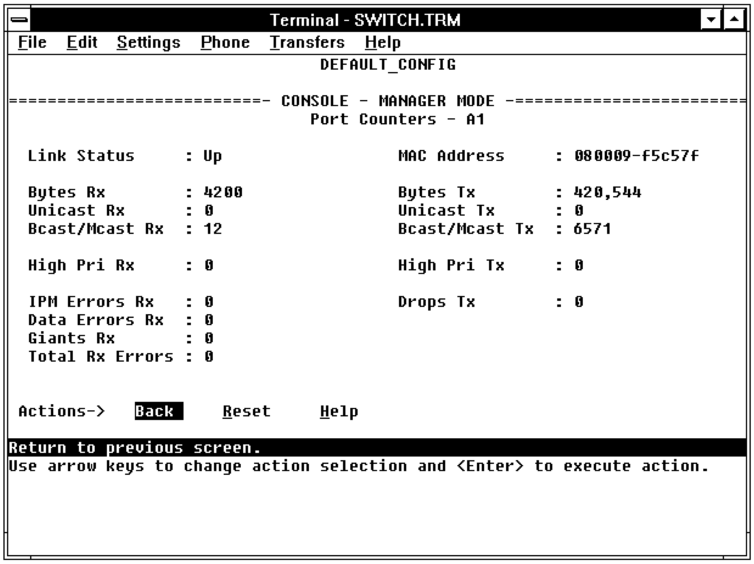
1. Select `Status and Counters` from the Main Menu.
2. Select `Port Counters` in the Statistics menu.
3. Select the desired port.
4. Select the `Show details` option to display the port counter details for the selected port. Included will be the MAC address assigned to that port. If VLANs are configured, refer to “VLAN MAC Address” on page F-3.

# VLAN MAC Addresses

If you add VLANs to the Switch 2000, each VLAN is automatically assigned a different MAC address. All ports in a particular VLAN will have the same MAC address. To determine the MAC address assigned to a particular VLAN, display the port data for any port assigned to that VLAN.

**To display the MAC address and other data for a selected port:**

1. From the Main Menu, select `Status and Counters`.
2. Display the `Port Counters` screen.
3. Select a port that is assigned to the VLAN for which you want to determine the corresponding MAC address.
4. Select the `Show details` option to display the port counter details for the selected port. Included will be the MAC address assigned to that port (and the corresponding VLAN).



```
                                   DEFAULT_CONFIG

==========================- CONSOLE - MANAGER MODE -=========================
                                 Port Counters - A1

  Link Status     : Up                    MAC Address     : 080009-f5c57f

  Bytes Rx        : 4200                  Bytes Tx        : 420,544
  Unicast Rx      : 0                     Unicast Tx      : 0
  Bcast/Mcast Rx  : 12                    Bcast/Mcast Tx  : 6571

  High Pri Rx     : 0                     High Pri Tx     : 0

  IPM Errors Rx   : 0                     Drops Tx        : 0
  Data Errors Rx  : 0
  Giants Rx       : 0
  Total Rx Errors : 0


 Actions->   Back     Reset     Help

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

**Figure F-2. Example of the Port Counter Details for a Selected Port**

# MAC Addresses (for Spanning Tree Operation)

When no VLANs are configured, STP uses the MAC address assigned to the switch. (This is the MAC address printed on the label on the front of the switch.) When VLANs are configured, STP must be configured separately for each VLAN. In this case, the MAC address assigned to each instance of STP is the MAC address assigned to the corresponding VLAN. These addresses appear in the Spanning Tree Information screen . Refer to the "Switch (Default) MAC Address" on page F-2, or "VLAN MAC Addresses" on page F-3.)

# Safety and Regulatory Statements

## Safety Information

### Safety Symbols.

| | |
|---|---|
| ⚠ | Documentation reference symbol. If the product is marked with this symbol, refer to the product documentation to get more information about the product. |
| **WARNING** | A WARNING in the manual denotes a hazard that can cause injury or death. |
| **CAUTION** | A CAUTION in the manual denotes a hazard that can damage equipment. |

Do not proceed beyond a WARNING or CAUTION notice until you have understood the hazardous conditions and have taken appropriate steps.

### Grounding.

These are safety class I products and have protective earthing terminals. There must be an uninterruptible safety earth ground from the main power source to the product's input wiring terminals, power cord, or supplied power cord set. Whenever it is likely that the protection has been impaired, disconnect the power cord until the ground has been restored.

For LAN cable grounding:

- If your LAN covers an area served by more than one power distribution system, be sure their safety grounds are securely interconnected.
- LAN cables may occasionally be subject to hazardous transient voltages (such as lightning or disturbances in the electrical utilities power grid). Handle exposed metal components of the network with caution.

### Servicing.

There are no user-serviceable parts inside these products. Any servicing, adjustment, maintenance, or repair must be performed only by service-trained personnel.

These products do not have a power switch; they are powered on when the power cord is plugged in.

# Informations concernant la sécurité

## Symboles de sécurité

| | |
|---|---|
| ⚠ | Symbole de référence à la documentation. Si le produit est marqué de ce symbole, reportez-vous à la documentation du produit afin d'obtenir des informations plus détaillées. |
| **WARNING** | Dans la documentation, un WARNING indique un danger susceptible d'entraîner des dommages corporels ou la mort. |
| **CAUTION** | Un texte de mise en garde intitulé CAUTION indique un danger susceptible de causer des dommages à l'équipement. |
| | Ne continuez pas au-delà d'une rubrique WARNING ou CAUTION avant d'avoir bien compris les conditions présentant un danger et pris les mesures appropriées. |

Cet appareil est un produit de classe I et possède une borne de mise à la terre. La source d'alimentation principale doit être munie d'une prise de terre de sécurité installée aux bornes du câblage d'entrée, sur le cordon d'alimentation ou le cordon de raccordement fourni avec le produit. Lorsque cette protection semble avoir été endommagée, débrancher le cordon d'alimentation jusqu'à ce que la mise à la terre ait été réparée.

Mise à la terre du câble de réseau local:

- si votre réseau local s'étend sur une zone desservie par plus d'un système de distribution de puissance, assurez-vous que les prises de terre de sécurité soient convenablement interconnectées.
- Les câbles de réseaux locaux peuvent occasionnellement être soumis à des surtensions transitoires dangereuses (telles que la foudre ou des perturbations dans le réseau d'alimentation public). Manipulez les composants métalliques du réseau avec précautions.

Aucune pièce contenue à l'intérieur de ce produit ne peut être réparée par l'utilisateur. Tout dépannage, réglage, entretien ou réparation devra être confié exclusivement à un personnel qualifié.

Cet appareil ne comporte pas de commutateur principal ; la mise sous tension est effectuée par branchement du cordon d'alimentation.

# Hinweise zur Sicherheit

### Sicherheitssymbole.

⚠ Symbol für Dokumentationsverweis. Wenn das Produkt mit diesem Symbol markiert ist, schlagen Sie bitte in der Produktdokumentation nach, um mehr Informationen über das Produkt zu erhalten.

**WARNING** Eine WARNING in der Dokumentation symbolisiert eine Gefahr, die Verletzungen oder sogar Todesfälle verursachen kann.

**CAUTION** CAUTION in der Dokumentation symbolisiert eine Gefahr, die das Gerät beschädigen kann.

Fahren Sie nach dem Hinweis WARNING oder CAUTION erst fort, nachdem Sie den Gefahrenzustand verstanden und die entsprechenden Maßnahmen ergriffen haben.

Dies ist ein Gerät der Sicherheitsklasse I und verfügt über einen schützenden Erdungsterminal. Der Betrieb des Geräts erfordert eine ununterbrochene Sicherheitserdung von der Hauptstromquelle zu den Geräteingabeterminals, den Netzkabeln oder dem mit Strom belieferten Netzkabelsatz voraus. Sobald Grund zur Annahme besteht, daß der Schutz beeinträchtigt worden ist, das Netzkabel aus der Wandsteckdose herausziehen, bis die Erdung wiederhergestellt ist.

Für LAN-Kabelerdung:

- Wenn Ihr LAN ein Gebiet umfaßt, das von mehr als einem Stromverteilungssystem beliefert wird, müssen Sie sich vergewissern, daß die Sicherheitserdungen fest untereinander verbunden sind.
- LAN-Kabel können gelegentlich gefährlichen Übergangsspannungen ausgesetzt werden (beispielsweise durch Blitz oder Störungen in dem Starkstromnetz des Elektrizitätswerks). Bei der Handhabung exponierter Metallbestandteile des Netzwerkes Vorsicht walten lassen.

Dieses Gerät enthält innen keine durch den Benutzer zu wartenden Teile. Wartungs-, Anpassungs-, Instandhaltungs- oder Reparaturarbeiten dürfen nur von geschultem Bedienungspersonal durchgeführt werden.

Dieses Gerät hat keinen Netzschalter; es wird beim Anschließen des Netzkabels eingeschaltet.

# Considerazioni sulla sicurezza

### Simboli di sicurezza.

| | |
|---|---|
| ⚠ | Simbolo di riferimento alla documentazione. Se il prodotto è contrassegnato da questo simbolo, fare riferimento alla documentazione sul prodotto per ulteriori informazioni su di esso. |
| **WARNING** | La dicitura WARNING denota un pericolo che può causare lesioni o morte. |
| **CAUTION** | La dicitura CAUTION denota un pericolo che può danneggiare le attrezzature. |

Non procedere oltre un avviso di WARNING o di CAUTION prima di aver compreso le condizioni di rischio e aver provveduto alle misure del caso.

Questo prodotto è omologato nella classe di sicurezza I ed ha un terminale protettivo di collegamento a terra. Dev’essere installato un collegamento a terra di sicurezza, non interrompibile che vada dalla fonte d’alimentazione principale ai terminali d’entrata, al cavo d’alimentazione oppure al set cavo d’alimentazione fornito con il prodotto. Ogniqualvolta vi sia probabilità di danneggiamento della protezione, disinserite il cavo d’alimentazione fino a quando il collegamento a terra non sia stato ripristinato.

Per la messa a terra dei cavi LAN:

- se la vostra LAN copre un’area servita da più di un sistema di distribuzione elettrica, accertatevi che i collegamenti a terra di sicurezza siano ben collegati fra loro;
- i cavi LAN possono occasionalmente andare soggetti a pericolose tensioni transitorie (ad esempio, provocate da lampi o disturbi nella griglia d’alimentazione della società elettrica); siate cauti nel toccare parti esposte in metallo della rete.

Nessun componente di questo prodotto può essere riparato dall’utente. Qualsiasi lavoro di riparazione, messa a punto, manutenzione o assistenza va effettuato esclusivamente da personale specializzato.

Questo apparato non possiede un commutatore principale; si mette scotto tensione all’inserirsi il cavo d’alimentazione.

# Consideraciones sobre seguridad

### Símbolos de seguridad.

| | |
|---|---|
| ⚠ | Símbolo de referencia a la documentación. Si el producto va marcado con este símbolo, consultar la documentación del producto a fin de obtener mayor información sobre el producto. |
| **WARNING** | Una WARNING en la documentación señala un riesgo que podría resultar en lesiones o la muerte. |
| **CAUTION** | Una CAUTION en la documentación señala un riesgo que podría resultar en averías al equipo. |

No proseguir después de un símbolo de WARNING o CAUTION hasta no haber entendido las condiciones peligrosas y haber tomado las medidas apropiadas.

Este aparato se enmarca dentro de la clase I de seguridad y se encuentra protegido por una borna de puesta a tierra. Es preciso que exista una puesta a tierra continua desde la toma de alimentación eléctrica hasta las bornas de los cables de entrada del aparato, el cable de alimentación o el juego de cable de alimentación suministrado. Si existe la probabilidad de que la protección a tierra haya sufrido desperfectos, desenchufar el cable de alimentación hasta haberse subsanado el problema.

Puesta a tierra del cable de la red local (LAN):

- Si la LAN abarca un área cuyo suministro eléctrico proviene de más de una red de distribución de electricidad, cerciorarse de que las puestas a tierra estén conectadas entre sí de modo seguro.
- Es posible que los cables de la LAN se vean sometidos de vez en cuando a voltajes momentáneos que entrañen peligro (rayos o alteraciones en la red de energía eléctrica). Manejar con precaución los componentes de metal de la LAN que estén al descubierto.

Este aparato no contiene pieza alguna susceptible de reparación por parte del usuario. Todas las reparaciones, ajustes o servicio de mantenimiento debe realizarlos solamente el técnico.

Este producto no tiene interruptor de potencia; se activa cuando se enchufa el cable de alimentación.

# Safety Information

安全性の考慮

安全記号

⚠ マニュアル参照記号。製品にこの記号がついている場合はマニュアルを参照し、注意事項等をご確認ください。

WARNING マニュアル中の「WARNING」は人身事故の原因となる危険を示します。

CAUTION マニュアル中の「CAUTION」は装置破損の原因となる危険を示します。

「WARNING」や「CAUTION」の項は飛ばさないで必ずお読みください。危険性に関する記載事項をよく読み、正しい手順に従った上で次の事項に進んでください。

これは安全性クラス I の製品で保護用接地端子を備えています。主電源から製品の入力配線端子、電源コード、または添付の電源コード・セットまでの間、切れ目のない安全接地が存在することが必要です。もしこの保護回路が損なわれたことが推測されるときは、接地が修復されるまで電源コードを外しておいてください。

LAN ケーブルの接地に関して:

- もし貴社の LAN が複数の配電システムにより電力を受けている領域をカバーしている場合には、それらのシステムの安全接地が確実に相互に結合されていることを確認してください。
- LAN ケーブルは時として危険な過度電圧（例えば雷や、配電設備の電力網での障害）にさらされることがあります。露出した金属部分の取扱いには十分な注意をはらってください。

本製品の内部にはユーザーが修理できる部品はありません。サービス、調整、保守および修理はサービス訓練を受けた専門家におまかせください。

本製品には電源スイッチがありません。電源コードを接続したとき電源入となります。

# Regulatory Statements

## FCC Statement (U.S.A.)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

**VCCI Class 1 (For Japan Only).**

注意

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

## European Community

This equipment complies with CISPR22/EN55022 Class A.

**Note**

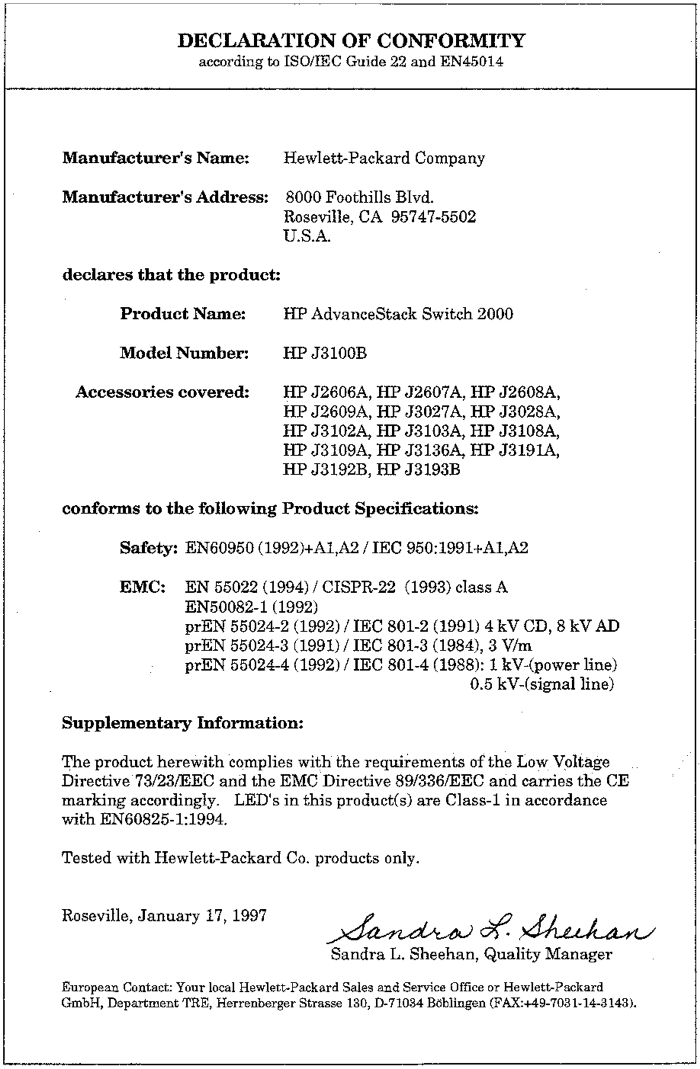
This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

## DOC Statement (Canada)

Complies with Canadian EMC Class A requirements.

# Declaration of Conformity

The following Declaration of Conformity for the HP AdvanceStack Switch 2000 complies with ISO/IEC Guide 22 and EN 45014. The declaration identifies the product and related accessories, the manufacturer's name and address, and the applicable specifications that are recognized in the European community.



**DECLARATION OF CONFORMITY**
according to ISO/IEC Guide 22 and EN45014

**Manufacturer's Name:** Hewlett-Packard Company

**Manufacturer's Address:**
8000 Foothills Blvd.
Roseville, CA 95747-5502
U.S.A.

**declares that the product:**

**Product Name:** HP AdvanceStack Switch 2000

**Model Number:** HP J3100B

**Accessories covered:**
HP J2606A, HP J2607A, HP J2608A,
HP J2609A, HP J3027A, HP J3028A,
HP J3102A, HP J3103A, HP J3108A,
HP J3109A, HP J3136A, HP J3191A,
HP J3192B, HP J3193B

**conforms to the following Product Specifications:**

**Safety:** EN60950 (1992)+A1,A2 / IEC 950:1991+A1,A2

**EMC:**
EN 55022 (1994) / CISPR-22 (1993) class A
EN50082-1 (1992)
prEN 55024-2 (1992) / IEC 801-2 (1991) 4 kV CD, 8 kV AD
prEN 55024-3 (1991) / IEC 801-3 (1984), 3 V/m
prEN 55024-4 (1992) / IEC 801-4 (1988): 1 kV-(power line)
0.5 kV-(signal line)

**Supplementary Information:**

The product herewith complies with the requirements of the Low Voltage Directive 73/23/EEC and the EMC Directive 89/336/EEC and carries the CE marking accordingly. LED's in this product(s) are Class-1 in accordance with EN60825-1:1994.

Tested with Hewlett-Packard Co. products only.

Roseville, January 17, 1997

Sandra L. Sheehan
Sandra L. Sheehan, Quality Manager

European Contact: Your local Hewlett-Packard Sales and Service Office or Hewlett-Packard GmbH, Department TRE, Herrenberger Strasse 130, D-71034 Böblingen (FAX:+49-7031-14-3143).

# Index

HEWLETT®
PACKARD

Technical information in this document is subject to change without notice.

Printed in Singapore 3/97

Manual Part Number
5966-5212