

---

# HP ProCurve Switch 212M and 224M

## Management and Configuration Guide

---

HP Networking



*For world-wide support on all  
HP Network Connectivity Products  
visit our web site at:*

[http://www.hp.com/go/network\\_city](http://www.hp.com/go/network_city)

Less Work, More Network



---

# HP ProCurve Switch 212M and 224M

---

## Management and Configuration Guide

© Copyright 1998 Hewlett-Packard Company  
All Rights Reserved.

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

### **Publication Number**

5967-2146  
June 1998

### **Applicable Products**

HP ProCurve Switch 212M (HP J3298A)  
HP ProCurve Switch 224M (HP J3299A)

### **Disclaimer**

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

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

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

### **Warranty**

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

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

---

Hewlett-Packard Company  
8000 Foothills Boulevard, m/s 5552  
Roseville, California 95747-5552  
[http://www.hp.com/go/network\\_city](http://www.hp.com/go/network_city)

---

# Contents

## 1 Selecting a Management Interface

<b>Understanding Management Interfaces</b> .....	1-1
<b>Advantages of Using the HP Web Browser Interface</b> .....	1-2
<b>Advantages of Using the Switch Console</b> .....	1-3
<b>HP TopTools for Hubs &amp; Switches</b> .....	1-4

## 2 Configuring an IP Address on the Switch

<b>Methods for Configuring an IP Address and Subnet Mask</b> .....	2-2
<b>Manually Configuring an IP Address</b> .....	2-2
Where To Go From Here .....	2-4

## 3 Using the HP Web Browser Interface

<b>Overview</b> .....	3-1
<b>Web Browser Interface Requirements</b> .....	3-2
<b>Starting an HP Web Browser Interface Session</b> .....	3-3
Using a Standalone Web Browser in a PC or UNIX Workstation . . . .	3-3
Using HP TopTools for Hubs & Switches .....	3-4
<b>Tasks for Your First HP Web Browser Interface Session</b> .....	3-6
Viewing the “First Time Install” Window .....	3-6
Creating User Names and Passwords in the Web Browser Interface	3-8
Online Help for the HP Web Browser Interface .....	3-10
<b>The Web Browser Interface Screen Layout</b> .....	3-12
The Overview Window .....	3-12
The Port Utilization and Status Displays .....	3-14
The Alert Log .....	3-16
The Tab Bar .....	3-21
Setting Fault Detection Policy .....	3-25

<b>4</b>	<b>Using the Switch Console</b>	
	<b>Overview</b>	4-1
	<b>Starting and Ending a Console Session</b>	4-2
	How To Start a Console Session:	4-2
	How To End a Console Session:	4-3
	<b>Main Menu Features</b>	4-4
	<b>Screen Structure and Navigation</b>	4-6
	<b>Using Password Security</b>	4-9
	To set Manager and Operator passwords:	4-10
	<b>Rebooting the Switch</b>	4-12
	<b>Using the Command Prompt</b>	4-14
<b>5</b>	<b>Using HP TopTools To Monitor and Manage the Switch</b>	
	<b>Overview</b>	5-1
	<b>SNMP Management Features</b>	5-2
	<b>SNMP Configuration Process</b>	5-3
	<b>Advanced Management: RMON and HP Extended RMON Support</b>	5-4
	RMON	5-4
	Extended RMON	5-4
<b>6</b>	<b>Configuring the Switch</b>	
	<b>Overview</b>	6-1
	Configuration Features	6-2
	<b>Support/Management URLs Feature</b>	6-3
	Support URL	6-3
	Management Server URL	6-4
	<b>IP Configuration</b>	6-5
	Configuring IP Address from the Web Browser Interface	6-6
	Configuring IP Address from the Switch Console	6-8
	How IP Addressing Affects Switch Operation	6-9
	DHCP/Bootp Operation	6-10
	Globally Assigned IP Network Addresses	6-14

<b>SNMP Communities</b> .....	6-15
Configuring SNMP Communities from the Switch Console .....	6-15
<b>Trap Receivers</b> .....	6-18
<b>Console/Serial Link</b> .....	6-20
Using the Switch Console To Configure the Console/Serial Link ...	6-21
<b>System Information</b> .....	6-22
Configuring System Parameters from the Web Browser Interface .	6-22
Configuring System Information from the Console .....	6-23
<b>Port Settings</b> .....	6-24
Configuring Port Parameters from the Web Browser Interface ....	6-26
Configuring Port Parameters from the Switch Console .....	6-27
<b>Network Monitoring Port Features</b> .....	6-28
Configuring Port Monitoring from the Web Browser Interface ....	6-28
Configuring Port Monitoring from the Switch Console .....	6-29
<b>Spanning Tree Protocol (STP)</b> .....	6-30
Enabling STP from the Web Browser Interface .....	6-31
Using the Switch Console To Configure STP .....	6-32
How STP Operates .....	6-33
<b>IP Multicast (IGMP) Service Features—Multimedia Traffic Control</b>	
6-34	
Configuring IGMP from the Web Browser Interface .....	6-35
Using the Switch Console To Configure IGMP .....	6-36
How IGMP Operates .....	6-38
Special Case IGMP Configuration .....	6-42

## **7 Monitoring and Analyzing Switch Operation**

<b>Overview</b> .....	7-1
<b>Switch Console Status and Counters Menu</b> .....	7-2
<b>General System Information</b> .....	7-3
<b>Switch Management Address Information</b> .....	7-4
<b>Port Status</b> .....	7-5
Displaying Port Status from the Web Browser Interface .....	7-5
Displaying Port Status from the Switch Console .....	7-6

<b>Port Counters</b> .....	7-7
Displaying Port Counters from the Web Browser Interface .....	7-8
Displaying Port Counters from the Console Interface .....	7-9
<b>Address Table</b> .....	7-11
<b>Port Address Table</b> .....	7-12
<b>Spanning Tree (STP) Information</b> .....	7-14
<b>IP Multicast (IGMP) Status</b> .....	7-16

## **8 Troubleshooting**

<b>Troubleshooting Approaches</b> .....	8-2
<b>Web Browser Interface or Switch Console Access Problems</b> .....	8-3
<b>Unusual Network Activity</b> .....	8-4
<b>Using the Event Log to Identify Problem Sources</b> .....	8-6
<b>Diagnostics</b> .....	8-9
Ping and Link Tests .....	8-9
The Configuration File .....	8-13
Using the Command Prompt .....	8-15
<b>Restoring the Factory Default Configuration</b> .....	8-16

## **A File Transfers**

<b>Overview</b> .....	A-1
<b>Downloading an Operating System (OS)</b> .....	A-1
Using TFTP To Download the OS File .....	A-2
Using Xmodem to Download the OS File .....	A-4
Using the SNMP-Based HP Download Manager .....	A-5
Switch-to-Switch Download .....	A-5
<b>Troubleshooting TFTP Downloads</b> .....	A-6
<b>Transferring Switch Configurations</b> .....	A-8



## **B MAC Address Management**

<b>Overview</b> .....	B-1
<b>Determining the MAC Addresses</b> .....	B-1
Base MAC Address .....	B-2
Switch Port MAC Addresses .....	B-3

## **Index**



# Selecting a Management Interface

---

This chapter describes the following:

- Management interfaces for the Switch 212M and the Switch 224M
  - Advantages of using each interface
- 

## Understanding Management Interfaces

Management interfaces enable you to reconfigure the switch, monitor switch status and performance, and perform troubleshooting tasks.

The Switch 212M and 224M offer the following interfaces:

- The HP web browser interface—an interface that is built into the switch and can be accessed using a standard web browser (such as Netscape Navigator or Microsoft Internet Explorer)
- The switch console—a VT-100/ANSI console interface built into the switch
- HP TopTools for Hubs & Switches—an easy-to-use, browser-based network management tool that works with HP proactive networking features that are built into managed HP hubs and switches (included on a CD with the switch)

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

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

To use HP TopTools for Hubs & Switches, refer to the *HP TopTools User's Guide* and the TopTools online help, both of which are available on the CD-ROM shipped with your HP switch.

## Advantages of Using the HP Web Browser Interface

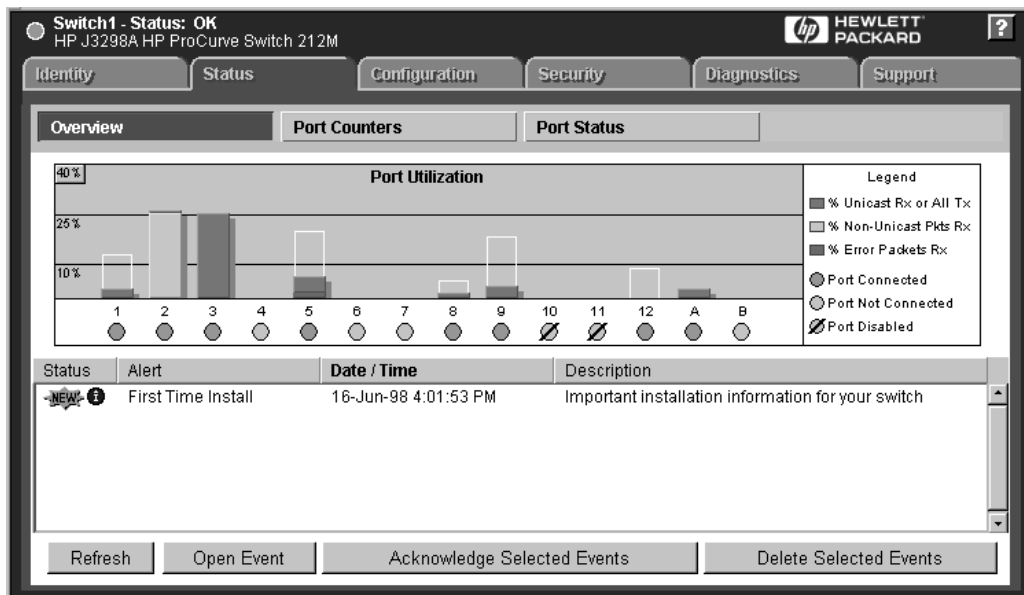


Figure 1-1. Example of the HP Web Browser Interface Display

- **Easy access** to the switch from anywhere on the network, using the device's IP address
- **Familiar browser interface**--locations of window objects consistent with known standard, uses mouse clicking for navigation; no terminal setup.
- **More visual cues**, using colors, status bars, device icons, and other graphical objects to represent values rather than numeric values
- **Display of acceptable ranges of values available** in configuration list boxes

## Advantages of Using the Switch Console

```
HP ProCurve Switch 212M          Switch1          18-Jun-1998 16:26:43
----- TELNET - MANAGER MODE -----
                          Main Menu

  1. Status and Counters...
  2. Switch Management Access Configuration (IP, SNMP, Console)...
  3. Switch Configuration...
  4. Event Log
  5. Diagnostics...
  6. Reboot Switch
  7. Download OS
  8. Logout

Provides the menu to display configuration, status, and counters.
To select menu item, press item number, or highlight item and press <Enter>.
```

Figure 1-2. Example of the Switch Console Display

- **More comprehensive set of features and parameters** to work with than the web browser interface
- **Out-of-band access** (through direct cable connection) to switch, so network bottlenecks, crashes, and network downtime do not slow or prevent access
- **Telnet access** to the full console functionality
- **Ability to configure management access**, for example, creating an IP address, and setting Community Names and Authorized Managers
- **Rebooting the switch** through either direct or Telnet access
- **Faster navigation**, avoiding delays for slower display of graphical objects over a browser interface

## HP TopTools for Hubs & Switches

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

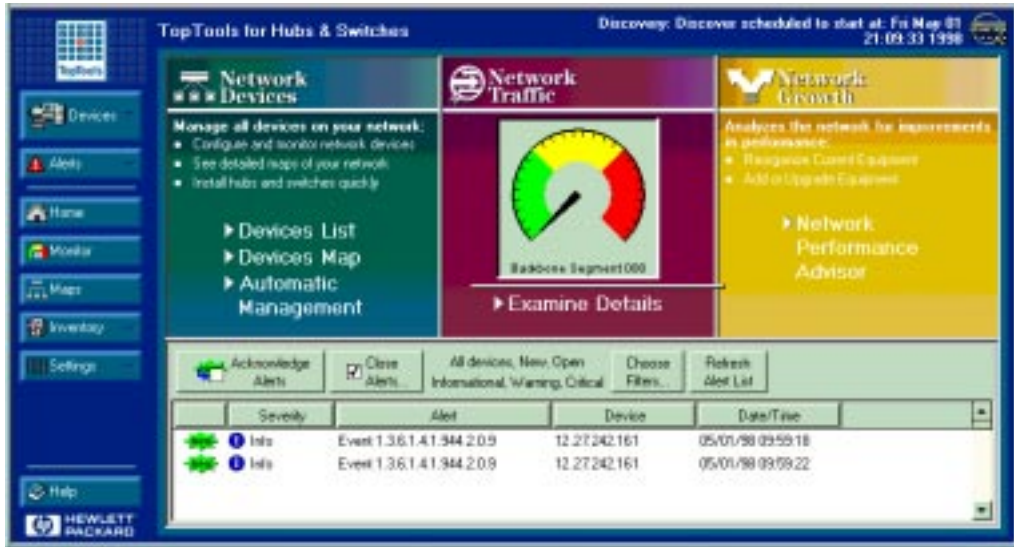


Figure 1-3. Example of HP TopTools Main Screen

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

### Network Devices:

- Enables fast installation of hubs and switches
- Quickly finds and notifies you of the location of problems, saving valuable time
- Notifies you when HP hubs and switches use “self-healing” features to fix or limit common network problems
- Identifies users by port and lets you assign easy-to-remember names to any network device
- Enables you to configure and monitor network devices from your PC

**Network Traffic:**

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

**Network Growth:**

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





# Configuring an IP Address on the Switch

---

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

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

- HP Web Browser Interface built into the switch
- HP TopTools for Hubs & Switches—SNMP-based network management software shipped with the switch
- the switch console through a Telnet connection

For more information on this topic, refer to “IP Configuration” on page 6-5.

---

## Note

An IP address and subnet mask for the switch should be assigned by your network administrator and be compatible with the IP addressing used in your network. For more information about IP addressing, refer to “IP Configuration” on page 6-5.

If your network is a standalone network, your IP addressing and subnet mask scheme can be set up in any way that meets your local needs. However, if you will be connecting your network to other networks that use globally assigned IP addresses, refer to “Globally Assigned Network Addresses” on page 6-14.

---

## Methods for Configuring an IP Address and Subnet Mask

Use either of the following two methods to configure the switch with an IP address and subnet mask compatible with your network:

- **Manually through the switch's console:** This is the easiest method when you are initially setting up the switch. The switch comes with a console cable that you can use to connect the switch to a PC running a VT-100 terminal emulator (such as HyperTerminal in Windows 95 or Windows NT), or to a VT-100 terminal. Refer to “Manually Configuring an IP Address”, below.
- **Configure your DHCP/Bootp server to support the switch:** By default, the switch is configured to acquire an IP address configuration from a DHCP or Bootp server. To use DHCP/Bootp, refer to “DHCP/Bootp Operation” on page 6-10.

---

## Manually Configuring an IP Address

This section describes how to use the switch console to configure an IP address.

1. Use the instructions in chapter 2, “Installing the Switch 212M and 224M” of your switch installation manual to connect a PC running a terminal emulator, or a terminal, to the Console port on the switch, and display the Main Menu.
2. From the console Main Menu, select:
  2. Switch Management Access Configuration (IP, SNMP, Console) ...
    1. IP Configuration

You will see the screen similar to the one shown in figure 2-2, but with the IP Address, Subnet Mask, and Gateway fields blank.

```
HP ProCurve Switch 212M          Switch1          18-Jun-1998  17:48:52
----- TELNET - MANAGER MODE -----
          Switch Management Access Configuration - Internet (IP) Service

Time Protocol Config [DHCP] : DHCP
TimeP Poll Interval (min) [720] : 720

IP Config [DHCP/Bootp] : Manual
IP Address : 11.22.33.44
Subnet Mask : 255.255.248.0
Gateway : 11.22.33.1

Actions->  Cancel      Edit      Save      Help

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

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

3. Press **[E]** to select the **E**dit action, then use the down arrow key (**[↓]**) to select the **IP Config [DHCP/Bootp]** field.
4. Use the Space bar to display **Manual** for this field.
5. Press the down arrow key (**[↓]**) to display the three IP configuration parameters, as shown in figure 2-2, and select the **IP Address** field.
6. Enter the IP address you want to assign to the switch.
7. Select the **Subnet Mask** field and enter the subnet mask for your network.
8. If you want to reach off-subnet destinations, select the **Gateway** field and enter the address of the gateway router for your subnet.
9. Press **[Enter]**, then **[S]** (for **S**ave), then proceed with any other console tasks.  
To test the IP address, you can try a Ping test to the switch's IP address from another IP device in your network.

## Where To Go From Here

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

- To access the switch using a web browser, refer to chapter 3, “Using the HP Web Browser Interface”.
- To continue to use the switch console, refer to chapter 4, “Using the Switch Console”.
- To access the switch using a network management tool, refer to chapter 5, “Using HP TopTools to Monitor and Manage the Switch”.
- Inbound Telnet access to the switch is enabled in the factory default configuration.
  - To change the Telnet access parameter, refer to “Using the Switch Console to Configure the Console/Serial Link” on page 6-21.
  - To use Telnet to access the switch console refer to “Starting and Ending a Console Session” on page 4-2.
- For problems or error indications, refer to chapter 8, “Troubleshooting”.

# Using the HP Web Browser Interface

---

## Overview

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

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

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

- system requirements for using the HP web browser interface (page 3-2)
- starting a web browser interface session (page 3-3)
- tasks for your first HP web browser interface session (page 3-6)
  - configuring user names and passwords in the web browser interface (page 3-8)
  - selecting the fault detection configuration for the Alert Log operation (page 3-25)
  - getting access to online help for the web browser interface (page 3-10)
- Description of the web browser interface:
  - the Overview window and tabs (page 3-12)
  - the Port Utilization and Status displays (page 3-14)
  - the Alert Log and Alert types (page 3-16)
  - setting the Fault Detection Policy (page 3-25)

---

### Note

If you want security beyond that achieved with user names and passwords, you can disable access to the web browser interface. This is done by changing the Web Agent Enabled parameter setting in the Console/Serial Link configuration screen in the switch console. See “Console/Serial Link” on page 6-20.

---

## Web Browser Interface Requirements

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

**Table 3-1. Supported Network Devices and System Requirements**

Platform Entity and OS Version	Minimum	Recommended
PC Platform	90 MHz Pentium	120 MHz Pentium
HP-UX Platform (9.x or 10.x)	100 MHz	120 MHz
RAM	16 Mbytes	32 Mbytes
Screen Resolution	800 X 600	1,024 x 768
Color Count	256	65,536
Internet Browser* (English-language browser only)	<b>PCs:</b> <ul style="list-style-type: none"><li>• Netscape® Communicator 4.x</li><li>• Microsoft® Internet Explorer 4.x</li></ul> <b>UNIX:</b> Netscape Navigator 3.x or later	<b>PCs:</b> Netscape Communicator 4.03 or later <b>UNIX:</b> Netscape Navigator 3.x or later
PC Operating System	Microsoft Windows® 95 and Windows NT	
UNIX® Operating System	Standard UNIX® OS	
HP TopTools for Hubs & Switches (Optional)	HP J2569M or later	
* For notes on using Netscape and Microsoft web browsers, go to HP's Network City web site, <a href="http://www.hp.com/go/network_city">http://www.hp.com/go/network_city</a> .		

---

# Starting an HP Web Browser Interface Session

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

- Using a standalone Web browser on a network connection from a PC or UNIX workstation:
  - Directly connected to your network
  - Connected through remote access to your network
- Using a management station running HP TopTools for Hubs & Switches on your network (the same browser interface is presented when you access a device through HP TopTools)

---

## Note

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

---

## Using a Standalone Web Browser in a PC or UNIX Workstation

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

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

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

10.11.12.195

If you are using a Domain Name Server (DNS), your device may have a name associated with it (for example, **switch20**) that you can type in the **Location or Address** field instead of the IP address. Using DNS names typically improves browser performance. As such, we recommend that you assign a DNS name to each device that you access with the web browser interface.

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

## Using HP TopTools for Hubs & Switches

For more on installing and using HP TopTools for Hubs & Switches, refer to the HP TopTools for Hubs & Switches booklet and CD-ROM that came with your switch.

This procedure assumes the following:

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

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

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



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

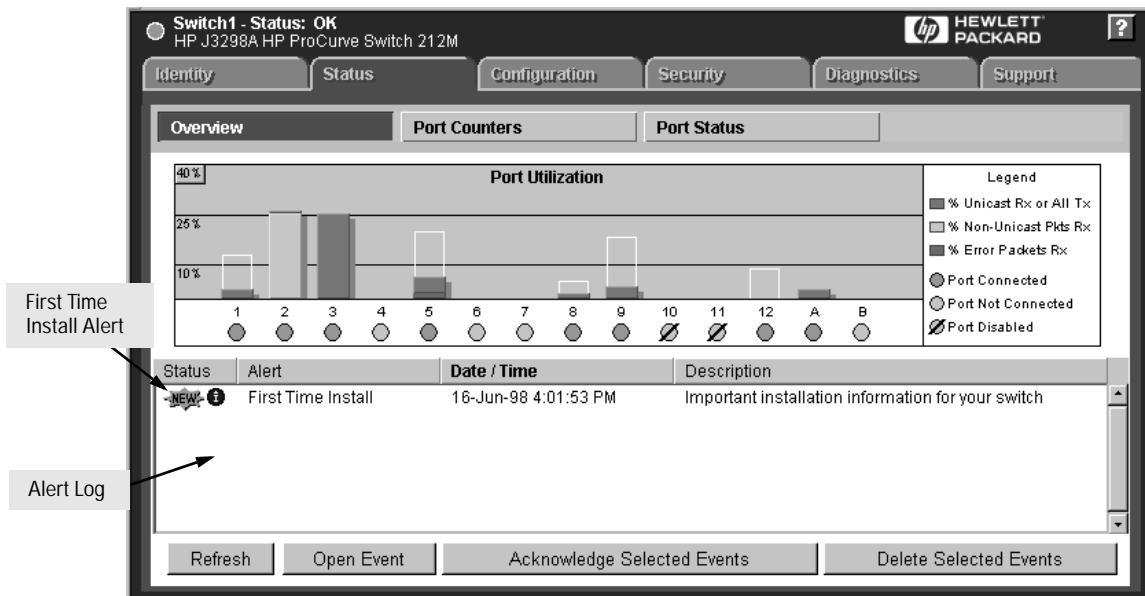


Figure 3-1. Status Overview Screen

---

## Tasks for Your First HP Web Browser Interface Session

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

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

### Viewing the “First Time Install” Window

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

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

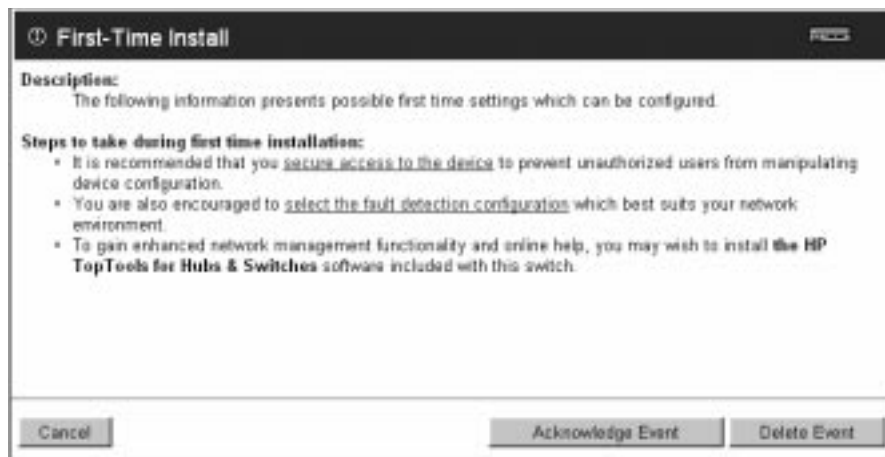


Figure 3-2. First-Time Install Window

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

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

To set Fault Detection policy, click on the jump string **select the fault detection configuration** in the second bullet in the window and go to the section, "Setting Fault Detection Policy" on page 3-25.

## Creating User Names and Passwords in the Web Browser Interface

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

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

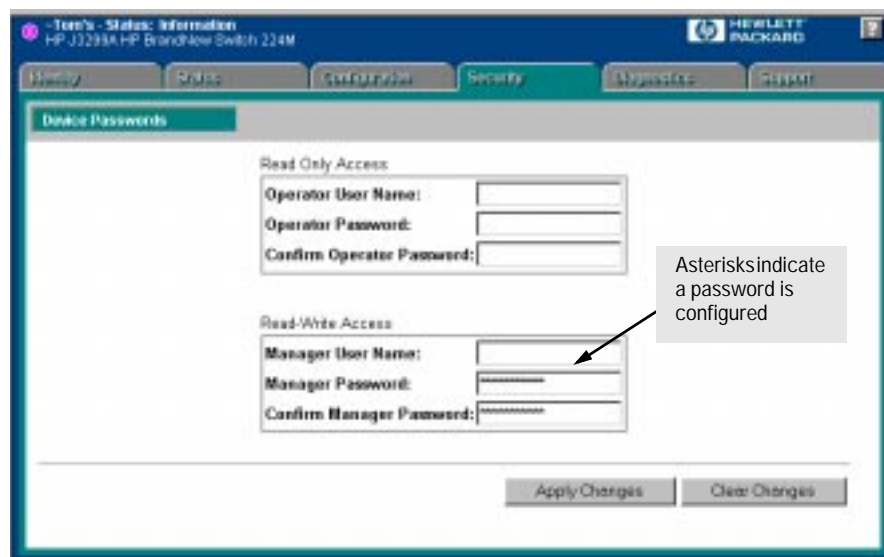


Figure 3-3. The Device Passwords Window

To set the passwords:

1. Access the Device Passwords screen by one of the following methods:
  - If the Alert Log includes a “First Time Install” event entry, double click on this event, then, in the resulting display, click on the **secure access to the device** link.
  - Select the Security tab.
2. Click in the appropriate box in the Device Passwords window and enter user names and passwords. You will be required to repeat the password strings in the confirmation boxes.

Both the user names and passwords can be up to 16 printable ASCII characters. Spaces can be included in user names, but not in passwords (to represent spaces in passwords, you can use the underscore ( \_ ) character).

3. Click on **Apply Changes** to activate the user names and passwords.

---

## Note

---

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

## Using the Passwords

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

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

## Using the User Names

If you also set user names in the web browser interface screen, you must supply the correct user name and password combination for web browser interface access. If a user name has not been set, the User Name field in the web browser interface access popup must be left blank.

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

## If You Lose a Password

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

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

## Online Help for the HP Web Browser Interface

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

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

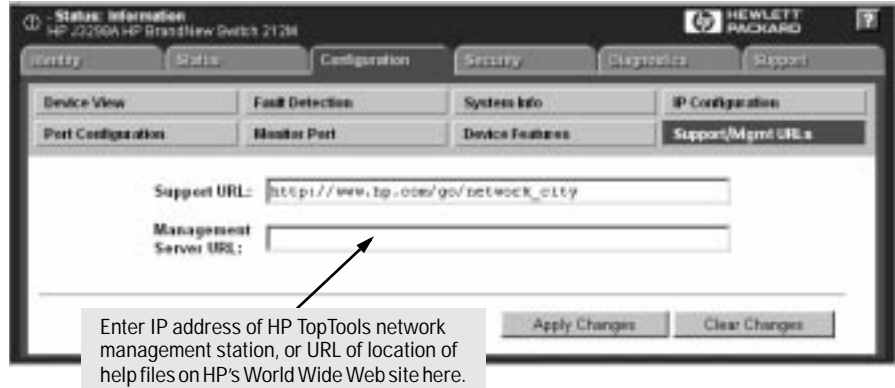
Retrieval of the Help files, as described above, is controlled by automatic entries in the **Management Server URL** field on the **Configuration / Support URLs** screen, shown in figure 3-4 on page 3-11. The switch is shipped with the URL set to the HP World Wide Web site. However, if HP TopTools for Hub & Switches is installed on a management station in your network, and TopTools discovers your switch, the Management Server URL value is automatically changed to point to the management station to retrieve the help.

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

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

**[http://www.hp.com/rnd/device\\_help](http://www.hp.com/rnd/device_help)**

See figure 3-4 on page 3-11.



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

If you do not have HP Top Tools for Hubs & Switches installed on a computer in your network, and you do not have an active connection to the World Wide Web, then online help for the web browser interface will not be available.

See also “Support URLs Feature” on page 6-3.

# The Web Browser Interface Screen Layout

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

## The Overview Window

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

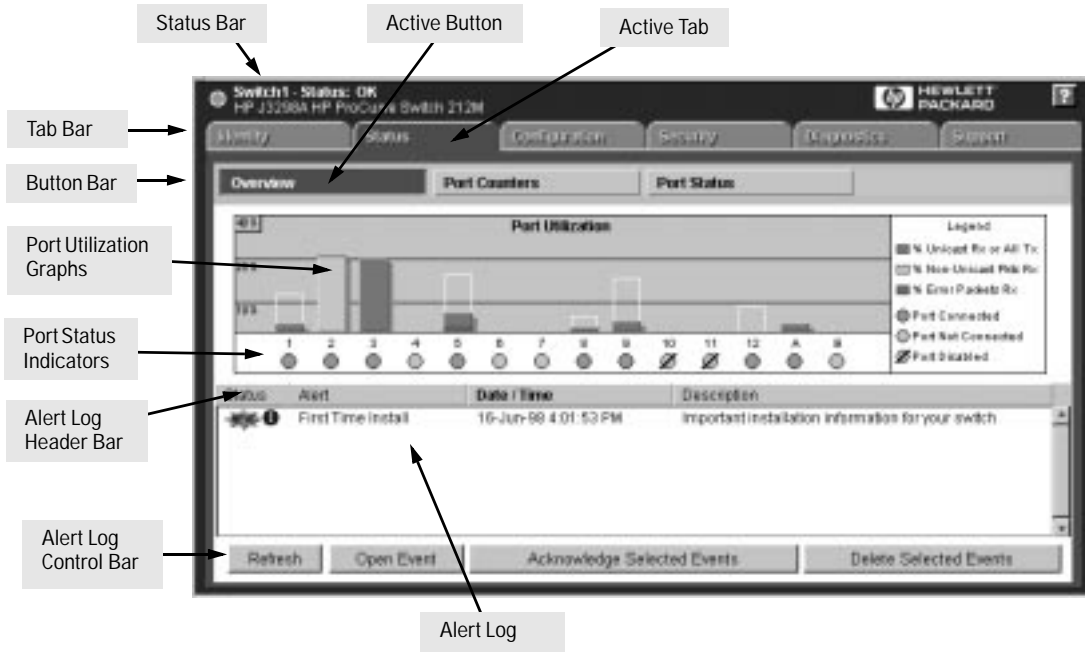


Figure 3-5. The Overview Window

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



- **Tab Bar.** The row of tabs displaying all the Browser Interface Top Level menus.
- **Active Tab.** The current tab selected. The tab is darkened and all the buttons under the tab are displayed.
- **Status Bar.** The region above the Tab Bar that displays status and device name information.
- **Port Utilization and Status Displays.** The region containing graphs that indicate network traffic on each switch port and symbols indicating the status of each port.
- **Button Bar.** The row(s) of buttons that are contained within the Active Tab.
- **Active Button.** The current button selected. The button is darkened and the window associated with the button is displayed.
- **Alert Log.** A list of all events, or alerts, that can be retrieved from the switch's firmware at the current time. Information associated with the alerts is displayed, including Status, Alert Name, the date and time the Alert was reported by the switch, and a short description of the alert. You can double click on any of the entries in the log and get a detailed description. See "The Alert Log" on page 3-16.
- **Alert Log Header Bar.** The row of column heads running across the top of the Alert Log.
- **Alert Log Control Bar.** The region at the bottom of the Alert Log containing buttons that enable you to refresh the Alert Log to display all alerts that have been reported since you first displayed the log. Also available in the bar are a button to acknowledge new alerts and a button to delete alerts.

## The Port Utilization and Status Displays

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

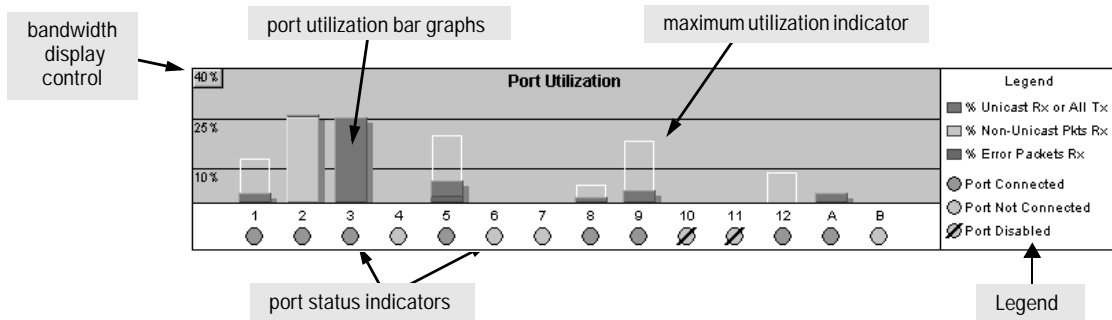


Figure 3-6. The Graphs Area

### Port Utilization

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

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

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

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

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

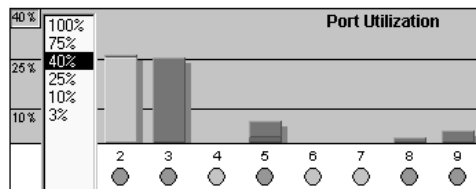


Figure 3-7. Changing the Graph Area Scale

**To display values for each graph bar.** Hold the mouse cursor over any of the bars in the graph, and a pop-up display is activated showing the port identification and numerical values for each of the sections of the bar, as shown in figure 3-8.

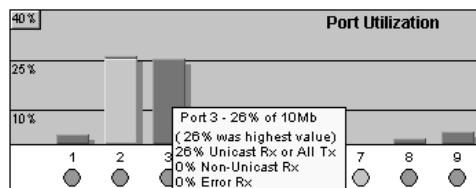


Figure 3-8. Display of Numerical Values for the Bar

## Port Status

The Port Status indicators are symbols for each port that show the general status of the port. There are four possible status symbols:

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

## The Alert Log

The Alert Log, shown in the lower half of the screen, shows a list of network occurrences, or *alerts*, that were detected by the switch. Typical alerts are, **Broadcast Storm**, indicating an excessive number of broadcasts received on a port, and **Problem Cable**, indicating a faulty cable. A full list of alerts is shown in Table 3-2 on page 3-18.

































Status	Alert	Date/Time	Description
 	Loss of Link	15-Sep-97 1:46:21 PM	Lost connection to multiple devices on port 1.
 	Network Loop	15-Sep-97 1:46:13 PM	Network loop detected on port 1.
 	Polarity Reversal	15-Sep-97 1:46:17 PM	Mis-wired cable detected on port 1.
 	Mis-configured SGE	15-Sep-97 1:46:15 PM	Transceiver misconfigured on port 1.
 	Auto Fastrin	15-Sep-97 1:46:13 PM	Repeater loop or problem cable on port 1.
 	Broadcast Storm	15-Sep-97 1:46:11 PM	Excessive broadcasts detected on port 1.
 	Over Bandwidth	15-Sep-97 1:46:03 PM	Excessive network traffic on port 1.
 	Cable Length	15-Sep-97 1:46:03 PM	Packet loss detected, which could be due to excessive cable length or repeater hops on port 1.
 	Feeder Hops		
 	Problem Cable	15-Sep-97 1:46:05 PM	Problem cable detected on port 1.
 	Problem XCVR or NIC	15-Sep-97 1:46:04 PM	Problem XCVR or NIC detected on port 1.
 	Problem Driver or NIC	15-Sep-97 1:46:02 PM	Problem driver or NIC detected on port 1.
 	Auto Fastrin	15-Sep-97 1:45:24 PM	Repeater loop or problem cable on port 1.
 	Broadcast Storm	15-Sep-97 1:45:22 PM	Excessive broadcasts detected on port 1.
 	Over Bandwidth	15-Sep-97 1:45:23 PM	Excessive network traffic on port 1.
 	Cable Length	15-Sep-97 1:45:13 PM	Packet loss detected, which could be due to excessive cable length or repeater hops on port 1.

Figure 3-9. The Alert Log

Each alert has the following fields of information:

- **Status** – The level of severity of the event generated. Severity levels can be Information, Normal, Warning, and Critical. If the alert is new (has not yet been acknowledged), the New symbol is also in the Status column.
- **Alert** – The specific event identification.
- **Date/Time** – The date and time the event was received by the Browser Interface. This value is shown in the format: DD-MM-YY HH:MM:SS AM/PM, for example, 12-Sep-97 3:57:20 PM.
- **Description** – A short narrative statement that describes the event. For example, Lost connection to multiple devices on port 1.

### Sorting the Alert Log Entries

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

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

## Alert Types

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

**Table 3-2. Alert Strings and Descriptions**

Alert String	Alert Description
First Time Install	Important installation information for your switch.
Problem Driver or NIC	Problem software driver or LAN adapter detected on port.
Problem XCVR or NIC	Problem transceiver or LAN adapter card detected on port.
Problem Cable	Problem cable detected on port.
Cable Length/Repeater Hops	Problem cable detected on port. Packet loss detected, which could be due to excessive number of gateways to traverse.
Over Bandwidth	Excessive network traffic on port.
Broadcast Storm	Excessive broadcasts detected on port.
Fault-Disabled Port	The port has been automatically disabled due to a detected fault condition, for example, an incorrect transceiver installed in a transceiver slot.
Polarity Reversal	Miswired cable detected on port.
Network Loop	Network loop detected by switch. Network loop detected on port.
Loss of Link	Lost connection to multiple devices on port.

---

### Note

When troubleshooting the sources of alerts, it may be helpful to also check the switch's Port Status and Port Counters windows (page 7-7 and page 7-9 respectively) and the Event Log in the switch console (page 8-6).

## Viewing Detail Views of Alert Log Entries

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

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

A sample Detail View describing a Cable Length/Repeater Hops alert is shown here.



Figure 3-10. Detail View of Alert Log Entry

## The Alert Control Bar

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

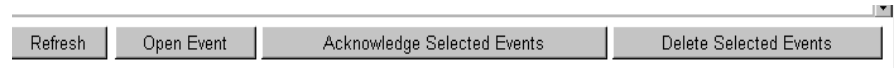


Figure 3-11. The Alert Control Bar

The buttons in the control bar are:

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

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

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



## The Tab Bar

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

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

### Identity Tab



Figure 3-12. The Identity Tab

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

- **Editable Information (System Name, Location, and Contact)** – is maintained in the Administration dialog box.
- **Read-Only Information** – The System Up Time shows the elapsed time since the switch was last rebooted. Product is the switch product name. Version is the software (operating system) version currently running in the switch. IP Address is the IP address assigned to the switch. Management Server is the currently assigned Management Server URL (page 6-4).

### Status Tab



Figure 3-13. The Status Tab and Buttons

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

- **Overview** – the home position for the web browser interface. Displays the screen shown in figure 3-5 on page 3-12.

- **Port Counters** – displays a summary of the network activity statistics for all the switch ports, with access to detailed port-level statistics. See page 7-8 for an image of this window.
- **Port Status** – displays a summary table of the operational status of all the switch ports. See page 7-5 for an image of this window.

## Configuration Tab

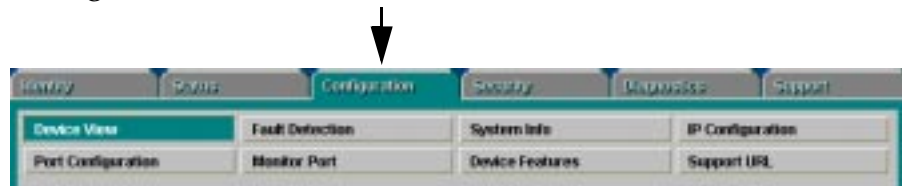


Figure 3-14. The Configuration Tab and Buttons

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

- **Device View.** Displays a graphical representation of the front panel of the device, allowing you to enable and disable ports on the device by clicking on port graphics and an enable or disable port button.
- **Fault Detection.** Controls the alert log sensitivity, and port disabling.
- **System Information.** Enables you to view and set system information for a selected device.
- **IP Configuration.** Enables you to change existing value for an IP address, subnet mask, and the gateway address for the switch.
- **Port Configuration.** Enables you to enable and disable ports in addition to viewing the security and source address information.
- **Monitor Port.** Enables you to designate a port for monitoring traffic on one of the other switch ports.
- **Device Features.** Enables you to configure some key features for the entire switch.
- **Support/Mgmt URLs.** Specifies the URL of the web site that will be automatically accessed when you open the Support tab, and the URL for the source of online Help for the web browser interface (page 6-3). The Support URL is configured to automatically access HP's Network City website on the World Wide Web. However, if you have an internal support structure, you may wish to change the Support URL to access that structure.

## Security Tab



Figure 3-15. The Security Tab and Buttons

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

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

## Diagnostics Tab

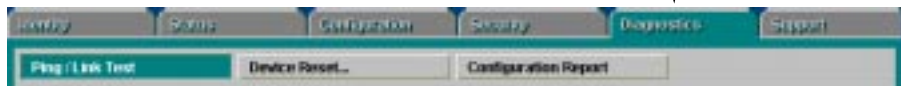


Figure 3-16. The Diagnostics Tab and Buttons

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

- **Ping/Link Test.** Enables you to send test packets to devices connected to a port, using both the IP address (Ping) and the MAC address (Link) as criteria for a valid connection.
- **Device Reset.** Resets the switch, which clears most temporary error conditions, and resets the traffic counters and system up time to zero.
- **Configuration Report.** Displays a master list of various settings for the switch, including information about port status, authorized managers, community names, backup links, IP addresses, security configuration, and general system information.

## The Support Tab



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

## The Status Bar

The Status Bar is displayed in the upper left corner of the web browser interface screen. Figure 3-15 shows an expanded view of the status bar.

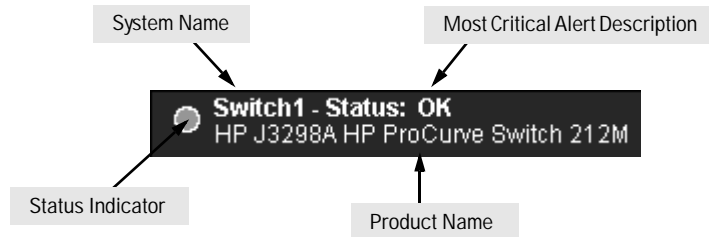





Figure 3-17. The Status Bar

The Status Bar consists of four objects:

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

Table 3-3. Status Indicator Key

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

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

## Setting Fault Detection Policy

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

Set this policy in the Fault Detection Window, shown in figure 3-16.

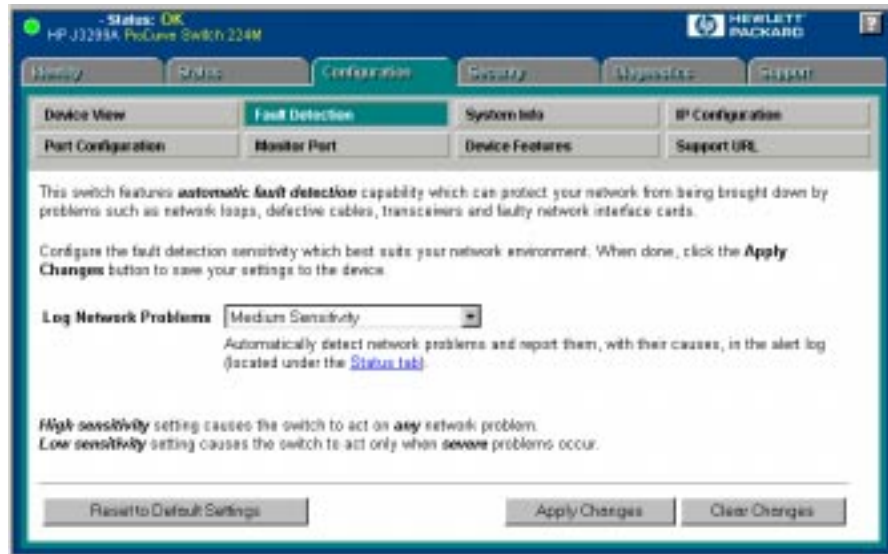


Figure 3-18. The Fault Detection Window

## Working With Fault Detection

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

The sensitivity levels for both list boxes are:

- Never
- Low Sensitivity
- Medium Sensitivity
- High Sensitivity

The Fault Detection settings are:

- **High Sensitivity.** This policy directs the switch to send all alerts to the Alert Log. This setting is most effective on networks that have no or few problems.
- **Medium Sensitivity.** (the default setting) This policy directs the switch to send alerts related to network problems to the Alert Log. If you want to be notified of problems which cause a noticeable slowdown on the network, use this setting.
- **Low Sensitivity.** This policy directs the switch to send only the most severe alerts to the Alert Log and to rarely or never disable a port generating the alert. This policy is most effective on a network that normally has a lot of problems and you want to be informed of only the most severe ones.
- **Never.** Use this setting if you do *not* want network events displayed in the Alert Log.

The Fault Detection Window also contains three Change Control Buttons. They are:

- **Apply Changes.** This button stores the settings you have selected for all future sessions with the Browser Interface until you decide to change them.
- **Clear Change.** This button removes your settings and returns the settings for both list boxes to the levels they were at in the last saved detection setting session.
- **Reset to Default Settings.** This button reverts the policy setting to Medium Sensitivity for Log Network Problems.

# Using the Switch Console

---

This chapter describes the following features:

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

## Overview

**About the Switch Console.** The switch console enables you to use a PC or a terminal to do the following:

- modify the switch's configuration (see chapter 6)
- configure the switch with an IP address that allows you to manage the switch from an SNMP-based network management station (see chapter 5), through the switch's web browser interface (see chapter 3), or through Telnet access to the console (see this chapter)
- monitor the switch and its port status (see chapter 7)
- monitor the network activity through the switch (see chapter 7)
- control console security by configuring passwords (see this chapter)
- view the event log and run diagnostics to troubleshoot any switch problems (see chapter 8)
- download new software to the switch (see appendix A)

**Switch Console Interaction with the Web Browser Interface.** Configuration changes made through the console will overwrite previous changes made through the web browser interface. Similarly, configuration changes made through the web browser interface will overwrite any prior changes made through the console. The console gives you access to all switch configuration parameters; the web browser interface gives you access to a subset of these. Refer to chapter 3, "Using the HP Web Browser Interface" and chapter 6, "Configuring the Switch".

## Starting and Ending a Console Session

You can access the switch console using either:

- a direct serial cable connection to the switch's console port, as described in the installation guide that came with the switch
- through a Telnet session from a remote terminal device or from the switch's web browser interface (the web browser interface provides for a Telnet connection from some of its screens)

---

### Note

This section assumes that either a terminal device is already configured and connected to your Switch 212M or 224M (as described in chapter 1, "Installation" of the *HP Switch 212M and 224M Installation Guide*) or that you have already configured an IP address on the switch so you can start a Telnet session with the switch.

---

### How To Start a Console Session:

1. Start your PC terminal emulator, or terminal, or Telnet to the switch from a remote terminal device or from the web browser interface.
2. Do one of the following:
  - If you are using Telnet, go to step 3.
  - If you are using a PC terminal emulator or a terminal, press **Enter** twice.
3. The screen briefly displays a message indicating the baud rate at which the serial interface is operating, followed by the copyright screen. Do one of the following:
  - If a password has been set, the Password prompt appears. Type the password and press **Enter** to display the Main Menu (figure 4-1). Figure 4-1 shows the Main Menu for manager-level access. If you enter the operator password to start the console session, the Main Menu has a subset of these items.
  - If no password has been set, you will see this prompt:  
**Press any key to continue.**  
Press any key to display the Main Menu (figure 4-1).



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

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

## How To End a Console Session:

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

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

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

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

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

---

### Note

The Switch 212M and 224M serial interface does not support all modem lines, including automatic disconnect. As a result, if you are concerned about security for console access, in addition to using passwords, you should always make sure you select the Logout option from the Main Menu to terminate the console session. This option also disconnects the serial connection so that the next person to use the console is required to go through the password-protected logon process.

There is also an “inactivity timeout” parameter that can be set on the Console/Serial Link configuration screen under the Switch Management Access Configuration menu. See page 6-20 for more information on setting this parameter.

## Main Menu Features

```
HP ProCurve Switch 212M                Switch1                18-Jun-1998  16:26:43
----- TELNET - MANAGER MODE -----
Main Menu

1. Status and Counters...
2. Switch Management Access Configuration (IP, SNMP, Console)...
3. Switch Configuration...
4. Event Log
5. Diagnostics...
6. Reboot Switch
7. Download OS
8. Logout

Provides the menu to display configuration, status, and counters.
To select menu item, press item number, or highlight item and press <Enter>.
```

Figure 4-1. The Main Menu (manager mode)

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

- **Status and Counters:** Provides access to display screens providing information on switch and port status, network activity, the address tables, spanning tree operation, and IGMP status. (Refer to chapter 7, “Monitoring and Analyzing Switch Operation”.)
- **Switch Management Access Configuration:** Provides access to configuration screens that control interaction between the switch and network management, including IP address, SNMP community names and trap receivers, console/serial link parameters, and console passwords.
- **Switch Configuration:** Provides access to configuration screens that enable you to display the current configuration settings and to customize the configuration of the switch features. (Refer to chapter 6, “Configuring the Switch”.) This feature is available only in Manager Mode console sessions. If you access the console at the Operator level (controlled by passwords), no configuration is available.

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

## Screen Structure and Navigation

Console screens include these three elements:

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

For example, in the System configuration screen:

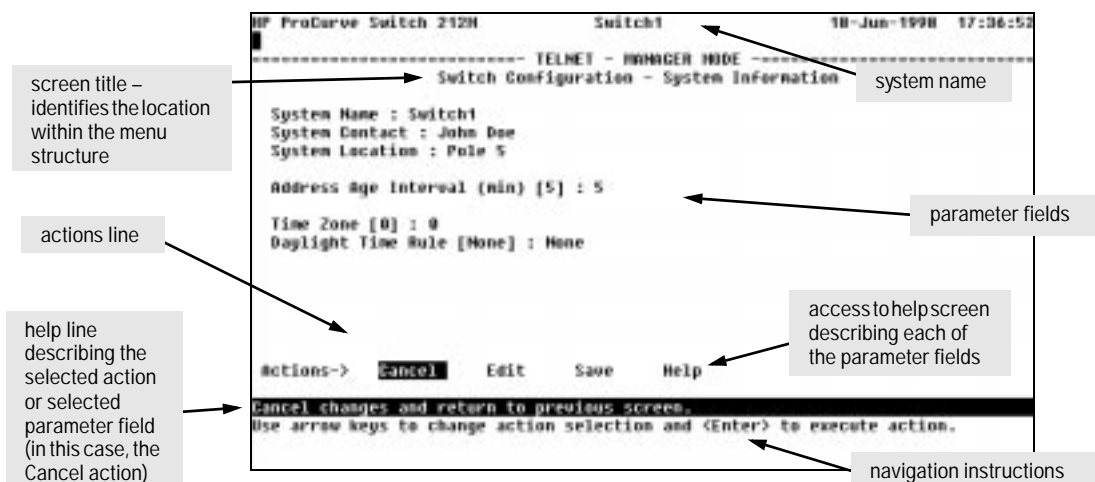


Figure 4-2. Elements of the Screen Structure

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

1. Press **[E]** to select the **Edit** action.
2. Navigate through the screen making **ALL** the necessary configuration changes. See table 4-1.
3. Press **[Enter]** to return to the Actions line. From there you can save the configuration changes or cancel the changes. Cancel returns the configuration to the values you saw when you first entered the screen.

See the next page for specific instructions on using the console screens.

**Table 4-1. How To Navigate in the Console**

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

**To get full screen Help.** In all screens except the Command Prompt screen there is a **Help** option in the Actions line. Press **[H]** to select the Help action, and a separate help screen is displayed.

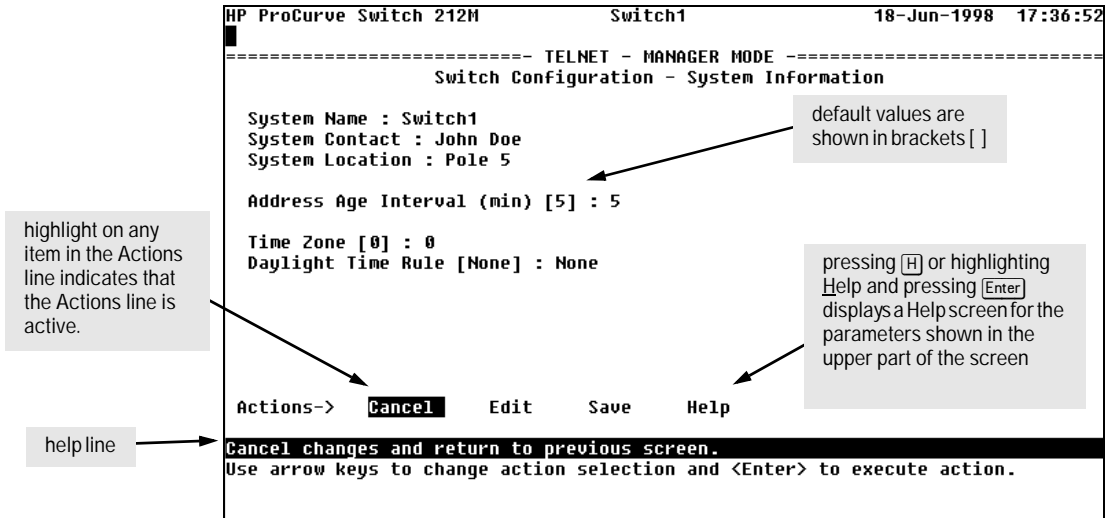


Figure 4-3. Example Showing How To Display Help

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

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

---

## Using Password Security

There are two levels of console access: Manager and Operator. For security, you can set a password on each of these levels. The manager and operator passwords control access to both the web browser interface and the switch console.

---

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

---

To use password security:

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

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

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

---

**Note**

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, but simply pressing **Enter** at the password prompt.*

---

The rest of this section covers how to:

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

## To set Manager and Operator passwords:

1. From the Main Menu select:
  2. Switch Management Access Configuration
  3. Console Passwords

```
HP ProCurve Switch 212M          Switch1          18-Jun-1998  17:39:12
|
----- TELNET - MANAGER MODE -----
                Set Password Menu

1. Set Operator Password
2. Set Manager Password
3. Delete Password Protection
4. Return to Previous Menu...
0. Return to Main Menu...

Prompts you to enter an Operator-level password.
To select menu item, press item number, or highlight item and press <Enter>.
```

Figure 4-4. The Password Menu Screen



2. To set a new password:
  - a. Select **Set Manager Password** or **Set Operator Password**. You will then be prompted with Enter new password.
  - b. Type a password of up to 16 ASCII characters with no spaces and press . (The passwords are case-sensitive.)
  - c. When prompted with **Enter new password again**, retype the new password and press .
3. When you have finished all password configuration, select **0. Return to Main Menu** to return to the Main menu, or **4. Return to the Previous Menu** to return to the Switch Management Access Configuration menu.

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

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

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

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

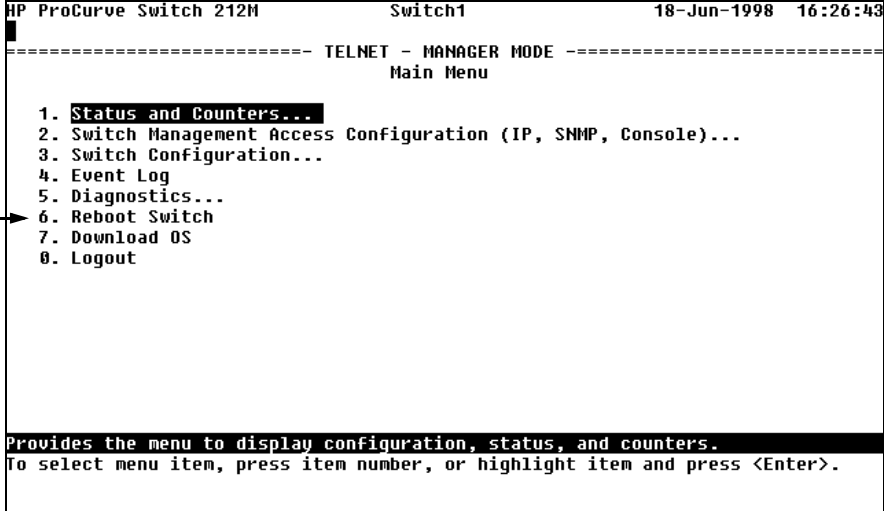
**To Recover from a Lost Manager Password:** If you cannot start a console session at the manager level because of a lost Manager password, you can clear the password by getting physical access to the switch and pressing the Clear button. This action deletes all passwords and user names (Manager and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

## Rebooting the Switch

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

- Activating certain configuration changes that require a reboot
- Resetting statistical counters to zero

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



```
HP ProCurve Switch 212M          Switch1          18-Jun-1998  16:26:43
----- TELNET - MANAGER MODE -----
                          Main Menu

  1. Status and Counters...
  2. Switch Management Access Configuration (IP, SNMP, Console)...
  3. Switch Configuration...
  4. Event Log
  5. Diagnostics...
  6. Reboot Switch
  7. Download OS
  8. Logout

Provides the menu to display configuration, status, and counters.
To select menu item, press item number, or highlight item and press <Enter>.
```

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

**Rebooting To Activate Configuration Changes.** Configuration changes for some parameters become effective as soon as you save them. However, you must reboot the switch in order to implement any changes to the parameters on the **Console/Serial Link** screen (under **Switch Management Access Configuration** menu).

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

```
HP ProCurve Switch 212M                Switch1                18-Jun-1998  17:42:36
----- TELNET - MANAGER MODE -----
Main Menu

  1. Status and Counters...
 *2. Switch Management Access Configuration (IP, SNMP, Console)...
  3. Switch Configuration...
  4. Event Log
  5. Diagnostics...
  6. Reboot Switch
  7. Download OS
  8. Logout

Displays menu to configure access for network management, including IP address.
To select menu item, press item number, or highlight item and press <Enter>.
(*Needs reboot to activate changes.)
```

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

Reminder to reboot the switch to activate configuration changes

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

## Using the Command Prompt

In addition to the menu-based part of the console interface, under the Diagnostics Menu, a command-line based interface is available. The commands are primarily for the expert user and for diagnostics purposes. Selecting **Command Prompt** from the Diagnostics Menu presents a command prompt from which you can enter commands.

The use of the commands is described in chapter 8, “Troubleshooting”, on page 8-15.

# Using HP TopTools To Monitor and Manage the Switch

---

## Overview

You can manage the Switch 212M and 224M from an SNMP-based network management station. Included with your switch is a CD-ROM containing a copy of **HP TopTools for Hubs & Switches**, an easy to install and use network management application that runs on your Windows NT- or Windows 95-based PC. It can be used as an application under the HP TopTools network management environment, or it can be run as a stand-alone application running directly under Windows.

HP TopTools for Hubs & Switches provides complete control of your Switch 212M or 224M through its graphical interface. In addition, it makes use of the HP Extended RMON and standard RMON agent software that is on the switch to provide powerful but easy to use traffic monitoring and network activity analysis tools.

This chapter provides an overview of SNMP management for the Switch 212M and 224M and provides an overview of the configuration process for supporting SNMP management of the switch. For configuration procedures for specific features, see chapter 6, "Configuring the Switch".

## SNMP Management Features

SNMP management features provided by the Switch 212M and 224M include:

- Security via configuration of SNMP communities
- Event reporting via SNMP traps and RMON
- Managing the switch with a network management tool such as HP TopTools for Hubs & Switches
- Monitoring data normally associated with the SNMP v2 agent (“Get” operations). Supported *Standard* MIBs include:
  - Bridge MIB (RFC 1493)
  - Ethernet MAU MIB (RFC 1515)
  - Interfaces Evolution MIB (RFC 1573)
  - RMON MIB (RFC 1757)—etherstats, events, alarms, and history
  - SNMP MIB-II (RFC 1213)
  - Entity MIB (RFC 2037)

*HP Proprietary* MIBs include:

- Statistics for message and packet buffers, tcp, telnet, and timep (netswtst.mib)
- Port counters, forwarding table, and CPU statistics (stat.mib)
- tftp download (downld.mib)
- Integrated Communications Facility Authentication Manager and SNMP communities (icf.mib)
- HP ProCurve Switch 212M and 224M configuration (config.mib)

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

[http://www.hp.com/go/network\\_city](http://www.hp.com/go/network_city)

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

---

## SNMP Configuration Process

If you are using IP, you must either configure the switch with the appropriate IP address or, if you are using DHCP/Bootp to configure the switch, ensure that the DHCP/Bootp process provides the IP address.

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

1. From the Main Menu, select **Switch Management Access Configuration**.
2. Configure a network address for the switch, including any necessary gateways:
  - a. Use DHCP/Bootp, which is enabled by default, to acquire an IP address. Make sure the DHCP/Bootp server is configured to support this switch. (Refer to “DHCP/Bootp Operation” on page 6-10 for more information.)
  - b. Manually configure an IP address. (Refer to chapter 2, “Configuring an IP Address on the Switch” for more information.)
3. Configure the appropriate SNMP communities. (The “public” community exists by default and is used by HP’s network management applications.) (For more on configuring SNMP communities, refer to “SNMP Communities” on page 6-15.)
4. Configure the appropriate trap receivers. (For more on configuring trap receivers, refer to “Trap Receivers” on page 6-18.)

## Advanced Management: RMON and HP Extended RMON Support

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

### RMON

The following RMON groups are supported:

- Ethernet Statistics
- Alarm
- History (of the supported Ethernet statistics)
- Event

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

### Extended RMON

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



# Configuring the Switch

---

## Overview

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

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

**Why Reconfigure?** In its factory default configuration, the switch operates as a multiport learning bridge. However, to enable specific management features and to “fine-tune” your switch for the specific performance and security needs in your network, you may want to reconfigure individual switch parameters.

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

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

To find a specific feature, see the table on the next page.

## Configuration Features

The following table lists the configuration features available for the switch.

**Table 6-1. Configurable Feature Comparison**

Feature	Switch Console	Web Browser Interface	Page
Time Protocol	Yes	—	page 6-8
IP Configuration	Yes	Yes	page 6-5
SNMP Communities	Yes	—	page 6-15
Trap Receivers and Authentication Traps	Yes	—	page 6-18
Console/Serial Link:			page 6-20
• Inbound Telnet	Yes	—	
• Web Agent Enabled	Yes	—	
• Terminal Settings	Yes	—	
Operator and Manager Usernames	—	Yes	page 3-8
Operator and Manager Passwords	Yes	Yes	page 4-10, page 3-8
System Information	Yes	Yes	page 6-22
Address Age Interval	Yes	—	
System Time	Yes	—	
Port Settings	Yes	Yes	page 6-24
Network Monitoring Port	Yes	Yes	page 6-28
Spanning Tree Enable/Disable	Yes	Yes	page 6-30
Spanning Tree Parameters	Yes	—	
IGMP Enable/Disable	Yes	Yes	page 6-34
	Yes	—	
Support/Management URLs	—	Yes	page 6-3

**Note:**

In the factory default configuration, the Spanning Tree Protocol (STP—which automatically blocks redundant links) is disabled. Generally, you should enable STP to prevent broadcast storms if there are redundant links in your network. For more information, refer to “Spanning Tree Protocol” on page page 6-30.

## Support/Management URLs Feature

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

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

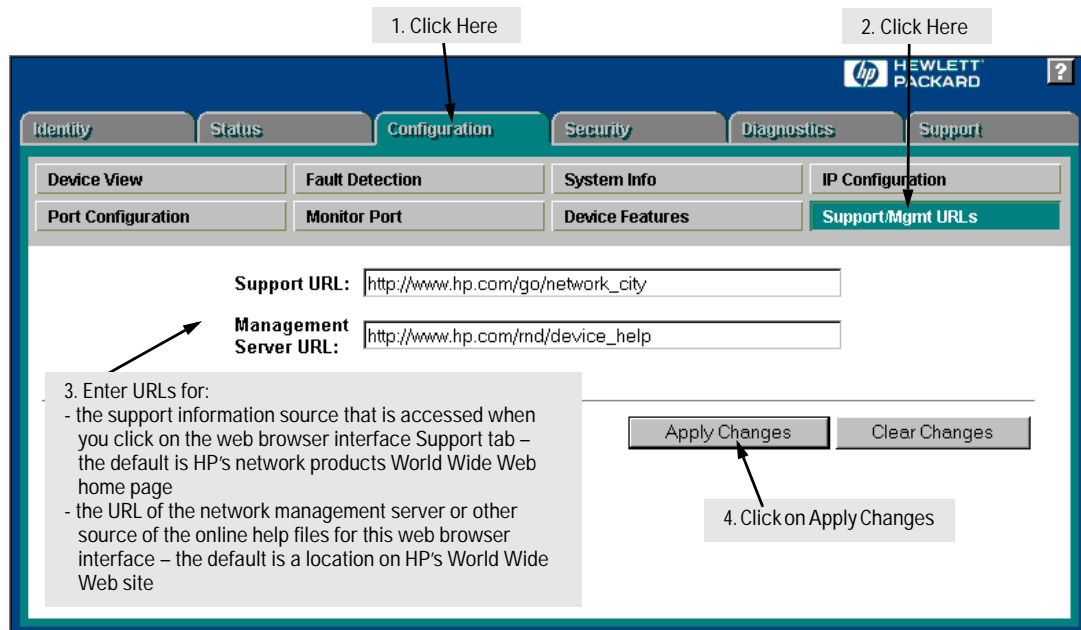


Figure 6-1. The Support/Mgmt URLs Window

### Support URL

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

[http://www.hp.com/go/network\\_city](http://www.hp.com/go/network_city)

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

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

## Management Server URL

This is the site for two purposes:

- the location of online help for the web browser interface
- the URL of a network management station running HP TopTools for Hubs & Switches

The default URL is:

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

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

Alternatively, you can enter the IP address or DNS name of a network management station on your network that is running HP TopTools for Hubs & Switches. That product also includes the help files for the web browser interface.

Additionally, HP Top Tools for Hubs & Switches has the capability of performing network-wide policy management and configuration of your switch. This field identifies the management station that is performing that function. If HP TopTools for Hubs & Switches is running on your network and has discovered your switch as it builds the network topology image, TopTools will automatically overwrite the Management Server URL field with the address or name of the management station on which it is running.

---

## IP Configuration

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

- IP address, subnet mask, and (optionally) the gateway address for the switch so that it can be managed in an IP network from the web browser interface, SNMP-based network management station, or by the switch console through a Telnet session.
- The time server information (used if you want the switch to get its time information from another device operating as a Timep server)

The initial IP configuration process is described in chapter 2, “Configuring an IP Address on the Switch”.

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

---

### Note

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

By default, the switch is configured to receive IP addressing from a DHCP/Bootp server that you have configured correctly with information for your switch. Refer to “DHCP/Bootp Operation” on page 6-10 for information on setting up automatic configuration from a server.

Through the web browser interface or switch console, you can manually enter a different address, or you can disable the IP operation.

---

### Notes:

- The IP addressing used in the switch should be compatible with your network. The IP address must be unique; the subnet mask must be the same for all devices on the same IP network.
- If you plan to connect to other networks that use globally administered IP addressing, refer to “Globally Assigned IP Network Addresses” on page 6-14.

For information on how IP addressing affects switch performance, refer to “How IP Addressing Affects Switch Operation” on page 6-9.

## Configuring IP Address from the Web Browser Interface

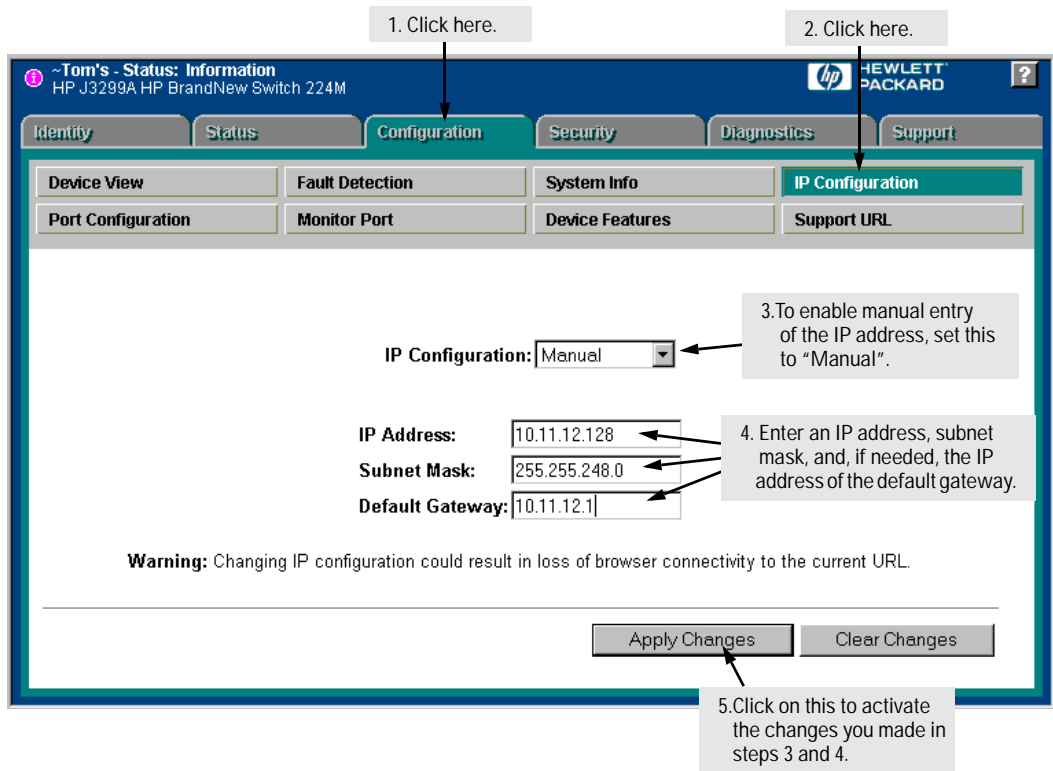


Figure 6-2. Configuring IP Addressing on the Web Browser Interface

Parameter	Description
IP Configuration	The method the switch uses to acquire its IP service configuration. <ul style="list-style-type: none"><li>• DHCP/Bootp: The switch attempts to get its IP configuration or its complete configuration from a DHCP or Bootp server.</li><li>• Manual: Enables you to manually enter the IP configuration into the next three fields.</li><li>• Disabled: Network management access to the switch over IP is disabled.</li></ul>
IP Address	IP address for the switch IP interface. If DHCP/Bootp is selected for IP Configuration, this is a read-only field displaying the value received from a DHCP or Bootp server.
Subnet Mask	The same subnet mask that is used by all devices in the IP subnet being configured. If DHCP/Bootp is selected for IP Configuration, this is a read-only field displaying the value received from a DHCP or Bootp server.
Default Gateway	The IP address of the next-hop gateway node for reaching off-subnet destinations. Used as the default gateway if the requested destination address is not on the local subnet. If DHCP/Bootp is selected for IP Configuration, this is a read-only field displaying the value received from a DHCP or Bootp server.

## Configuring IP Address from the Switch Console

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

Do one of the following:

- To use the console, set the **IP Config** parameter to **Manual** and then manually enter the IP address and subnet mask you want for the switch.
- If you plan to use DHCP or Bootp, use the console to ensure that the IP Config parameter is set to DHCP/Bootp, then refer to “DHCP/Bootp Operation” on page 6-10.

### To Access IP Addressing:

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

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

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

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

```
HP ProCurve Switch 212M          Switch1          18-Jun-1998  17:48:52
----- TELNET - MANAGER MODE -----
          Switch Management Access Configuration - Internet (IP) Service

Time Protocol Config [DHCP] : DHCP
TimeP Poll Interval (min) [720] : 720

IP Config [DHCP/Bootp] : Manual
IP Address : 11.22.33.44
Subnet Mask : 255.255.248.0
Gateway : 11.22.33.1

Actions->  Cancel      Edit      Save      Help

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

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



2. Press **[E]** (for **E**dit).
3. Select the **IP Config** field and use the Space bar to select **Manual**.
4. Select the **IP Address** field and enter the IP address 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 **S**ave) and return to the Switch Management Access Configuration menu.

## How IP Addressing Affects Switch Operation

Without an IP address and subnet mask compatible with your network, your control of the switch is limited to what you can do through a direct console connection, and some of the switch features will not be available. To be able to use the full performance capabilities HP proactive networking offers through the switch, you should configure the switch with an IP address and subnet mask compatible with your network. The following table compares the features available on the switch without and with an IP address.

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

## DHCP/Bootp Operation

### Overview

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

---

#### Note

The Switch 212M and Switch 224M are compatible with both DHCP and Bootp servers.

Once the switch acquires an IP configuration from either a DHCP or Bootp server, it displays the IP address, subnet mask, and gateway information in the IP Configuration screen.

---

### The DHCP/Bootp Process

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

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

The switch properly handles replies from either type of server. If multiple replies are returned, the switch tries to use the first DHCP reply.

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

## DHCP Operation

A significant difference between a DHCP configuration and a Bootp configuration is that an IP address assignment from a DHCP server is automatic, requiring no configuration of the DHCP server. Using that automatic feature, though, the address is temporarily leased. Periodically the switch is required to renew its lease of the IP configuration.

As a result, the IP addressing provided by the server may be different each time the switch reboots or renews its configuration from the server. This may cause a problem for you if you access the switch through the web browser interface, since the IP address is used as the browser URL.

However, you can fix the address assignment for the switch by doing either of the following:

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

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

## Bootp Operation

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

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

```
j3299switch:\  
  ht=ether:\  
  ha=0060b0123456:\  
  ip=11.22.33.44:\  
  sm=255.255.248.0:\  
  vm=rfc1048
```

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

```
j3299switch:\  
  ht=ether:\  
  ha=080009123456:\  
  ip=11.22.33.44:\  
  sm=255.255.248.0:\  
  gw=11.22.33.1:\  
  lg=55.66.77.88:\  
  ts=11.22.33.55:\  
  T144="switch.cfg":\  
  vm=rfc1048
```

*where:*

j3299switch	is a user-defined symbolic name to help you find the correct section of the bootptab file. If you have multiple switches that will be using Bootp to get their IP configuration, you should use a unique symbolic name for each switch.
ht	is the "hardware type". For the Switch 212M and Switch 224M, set this to <b>ether</b> (for Ethernet). <i>This tag must precede the ha tag.</i>
ha	is the "hardware address". Use the switch's 12-digit base MAC address.
ip	is the IP address to be assigned to the switch.
sm	is the subnet mask of the subnet in which the switch is installed.
gw	is the IP address of the default gateway for the switch.
lg	is the TFTP server address (source of switch configuration file).
ts	is the IP address of the time server.
T144	is the vendor-specific "tag" identifying the configuration file to download.
vm	is a required entry that specifies the Bootp report format. For the Switch 212M and Switch 224M, set this parameter to <b>rfc1048</b> .

---

## Note

---

The above Bootp table entry is a sample that will work for the Switch 212M and 224M when the appropriate addresses and file names are used. There are other features and parameters that can be implemented with Bootp. See the documentation for your Bootp server for more information.

## Configuring DHCP/Bootp

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

This procedure assumes that, for Bootp operation:

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

and, for DHCP operation:

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

### To configure the switch for DHCP/Bootp:

1. From the switch console Main Menu, select
  2. **Switch Management Access Configuration (IP, SNMP, Console) ...**
    1. **IP Configuration**
2. Press **[E]** (for Edit mode), then use **[↓]** to move the cursor to the **IP Config** parameter field.
3. Use the Space bar to select the **DHCP/Bootp** option for the **IP Config** parameter. (This causes the IP Address, Subnet Mask, and Gateway parameters to not be accessible.)
4. Press **[Enter]** to exit from edit mode, then press **[S]** to save the configuration change.

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

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

## Globally Assigned IP Network Addresses

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

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

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

---

## SNMP Communities

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

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

For more on this topic, refer to chapter 5, “Using HP TopTools To Monitor and Manage Your Network”, and to the console online help.

### Configuring SNMP Communities from the Switch Console

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

---

**Caution:**

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

---

## To View, Edit, or Add SNMP Communities:

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

```
HP ProCurve Switch 212M          Switch1          18-Jun-1998 17:51:48
----- TELNET - MANAGER MODE -----
Switch Management Access 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.
```

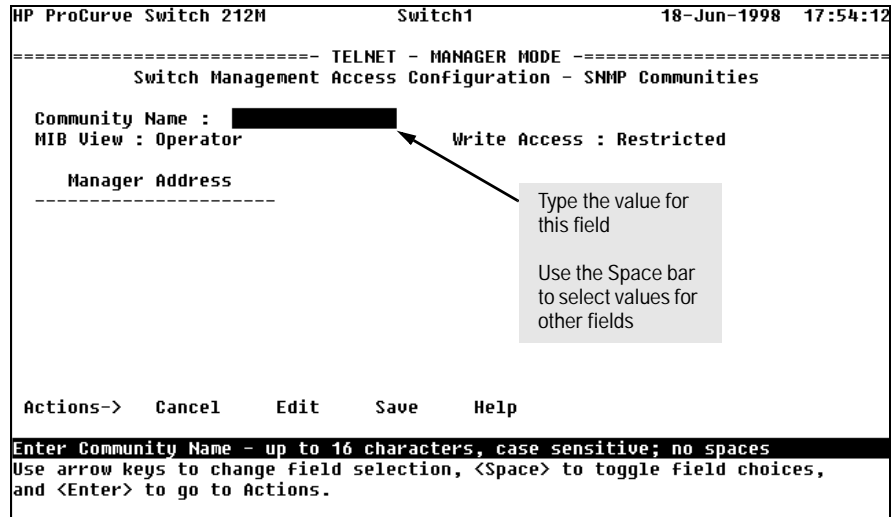
Add and Edit options are used to modify the SNMP options. See figure 6-5.

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

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

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





If you are adding a community, the Community Name field is blank.

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

Type the value for this field

Use the Space bar to select values for other fields

Figure 6-5. The SNMP Add or Edit Screen

**Note:**

In the default configuration, no manager addresses are configured. In this case, all management stations using the correct community name may access the switch with the View and Access levels configured for that community. If you want to limit access to the switch, you can enter up to ten IP addresses of authorized management stations into the Manager Address field. Entering the IP addresses in the Manager Address field limits access to only those addresses.

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

# Trap Receivers

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

If the **Send Authentication Traps** field is set to Yes, an authentication trap is sent to the addresses on the screen if any management station attempts an unauthorized access of the switch. Check the event log to help determine why the authentication trap was sent. (Refer to “Using the Event Log To Identify Problem Sources” on page 8-6.)

To configuring Trap Receivers from the switch console, follow these steps:

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

```
HP ProCurve Switch 212M          Switch1          18-Jun-1998  17:59:25
----- TELNET - MANAGER MODE -----
Switch Management Access Configuration - Trap Receivers

Send Authentication Traps [No] : No

-----
Address          Community      Events Sent in Trap
-----
11.22.33.55      public         Not INFO
11.22.33.57      public         Not INFO
10.4.8.12        public         Not INFO
11.22.44.11      public         Not INFO
11.22.44.22      public         Not INFO
11.22.33.66      public         Not INFO
11.22.33.77      public         Not INFO
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 6-6. The Trap Receivers Configuration Screen (Default Values)

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

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

7. Press **[Enter]**, then press **[S]** (for **S**ave) and return to the Switch Management Access Configuration menu.

## Console/Serial Link

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

- Enable or disable inbound Telnet access (default: enabled)
- Enable or disable web browser interface access (default: enabled)
- Specify:
  - Terminal type (default: VT100)
  - Console screen refresh interval for statistics screens (the frequency with which statistics are updated on the screen—default: 3 seconds)
  - The types of events displayed in the console event log (default: all)
- Adjust the console configuration to customize the connection with the PC or terminal you are using for console access.
  - Baud Rate (default: Speed Sense)
  - Connection Inactivity Time (default: 0—off)

In most cases, the default configuration works well. If you need to change any of the above parameters, use the switch console.

---

### Note:

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

---

## Using the Switch Console To Configure the Console/Serial Link

This screen enables you to:

- Enable or disable inbound Telnet, and web browser interface access (identified as Web Agent Enabled)
- Modify console and serial link parameters

### To Access Console/Serial Link Features

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

```

HP ProCurve Switch 212H          Switch1          18-Jun-1998  18:01:17
----- TELNET - MANAGER MODE -----
Switch Management Access Configuration - Console/Serial Link

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

Baud Rate [Speed Sense] : Speed Sense

Connection Inactivity Time (min) [0] : 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 6-7. The Console/Serial Link Configuration Screen (Default Values)

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

## System Information

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

### Configuring System Parameters from the Web Browser Interface

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

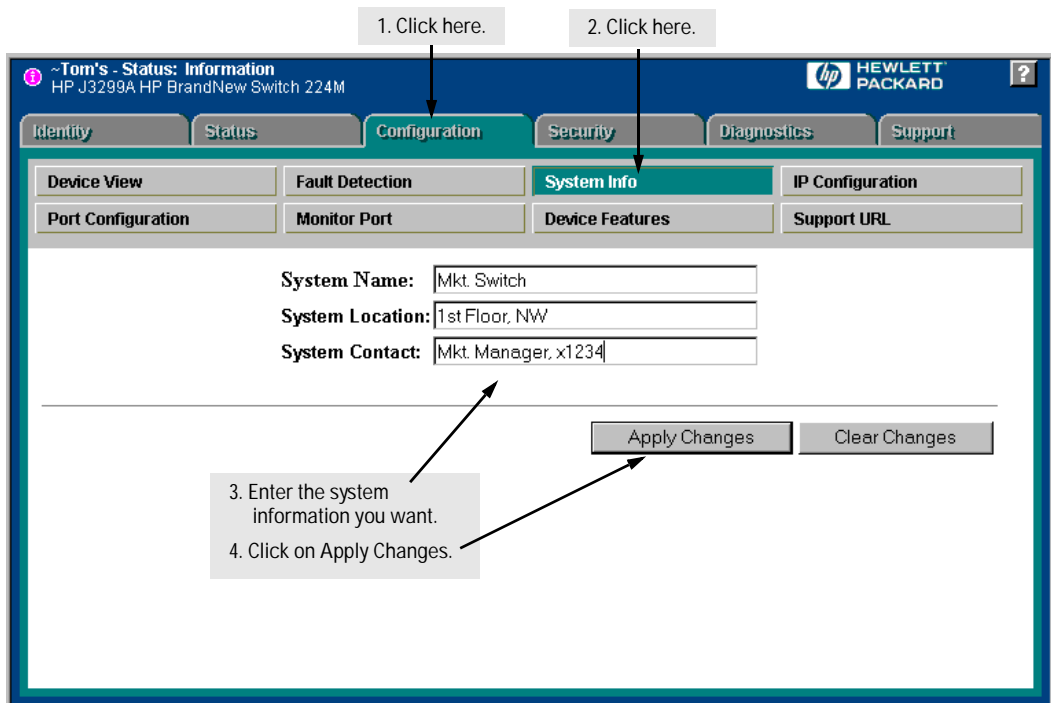


Figure 6-8. Configuring System Information from the Web Browser Interface

## Configuring System Information from the Console

To Access System Information:

1. From the Main Menu, select:
  3. Switch Configuration...
    1. System Information

```

HP ProCurve Switch 212M                Switch1                18-Jun-1998 17:36:52
----- TELNET - MANAGER MODE -----
Switch Configuration - System Information
System Name
System Name : Switch1
System Contact : John Doe
System Location : Pole 5

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

**Note:**

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

To set the time and date, set the Time Protocol parameters under “IP (Internet) Service” (page page 6-5) for your time server, or use the time and date commands described in chapter 7, “Monitoring and Analyzing Switch Operation”.

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

## Port Settings

From the **web browser interface and switch console** you can configure the operating state for each switch port.

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

**Table 6-2. Port Settings Parameters**

Parameter	Description
Enabled	<p><b>Yes</b> (default): The port is ready to be connected in a network.</p> <p><b>No</b>: The port will not operate, even if properly connected in a network. Use this setting if the port needs to be shut down for diagnostic purposes or while you are making topology changes, for example.</p>
Mode or Config Mode	<p>For 10T ports:</p> <p><b>10HDx</b> (default): 10 Mbps, Half Duplex</p> <p><b>10FDx</b>: 10 Mbps, Full Duplex</p> <p>For 10/100TX ports:</p> <p><b>Auto</b> (default): Auto-negotiates with the port at the other end of the link for speed (10 Mbps or 100 Mbps) and data transfer operation (half-duplex or full-duplex). <b>Note</b>: Ensure that the device attached to the port is configured for the same setting that you select here. Also, if "Auto" is used the device to which the port is connected must operate in compliance with the IEEE 802.3u "Auto Negotiation" standard for 100Base-T networks. See the Auto Negotiation Note on the next page.</p> <p><b>10HDx</b>: 10 Mbps, Half Duplex</p> <p><b>100HDx</b>: 100 Mbps, Half Duplex</p> <p><b>10FDx</b>: 10 Mbps, Full Duplex</p> <p><b>100FDx</b>: 100 Mbps, Full Duplex</p>
Flow Control	<p><b>Disabled</b> (default): No flow control is applied to inbound traffic.</p> <p><b>Enabled</b>: The flow control method implemented depends on whether the ports is configured to operate in full-duplex or half-duplex mode:</p> <ul style="list-style-type: none"> <li>• If Full Duplex - IEEE 802.3x Flow Control is applied.</li> <li>• If Half Duplex - Back pressure is applied.</li> </ul> <p>See the Flow Control Note on the next page for an explanation of these methods.</p>

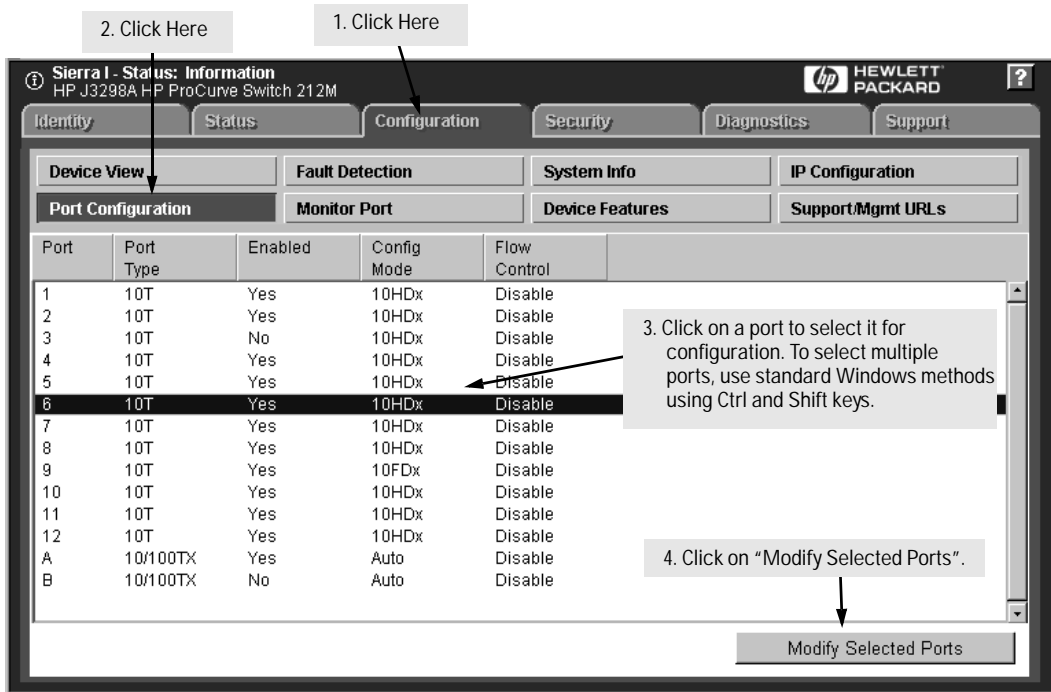


**Auto-Negotiation Note:** This feature complies with the IEEE 802.3u Auto Negotiation standard, and is the default setting for the 10/100TX ports on the switch. Using Auto, the port automatically selects the network speed (10 or 100 Mbps) and the data transfer operation (full- or half-duplex) for the connection to another device, provided that the other device also complies with the IEEE 802.3u Auto Negotiation protocol and is set to Auto. If the other device does not comply with the 802.3u standard, or is not set to Auto, then the port configuration on the switch must be manually set to match the port configuration on the other device.

**Flow Control Note:**

- **IEEE 802.3 Flow Control** is applied to ports that are configured to operate in full-duplex mode only. When the switch detects congestion on a port, it transmits a special “pause” (XOFF) packet out the port. *The receiving device must support 802.3x flow control in order to interpret this packet.* The receiving device will halt transmission of any packets until the switch sends a “resume” (XON) packet.
- **Back pressure** is applied to ports that are configured to operate in half-duplex mode. When the switch detects congestion on the port, it issues a JAM signal, simulating a collision that prevents other attached stations from transmitting. *It is recommended that if you use this flow control method, it should be configured only on those ports that are connected to a single end node, not on ports that are connected to a switch, hub, bridge, or router.*

## Configuring Port Parameters from the Web Browser Interface



Clicking on **Modify Selected Ports** opens up the following screen.

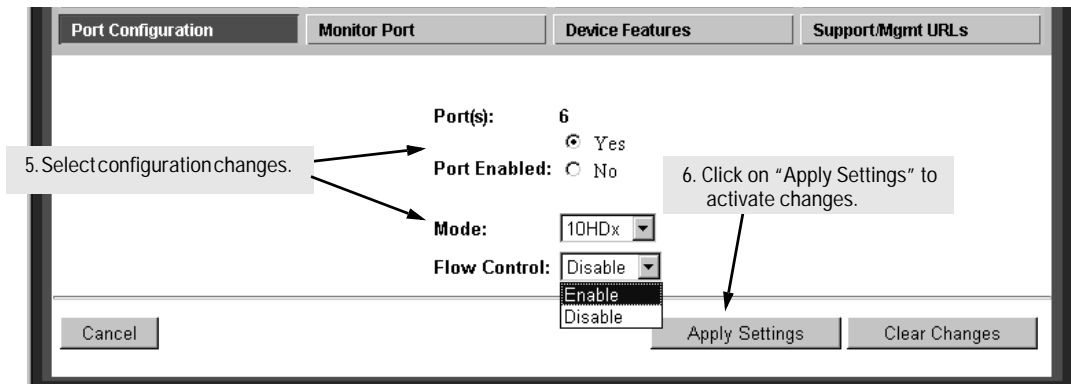


Figure 6-10. Example of Port Configuration and Modify Selected Ports Windows on the Web Browser Interface

## Configuring Port Parameters from the Switch Console

To Access Port Configuration:

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

```

HP ProCurve Switch 212M          Switch1          18-Jun-1998  21:38:10
----- CONSOLE - MANAGER MODE -----
Switch Configuration - Port Settings
-----
Port   Type   Enabled   Mode   Flow Ctrl
-----
 1     10T   | Yes     10FDx  Enable
 2     10T   | Yes     10HDx  Disable
 3     10T   | Yes     10HDx  Disable
 4     10T   | Yes     10HDx  Disable
 5     10T   | Yes     10HDx  Disable
 6     10T   | Yes     10HDx  Enable
 7     10T   | Yes     10HDx  Disable
 8     10T   | Yes     10HDx  Disable
 9     10T   | Yes     10HDx  Enable
10     10T   | Yes     10HDx  Disable
11     10T   | Yes     10HDx  Disable

Actions->  Cancel  Edit  Save  Help
Edit the fields displayed above.
Use arrow keys to change action selection and <Enter> to execute action.
    
```

Figure 6-11. Example of the Port Settings Screen

2. Press **[E]** (for **Edit**). The cursor moves to the **Enabled** field for the first port.
3. See table 6-2 on page 6-24 for the available values for each parameter and definitions of each value. Or, refer to the online help provided with this screen.
4. When you have finished making changes to the above parameters, press **[Enter]**, then press **[S]** (for **Save**) and return to the Switch Configuration menu.

## Network Monitoring Port Features

From the **web browser interface and switch console** you can designate a port for monitoring traffic on one of the other switch ports. The monitoring is accomplished by copying all traffic from the specified monitored port to the designated monitoring port.

**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.

### Configuring Port Monitoring from the Web Browser Interface

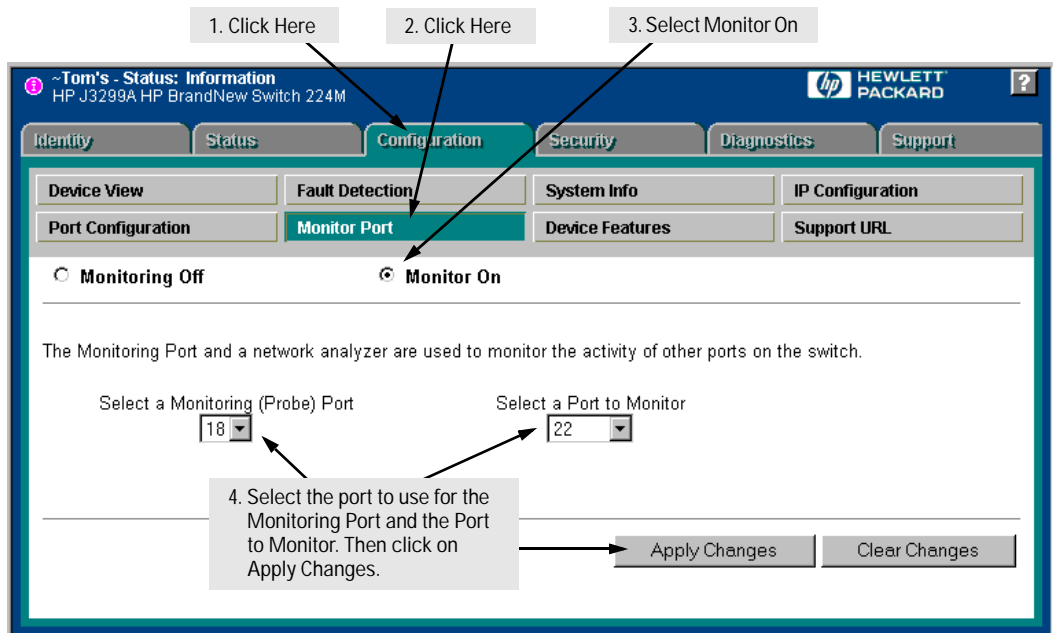


Figure 6-12. Setting Up Port Monitoring from the Web Browser Interface

## Configuring Port Monitoring from the Switch Console

To Access Port Monitoring:

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

```
HP ProCurve Switch 212M          Switch1          18-Jun-1998  21:41:46
----- CONSOLE - MANAGER MODE -----
Switch Configuration - Network Monitoring Port

Monitoring Enabled [No] : Yes
Monitoring Port : 4
Monitored Port : 5

Actions->  Cancel    Edit    Save    Help

Select the port whose traffic is to be monitored.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

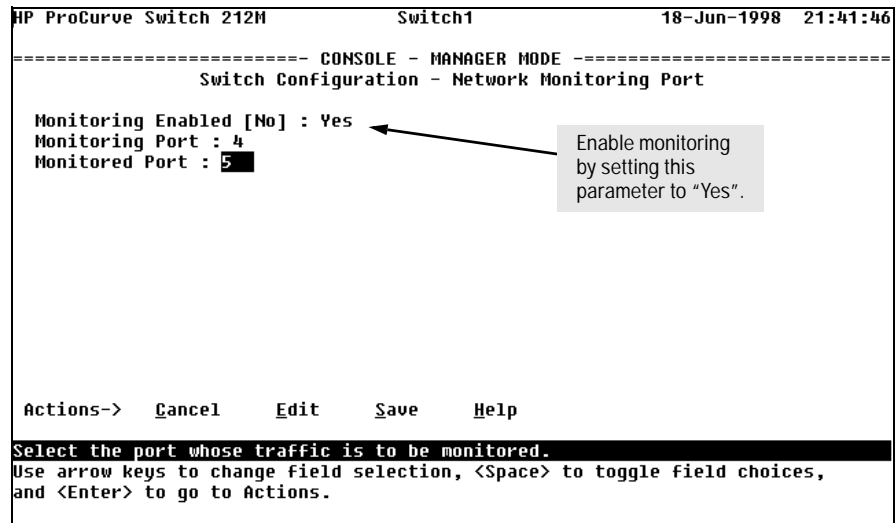


Figure 6-13. Network Monitoring Port Configuration Screen

2. In the Actions menu, press **[E]** (for **E**dit).
3. If monitoring is currently disabled (the default) then enable it by pressing the Space bar (or **[Y]**) to select **Yes**.
4. Press **[↓]** to display a screen similar to figure 6-13 and move the cursor to the **Monitoring Port** and **Monitored Port** parameters and type in the port number or press the **[Space]** bar to scroll through the available ports and display the port you want to use for each of these functions.
5. When you are finished, press **[Enter]**, then press **[S]** (for **S**ave) and return to the Switch Configuration menu.

## Spanning Tree Protocol (STP)

The switch uses the IEEE 802.1d Spanning Tree Protocol (STP), when enabled, to ensure that only one path at a time is active between any two nodes on the network. In networks where there is more than one physical path between any two nodes, STP ensures a single active path between them by blocking all redundant paths.

Enabling STP is necessary in such networks because having more than one path between a pair of nodes causes loops in the network, which can result in a switch detecting the same node on more than one port. This results in duplication of messages, leading to a “broadcast storm” that can bring down the network.

Enabling STP also allows you to intentionally create redundant links in your network for critical communication paths. 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.

From the **web browser interface** you can activate the IEEE 802.1d Spanning Tree Protocol (STP); from the **switch console** you can activate STP and adjust spanning tree parameters. In the factory default configuration, STP is off. If there are any redundant paths (loops) between nodes in your network, you should set the Spanning Tree Enabled parameter to Yes.

---

### Caution

Because the switch automatically gives faster links a higher priority, STP selects the higher speed links as the active links unless there is an equipment problem. Thus, 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, read the IEEE 802.1d standard.

---

## Enabling STP from the Web Browser Interface

This procedure enables or disables STP on the switch.

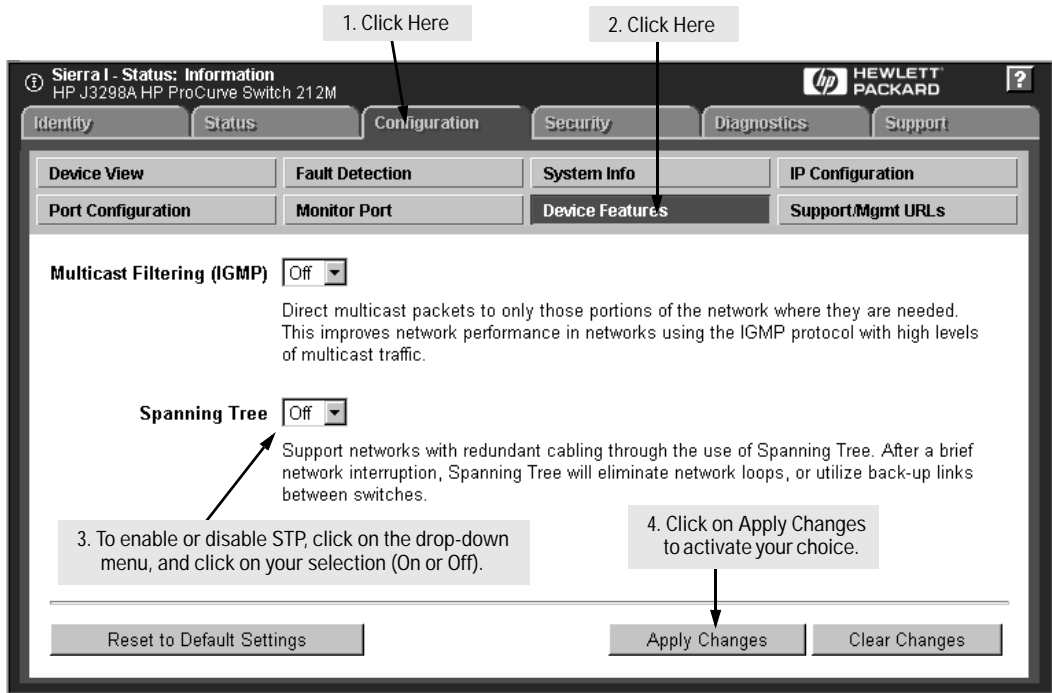


Figure 6-14. Device Features Screen for Enabling Spanning Tree

Parameter	Description
Spanning Tree (Default: Off)	Enables or disables Spanning Tree Protocol across all ports on the switch. Other STP parameters are available through the console interface. Enabling or disabling STP through the web browser interface does not affect the settings of these other parameters. For more information on STP operation, refer to "How STP Operates" on page page 6-33.

## Using the Switch Console To Configure STP

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

### Caution

If you enable STP, it is recommended that you leave the remainder of the STP parameter settings at their default values until you have had an opportunity to evaluate STP performance in your network. Because incorrect STP settings can adversely affect network performance, you should avoid making changes without having a strong understanding of how STP operates. To learn the details of STP operation, refer to the IEEE 802.1d standard. For an overview, see “How STP Operates” on page 6-33.

### To Access STP:

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

```
HP ProCurve Switch 212M                Switch1                18-Jun-1998 17:23:59
----- TELNET - MANAGER MODE -----
Switch Configuration - Spanning Tree Operation

Spanning Tree Enabled [No] : Yes
STP Priority [32768] : 32768           Hello Time [2] : 2
Max Age [20] : 20                     Forward Delay [15] : 15

Port  Type      Cost  Priority | Port  Type      Cost  Priority
-----+-----+-----+-----|-----+-----+-----+-----
 1   10T         100   128     | 8     10T         100   128
 2   10T         100   128     | 9     10T         100   128
 3   10T         100   128     | 10    10T         100   128
 4   10T         100   128     | 11    10T         100   128
 5   10T         100   128     | 12    10T         100   128
 6   10T         100   128     | 13    10/100TX    10    128
 7   10T         100   128     | 14    10/100TX    10    128

Actions->  Cancel  Read-Only Fields  Help

Select whether to enable Spanning Tree operation for the switch.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

Figure 6-15. Example of the STP Configuration Screen



4. If the remaining STP parameter settings are correct for your network, go to step 7.
5. Use **[Tab]** or the arrow keys to select the next parameter you want to change, then type in the new value. (If you need information on STP parameters, press **[Enter]** to select the **Actions** line, then press **[H]** to get help.)
6. Repeat step 5 for each additional parameter you want to change.
7. When you are finished editing parameters, press **[Enter]**, then press **[S]** (for **Save**) and return to the Switch Configuration menu.

## How STP Operates

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

In the event of a topology change such as a switch, bridge, or data link failure in the network, STP develops a new spanning tree that may result in changing some ports from the blocking state to the forwarding state.

If an active path fails, STP automatically activates (unblocks) an available backup to serve as the new active path for as long as the original active path is down. As shown in the following illustration, the active path between nodes A and B uses links 1 and 3 which have a lower total path cost than the path using links 4, 2, and 3. If link 1 happens to go down, path 4→2→3 becomes the active path.

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

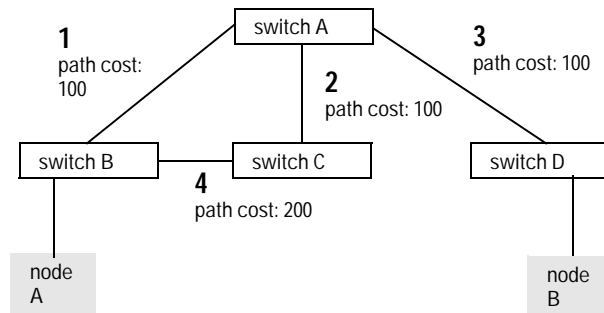


Figure 6-16. Example of Active and Backup Paths Between Two Nodes

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

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

IGMP is useful in multimedia applications such as LAN TV, desktop conferencing, and collaborative computing, where there is multipoint communication; that is, communication from one to many hosts, or communication originating from many hosts and destined for many other hosts. In such multipoint applications, IGMP will be configured on the hosts, and multicast traffic will be generated by one or more servers, inside or outside of the local network. Switches in the network that support IGMP can then be configured to direct the multicast traffic to only the ports where needed. In addition to the Switch 212M and Switch 224M, other HP switches that support IGMP include:

- HP Switch 1600M
- HP Switch 2400M
- HP Switch 4000M
- HP Switch 8000M
- HP Switch 2000 (B-version)
- HP Switch 800T

Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. If no other querier is detected, the switch will also function as the querier. (If you need to disable the querier feature, you can do so through the IGMP configuration MIB. Refer to “Changing the Querier Configuration Setting” on page 6-42.)

---

### Note

In order for IGMP service to take effect, an IP address must be configured on the switch. Refer to “IP Configuration” on page 6-5.

For more information on IGMP operation, refer to “How IGMP Operates” on page 6-38.

## Configuring IGMP from the Web Browser Interface

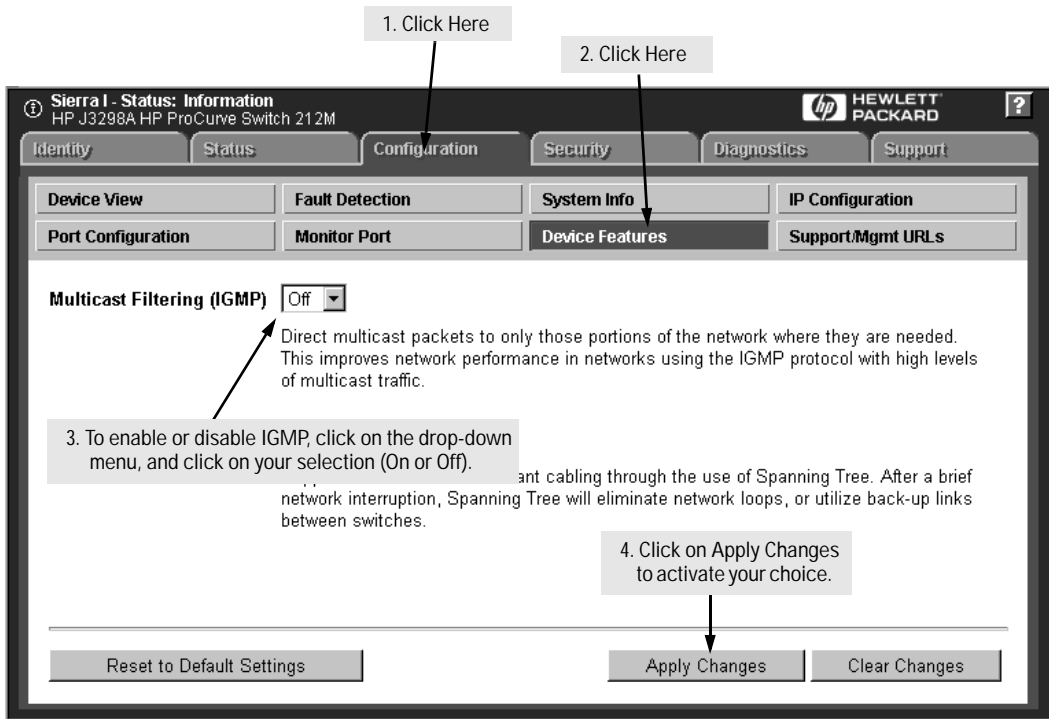


Figure 6-17. Configuring IGMP from the Web Browser Interface

Parameter	Description
Multicast Filtering (IGMP)	Determines whether the switch uses IGMP on a per-port basis to manage IP Multicast traffic.
Default: Off	When Off, all ports on the switch simply forward IP multicast traffic.
	When On, the feature enables each port on the switch to detect IGMP queries and report packets, and to manage IP multicast traffic.
	When you use the web browser Interface to enable Multicast Filtering, the default operation is for each port in the switch to automatically forward or drop IGMP traffic, depending on whether there are any IGMP hosts or multicast routers on the port.

Parameter	Description
Further Options Available in the Switch Console	<p>By using the switch console, you can make these further changes to IGMP operation:</p> <ul style="list-style-type: none"><li>• On a per-port basis, block or forward all IP multicast traffic.</li><li>• For all ports on the switch, forward IP multicast traffic at high priority. (The default is for the switch to process IGMP traffic, along with other traffic, in the order received.)</li><li>• Change the querier configuration setting. (By default, the switch will act as a querier if a multicast router is not present to perform this function.)</li></ul> <p>For more information, refer to “Using the Switch Console to Configure IGMP” (page 6-36) and “How IGMP Operates” (page 6-38).</p>

## Using the Switch Console To Configure IGMP

In the factory default configuration, IGMP is disabled. When you use either the console or the web browser interface to enable IGMP on the switch, the switch forwards IGMP traffic only to ports belonging to multicast groups. Using the console enables these additional options:

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

For more information, refer to “How IGMP Operates” on page 6-38.

## To Access IGMP Service:

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

1. From the Main Menu, select:

### 3. Switch Configuration

#### 5. Advanced Features

#### 1. IP Multicast (IGMP) Service

```

HP ProCurve Switch 212M                Switch1                19-Jun-1998  0:37:28
-----
                CONSOLE - MANAGER MODE -----
                Switch Configuration - Advanced Features - IGMP Service

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

Port   Type   IP Mcast | Port   Type   IP Mcast
-----+-----+-----+-----+-----+-----
 1    10T    | Auto   |  8    10T    | Auto
 2    10T    | Auto   |  9    10T    | Auto
 3    10T    | Blocked| 10    10T    | Auto
 4    10T    | Auto   | 11    10T    | Auto
 5    10T    | Forward| 12    10T    | Auto
 6    10T    | Auto   |  A    100FX   | Auto
 7    10T    | Auto   |  B    10/100TX  | Auto

Actions->  Cance1  Edit  Save  Help
Edit the fields displayed above.
Use arrow keys to change action selection and <Enter> to execute action.
    
```

Figure 6-18. Example of the IGMP Service Screen

2. Press **[E]** (for **Edit**) to highlight the **IGMP Enabled** parameter
3. Press the Space bar to select **Yes** (to enable IGMP).
4. Use **[↓]** to highlight the **Forward with High Priority** parameter.
5. If you want IGMP traffic to be forwarded with a higher priority than other traffic on the switch, use the Space bar to select **Yes**. Otherwise, leave this parameter set to **No**.
6. Use **[↓]** to highlight the **IP Mcast** parameter setting for a port you want to reconfigure. (The options are: **Auto**, **Blocked**, and **Forward**. Refer to the online Help for further information on these choices.)
7. Repeat step 6 for each port you want to configure.

8. 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 and return to the Advanced Features menu.

(It is not necessary to reboot the switch. The new IGMP configuration is implemented when you select "Save" in step 8.)

## How IGMP Operates

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

- **Query:** A message sent from the querier (multicast router or switch) asking for a response from each host belonging to the multicast group. If a multicast router supporting IGMP is not present, then the switch must assume this function in order to elicit group membership information from the hosts on the network. (If you need to disable the querier feature, you can do so through console, using the IGMP configuration MIB. Refer to "Changing the Querier Configuration Setting" on page 6-42.)
- **Report:** A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
- **Leave Group:** A message sent by a host to the querier to indicate that the host has ceased to be a member of a specific multicast group.

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

**IGMP Data.** To display data showing active group addresses, reports, queries, querier access port, and active group address data (port, type, and access), see "IP Multicast (IGMP) Status" on page 7-16.

## Role of the Switch

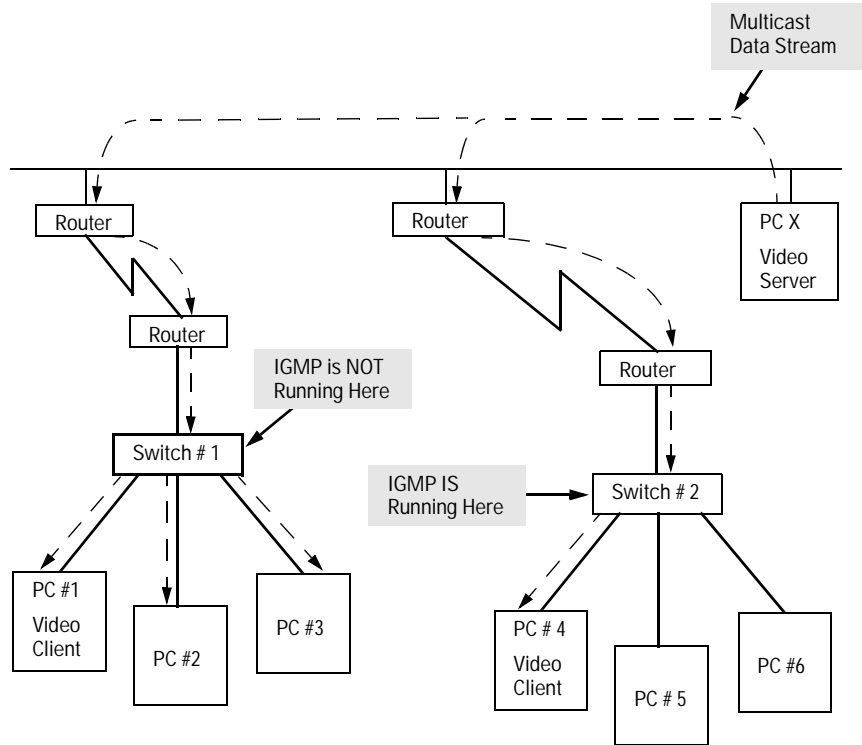
When IGMP is enabled on the switch, it examines the IGMP packets it receives:

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

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

Figure 6-19 on page 6-40 shows a network running IGMP.

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



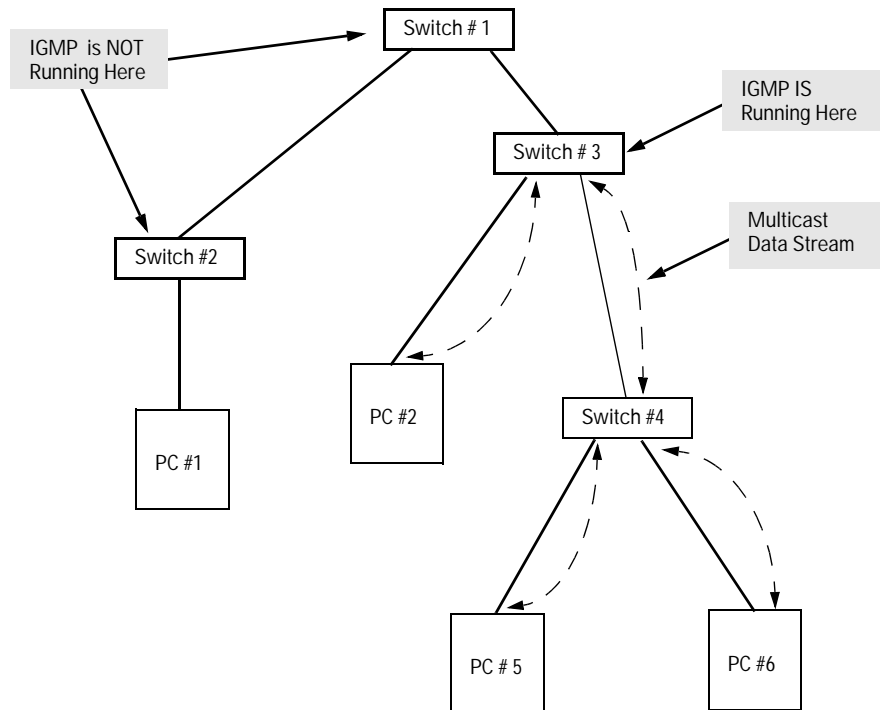
**Figure 6-19. The Advantage of Using IGMP**

The next figure (6-20) shows a network running IP multicasting using IGMP without a multicast router. In this case, the IGMP-configured switch runs as a querier.

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

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





**Figure 6-20. 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.

## Number of IP Multicast Addresses Allowed

The total number of IGMP filters (addresses) allowed in the switch is 255.

## 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.

---

### Note

---

The following commands are all case sensitive.

To disable the querier setting, select **Command Prompt** from the Diagnostics Menu and enter this command:

```
setmib hpSwitchIgmPQuerierState.1 -i 2
```

To enable the querier setting, enter this command:

```
setmib hpSwitchIgmPQuerierState.1 -i 1
```

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

```
getmib hpSwitchIgmPQuerierState.1
```

---

### Note

---

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

## Special Case IGMP Configuration

Normally, all members of a multicast group, both senders and receivers, join the multicast group through IGMP “join” requests. Certain applications, though, for example Microsoft® NetShow®, do not require the server to join the multicast group before they start sending the multicast data stream.

Because these applications operate in this way, the Switch 212M and 224M will not be able to recognize the server as part of the multicast group, and will disable the multicast communication between the server and the client members of the multicast group.

If you are using one of these applications, you must first configure the switch port to which the server is connected to **Forward** mode.

1. From the console Main Menu, select:

### 3. Switch Configuration

#### 5. Advanced Features

##### 1. IP Multicast (IGMP) Service

IGMP Service configuration screen similar to figure 6-18 on page 6-37 is displayed.

2. In the IGMP Service screen, press **[E]** (for **E**dit)
3. Use the arrow keys to highlight the **IP Mcast** parameter setting for the port to which the server is connected.
4. Press **[F]** or press the Space bar until **Forward** appears for the parameter value.
5. Press **[Enter]** and **[S]** (for **S**ave) to activate the changes you've made to the IGMP configuration and return to the Advanced Features menu.

The multicast communication between the server and the clients will now operate correctly.

---

## Note

If the server is not directly connected to the switch, and the server's multicast traffic is arriving at the switch through the querier port, the above procedure is *not* necessary. The querier device will automatically be a member of the multicast group and the multicast application traffic will be distributed properly.

If your switch, and not some other device, is acting as the querier, the above procedure *will* have to be completed.

---



# Monitoring and Analyzing Switch Operation

## Overview

You can use the switch console (and, in some cases, the web browser interface) to access read-only status and counter information to help you monitor, analyze, and troubleshoot switch operation.

This chapter describes the status and counters screens available through the switch console and/or the web browser interface.

### Note

The Event Log, a diagnostic tool that is often used for troubleshooting switch operation, is described in chapter 8, Troubleshooting. See “Using the Event Log To Identify Problem Sources” on page 8-6.

**Table 7-1. Available Status and Counters Information**

Status or Counters Type	Interface	Purpose
General System Information	Console	Lists switch-level operating information (page 7-3).
Management Address Information	Console	Lists the MAC address, IP address, and IPX network number for the switch (page 7-4).
Port Status Overview	Browser	Shows port utilization and the Alert Log (page 3-16).
Port Status	Browser Console	Displays the operational status of each port (page 7-5).
Port Counters	Browser Console	Summarizes port activity (page 7-7).
Address Table (Address Forwarding Table)	Console	Lists the MAC addresses of nodes the switch has detected on the network, with the corresponding switch port (page 7-11).
Port Address Table	Console	Lists the MAC addresses that the switch has learned from the selected port (page 7-12).
Spanning Tree Information	Console	Lists Spanning Tree data for the switch and for individual ports (page 7-14).
IP Multicast (IGMP) Status	Console	Lists IGMP groups, reports, queries, and port on which the querier is located (page 7-16).

# Switch Console Status and Counters Menu

To display the switch console Status and Counters menu, from the console Main Menu select:

## 1. Status and Counters

```
HP ProCurve Switch 212H          DEFAULT_CONFIG          12-Jun-2000  8:31:15
----- CONSOLE - MANAGER MODE -----
                          Status and Counters Menu

  1. General System Information
  2. Switch Management Address Information
  3. Port Status
  4. Port Counters
  5. Address Table
  6. Port Address Table
  7. Spanning Tree Information
  8. Advanced Features Status...
  0. Return to Main Menu...

Displays switch management information including software versions.
To select menu item, press item number, or highlight item and press <Enter>.
```

Figure 7-1. The Status and Counters Menu

Each of the above menu items accesses the read-only screens described on the following pages. Refer to the online help for a description of the entries displayed in these screens.

# General System Information

To access this screen from the console Main Menu, select:

## 1. Status and Counters

### 1. General System Information

```
HP ProCurve Switch 212M          Switch1          18-Jun-1998  16:58:27
----- TELNET - MANAGER MODE -----
                Status and Counters - General System Information

System Contact   : John Doe
System Location  : Pole 5

Firmware revision : D.05.X1          Base MAC Addr   : 0060b0-8ae220
ROM Version      : D.05.X2          Serial Number    : SD300CI00194

Up Time         : 2 days
CPU Util (%)    : 16

IP Mgmt - Pkts Rx : 347,954          Packet - Total  : 200
          Pkts Tx : 146,806          Buffers Free   : 198
                                          Lowest        : 162
                                          Missed       : 0

Actions->  Back  Help

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

Figure 7-2. Example of General Switch Information

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

# Switch Management Address Information

To access this screen from the Main Menu, select:

1. Status and Counters
2. Switch Management Address Information

```
HP ProCurve Switch 212M          DEFAULT_CONFIG          12-Jun-2000  8:50:41
----- CONSOLE - MANAGER MODE -----
                Status and Counters - Management Address Information

Time Server Address :

MAC Address       : 0060b0-8a6ca0
IP Address        : 11.22.33.44
IPX Network Number :

Actions->  Back  Help

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

Figure 7-3. Example of Management Address Information

This screen displays addresses that are important for management of the switch. See the online Help for details.



# Port Status

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

## Displaying Port Status from the Web Browser Interface

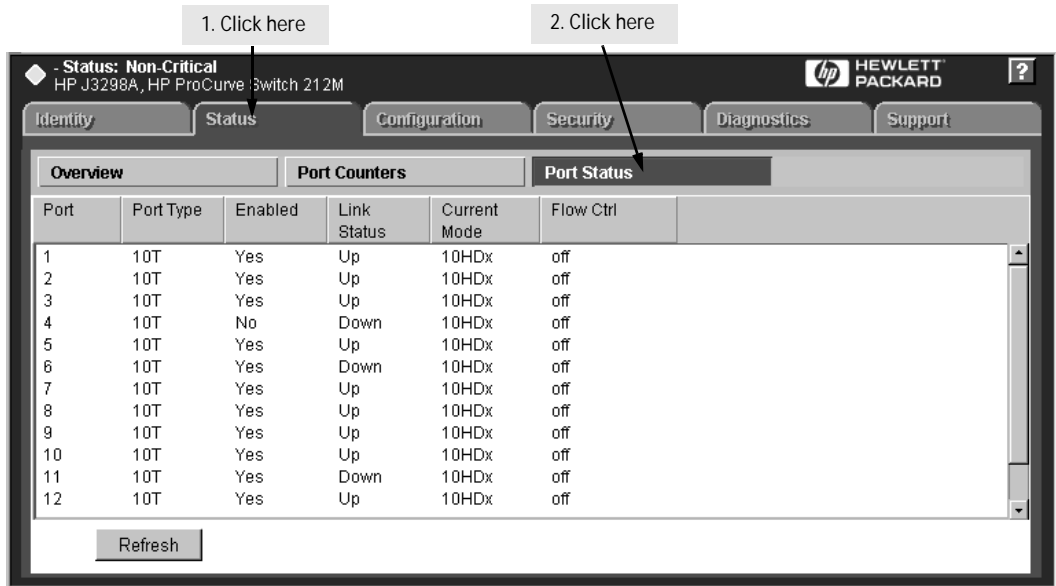


Figure 7-4. Example of Port Status on the Web Browser Interface

## Displaying Port Status from the Switch Console

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

### 1. Status and Counters

### 3. Port Status

```
HP ProCurve Switch 212M          DEFAULT_CONFIG          2-Jan-1990  8:56:53
----- CONSOLE - MANAGER MODE -----
                Status and Counters - Port Status

Port   Type   Enabled  Status   Mode     Flow Ctrl
-----
1      10T    Yes      Up       10HDx    off
2      10T    Yes      Down     10HDx    off
3      10T    Yes      Up       10HDx    off
4      10T    No       Down     10HDx    off
5      10T    Yes      Down     10HDx    off
6      10T    Yes      Down     10HDx    off
7      10T    Yes      Down     10HDx    off
8      10T    Yes      Down     10HDx    off
9      10T    Yes      Down     10HDx    off
10     10T    Yes      Down     10HDx    off
11     10T    Yes      Down     10HDx    off

Actions->  Back  Help

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

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

## Port Counters

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

These screens enable you to determine the traffic patterns for each port. Port Counter features include:

- Dynamic display of counters summarizing the traffic on each port since the last reboot or reset
- Option to reset the counters to zero (for the current console session). This is useful for troubleshooting. Refer to the Note, below.
- An option to display the link status, and further port activity details for a specific port (console: **Show details** or browser: **Details for Select Port**).

---

### Note

The **Reset** action resets the counter display to zero for the current session, but does not affect the cumulative values in the actual hardware counters. (In compliance with the SNMP standard, the values in the hardware counters are not reset to zero unless you reboot the switch.) Exiting from the console session and starting a new session restores the counter displays to the accumulated values in the hardware counters.

---

## Displaying Port Counters from the Web Browser Interface

1. Click here

2. Click here

3. To view details about the traffic on a particular port, highlight that port number, then click on **Details for Select Port**.

Port	MCast Rx	MCast Tx	BCast Rx	BCast Tx	Pkts Rx	Pkts Tx	Errors Rx
1	174208	6	290504	211	10427992	1062677	1281960
2	0	0	0	0	0	0	0
3	2762	88971	205	156560	8364	265946	1
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0

Refresh    Details for Select Port

Clicking on the **Details for Select Port** button displays the next screen.

4. Click here to return to the Port Counters screen.

Status and Counters - Port Counters - 1

Link Status : Up

Bytes Rx : 1,478,397,758      Bytes Tx : 12,955,020

Unicast Rx : 9,969,326      Unicast Tx : 1,062,892

Bcast/Mcast Rx : 465,451      Bcast/Mcast Tx : 217

Drops Rx : 8,747,277

FCS/Align Rx : 772      Collisions Tx : 1898

Return to Summary

Figure 7-6. Example of Port Counters and Details on the Web Browser Interface

## Displaying Port Counters from the Console Interface

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

1. Status and Counters

4. Port Counters

```

HP ProCurve Switch 212M          DEFAULT_CONFIG          2-Jan-1990  8:08:18
----- CONSOLE - MANAGER MODE -----
                Status and Counters - Port Counters

Port  Total Bytes  Total Frames  Errors Rx
-----
1    1,561,866,254  12,824,626   1,282,054
2              0              0              0
3    30,721,076   279,226      1
4              0              0              0
5              0              0              0
6              0              0              0
7              0              0              0
8              0              0              0
9              0              0              0
10             0              0              0
11             0              0              0

Actions->  Back    Show details  Reset    Help

Show detailed port information.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
    
```

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

To view details about the traffic on a particular port, highlight that port number (figure 7-7), then select **Show Details**. For example, selecting port 1 displays a screen similar to figure 7-8, on the next page.

```
HP ProCurve Switch 212M          DEFAULT_CONFIG          2-Jan-1990  8:09:13
-----
----- CONSOLE - MANAGER MODE -----
                          Status and Counters - Port Counters - 1

Link Status      : Up

Bytes Rx         : 1,483,833,339          Bytes Tx         : 12,975,209
Unicast Rx       : 9,995,122            Unicast Tx       : 1,063,002
Bcast/Mcast Rx   : 469,038              Bcast/Mcast Tx   : 220

Drops Rx         : 8,747,279            Collisions Tx    : 1900

FCS/Align Rx     : 780
Fragments/Runts Rx : 1,281,276
Giants Rx        : 0
Total Rx Errors  : 1,282,056

Actions->  Back  Reset  Help

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

Figure 7-8. Example of the Display for Show details on a Selected Port

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

# Address Table

To access the Address Table screen from the Main Menu, click on:

1. Status and Counters
5. Address Table

```

HP ProCurve Switch 212M          Switch1          18-Jun-1998  17:14:25
----- TELNET - MANAGER MODE -----
                          Status and Counters - Address Table

  MAC Address  Located on Port
-----
00000c-07ac00  5
00000c-73a205  5
000077-85494f  5
000077-854954  5
000077-867349  5
000077-8673c9  5
000077-88addf  5
000077-88ade5  5
000077-89967c  5
000077-89969b  5
000077-8996ba  5

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 7-9. Example of the Address Table

This screen lets you determine which switch port is being used to communicate with a specific device on the network. The listing includes:

- The MAC addresses that the switch has learned from network devices attached to the switch
- The port on which each MAC address was learned

Use the **Search** action at the bottom of the screen to locate a specific device (MAC address).

## Port Address Table

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

To access the port address table:

1. From the Main Menu click on:
  1. Status and Counters
    6. Port Address Table

```
HP ProCurve Switch 212M          Switch1          18-Jun-1998 17:17:49
----- TELNET - MANAGER MODE -----
                          Status and Counters Menu

  1. General System Information
  2. Switch Management Address Information
  3. Port Status
  4. Port Counters
  5. Address Table
  6. Port Address Table
  7. Spanning Tree Information
  8. Advanced Features Status...
  0. Return to Main Menu...

Select port : 5

Type port number or press <Space> to scroll ports. Press <Enter> to select.
To select menu item, press item number, or highlight item and press <Enter>.
```

Figure 7-10. Example of How To Access the Port Address Table

2. When the prompt appears, press the Space bar or type the port number to display the port you want to examine, then press **[Enter]**. (See figure 7-10, above.)

You will then see a list of the MAC addresses that have been detected on the selected port, as shown in figure 7-11 on the next page. Each port is identified by the sequential port numbers on the front of the switch.



```
HP ProCurve Switch 212M          Switch1          18-Jun-1998  17:20:01
----- TELNET - MANAGER MODE -----
                Status and Counters - Port Address Table - Port 5

    MAC Address
-----
00000c-07ac00
00000c-73a205
000077-85494f
000077-854954
000077-867349
000077-8673c9
000077-88addf
000077-88ade5
000077-89967c
000077-89969b
000077-8996ba

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 5 appear in the initial listing. To view any additional addresses that may be in the listing, use the **Next page** action.

Figure 7-11. Example of a Port Address Table for a Specific Port

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

## Spanning Tree (STP) Information

To access the Spanning Tree Information screen from the Main Menu, click on:

1. Status and Counters

7. Spanning Tree Information

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

```
HP ProCurve Switch 212M          Switch1          18-Jun-1998  17:26:49
----- TELNET - MANAGER MODE -----
                Status and Counters - Spanning Tree Information

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

Topology Change Count : 1
Time Since Last Change : 81 secs

Root MAC Address     : 0060b0-8ae220
Root Path Cost       : 0
Root Port            : This switch is root
Root Priority         : 32768

Actions->  Back  Show ports  Help

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

Figure 7-12. Example of Spanning Tree Information

Use this screen to determine current switch-level STP parameter settings and statistics.

You can use the **Show ports** action at the bottom of the screen to display port-level information and parameter settings for each port in the switch (including port type, cost, priority, operating state, and designated bridge) as shown in figure 7-13.

```

HP ProCurve Switch 212M                Switch1                18-Jun-1998  17:28:44
----- TELNET - MANAGER MODE -----
                Status and Counters - Spanning Tree - Port Information
-----
Port   Type   Cost  Priority  State      Designated Bridge
-----
1     10T    100   128     Disabled
2     10T    100   128     Disabled
3     10T    100   128     Disabled
4     10T    100   128     Disabled
5     10T    100   128     Forwarding 0060b0-8ae220
6     10T    100   128     Disabled
7     10T    100   128     Disabled
8     10T    100   128     Disabled
9     10T    100   128     Disabled
10    10T    100   128     Disabled
11    10T    100   128     Disabled

Actions->  Back   Help

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

```

Figure 7-13. Example of STP Port Information

## IP Multicast (IGMP) Status

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

1. Status and Counters

8. Advanced Features Status

1. IP Multicast (IGMP) Status

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.

```
HP ProCurve Switch 212M                Switch1                18-Jun-1998  17:30:26
----- TELNET - MANAGER MODE -----
                Status and Counters - IP Multicast (IGMP) Status
Active Group Addresses  Reports  Queries  Querier Access Port
-----
224.0.1.24             1518    1512    5
-----

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 7-14. Example of IGMP Status Screen

You can also display the port status of the individual multicast groups. (That is, you can display the ports, port types, and whether the IGMP devices connected to the switch via the port are hosts, routers, or both.) To do so, select the group from the above screen and press [S] for **Show ports**. For example, suppose you wanted to view the status of the IP multicast group 224.0.1.24 shown in the above screen. You would highlight the row beginning with that group number, then press [S]. You would then see a screen similar to the following:

```
HP ProCurve Switch 212M          Switch1          18-Jun-1998  17:32:11
----- TELNET - MANAGER MODE -----
                Status and Counters - IGMP Status - Ports

Active Group Address : 224.0.1.24

Port   Type   Access
-----
5      10T   host-router

Actions->  Back   Help

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

Figure 7-15. Example of an IGMP Status Screen for a Selected Multicast Group



# Troubleshooting

---

This chapter addresses performance-related network problems that can be caused by topology, switch configuration, and the effects of other devices or their configurations on switch operation. (For switch-specific information on hardware problems indicated by LED behavior, cabling requirements, and other potential hardware-related problems, refer to the installation guide you received with the switch.)

This chapter includes:

- Troubleshooting Approaches (page 8-2)
- Browser or Switch Console Problems (page 8-3)
- Unusual Network Activity (page 8-4)
  - General Problems (page 8-4)
  - IGMP-Related Problems (page 8-5)
- Using the Event Log To Identify Problem Sources (page 8-6)
- Diagnostic and management tools, including:
  - Link test (page 8-9)
  - Ping test (page 8-9)
  - Browse configuration (page 8-13)
  - Command prompt (page 8-15)
  - Restoring the factory default configuration (page 8-16)

For information on support and warranty provisions, see the Support and Warranty booklet shipped with the switch.

## Troubleshooting Approaches

There are six primary ways to diagnose switch problems:

- Check the switch LEDs for indications of proper behavior:
  - Each switch port has a Link LED that should light whenever an active network device is connected to a the port.
  - Problems with the switch hardware and software are indicated by flashing the Fault and other switch LEDs.

See the *Installation Guide* shipped with the switch for information on using the switch LEDs for troubleshooting.

- Check the network topology/installation. See the *Installation Guide* shipped with the switch for topology information.
- Check cables for damage, correct type, and proper connections. See the *Installation Guide* shipped with the switch for cable types and connector pin-outs.
- Use HP TopTools for Hubs & Switches (if installed on your network) to help isolate problems and recommend solutions. HP TopTools is shipped at no extra cost with the switch.
- Use the Port Utilization Graph and Alert Log in the web browser interface included in the switch to help isolate problems. See chapter 3, “Using the HP Web Browser Interface” for operating information. These tools are available through the web browser interface:
  - Port Utilization Graph
  - Alert Log
  - Port Status screen
  - Port Counters screen
  - Diagnostic tools (Link test, Ping test, configuration file browser)
- For help in isolating problems, use the easy-to-access switch console built into the switch or telnet to the switch console. See chapter 4, “Using the Switch Console” for operating information. These tools are available through the switch console:
  - Status and Counters screens
  - Event Log
  - Diagnostics tools (Link test, Ping test, configuration file browser, and advanced-user commands)



---

# Web Browser Interface or Switch Console Access Problems

## **Cannot access the web browser interface:**

- Access may be disabled by the **Web Agent Enabled** parameter in the switch console. On the switch console, go to the Switch Management Access Configuration menu and check the configuration on the Console/Serial Link Configuration screen.
- The switch may not have the correct IP address, subnet mask, or gateway address. To find out the switch's IP address, connect a console to the switch's Console port and from the Status and Counters Menu, select **2. Switch Management Address Information**.
- If you are using DHCP to acquire the IP address for the switch, the IP address "lease time" may have expired so that the IP address has changed. For more information on how to "reserve" an IP address, refer to the documentation for the DHCP server application that you are using.
- Java™ applets may not be running on the web browser you are using. They are required for the switch web browser interface to operate correctly. See the online help on your web browser for instructions on how to run the Java applets.

## **Cannot Telnet into the switch console from a station on the network:**

- Telnet access may be disabled by the **Inbound Telnet Enabled** parameter in the switch console "Using the Switch Console to Configure the Console/Serial Link" on page 6-21.
- The switch may not have the correct IP address, subnet mask, or gateway address. To find out the switch's IP address, connect a console to the switch's Console port and from the Status and Counters Menu, select **2. Switch Management Address Information**.
- If you are using DHCP to acquire the IP address for the switch, there may not be a "Reservation" set up for the IP address, or the address "lease time" may have expired, so that the IP address has changed. For more information on how to "reserve" an IP address or set up an infinite lease time, refer to the documentation for the DHCP server application that you are using.
- There may be another telnet session accessing the switch. You can terminate the other session by directly connecting a console to the switch and executing the "kill" command from the Command Prompt under the Diagnostics menu.

## 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 as indicated by measurements from the switch console or from a network management tool such as the HP TopTools for Hubs & Switches. Refer to the installation guide you received with the switch for information on using LEDs to identify unusual network activity.

### General Problems

**The network runs slow; processes fail; users cannot access servers or other devices.** Broadcast storms may be occurring in the network. These may be due to loops in the network topology (redundant links between nodes).

- Inspect your network topology to make sure there are no loops in the network.
- If your network requires redundant links to guarantee maintenance of network connectivity, turn on Spanning Tree Protocol to maintain a single active path and provide for redundant links.

**Duplicate IP Addresses.** This is indicated by this Event Log message:

**ip: Invalid ARP source: *IP address* on *IP address***

*where:* both instances of *IP address* are the same address, indicating the IP address that has been duplicated somewhere on the network.

**Duplicate IP Addresses in a DHCP Network.** If you use a DHCP server to automatically assign IP addresses in your network and you find a device with a valid IP address that does not appear to communicate properly with the server or other devices, a duplicate IP address may have been issued by the server. This can occur if a client has not released a DHCP-assigned IP address after the intended expiration time and the server “leases” the address to another device. This can also happen, for example, if the server is first configured to issue IP addresses with an unlimited duration, then is subsequently configured to issue IP addresses that will expire after a limited duration. One solution is to configure “reservations” in the DHCP server for specific IP addresses to be assigned to devices having specific MAC addresses. For more information, refer to the documentation for the DHCP server.

**The Switch Has Been Configured for DHCP/Bootp Operation, But Has Not Received a DHCP or Bootp Reply.** When the switch is first configured for DHCP/Bootp operation, or if it is rebooted with this configuration, it immediately begins sending request packets on the network. If the switch does not receive a reply to its DHCP/Bootp requests, it continues to periodically send request packets, but with decreasing frequency. Thus, if a DHCP or Bootp server is not available or accessible to the switch when DHCP/Bootp is first configured, the switch may not immediately receive the desired configuration. After verifying that the server has become accessible to the switch, reboot the switch to re-start the process.

## IGMP-Related Problems

**IP Multicast (IGMP) Traffic Does Not Reach IGMP Hosts or a Multicast Router Connected to a Port.** IGMP must be enabled on the switch and the affected port must be configured for “Auto” or “Forward” operation.

**IP Multicast Traffic Floods Out All Ports; IGMP Does Not Appear To Filter Traffic.** The IGMP feature does not operate if the switch does not have an IP address configured manually or obtained through DHCP/Bootp. To verify whether an IP address is configured for the switch, access the switch console and from the Main Menu, select:

1. Status and Counters
2. Switch Management Address Information

```

HP ProCurve Switch 212M          DEFAULT_CONFIG          12-Jun-2008   8:50:41
-----
----- CONSOLE - MANAGER MODE -----
                Status and Counters - Management Address Information

Time Server Address :

MAC Address       : 0060b0-8a6ca0
IP Address        : 11.22.33.44
IPX Network Number :

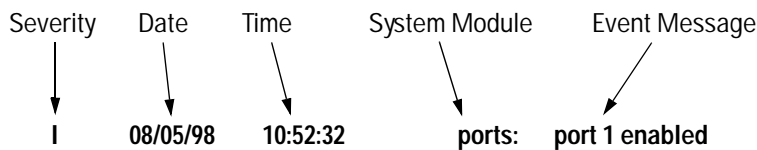
Actions->  Back  Help

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

Figure 8-1. Checking for an IP Address on the Switch

## Using the Event Log to Identify Problem Sources

The Event Log records operating events as single-line entries listed in chronological order, and serves as a tool for isolating problems. Each Event Log entry is composed of five fields:



**Severity** is one of the following codes:

- I (information) indicates routine events.
- W (warning) indicates that a service has behaved unexpectedly.
- C (critical) indicates that a severe switch error has occurred.
- D (debug) reserved for HP internal diagnostic information.

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

**Time** is the time in *hh:mm:ss* format that the entry was placed in the log.

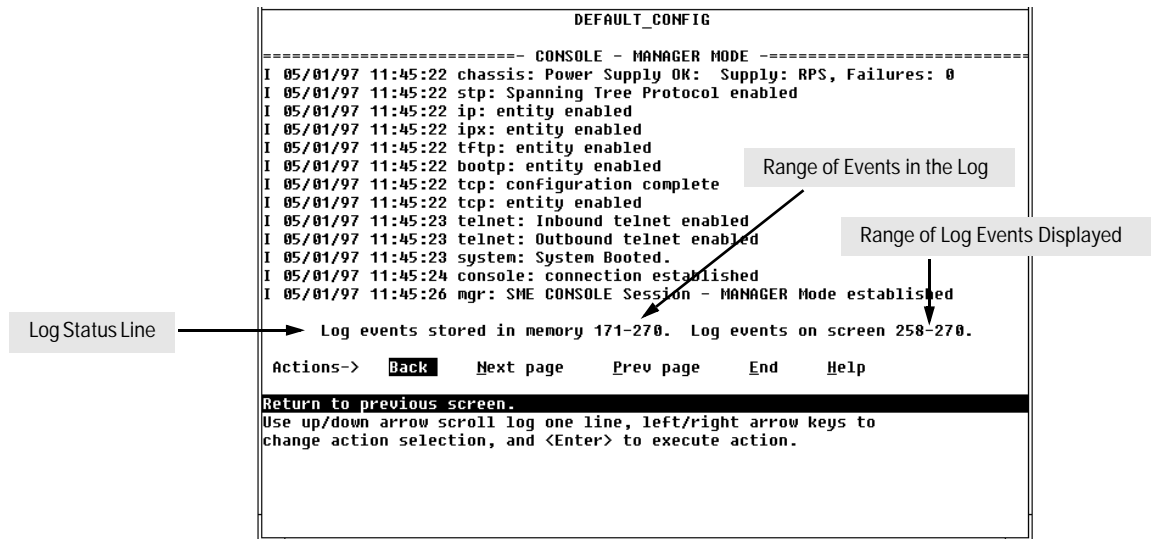
**System Module** is the internal module (such as “ports” for port manager) that generated the log entry. Table 8-1 lists the system modules that could be displayed in the Event Log.

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

**Table 8-2. Event Log System Modules**

System Module	Description	System Module	Description
addrMgr	Address table	mgr	Console management
bootp	Bootp addressing	ports	Change in port status
chassis	switch hardware	snmp	SNMP communications
console	switch console	stp	Spanning Tree
dhcp	DHCP addressing	sys, system	Switch management
download	file transfer	telnet	Telnet activity
fault	Web browser interface Alert Log	tcp	Transmission control
igmp	IP Multicast	tftp	File transfer for new OS or configuration
ip	IP-related	timep	Time protocol
ipx	Novell Netware	Xmodem	Xmodem file transfer

**Entering and Navigating in the Event Log Display.** From the Main Menu, select 4. Event Log.



**Figure 8-1. 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 (**N**ext page, **P**rev page, or **E**nd), or the keys described in the following table:

**Table 8-2. Event Log Control Keys**

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

The event log holds up to 1000 lines in chronological order, from the oldest to the newest. Each line consists of one complete event message. Once the log has received 1000 entries, it discards the current oldest line each time a new line is received. The event log window contains 14 log entry lines, and you can move it to any location in the log by using the **N**ext page, **P**rev page, and **E**nd actions on the screen.

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.

## Diagnostics

The switch's diagnostic tools include the following:

Feature	Switch Console	Web Browser Interface	Page
Link Test	Yes	Yes	8-9
Ping Test	Yes	Yes	8-10
Browse Config File	Yes	Yes	8-13
Command Prompt	Yes	No	8-15

### Ping and Link Tests

The Ping test and the Link test are point-to-point tests between your switch and another IEEE 802.3-compliant device on your network. These tests can tell you whether the switch is communicating properly with another device.

#### Note

To respond to a Ping test or a Link test, the device you are trying to reach must be IEEE 802.3-compliant.

**Ping Test.** This is a test of the path between the switch and another device on the same or another IP network that can respond to IP packets. (“Ping” is an acronym for “Packet INternet Groper”.) If the network device responds correctly, the test passes.

**Link Test.** This is a test of the connection between the switch and a designated network device on the same LAN. During the link test, IEEE 802.2 Test packets are sent to the designated network device. The remote device must return IEEE 802.2 Test Response packets to the switch. If the network device returns the packets, the test passes.

## Executing Ping or Link Tests from the Web Browser Interface

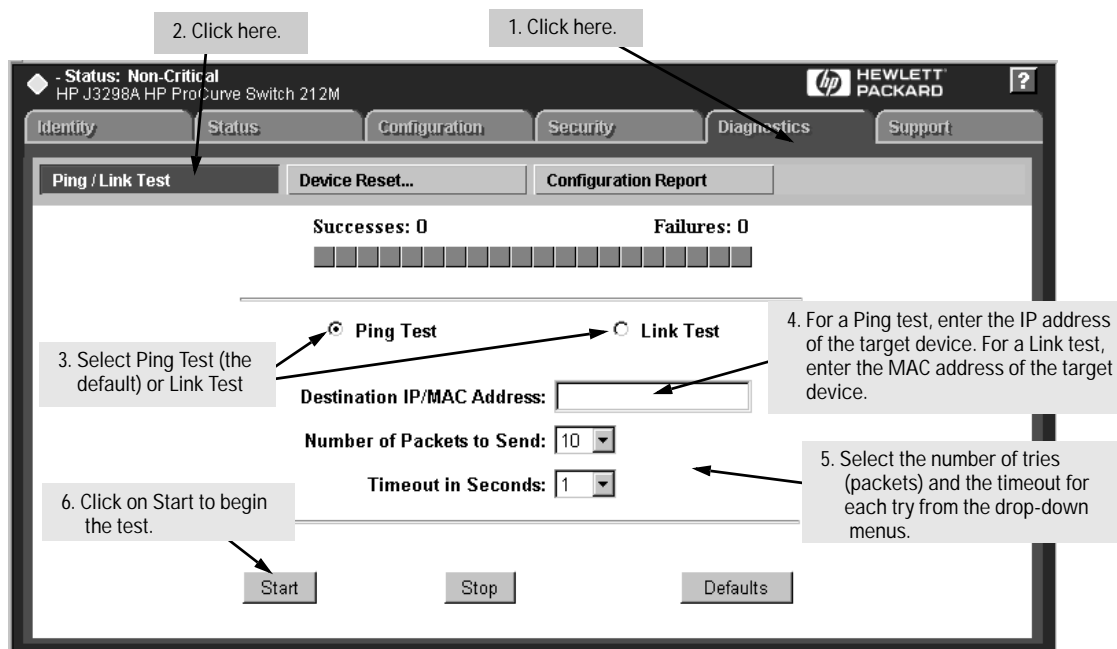


Figure 8-3. Ping and Link Test Screen on the Web Browser Interface

**Successes** indicates the number of Ping or Link packets that successfully completed the most recent test.

**Failures** indicates the number of Ping or Link packets that were unsuccessful in the last test. Failures indicate connectivity or network performance problems (such as overloaded links or devices).

**Destination IP/MAC Address** is the network address of the target, or destination, device to which you want to test a connection with the switch. An IP address is in the X.X.X.X format where X is a decimal number between 0 and 255. A MAC address is made up of 12 hexadecimal digits, for example, 0800c-070a00.

**Number of Packets to Send** is the number of times you want the switch to attempt to test a connection.

**Timeout in Seconds** is the number of seconds to allow per attempt to test a connection before determining that the current attempt has failed.

**To halt a Link or Ping test** before it concludes, click on the Stop button.  
**To reset the screen** to its default settings, click on the Defaults button.



## Executing Ping or Link Tests from the Switch Console

1. From the console Main Menu, select:

5. Diagnostics . . .

1. Link Test

or

2. Ping Test

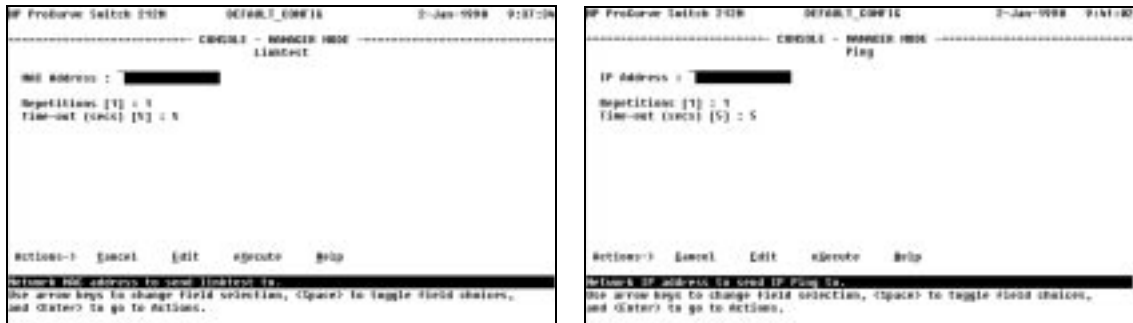


Figure 8-4. Examples of Link Test and Ping Test Screens

2. Do one of the following:

- For a Link test, enter the MAC address of the target device. (This is a 12-digit hexadecimal number. For an example, see the screen on page 7-11.)
- For a Ping test, enter the IP address of the target device.

3. Select the **Repetitions** parameter and type in the number of times you want the test to be made.

4. Select **Time-out** and select the number of seconds to allow for each test.

5. Press **[Enter]** to go to the Actions line, then press **[x]** (for **eXecute**) to start the test.

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

The console displays the result of each test. For example, if a Link test succeeds, you will see

**Linktest Command Successful.**

If the Link test fails, you will see

**Linktest Command Timed out.**

If a Ping test succeeds, you will see a message indicating the target IP address is “alive”, along with a test counter and elapsed time for each test. For example:

**12.10.8.207 is alive, iteration 1, time = 1 ms**

If a Ping test fails, you will see a message such as the following:

**Ping Failed or Target did not Respond**

## The Configuration File

The complete switch configuration is contained in a file that you can browse from either the web browser interface or the switch console. It may be useful in some troubleshooting scenarios to view the switch configuration.

### Browsing the Configuration File from the Web Browser Interface

To use the web browser interface to display the configuration file that is currently saved:

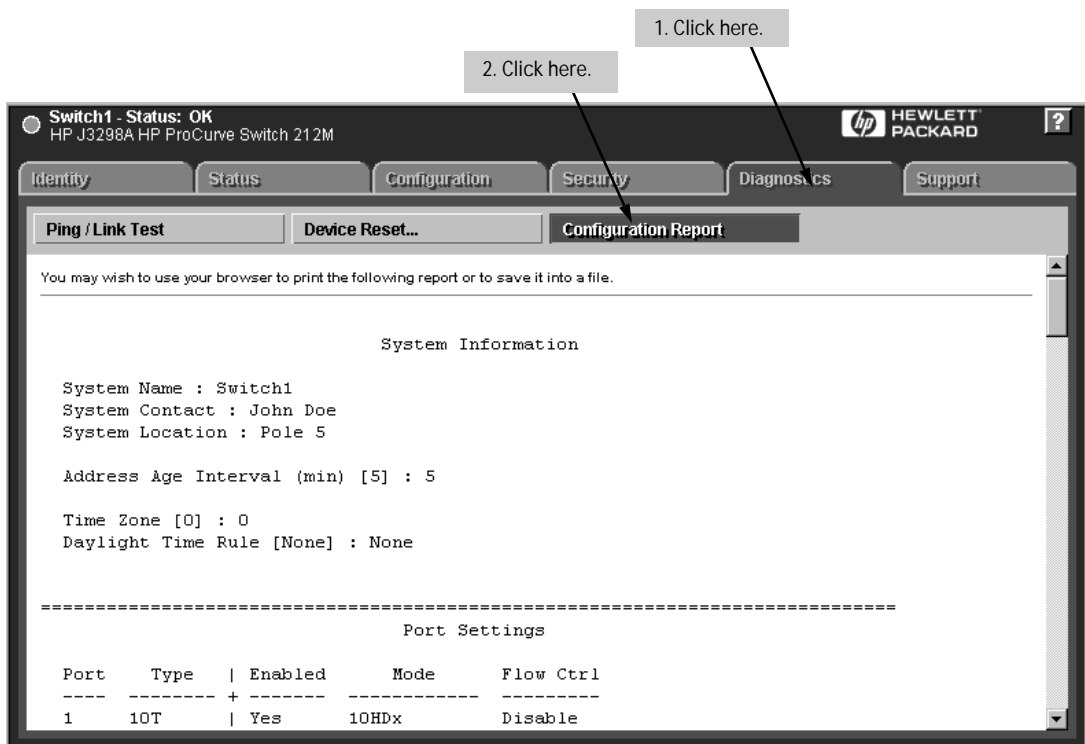


Figure 8-5. Example of the Web Browser Interface Configuration Report

## Browsing the Configuration File from the Switch Console

To use the switch console to display the configuration file that is currently saved:

1. From the console Main Menu, select:

### 5. Diagnostics

### 3. Browse Configuration File

```
HP ProCurve Switch 212M          DEFAULT_CONFIG          2-Jan-1998  9:47:32
-----
CONSOLE - MANAGER MODE
System Information

System Name :
System Contact :
System Location :

Address Age Interval (min) [5] : 5

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

-----
Port Settings

Port   Type   | Enabled   Mode       Flow Ctrl
-----+-----
1     10T   | Yes      10HDx     Disable
2     10T   | Yes      10HDx     Disable
3     10T   | Yes      10HDx     Disable
-- MORE --
```

When -- More -- appears, press **[Enter]** to see the next line; press the Space bar to see the next page

Figure 8-6. Example of the Browse Configuration Display

2. When -- MORE -- appears in the display, press **[Enter]** to see the next line of the configuration, or press the Space bar to display the next page of the configuration.

To halt a configuration listing, press **[Q]** (for Quit) and then press any key to return to the Diagnostics menu.

## Using the Command Prompt

In addition to the menu-based part of the switch console, under the Diagnostics Menu, a command-line based interface is available. The commands are primarily for the expert user and for diagnostics purposes. Selecting **Command Prompt** from the Diagnostics Menu presents a command prompt from which you can enter the following commands:

List of Commands Available at the Command Prompt			
Help	Delete	Log	SetMIB
Exit	History	Page	Version
Browse	Kill	Ping	WalkMIB
Config	Get	Print	Xget
Date	Put	Redo	Xput
Time	LinkTest	GetMIB	romversion

To get a definition of these commands and their syntax, enter **Help** at the command prompt. When you see -- **MORE** -- at the bottom of the screen:

- To advance the display one line at a time, use `[Enter]`.
- To advance the display one screen at a time, use the Space bar.

If you want to stop the help listing, press `[Q]`.

### How To Use the Command Prompt:

1. To access the command prompt, select **5. Diagnostics ...** in the Main Menu, then select **4. Command Prompt** from the Diagnostics Menu.
2. The command prompt appears near the bottom of the screen. The text in the prompt matches the System Name parameter. For example, in the factory default configuration (no system name configured), the command prompt is **DEFAULT\_CONFIG:**
3. Type in the command you want to execute and press `[Enter]`. For example, to set the time to 9:55 a.m. you would execute the following command:

```
DEFAULT_CONFIG: time 9:55 [Enter]
```

### How To Exit from the command prompt:

Type **exit** and press `[Enter]` to return to the Diagnostics Menu.

## Restoring the Factory Default Configuration

As part of your troubleshooting process, it may become necessary to return the switch configuration to the factory default settings. This process momentarily interrupts the switch operation, clears any passwords, clears the console event log, resets the network counters to zero, performs a complete self test, and reboots the switch into its factory default configuration including deleting an IP address.

To execute the factory default reset, perform these steps:

1. Using pointed objects, simultaneously press both the Reset and Clear buttons on the front of the switch.
2. Continue to press the Clear button while releasing the Reset button.
3. When the Self Test LED begins to flash, release the Clear button.

The switch will then complete its self test and begin operating with the configuration restored to the factory default settings.

# File Transfers

---

## Overview

You can download new switch software (operating system—OS) and upload or download switch configuration files. These features are useful for acquiring periodic switch software upgrades and for storing or retrieving a switch configuration.

This appendix includes the following information:

- Downloading an operating system (page A-1)
  - Transferring switch configurations (page A-8)
- 

## Downloading an Operating System (OS)

HP periodically provides switch operating system (OS) updates through the Network City website ([http://www.hp.com/go/network\\_city](http://www.hp.com/go/network_city)) and the HP FTP Library Service. For more information, see the support and warranty booklet shipped with the switch. After you acquire the new OS file, you can use one of the following methods for downloading the operating system (OS) code to the switch:

- TFTP transfer method (page A-2)
- Xmodem transfer method (page A-4)
- HP's SNMP Download Manager included in HP TopTools for Hubs & Switches (page A-5)
- A switch-to-switch file transfer (page A-5)

---

### Note

Downloading a new OS does not change the current switch configuration. The switch configuration is contained in a separate file that can also be transferred, for example, for archive purposes or to be used in another switch of the same model. See “Transferring Switch Configurations” on page A-8.

---

## Using TFTP To Download the OS File

This procedure assumes that:

- An OS file for the switch has been stored on a TFTP server accessible to the switch. (The OS file is typically available from HP's electronic services—see the Customer Support/Warranty booklet shipped with the switch.)
- The switch is properly connected to your network and has already been configured with a compatible IP address and subnet mask.
- The TFTP server is accessible to the switch.

Before you use the procedure, do the following:

- Obtain the IP address of the TFTP server in which the OS file has been stored.
- Determine the name of the OS file stored in the TFTP server for the switch (for example, A\_01\_01.swi).

### Note

*If your TFTP server is a Unix workstation, ensure that the case (upper or lower) that you specify for the filename in the switch console Download OS screen is the same case as the characters in the OS filenames on the server.*

1. In the console Main Menu, select **Download OS** to display this screen:

```
HP ProCurve Switch 212M          DEFAULT_CONFIG          2-Jan-1998  20:20:45
-----  CONSOLE - MANAGER MODE  -----
                          Download OS

Current Firmware revision : D.05.X1

Method [TFTP] : TFTP
TFTP Server :

Remote File Name :

Actions->  Cance_l    E_dit    e_xecute    H_e_l_p

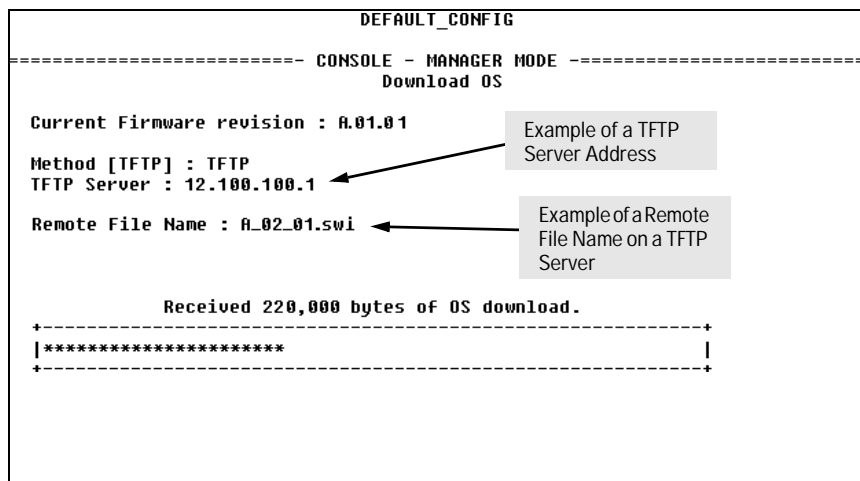
Select the file transfer method (TFTP and XMODEM are currently supported).
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

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

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



3. Ensure that the **Method** field is set to **TFTP** (the default).
4. In the **TFTP Server** field, type in the IP address of the TFTP server in which the OS file has been stored.
5. In the **Remote File Name** field, then type the name of the OS file. If you are using a UNIX system, remember that the filename is case-sensitive.
6. Press **[Enter]**, then **[X]** (for **eXecute**) to begin the OS download. The following screen then appears:



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

7. A “progress” bar indicates the progress of the download. When the entire operating system has been received, all activity on the switch halts and the following messages appear:

**Transfer completed**

**Validating and writing system software to FLASH...**

After the system flash memory has been updated with the new operating system, the switch reboots itself and begins running with the new operating system.

8. To confirm that the operating system downloaded correctly:
  - a. From the Main Menu, select
    1. Status and Counters
      1. General System Information
  - b. Check the **Firmware revision** line.

## Using Xmodem to Download the OS File

This procedure assumes that:

- The switch is connected via the Console port to a PC operating as a terminal. (Refer to the Installation Guide you received with the switch for information on connecting a PC as a terminal and running the switch console interface.)
- The switch operating system (OS) is stored on a disk drive in the PC.
- The terminal emulator you are using includes the Xmodem binary transfer feature. (For example, in the Windows 3.1 terminal emulator, you would use the **Send Binary File** option in the **Transfers** dropdown menu.)

### To Perform the OS Download:

1. From the console Main Menu, select

#### 7. Download OS

The screen shown in figure 8-1 is shown.

2. Press **[E]** (for **E**dit).
3. Use the Space bar to select **XMODEM** in the **Method** field.
4. Press **[Enter]**, then **[X]** (for **eX**ecute) to begin the OS download. The following message then appears:

**Press enter and then initiate Xmodem transfer  
from the attached computer.....**

5. Execute the terminal emulator command(s) to begin an Xmodem binary transfer of the switch OS file that is on the PC disk drive.

The download can take several minutes, depending on the baud rate used for the transfer.

6. When the download finishes, the switch automatically resets itself and begins running the new OS version.

7. To confirm that the operating system downloaded correctly:

- a. From the Main Menu, select:

#### 1. Status and Counters

##### 1. General System Information

- b. Check the **Firmware revision** line.

## Using the SNMP-Based HP Download Manager

Included with your switch is the HP TopTools for Hubs & Switches CD ROM. The HP Download Manager is included with HP TopTools and enables you to initiate a firmware (OS) download over the network to the switch. This capability assumes that the switch is properly connected to the network and has been discovered by HP TopTools. For further information, refer to the documentation and online Help provided with HP TopTools.

## Switch-to-Switch Download

If you have two or more Switch 212Ms and/or Switch 224Ms 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 212M and the Switch 224M use the same OS.)

To complete the file transfer:

1. From the switch console Main Menu in the switch to receive the download, select **7. Download OS**.
2. Select **Method: TFTP**.
3. In the **TFTP Server** field, enter the IP address of the remote Switch 212M or 224M containing the OS you want to download.
4. Enter **“os”** in the **Remote File Name** field.
5. Press **[Enter]**, then **[X]** (for **eXecute**) to begin the OS download.
6. A “progress” bar indicates the progress of the download. When the entire operating system has been received, all activity on the switch halts and the following messages appear:

**Validating and writing system software to FLASH...**

**Transfer completed**

After the system flash memory has been updated with the new operating system, the switch reboots itself and begins running with the new operating system.

7. To confirm that the operating system downloaded correctly:
  - a. From the Main Menu, select
    1. **Status and Counters**
      1. **General System Information**
  - b. Check the **Firmware revision** line.

## Troubleshooting TFTP Downloads

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

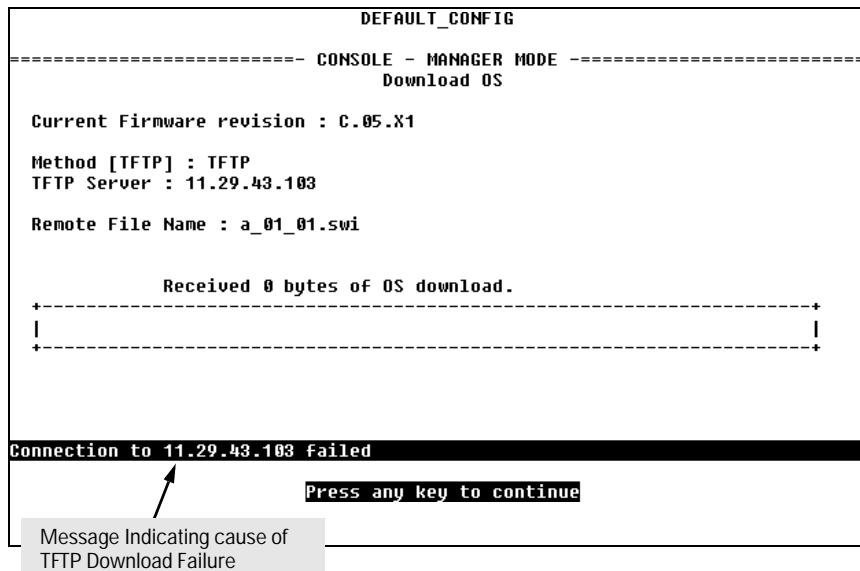


Figure 8-3. Example of Message for TFTP Download Failure

To find more information on the cause of a download failure, examine the messages in the switch's Event Log. (See "Event Log" on page 8-6.)

Some of the causes of download failures include:

- Incorrect or unreachable address specified for the **TFTP Server** parameter. This may include network problems.
- Incorrect name specified for the **Remote File Name** parameter, or the specified file cannot be found on the TFTP server. This can also occur if the TFTP server is a Unix machine and the case (upper or lower) for the filename on the server does not match the case for the filename entered for the **Remote File Name** parameter in the Download OS screen.
- One or more of the switch's IP configuration parameters are incorrect.
- For a Unix TFTP server, the file permissions for the OS file do not allow the file to be copied.

- Another console session (through either a direct connection to a terminal device or through Telnet) was already running when you started the session in which the download was attempted.

---

**Note**

---

If an error occurs in which normal switch operation cannot be restored, the switch automatically reboots itself. In this case, an appropriate message is displayed in the copyright screen that appears after the switch reboots. You can display the same information by selecting the **Command Prompt** option from the Diagnostics Menu and executing the History command.

---

## Transferring Switch Configurations

You can use the following commands to transfer Switch 212M and Switch 224M configurations between the switch and a PC or Unix workstation.

Command	Function
Get	Download a switch configuration file from a networked PC or Unix workstation using TFTP.
Put	Upload a switch configuration to a file in a networked PC or Unix workstation using TFTP.
XGet	Uses an Xmodem-compatible terminal emulation program to download a switch configuration file from a PC or Unix workstation connected to the switch's console port.
XPut	Uses an Xmodem-compatible terminal emulation program to upload a switch configuration to a file in a PC or Unix workstation connected to the switch's console port.

---

### Note

Get or Xget overwrites the switch's current configuration with the downloaded configuration. The switch then automatically reboots itself.

---

### Using Get and Put To Transfer a Configuration Between the Switch and a Networked PC or Unix Workstation

To use Get or Put, you need the following:

- The IP address of the remote PC or Unix workstation that is acting as a TFTP server
- The name assigned to the configuration file you will use on the remote PC or Unix workstation

---

### Note

For the "Put" operation, most Unix TFTP servers require that a file of the same name already exists on the server, in the TFTP directory, and that the file has "write" permissions.

1. From the Main Menu select
  5. Diagnostics...
  4. Command Prompt

2. At the command prompt, execute the following commands:

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

```
put IP_address CONFIG remote_file
```

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

```
get IP_address CONFIG remote_file
```

where: *IP address* is the address of the PC or Unix workstation in which the configuration is to be stored.

*remote\_file* is the name of the configuration file in the PC or Unix workstation

## Using XGet and XPut To Transfer a Configuration Between the Switch and a PC or Unix Workstation

The PC or workstation must be operating as a VT100 or ANSI terminal and connected directly to the switch's console port. Also, the PC or workstation must be running an Xmodem-compatible terminal emulation program. If a manager password has been set, you must log on to the switch using that password in order to execute the Xget or Xput commands.

---

### Note

---

XGet overwrites the switch's current configuration with the downloaded configuration. The switch then automatically reboots itself.

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

1. On the PC or workstation, start the Xmodem-compatible terminal emulation program, then follow the instructions provided with the program to prepare for a file transfer.
2. From the switch's Main Menu select:

    5. Diagnostics...

        4. Command Prompt

3. At the command prompt, execute one of the following commands:

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

**xput config *remote\_file* [pc/unix]**

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

**xget config *remote\_file* [pc/unix]**

where: *remote\_file* is the name of the file in which the configuration is to be stored (put), or is stored (get)

[pc/unix] is one of the following optional values:

- **unix** (the default) specifies the Unix file format.
- **pc** specifies the PC file format.

If the PC or workstation does not respond to an XPut or XGet command, the command times out and control returns to the **Command Prompt** line.



# MAC Address Management

---

## Overview

From the factory, the switch is assigned a block of MAC addresses:

- for network management functions, a base MAC address is assigned to the switch
  - for internal switch operations, one MAC address is assigned to each switch port
- 

## Determining the MAC Addresses

You can use the switch console to determine the base MAC address and the port MAC addresses for the switch. The methods are described in the rest of this appendix.

## Base MAC Address

The switch's base MAC address is displayed on a sticker on the back of the switch. You can also use the switch console to display the switch's base MAC address.

From the console Main Menu, select:

1. Status and Counters
2. Switch Management Address Information

A screen similar to figure B-1 is displayed.

```
HP ProCurve Switch 212M          DEFAULT_CONFIG          12-Jun-2008  8:50:41
----- CONSOLE - MANAGER MODE -----
                Status and Counters - Management Address Information

Time Server Address :

MAC Address       : 0060b0-8a6ca0 ← switch base MAC address
IP Address        : 11.22.33.44
IPX Network Number :

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

Figure 8-1. Example of the Management Address Information Screen

## Switch Port MAC Addresses

The MAC address assigned to each switch port is used internally by such features as Flow Control, and the Spanning Tree Protocol. Determining the MAC address assignments for individual ports can be useful when diagnosing switch operation. To display these addresses, use the **walkmib** command at the switch console command prompt.

From the console Main Menu, select:

### 5. Diagnostics

### 4. Command Prompt

Type the following command to display the MAC address all the switch ports:

```
walkmib ifPhysAddress
```

Figure B-2 is an example of the display you will see.

```
HP ProCurve Switch 212M          Switch1          19-Jun-1998  18:36:40
-----  CONSOLE -  MANAGER MODE  -----
ifPhysAddress.1 = 00 60 b0 8a 6c bf
ifPhysAddress.2 = 00 60 b0 8a 6c be
ifPhysAddress.3 = 00 60 b0 8a 6c bd
ifPhysAddress.4 = 00 60 b0 8a 6c bc
ifPhysAddress.5 = 00 60 b0 8a 6c bb
ifPhysAddress.6 = 00 60 b0 8a 6c ba
ifPhysAddress.7 = 00 60 b0 8a 6c b9
ifPhysAddress.8 = 00 60 b0 8a 6c b8
ifPhysAddress.9 = 00 60 b0 8a 6c b7
ifPhysAddress.10 = 00 60 b0 8a 6c b6
ifPhysAddress.11 = 00 60 b0 8a 6c b5
ifPhysAddress.12 = 00 60 b0 8a 6c b4
ifPhysAddress.13 = 00 60 b0 8a 6c b3
ifPhysAddress.14 = 00 60 b0 8a 6c b2
ifPhysAddress.27 = 00 60 b0 8a 6c a0

Switch1:
```

Figure 8-2. Example of Port MAC Address Assignments



---

# Index

## A

### access

- manager ... 6-15
- operator ... 6-15

### Actions line

- location on screen ... 4-6

### actions, console ... 4-7

### active button ... 3-13

### active path ... 6-30

### active tab ... 3-13

### address aging ... 6-22

### address table

- port ... 7-11

### address, manager ... 6-15, 6-17

### Alert Log ... 3-13, 3-16

- alert types ... 3-18

#### Control Bar ... 3-13

#### control bar ... 3-20

#### header bar ... 3-13

#### sorting the entries ... 3-17

#### viewing details of entries ... 3-19

### ANSI terminal ... A-10

### asterisk ... 4-7

### authentication trap ... 6-18

### auto port setting, IGMP ... 6-36

## B

### bandwidth, savings ... 6-39

### bar graph area

- error packet indicator ... 3-14
- maximum activity indicator ... 3-15
- non-unicast packet indicator ... 3-14
- unicast packet indicator ... 3-14

### base MAC address for the switch ... B-2

### baud rate ... 4-2

### blocked port, IGMP ... 6-36

### blocking state, spanning tree ... 6-33

### Bootp ... 6-8, 6-10

#### configuring ... 6-13

#### no reply ... 8-4

#### table file ... 6-12

#### Unix systems ... 6-11

### Bootp/DHCP differences ... 6-11

### Bootptab file ... 6-11

### broadcast storm ... 6-30

### browsing the configuration file ... 8-13

#### using the switch console ... 8-14

#### using the web browser interface ... 8-13

### button bar ... 3-13

## C

### Clear button

#### restoring factory default configuration ... 8-16

#### to delete password protection ... 4-11

### command prompt ... 4-5, 4-14, 8-15

#### exit ... 8-15

### communities, SNMP ... 6-16

### configuration ... 4-4

#### Bootp ... 6-11

#### browsing the configuration file ... 8-13

##### using the switch console ... 8-14

##### using the web browser interface ... 8-13

#### console ... 6-20

#### copying ... A-8

#### download ... A-1

#### factory default ... 6-2, 6-30, 8-15

#### features ... 6-2

### IGMP

#### from the console ... 6-37

#### from the web browser interface ... 6-35

### IP ... 6-5

### manager password ... 4-11

### network monitoring ... 6-28

### operator password ... 4-11

### ports ... 6-24

### restoring factory defaults ... 8-16

### serial link ... 6-20

### SNMP ... 6-15

### spanning tree ... 6-30

### switch management access ... 4-4

### system ... 6-22

### transferring ... A-8

### trap receivers ... 6-18

console  
  browsing the configuration file ... 8-14  
  configuration ... 6-20  
  ending a session ... 4-3  
  help ... 4-8  
  interaction with the web browser  
    interface ... 4-1  
  Main menu ... 4-4  
  navigation ... 4-7  
  operation ... 4-7  
  overview ... 4-1  
  Ping and link testing ... 8-11  
  resetting the switch ... 4-12  
  starting a session ... 4-2  
  status and counters access ... 4-4  
  switch management access configuration ... 4-4  
console configuration screen ... 6-20  
console session ... 4-2  
Control Bar  
  Alert Log ... 3-13  
copyright screen ... 4-2  
CPU utilization ... 7-3

## D

date format ... 8-6  
date parameter ... 6-23  
DEFAULT\_CONFIG  
  about this prompt ... 8-15  
Device Passwords Window ... 3-7  
DHCP ... 6-10  
  address problems ... 8-4  
  no reply ... 8-4  
DHCP/Bootp  
  differences ... 6-11  
  IP addressing process ... 6-10  
diagnostics ... 8-9  
diagnostics tab ... 3-23  
Domain Name Server (DNS) ... 3-4  
download  
  configuration ... A-8  
  SNMP-based ... A-5  
  switch-to-switch ... A-5  
  troubleshooting ... A-6  
  Xmodem ... A-4  
download configuration  
  Xget command ... A-8

download OS ... 4-5, A-5  
  erases the event log ... 8-8  
  TFTP method ... A-2

## E

ending a console session ... 4-3  
Event Log ... 4-3, 4-5, 6-18, 8-6, 8-8  
  navigation ... 8-7  
  severity code ... 8-6  
exiting from command prompt ... 8-15  
Extended RMON  
  description of ... 5-4

## F

factory default configuration ... 6-2  
  restoring ... 8-16  
failure, OS download ... A-6  
fault detection ... 3-7  
Fault Detection Policy  
  setting ... 3-25  
filter, IGMP  
  maximum allowed ... 6-42  
firmware version ... 7-3  
format  
  date ... 8-6  
  time ... 8-6  
forwarding port, IGMP ... 6-36  
forwarding state, spanning tree ... 6-33

## G

gateway address, IP ... 6-5  
Gateway field, IP address ... 6-9  
gateway router, for IP address ... 6-9  
Get command ... A-8  
getmib command ... 6-42  
graphs area, web browser interface ... 3-13

## H

Header Bar  
  Alert Log ... 3-13  
help  
  switch console ... 4-8

Help line  
  about ... 4-6  
  location on screens ... 4-6

History command ... A-7

HP proprietary MIB ... 5-2

HP TopTools for Hubs & Switches ... 5-1  
  managing the switch with ... 5-2

## I

IEEE 802.1d ... 6-30, 6-32

IGMP ... 6-34  
  configuring ... 6-36, 6-38  
  console configuration ... 6-37  
  example ... 6-39–6-40  
  forward with high priority ... 6-36  
  high priority forwarding ... 6-36–6-37  
  host not receiving ... 8-5  
  leave group ... 6-38  
  maximum address count ... 6-42  
  multicast group ... 6-38, 6-41  
  multimedia ... 6-34  
  not working ... 8-5  
  operation ... 6-38  
  port states ... 6-36  
  querier setting, changing ... 6-42  
  query ... 6-38  
  report ... 6-38  
  statistics ... 7-16  
  status ... 6-38  
  traffic priority ... 6-36  
  web browser interface configuration ... 6-35

Inbound Telnet Enabled parameter ... 8-3

IP address  
  configuration ... 6-5  
  duplicate address ... 8-4  
  duplicate address, DHCP network ... 8-4  
  gateway address ... 6-5  
  globally assigned addressing ... 6-14  
  subnet mask ... 6-5, 6-9  
  using for web browser interface ... 3-4

IPX network number ... 7-4

## J

Java, requirement for web browser interface ... 3-4

## L

leave group, *See* IGMP ... 6-38

link status, port ... 7-7

link test ... 8-9  
  executing from the switch console ... 8-11  
  executing from the web browser  
  interface ... 8-10

LOGOUT command ... 4-5

lost password ... 3-9

## M

MAC address ... 6-11, 7-3  
  base MAC address for the switch ... B-2  
  determining ... B-1  
  learned ... 7-11  
  on port ... 7-12  
  switch ports ... B-3

Main menu, console  
  features ... 4-4

management  
  access configuration from console ... 4-4

management server URL ... 6-4

manager access ... 6-15

manager address ... 6-15, 6-17

manager password ... 3-8, 4-11  
  actions permitted ... 4-9  
  setting ... 4-11

Manual, IP address configuration ... 6-9

MIB  
  changing IGMP querier settings ... 6-42  
  list of supported ones ... 5-2

monitoring traffic ... 6-28

multicast group  
  *See* IGMP ... 6-38

multimedia  
  *See* IGMP ... 6-34

## N

navigation  
  console ... 4-7  
  Event Log ... 8-8

network monitoring port  
  configuration screen ... 6-28  
  effect of traffic overload ... 6-28

network slow, troubleshooting ... 8-4

## O

online help location, specifying for web browser interface ... 6-4

operator access ... 6-15

operator mode

console ... 4-10

web browser interface ... 3-8

operator password ... 4-11

actions permitted ... 4-9

configuring ... 4-11

for web browser interface access ... 3-8

setting ... 4-11

OS

version ... A-3–A-5

OS download

erases the event log ... 8-8

failure message ... A-6

switch-to-switch ... A-5

TFTP method ... A-2

troubleshooting ... A-6

Xmodem method ... A-4

overview of the switch console ... 4-1

Overview window, web browser interface

active button ... 3-13

active tab ... 3-13

Alert Log ... 3-13

Alert Log control bar ... 3-13

Alert Log header bar ... 3-13

button bar ... 3-13

description ... 3-12

graphs area ... 3-13

status bar ... 3-13

tab bar ... 3-13

## P

password ... 3-7, 4-2

case-sensitive ... 4-11

creating ... 3-8

delete ... 4-11

deleting with the Clear button ... 4-11

if you lose the password ... 3-9

incorrect ... 4-10

length ... 4-11

lost ... 4-11

manager ... 3-8

actions permitted ... 4-9

operator ... 3-8

actions permitted ... 4-9

setting ... 4-10

using to access browser and console ... 3-9

path cost ... 6-33

Ping test ... 8-9

executing from the switch console ... 8-11

executing from the web browser

interface ... 8-10

port

auto, IGMP ... 6-36

blocked, IGMP ... 6-36

forwarding, IGMP ... 6-36

state, IGMP control ... 6-36

port address table ... 7-11

port cost

*See* spanning tree ... 6-33

port counters ... 7-7

reset ... 7-7

port utilization ... 3-14

port utilization and status displays

web browser interface ... 3-14

port, traffic patterns ... 7-7

priority

IGMP ... 6-36

spanning tree ... 6-33

proprietary MIB

list of ... 5-2

public SNMP community

effect of changing or deleting ... 6-15

where used ... 5-3

Put command ... A-8

## Q

querier ... 6-42

query

*See* IGMP ... 6-38

## R

reboot ... 4-5, 4-7

rebooting the switch ... 4-12

reconfigure ... 4-7

redundant path, spanning tree ... 6-30

report

*See* IGMP ... 6-38



- Reset button ... 8-8
  - restoring factory default configuration ... 8-16
- reset port counters ... 7-7
- resetting the switch
  - erases the Event Log ... 8-8
  - factory default reset ... 8-16
  - from the console ... 4-12
- restricted access, SNMP ... 6-15
- restricted write access ... 6-15
- RFC 1213 ... 5-2
- RFC 1493 ... 5-2
- RFC 1515 ... 5-2
- RFC 1573 ... 5-2
- RFC 1757 ... 5-2
- RFC 2037 ... 5-2
- RFC. *See Also* MIB. ... 5-2
- RMON ... 5-2
  - description ... 5-4
  - support ... 5-4
- router
  - gateway for IP address ... 6-9
  - use in IGMP ... 6-38

## S

- Self Test LED
  - behavior during factory default reset ... 8-16
- Serial Link Configuration screen ... 6-20
- serial number ... 7-3
- server
  - DHCP/Bootp ... 6-8
  - TFTP ... A-8
- setmib command, for IGMP configuration ... 6-42
- setting a password ... 4-10
- setting Fault Detection Policy ... 3-25
- severity code, Event Log ... 8-6
- slow network, troubleshooting ... 8-4
- SNMP ... 6-18
  - communities ... 6-15–6-16
  - Communities screen ... 6-15
  - community
    - restricted access ... 6-15
  - how to configure ... 5-3
  - IP address ... 5-3
  - manager address ... 6-15, 6-17
  - public community ... 6-15
  - traps ... 5-2
  - v2 agent ... 5-2

- SNMP-based download ... A-5
- software version ... 7-3
- software, OS ... 4-5
- sorting Alert Log entries ... 3-17
- spanning tree ... 6-30
  - configuration screen ... 6-30
  - default ... 6-30
  - forwarding state ... 6-33
  - global information ... 7-14
  - link priority ... 6-30
  - not in menu ... 6-33
  - port cost ... 6-33
  - priority ... 6-33
- starting a console session ... 4-2
- statistics ... 4-4
  - clear counters ... 4-12
- status and counters
  - access from the console ... 4-4
  - access from the web browser interface ... 7-5, 7-8
- status and counters menu ... 7-2
- status bar ... 3-13
- STP
  - root data ... 7-14
  - See* spanning tree ... 6-33
  - statistics ... 7-14
- subnet ... 6-38
- subnet mask ... 6-8–6-9
  - See also* IP. ... 6-8
- support information location, specifying ... 6-3
- support URL ... 6-3
  - changing default ... 6-3
  - default ... 6-3
- Support URL Window ... 6-3
- support/mgmt URLs ... 3-22

- switch console
  - browsing the configuration file ... 8-14
  - ending a session ... 4-3
  - help ... 4-8
  - interaction with the web browser
    - interface ... 4-1
  - Main menu ... 4-4
  - navigation ... 4-7
  - overview ... 4-1
  - Ping and link testing ... 8-11
  - resetting the switch ... 4-12
  - starting a session ... 4-2
  - status and counters access ... 4-4
  - switch management access configuration ... 4-4
- switch management
  - access configuration ... 4-4
- switch support information, location
  - specification ... 6-3
- switch-to-switch download ... A-5
- system configuration screen ... 6-22
- system name
  - configuring
    - console ... 6-23
    - web browser interface ... 6-22
  - location on screen
    - console ... 4-6
    - web browser interface ... 3-24
  - when none is specified ... 8-15

## T

- tab bar
  - web browser interface ... 3-13
- telnet
  - starting a console session ... 4-2
  - switch access problems ... 8-3
- terminal, VT100 or ANSI ... A-10
- TFTP
  - download ... A-2
  - server ... A-8
- TFTP OS download ... A-2
- time command
  - how to enter ... 8-15
- time format ... 8-6
- time parameter ... 6-22
- Time Protocol Enabled ... 6-23
- Time Protocol parameter ... 6-8
- time server ... 6-5

- timep ... 6-5
- Timep Poll Interval ... 6-8
- Timep Server ... 6-8
- traffic, monitoring ... 6-28
- traffic, port ... 7-7
- trap receiver
  - where to configure ... 5-3
- traps ... 6-18
  - authentication trap ... 6-18
  - limit ... 6-18
  - SNMP ... 6-18
  - Trap Receivers configuration screen ... 6-18
- troubleshooting
  - approaches ... 8-2
  - browsing the configuration file ... 8-13
  - diagnostics ... 8-9
  - OS download ... A-6
  - Ping and link tests
    - from the switch console ... 8-11
    - from the web browser interface ... 8-10
  - restoring factory default configuration ... 8-16
  - slow network ... 8-4
  - unusual network activity ... 8-4
- types of Alert Log entries ... 3-18

## U

- unauthorized access ... 6-18
- Unix, Bootp ... 6-11
- unrestricted write access ... 6-15
- unusual network activity ... 8-4
- up time ... 7-3
- upload configuration
  - Put command ... A-8
  - Xput command ... A-8
- URL
  - management server ... 6-4
  - support information
    - default address ... 6-3
    - location ... 6-3
  - support/Mgmt ... 3-22
  - web browser interface
    - changing default ... 6-3
    - online help location ... 6-4
- user names
  - creating ... 3-8
  - using for browser and console access ... 3-9
  - using the passwords ... 3-9

utilization, port ... 3-14

## V

version, OS ... A-3–A-5

VT100 terminal, for the console ... A-10

## W

web browser interface

- access parameters ... 3-7
- active button ... 3-13
- active tab ... 3-13
- advantages ... 1-2
- Alert Log ... 3-13, 3-16
- Alert Log control bar ... 3-13
- Alert Log header bar ... 3-13
- browsing the configuration file ... 8-13
- button bar ... 3-13
- configuration tab ... 3-22
- configuring IGMP ... 6-35
- diagnostics tab ... 3-23
- error packets display ... 3-14
- graph area ... 3-13
- graphs area ... 3-13
- how to access ... 3-3
- identity tab ... 3-21
- Java requirement ... 3-4
- maximum activity indicator ... 3-15
- non-unicast activity display ... 3-14
- online help location ... 6-4
- Overview window ... 3-12
- Ping and link testing ... 8-10
- port utilization and status displays ... 3-14
- screen layout ... 3-12
- security tab ... 3-23
- status bar ... 3-13
- status tab ... 3-21
- support information location ... 6-3
- support tab ... 3-23
- tab bar ... 3-13
- unicast activity display ... 3-14
- using IP address to access ... 3-4

web site

- accessing HP for MIB file ... 5-2

write access ... 6-15

## X

Xget command ... A-8

Xmodem OS download ... A-4

XPut command ... A-8





Technical information in this document  
is subject to change without notice.

©Copyright Hewlett-Packard Company  
1998. All rights reserved. Reproduction,  
adaptation, or translation without prior  
written permission is prohibited except  
as allowed under the copyright laws.

---

Printed in Singapore 6/98

Manual Part Number  
5967-2146



## Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>