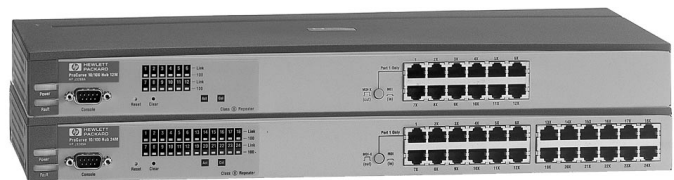


HP ProCurve Switches and Hubs

HP ProCurve

HP ProCurve  
10/100 Hub 12M and Hub 24M  
Management and Configuration Guide



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



---

**HP ProCurve**  
**10/100 Hub 12M and Hub 24M**

**Management and Configuration Guide**

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

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

### **Publication Number**

5967-9933  
January, 1999

### **Applicable Product**

HP ProCurve 10/100 Hub 12M (HP J3288A)  
HP ProCurve 10/100 Hub 24M (HP J3289A)

### **Trademark Credits**

MS-DOS® and Microsoft® are U.S. registered trademarks of Microsoft Corporation. Internet Explorer is a trademark of Microsoft Corporation. Ethernet is a registered trademark of Xerox Corporation. Netscape is a registered trademark of Netscape Corporation. NetCitizen is a trademark of Netscape Corporation.

### **Disclaimer**

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

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

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

### **Warranty**

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

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

---

# Contents

## **1 Introducing the Hub Management Interfaces**

## **2 Configuring an IP Address on the Hub**

**Methods for Configuring an IP Address and Subnet Mask** ..... 2-2

**Manually Configuring an IP Address** ..... 2-4

## **3 Using the Hub Console Interface**

**Overview of the Hub Console Interface** ..... 3-2

**Using the Hub Console** ..... 3-6

## **4 Using the HP Web Browser Interface**

**Overview** ..... 4-1

    System Requirements for Running the Web Browser Interface ..... 4-2

    Starting a Web Browser Interface Session with the Hub ..... 4-2

**Tasks for Your First HP Web Browser Interface Session** ..... 4-6

    Viewing the “First Time Install” Window ..... 4-6

    Creating User Names and Passwords in the Web Browser Interface 4-7

    Online Help for the HP Web Browser Interface ..... 4-10

**Understanding the Browser Interface Environment** ..... 4-12

    Understanding the Overview Window ..... 4-12

    The Segment Gauges Area ..... 4-13

    The Alert Log ..... 4-16

    Alert Types ..... 4-18

    Understanding The Tab Bar ..... 4-20

    Understanding the Status Bar ..... 4-24

    Setting Fault Detection Policy ..... 4-25

## 5 Using HP TopTools or Other SNMP Tools to Monitor and Manage the Hub

## 6 Configuration Reference

Console Main Menu .....	6-3
Hub Console Status and Counters Menu .....	6-5
General System Information .....	6-6
Port Status .....	6-8
Counters .....	6-11
Security Intruder Log .....	6-17
Clear Security-Flashing Port LEDs .....	6-20
Management Access Configuration Menu .....	6-22
IP Configuration .....	6-23
Community Name .....	6-28
Authorized Managers .....	6-30
User Names and Passwords .....	6-32
Telnet Enable/Disable .....	6-35
Web Enable/Disable .....	6-36
Serial Timeout .....	6-37
Hub Configuration Menu .....	6-38
System Information .....	6-40
Port Enable/Disable .....	6-42
Bridge Enable/Disable .....	6-45
Port Security .....	6-47
Configuring Port Security .....	6-48
Backup Links .....	6-52
Advanced Configuration Menu .....	6-55
Port Speed Configuration .....	6-56
Reset the Hub to Its Factory Default Configuration .....	6-58
Diagnostics Menu .....	6-60
Ping Test .....	6-61
Link Test .....	6-63
Browse Hub Configuration .....	6-65
Reboot the Hub .....	6-68
Download OS .....	6-70

Return to the Command Prompt .....	6-74
Management and Support URLs .....	6-75
Support .....	6-77

## **7 Troubleshooting**

### **Index**





# Introducing the Hub Management Interfaces

---

The interfaces enable you to reconfigure the hub and to monitor hub status and performance. The hub offers or operates with these interfaces:

- **The Web Browser Interface:** an interface that is built into the hub and accessed using a standard Web browser (Netscape Navigator or Microsoft Internet Explorer). See "System Requirements for Running the Web Browser Interface" on page 4-2.
- **The hub console:** an ASCII console interface built into the hub
- **HP TopTools for Hubs & Switches:** an easy-to-use, browser-based network management tool that works with HP proactive networking features built into managed HP hubs and switches

---

## Note

HP TopTools for Hubs & Switches 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 hub's web browser interface from a non-management PC or workstation. For HP TopTools requirements, see 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.

You can access the management features for each interface through either a menu-driven screen system or a split Window with tab navigation. Each approach has its advantages, which are described in the next sections.

This manual describes how to use the hub console (chapter 2) and the web browser interface (chapter 4). Chapter 6 is a management screen reference for both the web browser interface and the hub console. Use of HP TopTools for Hubs & Switches is described in the user's guide and online Help provided on the TopTools CD-ROM.

## Advantages of Using the HP Web Browser Interface

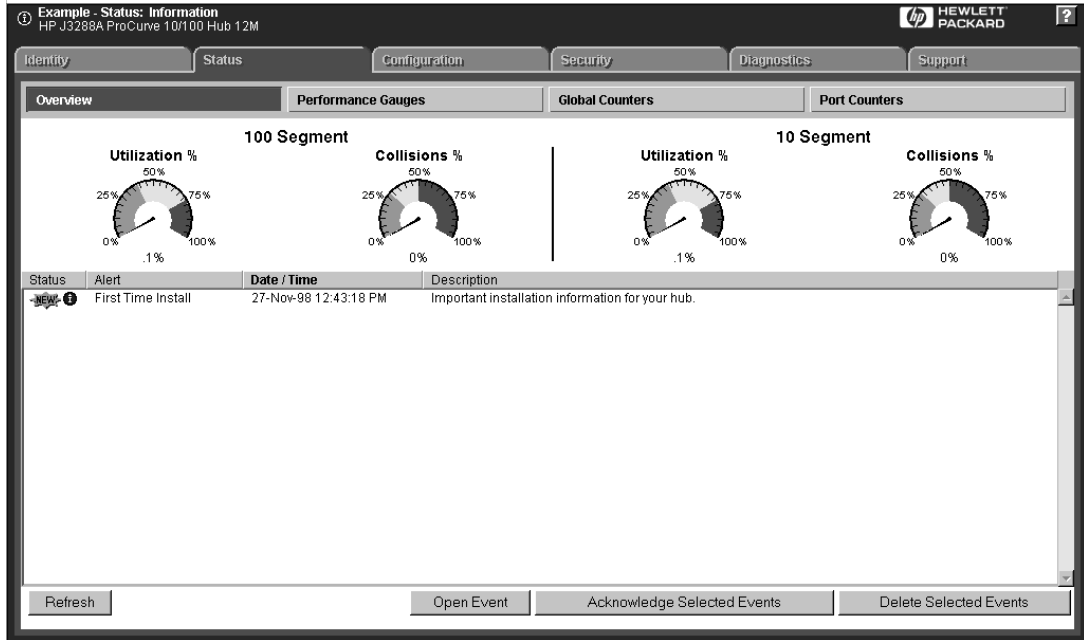


Figure 1-1. Example of the HP Web Browser Interface Display

- **Easy access** to the hub from anywhere on the network
- **Familiar browser interface**—locations of window objects consistent with commonly used browsers
- **Faster configuration**, avoiding cycling through a series of prompts—requires fewer keystrokes, using mouse clicking for navigation; no terminal setup and console menu access necessary
- **Many features have all their fields in one screen** so you can view all values at once
- **More visual cues**, using colors, status bars, device icons, and other graphical objects to represent values rather than numeric values
- **Display of acceptable ranges of values available** in configuration list boxes
- **Port security configuration** available
- **Automatic notification in the Alert Log (shown above)** when the hub detects common network problems and uses proactive features to fix or limit them

## Advantages of Using the Hub Console Interface

```
HP J3288A HP ProCurve 10/100 Hub 12M

                               Main Menu
-----
1. Hub Status and Counters...
2. Management Access Configuration... (IP, SNMP, console)
3. Hub Configuration...
4. Diagnostics...
5. Reboot Hub
6. Download Options...
7. Return to Command Prompt
0. Logout

Enter Selection =>
```

**Figure 1-2. Example of Hub Console Interface Display**

- **Out-of-band access** (through RS-232 connection) to hub, so network bottlenecks, crashes, lack of configured or correct IP address, and downtime do not slow or prevent access
- **Ability to configure management access**, for example, creating an IP address, and setting Community Names and Authorized Managers
- **Telnet access** from a management station to the full console functionality
- **Faster navigation**, avoiding delays for slower display of graphical objects over a web browser interface

## HP TopTools for Hubs & Switches

The manageable HP ProCurve 10/100 Hubs enable you to use HP TopTools from a PC on the network to monitor traffic, manage your hubs and switches, and proactively recommend network changes to increase network uptime and optimize performance. Easy to install and use—and provided at no additional cost— HP TopTools (formerly HP AdvanceStack Assistant) is the answer to your management challenges.

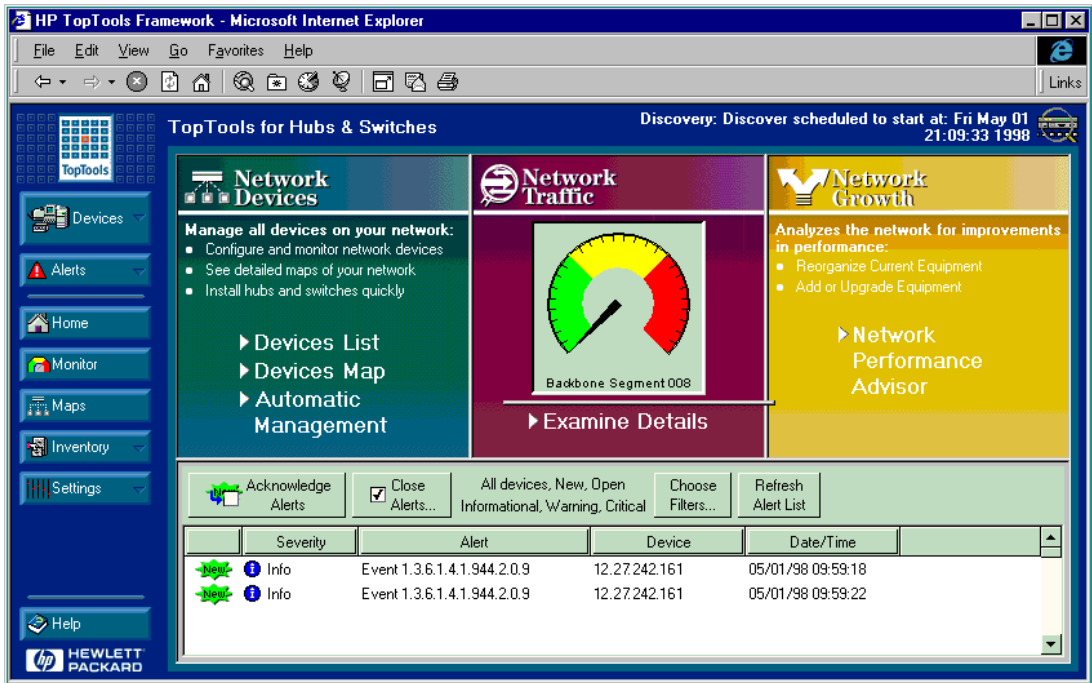


Figure 1-3. Example of HP TopTools Main Screen

### Network Devices:

- Enables fast installation of hubs and switches.
- Quickly finds and notifies you of the location of problems, saving valuable time.
- Notifies you when the hub uses a "self-healing" feature 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 traffic monitor diagrams to make bottlenecks easy to see.
- Improves network reliability through real-time fault isolation.
- Simultaneously sees the traffic on up to 1,500 segments without the use of probes.

Network Growth:

- Automatically 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 Hub

---

This chapter helps you to quickly configure an IP address and subnet mask in the hub so that you will have in-band (networked) access to the hub for any of the following interface options:

- Telnet access to the hub's console interface
- Web browser interface access to the hub
- SNMP network management access (such as HP TopTools for Hubs & Switches)

---

**Note**

In its factory-default configuration, the hub can acquire an IP address and subnet mask from a Bootp or DHCP server on your network if the server has been configured to supply the hub's IP addressing. In this case it is not necessary to manually configure IP addressing. However, if Bootp or DHCP support for the hub is not available, then it is necessary to manually configure the IP address and subnet mask, as described in this chapter, to enable the hub for management through the network.

Without an IP address and subnet mask—the factory default—you can access the hub's management features only through a direct or modem connection between the hub and a terminal or PC terminal emulator.

If you need more information on IP addressing than is provided in this chapter, refer to "IP Configuration" on 6-23.

## Methods for Configuring an IP Address and Subnet Mask

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

- **Manually, using the hub's RS-232 console port:** This is the easiest method if you have direct-connect or modem access to a terminal emulator on a PC (such as HyperTerminal in Windows 95 or Windows NT), or a direct connection to an ASCII terminal. See "Manually Configuring an IP Address" on the next page.
- **Automatically, using the DHCP/Bootp process:** This method is used to download a configuration from a Bootp or DHCP server (console not needed). To use this method, see "Automatically Acquiring an IP Address Using Bootp/DHCP" on 6-25.

An IP address and subnet mask for the hub should be assigned by your network administrator and be compatible with the IP addressing used in your network. The purpose of this section is to help you quickly configure an IP address and subnet mask in the hub. For more information about IP addressing, see "IP Configuration" on 6-23.

If your network is a standalone network, your IP addressing and subnet mask scheme can be set up in any way that meets your local needs. However, if you will be connecting your network to other networks that use globally assigned IP addresses, refer to "Globally Assigned IP Network Addresses" on 6-27.



## IP Configuration Parameters

**IP Address:** Uses the format X.X.X.X, where each X is a decimal number between 0 and 254. Every IP address on a network must be unique.

**Subnet Mask:** This (bit) mask defines which portion of the IP address is the subnet address and is written in the format X.X.X.X. All devices on your IP network must use the same subnet mask address.

**Default Router:** Also known as a "gateway" address, this is the routing IP address of the nearest router. The default is 0.0.0.0. Use this field if you want to reach off-subnet destinations. If no routers are in your network, enter the same IP address that you use for your hub.

**Time To Live:** The number of IP routers a packet is allowed to cross before the packet is discarded (default: 64). Increase this value if the hub is managed from a network management station that is more than 64 routers away.

## Manually Configuring an IP Address

1. Use the instructions in your hub installation manual to connect a PC running a terminal emulator, or a terminal, to the RS-232 Console port on the hub.
2. Start a hub console session and, at the Command Line prompt, enter **MENU** to access the menu system region.

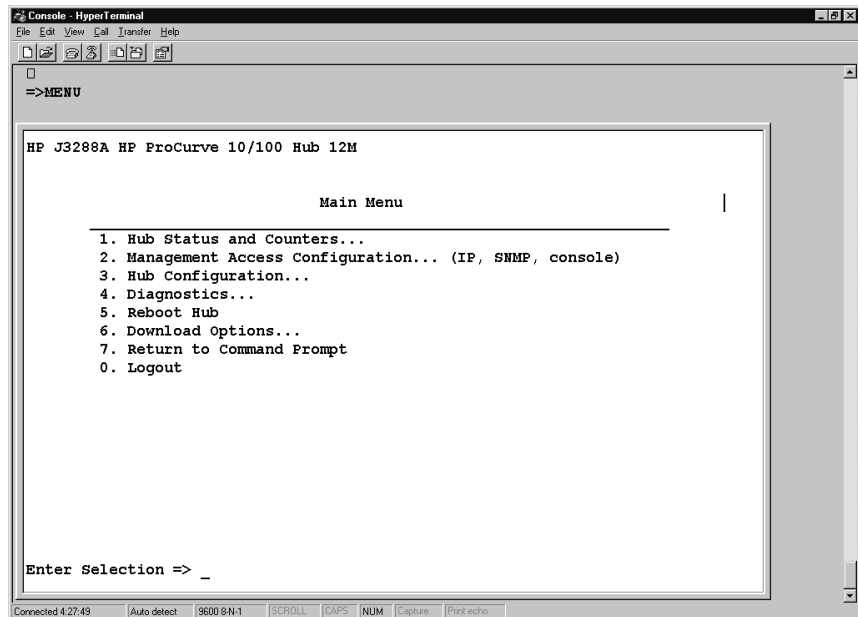


Figure 2-1. The Main Menu

3. From the Main menu, select
  2. **Management Access Configuration. . . (IP, SNMP, console)**
    1. **IP Configuration.**

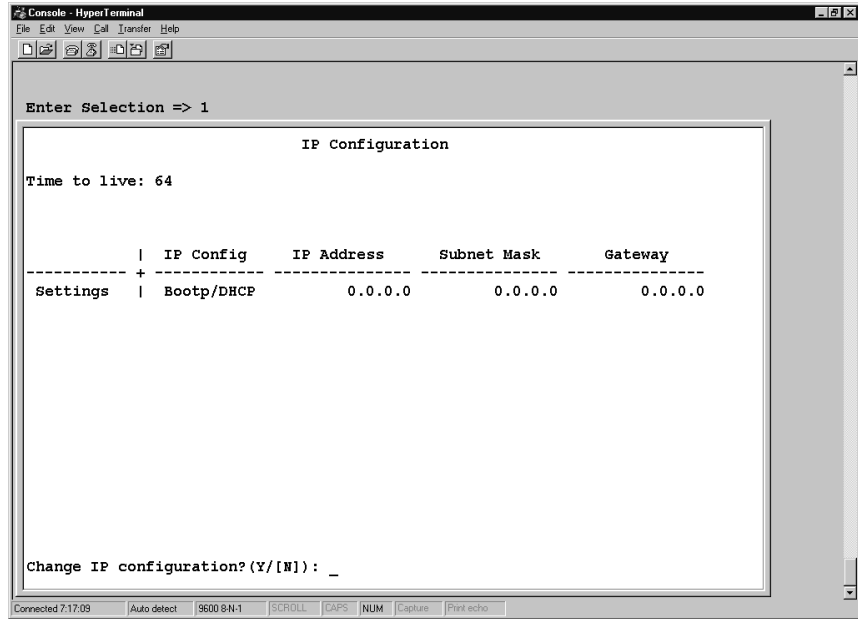


Figure 2-2. The IP Configuration Screen

4. Enter **Y** at the **Change IP configuration? (Y/[N]):** prompt.

The console prompts you to select the method by which you want to assign an IP address to your hub. The two options are **(B)ootp/DHCP** (the default setting) or **(M)anual Config**. (A third option, **Disable**, disables IP addressing.)

DHCP and Bootp are automatic network address selection protocols. If your network supports this capability, see “Automatically Acquiring an IP Address Using Bootp/DHCP” on page 6-25.

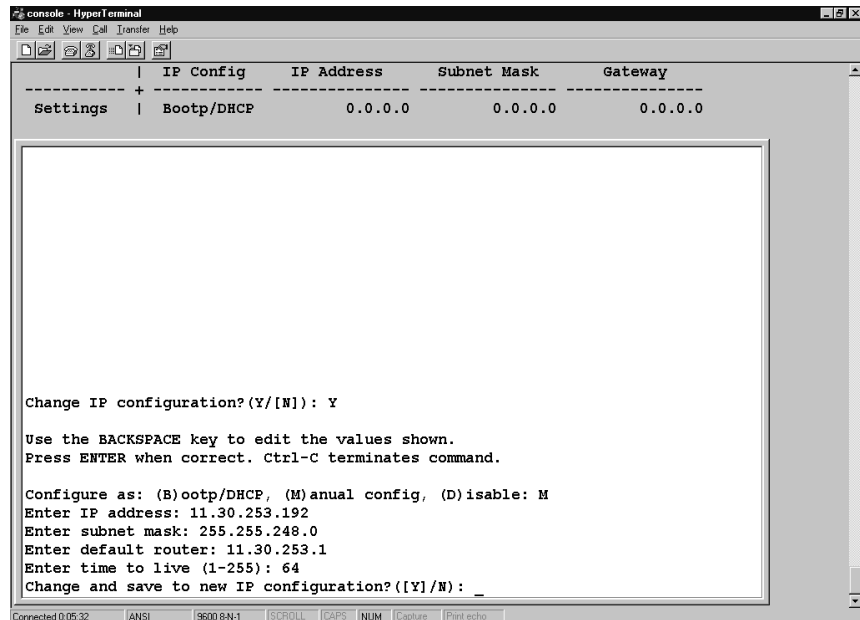
5. Enter **M** to manually assign the IP address information.
  - a. Enter the IP address you want to assign to the hub.
  - b. Enter the subnet mask for your network.

## Configuring an IP Address on the Hub

### Manually Configuring an IP Address

- c. If you want to reach off-subnet destinations, enter the address of the gateway router for your subnet in the **Gateway** field. If there are no routers in your network, enter the hub's IP address. Otherwise, leave this parameter set to (the default) **0.0.0.0**.
- d. Leave the Time to Live parameter set to 64 (the default) unless you have indications that another setting is warranted.

Type in each value at the appropriate prompt and press **Enter** to see the next prompt. Figure 3-2 shows you how the address assignment process appears.



**Figure 2-3. Setting an IP Address in the Hub Console.**

6. After you pass the **Time To Live** value, the console prompts you with:

**Change and save to new IP configuration?([Y]/N):**

7. Enter **Y** to save all of the values you have set. The console then returns you to the IP Configuration screen. Note the new address, Subnet Mask, Default Router, and Time To Live values that you have set and verify that they are correct.
8. Return to the Main menu.

Your hub is now ready to be managed as a network device through the web browser interface, or through HP TopTools for Hubs & Switches or other network management tools. To find out how to run the Browser Interface, see chapter 4, "Running the Browser Interface". For details on how to manage your hub from HP TopTools or HP OpenView, see the online help in those applications.

## Where To Go From Here

The above procedure configures your hub with an IP address, subnet mask, default router (gateway), and time to live parameters. With the proper network connections, you can now manage the hub from a network management station or from a PC equipped with a web browser.

<b>Topic</b>	<b>Title</b>	<b>Page</b>
To use the console interface:	Chapter 3, "Using the Hub Console Interface"	3-1 ff
To access the hub using a web browser:	Chapter 4, "Using the HP Web Browser Interface"	4-1 ff
To access the hub using a network management tool:	Chapter 5, "Using HP TopTools or other SNMP Tools to Monitor and Manage the Hub"	5-1 ff
To access specific hub configuration features:	Chapter 6, "Configuration Reference"	6-1 ff
To access the hub using inbound Telnet access:	"Starting a Session Through a Telnet Connection" "Telnet Enable/Disable"	3-5 6-35
Error indications, problems	"Chapter 7, Troubleshooting"	7-1 ff



# Using the Hub Console Interface

---

This chapter describes the following:

- overview of the hub console
- starting a hub console session through a:
  - direct (out-of-band) serial connection
  - modem (out-of-band) serial connection
  - Telnet (networked, or in-band) connection
- using the hub console's two regions:
  - the command prompt
  - the menu system

---

**Note**

The HP ProCurve 10/100 hubs are “plug-and-play” network devices. They are shipped with a factory default configuration that works for most network situations. In the default configuration:

- All hub ports are enabled.
- DHCP/BOOTP is enabled, allowing the hub to automatically acquire an IP address from a properly configured DHCP or BOOTP server.

For this basic hub operation, it is not necessary to use the console. However, you can use the console for the uses listed on the next page.

---

## Overview of the Hub Console Interface

The hub console interface enables you to do the following:

- Modify the hub's configuration
- Manually configure the hub with an IP address, which enables the hub to be managed:
  - From the hub's web browser interface (chapter 4)
  - Through Telnet access to the console interface (pages 3-5 and 6-35)
  - From an SNMP-based network management station
- Control console security by configuring passwords
- Monitor the hub and its port status
- Monitor network activity through a set of counters
- Download new software to the hub

### Starting a Hub Console Session

The hub console interface can run on either a PC-based terminal emulator program or on a standard ASCII or ANSI terminal. You can connect the console to the hub in the following ways:

- Direct, through the (out-of-band) RS-232 serial connection (using the serial cable provided with the hub)
- Remote, using an (out-of-band) modem connection
- Networked (in-band) access through a Telnet session (requires that the hub has an IP address)



## Starting a Session Through a Direct Serial Connection

1. Connect either a PC emulating an ASCII terminal or a standard ASCII terminal to the Console port on the hub using the serial cable supplied with your hub. (For pin-outs on the cable and Console port connector, see the Cables and Connectors appendix in the *HP ProCurve 10/100 Hubs Installation Guide*.) If the PC or terminal has a 25-pin serial connector, first attach a 9-pin to 25-pin “straight-through” adapter at one end of the console cable and attach that end to the terminal.
2. Power-on the PC and start the terminal emulation program, or power-on the terminal. Configure the terminal emulator or terminal as follows:
  - ASCII, ANSI, or VT-100 emulation or terminal
  - 8 bits per character
  - 1 stop bit
  - no parity
  - Xon/Xoff for flow control
  - a baud rate of 115200, 57600, 38400, 19200, 9600, 4800, 2400, or 1200.
3. Press **Enter** a few times until the console displays hub version information followed by the message and prompt:

**Type MENU to access the ASCII menu system  
or HE or ? for help on console commands.**

=>\_

The baud rate for communication between the hub and the terminal is set automatically when you press **Enter**.

---

**Note:**

If you have previously set a user name and password for the console, you will first be prompted to enter those values. For more information on the password response process, see “Responding to an Enter username Prompt” on page 3-10.

You are now in the command prompt region of the console interface. To see what commands are available, enter **HELP** or **?** at the prompt. To enter the console menu system, enter **MENU** at the prompt.

For more on commands, see “The Command Prompt Region” on page 3-7. For information on console menus, see “The Console Menu System” on page 3-9.

## Starting a Session Through a Modem Connection

To establish a remote session using a pair of modems and terminal, do the following:

1. Use full-duplex, asynchronous (character-mode) modems only. Initialize both modems.
2. Connect the modem for the hub end to the hub's Console port using a "straight-through" RS-232-C modem cable. (For pin-outs and recommended cables see the "Cables and Connectors" appendix in your *HP ProCurve 10/100 Hubs Installation Guide*).
3. At the remote site, connect the modem for the console end to the serial port on the PC or terminal.
4. Make sure the terminal and modems are functioning properly, then establish the link between the console's modem and the hub's modem according to the modem instructions. See your modem manufacturer's configuration guide for details.
5. Press  a few times until the console displays hub version information followed by the message:

**Type MENU to access the ASCII menu system  
or HE or ? for help on console commands.**

=>\_

The baud rate for communication between the hub and the terminal is set automatically when you press .

---

**Note:**

If you have previously set a user name and password for the console, you will first be prompted to enter those values. For more information on the password response process, see "Responding to an Enter username Prompt" on page 3-10.

You are now in the command prompt region of the console interface. You can enter **HELP** or **?** at the prompt to see what commands are available. To enter the console menu system, enter **MENU** at the prompt.

## Starting a Session Through a Telnet Connection

---

### Note

Running a Telnet session with the hub requires that the hub first be configured with an IP address. (This can be done manually or via DHCP/Bootp—if DHCP/Bootp is configured and operating in your network—page 6-25.) If you have not yet configured an IP address for the hub and are not using DHCP/Bootp, use either the serial (page 3-3) or modem (page 3-4) procedure to first start an out-of-band console session through which you can configure an IP address on the hub.

---

To begin a Telnet session:

1. Verify that the hub has been configured with an IP address, and that it is accessible through IP from your PC or workstation. (You can use the Ping command from your PC to verify hub accessibility.) See chapter 2, "Configuring an IP Address on the Hub" for details on configuring an IP address.
2. On your networked PC or workstation, enter the command **telnet** followed by the IP address or system name of the hub, for example:

```
telnet 192.1.1.10  
or  
telnet your_hub
```

(Your Telnet syntax depends on your TCP/IP software or your terminal server. You can use a system name if you have a name resolution system such as Domain Name Server--DNS.)

The console then displays hub version information followed by the message:

```
Type MENU to access the ASCII menu system  
or HELP or ? for help on console commands.
```

```
=>_
```

You are now in the command prompt region of the console interface. You can enter **HE** or **?** at the prompt to see what commands are available. To enter the console menu system, enter **MENU** at the prompt.

For more information on commands, see "The Command Prompt Region" on page 3-7. For information on the console menus, see "The Console Menu System" on page 3-9.

**To End a Telnet Session.** In the Main Menu, select **Logout**, then enter **Y** at the resulting prompt. Or, if the command prompt is displayed, enter **LO**, then enter **Y** at the resulting prompt.

## Using the Hub Console

The hub console is an easy-to-use, intuitive interface that prompts you for input and guides you through any configuration exercise. The hub console consists of these two regions:

- **the Command Prompt region** which appears when you first enter the console. This region enables you to perform tasks by issuing commands. For a listing of these commands, see Table on page 3-8.
- **the Menu System region** which you access by entering **MENU** from the command prompt. The menus enable you to configure hub and port settings through screens that contain fields and prompts. For an overview, see “The Console Menu System”. For details on each of the menus in this region, see chapter 6.

### User Name and Password Prompts

(To to add or change the password and user name, see "Passwords" on page 6-32.)

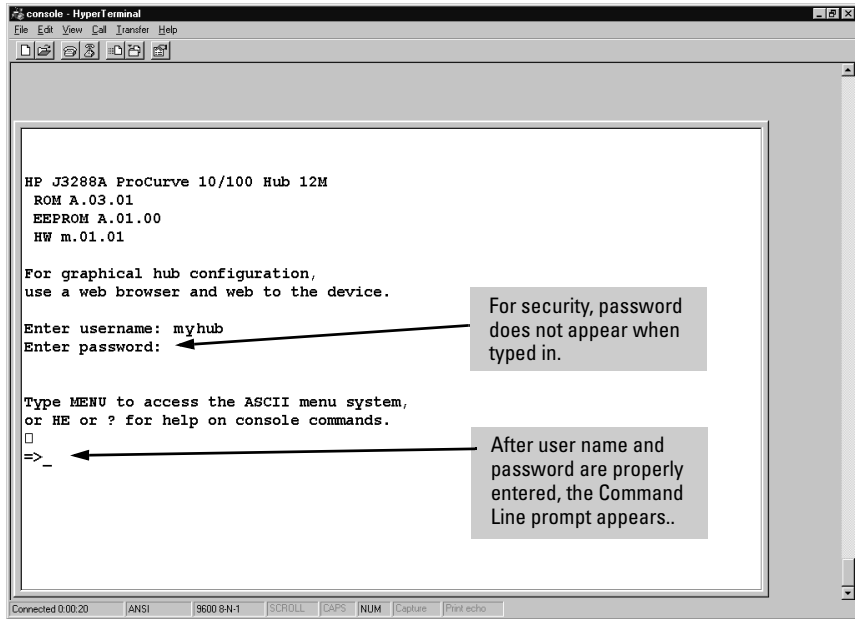
When you begin a Console session, if a user name and password were previously configured, you will see this prompt:

**Enter username:** \_

In this case, enter the correct user name and password to display the Command prompt (**=>**). To do so:

1. Type in the previously configured user name at the **Enter username** prompt and press **[Enter]**. The console then displays a **Password** prompt. (If you make a mistake, you will have three retries before the console disconnects.)
2. Type in the password required at the **Password** prompt and press **[Enter]**. Note that, when entered, the password is not displayed on the screen for security reasons. The console then displays the Command prompt. (If you make a mistake, you will have three retries before the console disconnects.)

After you enter the correct user name and password, the console interface displays the **=>** prompt as shown in figure 3-1, below.



**Figure 3-1. Example of a User Name and Password Session**

**What If I Lose the User Name or Password?** If you lose either the hub's user name or password, you can clear them from memory by pressing and holding the Clear button on the hub for 10 seconds.

---

**Caution**

---

Clearing the user name and password removes the hub's password protection, which makes it vulnerable to unauthorized access via Telnet or the web browser interface.

### The Command Prompt Region

The => prompt indicates you are at the command prompt region of the hub console. This region is a command-driven environment that enables you to perform several basic tasks. The tasks are performed by entering two-letter commands. To list these commands, enter **HELP** or **?** at the command prompt.

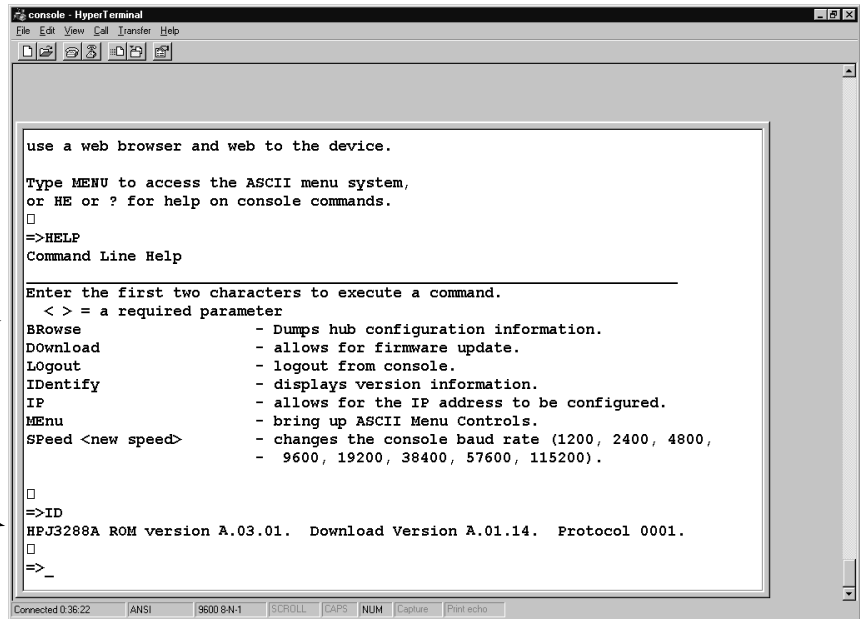
The available commands in the Command Prompt region are shown below

## Using the Hub Console Interface

### Overview of the Hub Console Interface

Output of HE (Help) Command

Output of ID (Identify) Command



**Figure 3-2. Command Prompt Screen Displaying Help and ID Commands**

Commands Issued from the Console Command Prompt.

Command	Command Name	Description
BR	Browse	Displays scrolling readout of hub's current configuration.
DO	Download	Prepares the hub to download a new version of firmware (operating system, or OS) from a server.
HE	Help	Displays some basic help on all console commands.
ID	Identify	Displays firmware revision number, for example, <b>A.01.01</b> .
LO	Logout	Terminates the hub console session.
DI	Disconnect	Terminates the hub console session.
ME	Menus	Displays the hub console Main Menu. The Main Menu enables you to access all top-level menus available in the Console interface.
SP	Speed	Enables you to set the Baud Rate for an out-of-band connection with the hub.

Figure 3-2 on page 3-8 shows a sample Command Prompt screen where the hub's product number and firmware information is displayed by the ID command.

## The Console Menu System

The console menu system starts at the Main Menu, which displays the top-level menus for the console interface. These menus contain submenu options grouped by common topic, and enable you to perform a number of tasks, including:

- viewing hub and port counter statistics
- configuring access settings
- configuring security settings
- configuring port and device settings
- performing diagnostic tests
- rebooting the hub
- downloading new firmware

To enter the hub console's menu system, enter **MENU** at the command prompt. The Main Menu then appears, as shown in figure 3-3, below.

To navigate through the menus, simply enter the number of the menu option that you want to use.

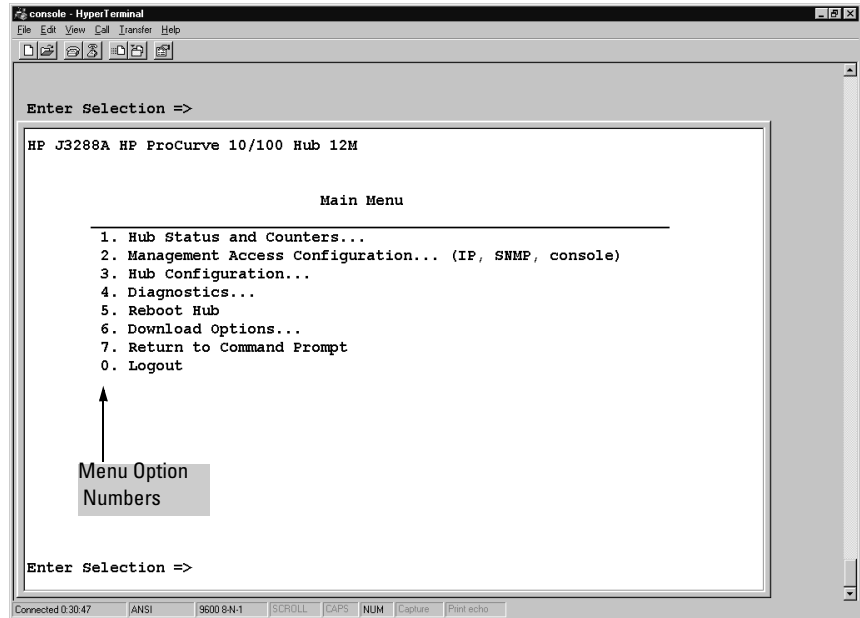


Figure 3-3. The Hub Console Main Menu.

### Responding to an **Enter username** prompt

If the console interface displays

**Enter username:** \_

when you attempt to display the Main Menu, then a user name and—most likely—a password, have been previously configured on the hub. In this case, you must enter the correct user name and password before the Command Prompt (= >) will appear. To do so:

1. Type in the previously configured user name at the **Enter username** prompt and press **[Enter]**. The console then displays a **Password** prompt. (If you make a mistake, you will have three retries before the console disconnects.)



2. Type in the password required at the **Password** prompt and press **[Enter]**. Note that, when entered, the password is not displayed on the screen for security reasons. The console then displays the Command Prompt. (If you make a mistake, you will have three retries before the console disconnects.)

After you enter the correct user name and password, the console interface displays the => prompt as shown in figure 2-3.

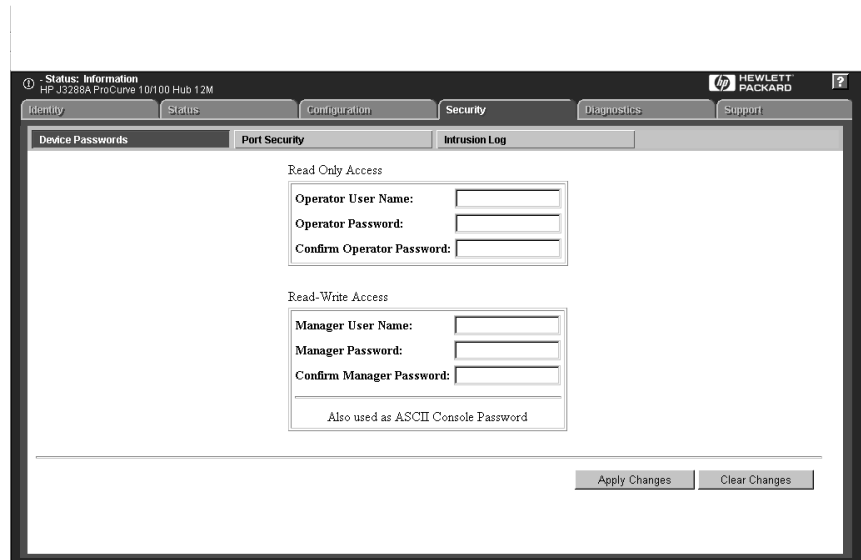


Figure 3-4. Example of a User Name and Password Session

---

**Note**

If you lose either the hub's user name or password, you can clear them from memory by pressing and holding the Clear button on the hub for 10 seconds. Once you have removed the password, you can issue commands in the Command Prompt region or enter the hub's console interface Menu System.

To use either the console or the web browser interface to add or change the password and user name, see "User Names and Passwords" on page 6-32.

---



# Using the HP Web Browser Interface

---

## Overview

The HP web browser interface built into the hub lets you easily access the hub 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 hub
- Maintain management access security by configuring user names and passwords
- Configure port security

Using the web browser interface to configure the hub is covered in chapter 6, “Configuration Reference”. This chapter covers the following:

Topic	Page
System requirements for using the web browser interface	4-2
Starting a web browser interface session using a standalone browser or HP TopTools for Hubs & Switches	4-2, 4-3
Viewing the "First-Time Install" window	4-6
User names and passwords in the web browser interface	4-7 thru 4-9
Online Help for the web browser interface	4-10
Features of the web browser interface environment	4-12
Fault detection policy in the Alert Log	4-25

---

### 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 Serial Link configuration screen in the hub console. See “Web Enable/Disable” on page 6-36.

---

## System Requirements for Running the Web Browser Interface

Use equipment meeting the following minimum requirements to access the web browser interface on your intranet.

**Table 4-1. 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	65,000
Internet Browser (English-Language browser only)	<b>PCs:</b> <ul style="list-style-type: none"><li>• Netscape® Communicator 4.03</li><li>• Microsoft® Internet Explorer 4.01 sp1</li></ul> <b>UNIX:</b> Netscape Navigator 4.03 or later	<b>PCs:</b> Netscape Communicator 4.03 or later <b>UNIX:</b> Netscape Navigator 4.05 or later.
PC Operating System	Microsoft Windows® 95 and Windows NT	
Unix® Operating System	Standard Unix® OS	

## Starting a Web Browser Interface Session with the Hub

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

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

---

### Note

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

---

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

This procedure assumes that you have a supported web browser (table 4-2 on page 4-2) installed on your PC or workstation, and that an IP address has been configured on the hub. (For more on assigning an IP address, see chapter 2, “Configuring an IP Address on the Hub”.)

1. Make sure the Java™ applets are enabled for your browser. If they are not, do one of the following:
  - In Netscape 4.x, 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 (for expert users)**

Then scroll to the **Java Permissions** and refer to the online Help for specific information on enabling the Java applets.

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

**hub3288**  (example of a DNS-type name)

**10.11.12.195**  (example of an IP address)

If you are using a Domain Name Server (DNS), your device may have a name associated with it (for example, **hub3298**) that you can type in the **Location or Address** field instead of the IP address. Using DNS names typically improves browser performance. See your network administrator for any name associated with the hub.

The web browser interface automatically starts with the Status Overview window displayed for the selected device as shown in figure 4-1 on page 4-5.

## Using HP TopTools for Hubs & Switches

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

This procedure assumes that:

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

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

1. Make sure the Java™ applets are enabled for your web browser. If they are not, refer to the web browser online Help for specific information on enabling the Java applets.
2. Do *one* of the following tasks:
  - On the HP TopTools Maps view, double-click on the symbol for the networking device that you want to access.
  - In HP TopTools, in the Topology Information dialog box, in the device list, double-click on the entry for the device you want to access (IP address or DNS name).
3. The web browser interface automatically starts with the Status Overview window displayed for the selected device, as shown in figure 4-1 on page 4-5.

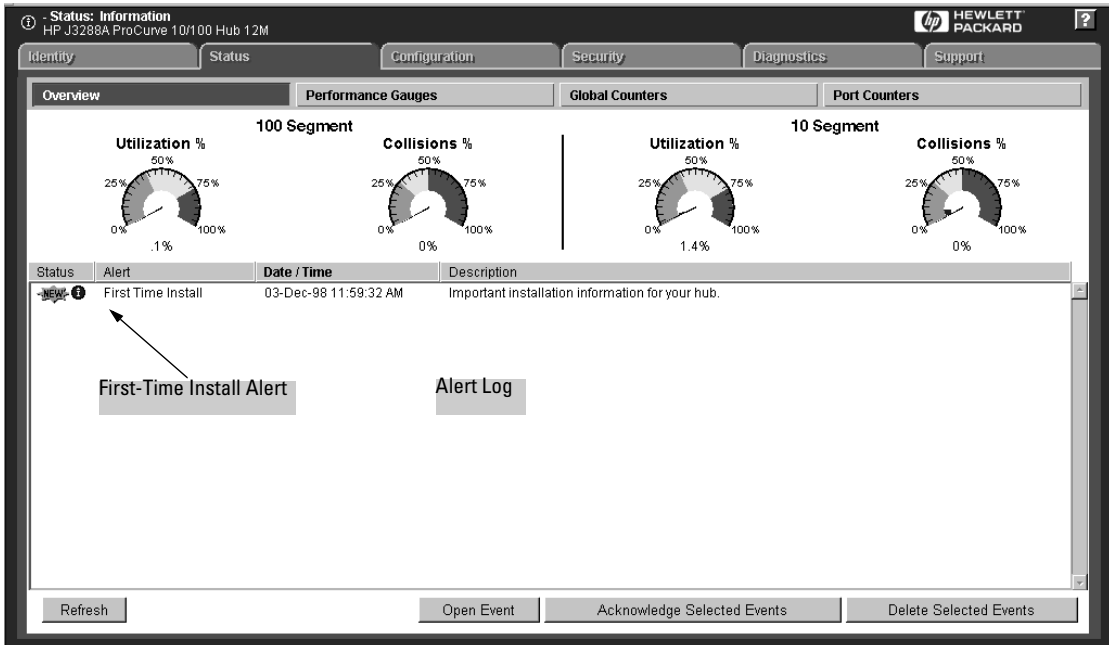


Figure 4-1. Status Overview Screen

## 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 hub’s web browser interface for the first time, the Alert log contains a “First Time Install” alert, as shown in figure 4-1. 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. Doing so determines the types of messages that will be displayed in the Alert Log and/or any actions to take upon detection of a fault.

Double click on **First Time Install** in the Alert log. The web browser interface then displays the “First Time Install” window, as shown in figure 4-2, below.

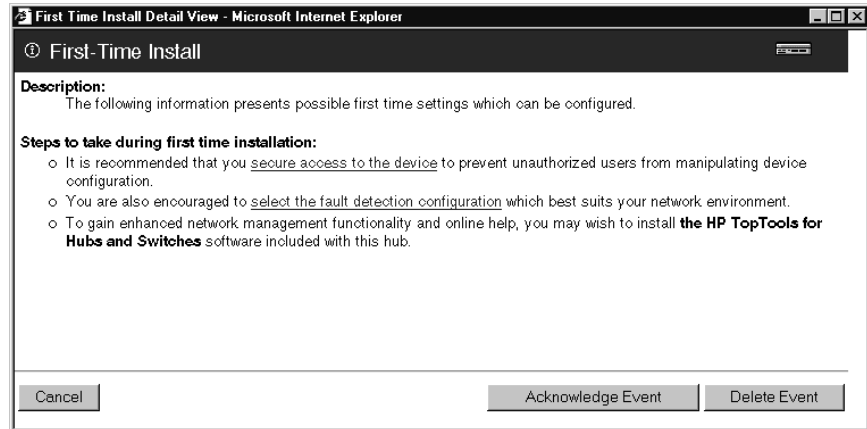


Figure 4-2. First-Time Install Window



This window is a launching point for setting passwords and for configuring Fault Detection policy (which determines the types of messages that will be displayed in the Alert Log and/or any actions to be taken upon detection of a fault).

**To set web browser interface passwords:** Click on  
**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.

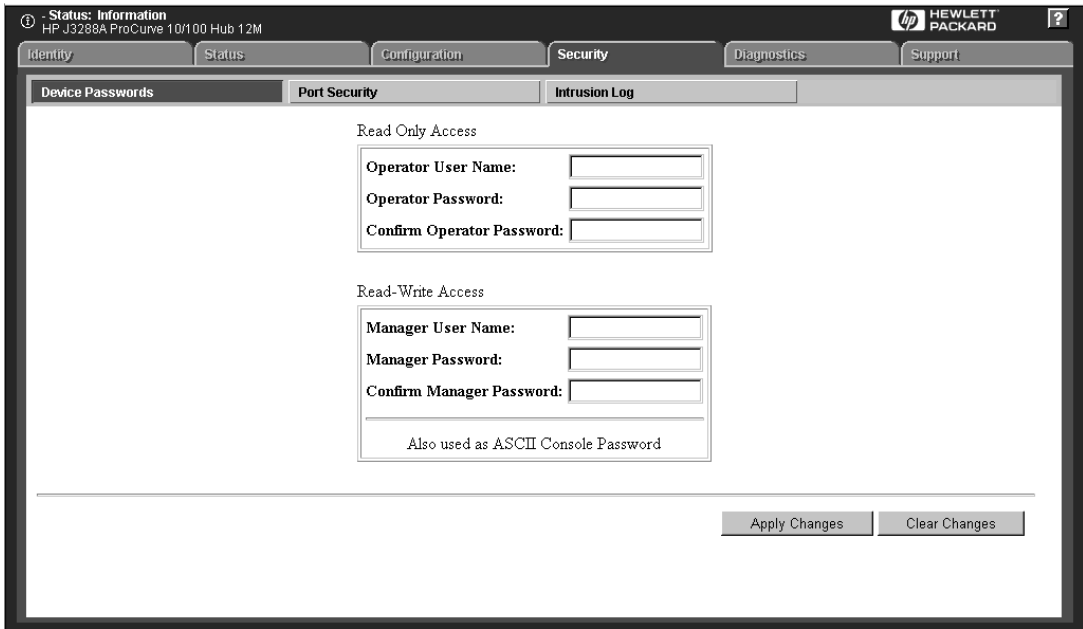
**To set Fault Detection policy:** Click on  
**select the fault detection configuration**

in the second bullet in the window and go to the section, “Setting Fault Detection Policy” on page 4-25.

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

In the hub console interface, you can set one user name and one password on the manager level. However, in the web browser interface you can set user names and passwords on both the Operator and Manager levels to create multi-level access security for your hub.

- **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 4-3. The Device Passwords Window**

To set the passwords:

1. Access the Device Passwords screen by either 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 15 printable ASCII characters.

3. Click on [Apply Changes](#) to activate the user names and passwords.

---

**Note**

---

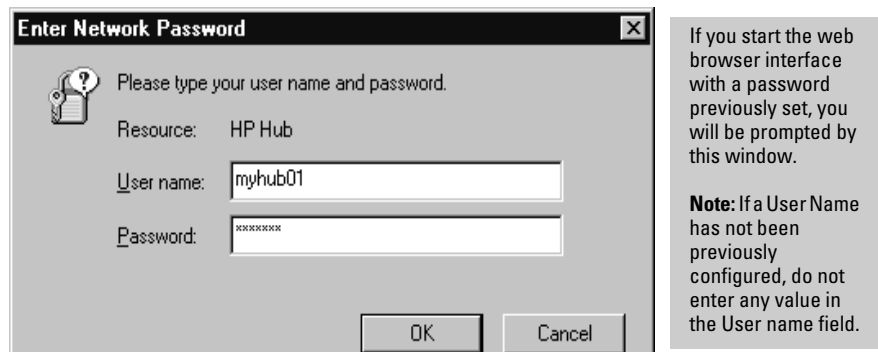
A manager user name and password you assign in the web browser interface will overwrite a previous manager user name and password assigned in either the web browser interface or the hub console.

## Using the User Name and Password Feature

The manager user name and password control access to both the web browser interface and the hub console. (The operator user name and password control access only to the web browser interface.) Once set, you will be challenged to supply the password every time you try to access either the web browser interface or hub console. The user name and password you enter determines the capability you have during that session:

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

*If a user name has not been set, you must leave the User Name field in the web browser **Enter Network Password** window blank.*



**Figure 4-4. Example of the User Name and Password Window**

The hub console uses only the Manager user name and password, and does not prompt you for an Operator user name and password, even if they have been configured in the web browser interface.

### If You Lose a Password

If you lose the passwords, you can clear them by pressing and holding the Clear button on the front of the hub for approximately 10 seconds. This action deletes all password and user name protection for both the web browser interface and the hub console.

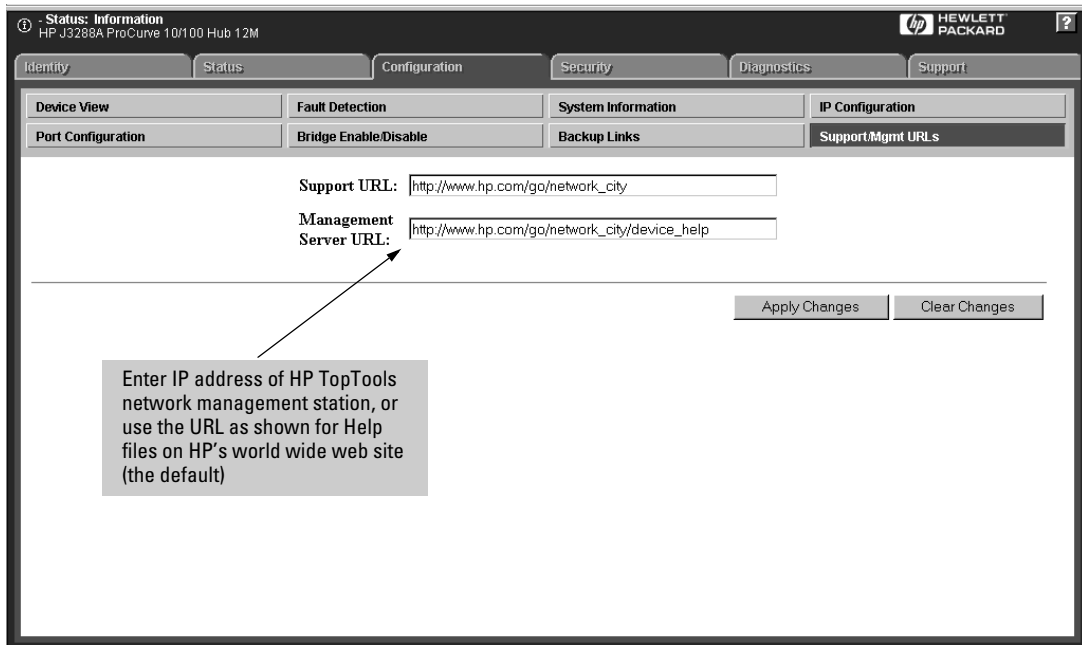
**Note**

*The Clear button is provided for your convenience, but its presence means that if you are concerned with the security of the hub configuration and operation, you should make sure the hub 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.

**Providing Online Help.** *The Help files are automatically available if you install HP TopTools for Hubs & Switches on your network or if you already have Internet access to the World Wide Web. (The Help files are included with HP TopTools for Hubs & Switches, and are also automatically available from HP via the World Wide Web.) Retrieval of the Help files as described above is controlled by automatic entries to the **Management Server URL** field on the **Configuration / Support URLs** screen, shown in figure 4-5.*



**Figure 4-5. How To Access Web Browser Interface Online Help**

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

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

- If HP TopTools for Hubs & Switches is installed and running on your network, enter the IP address or DNS name of the network management station in the Management Server URL field shown in figure 4-5 on page 4-10.
- If you have World Wide Web access from your PC or workstation, and do not have HP TopTools installed on your network, enter the following URL in the Management Server URL field, as shown in figure 4-5 on page 4-10:

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

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

See also “Management and Support URLs” on page 6-75.

## Understanding the Browser Interface Environment

Now that you have successfully run the web browser interface and created a password and user name, become comfortable with the environment. The web browser interface is a powerful tool that enables you to perform complex network configuration procedures with the simplicity of a mouse click. Spend a little bit of time reviewing the following sections to learn about the different pieces of this tool.

### Understanding the Overview Window

The web browser interface Overview Window is the home environment for any entry into the web browser interface. The following figure details the different parts.

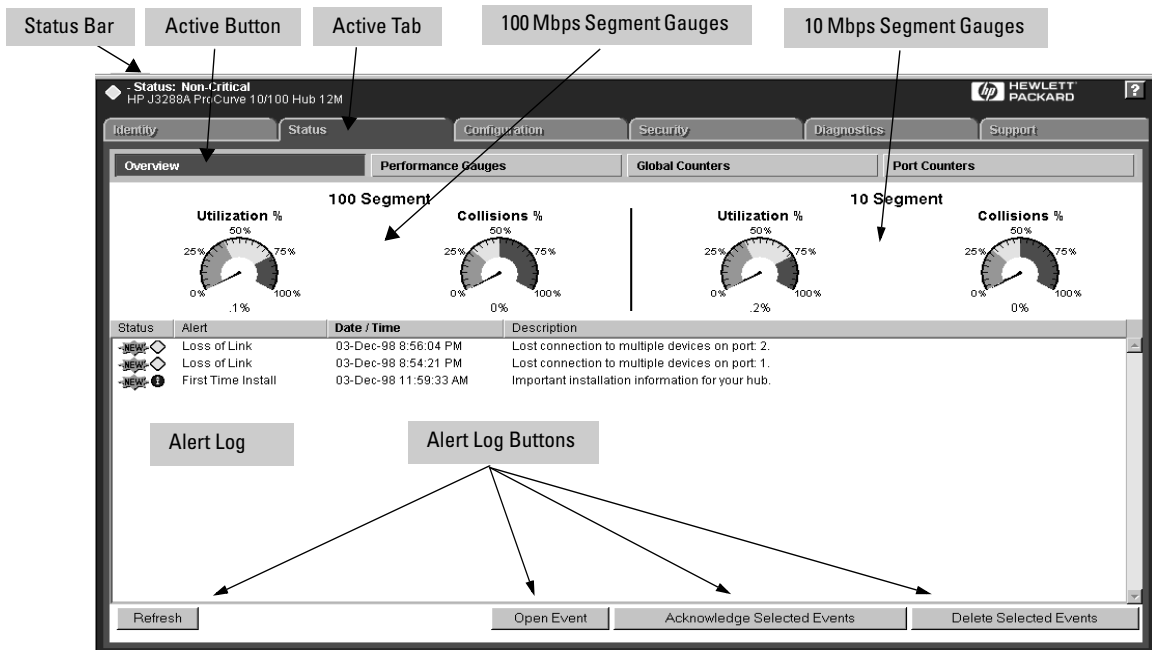


Figure 4-6. The Overview Window

The areas and fields in the Overview Window are:

**Active Tab.** The current tab selected. The tab is darkened and all the buttons contained by the tab are displayed.

**Status Bar.** The region above the tab bar that displays status and device name information.

**100 Mbps Segment Gauges Area.** The region containing gauge graphics that indicate performance trends for the 100 Mbps segment of the hub.

**10 Mbps Segment Gauges Area.** The region containing gauge graphics that indicate performance trends for the 10 Mbps segment of the hub.

**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 hub'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 hub, and a short description of the alert.

**Alert 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 Segment Gauges Area

The two Segment Gauges Areas each contain two separate graphical meters or *gauges* that display values associated with collisions and utilization in the 100 Mbps and 10 Mbps segments of the hub. The following figure shows a sample reading of the Gauges Area.

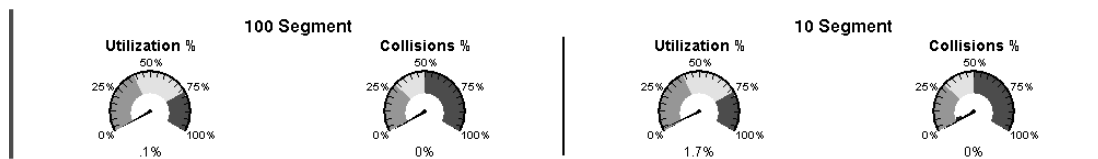


Figure 4-7. The Segments Gauges Area

**Utilization.** Generally, Utilization is the percentage of a network's bandwidth that is currently being consumed by network traffic. Consistently high (>40%) utilization indicates points of network slowdown (or failure) and a need for changes or upgrades in your network infrastructure.

The pointer on any of the hub's utilization gauges indicates the amount of bandwidth used for traffic during the last five-second interval. The inner ring on the gauges represents the highest utilization of traffic received during the current window session. (Each time you display a window showing gauges, the "Highest Reading" indicator for those gauges restarts from zero.) For the 10T and 100T segments, the utilization gauges indicate the total traffic transmitted and received. For individual ports, the gauge(s) showing LAN utilization indicate received (Rx) traffic only. For an example of how utilization is calculated, see the online Help available through the hub's web browser interface.

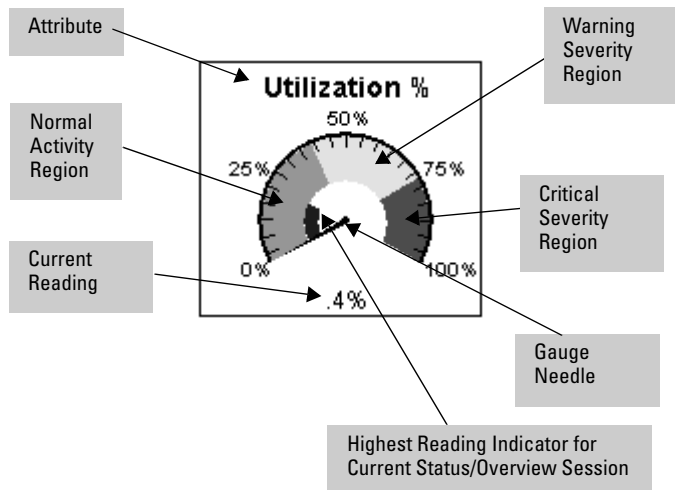
The utilization value is a total of all unicast, multicast, and broadcast traffic through the selected hub segment or port. For example, if one port is receiving heavy broadcast or multicast traffic, bandwidth for all ports on the segment will be consumed. To discover the exact source of the heavy traffic, examine counter data in the Global Counters or Port Counters screens in the web browser interface.

**Collisions.** This value is the number of collisions, expressed as a percent of all packets received on the hub.

A collision is an event that occurs when two or more devices try to transmit a message on the same segment at the same time. The transmissions collide and no messages involved in the collision are successfully delivered. Each device involved in a collision will then wait a random period of time before trying to resend. This random wait period increases the likelihood that the messages will not collide again. The number of collisions should be proportional to the number of packets transmitted over time and the number of nodes on the network. Collisions are a normal occurrence on a CSMA/CD network collision domain.



Take a moment to review the various gauge components to understand how the feature works.



**Figure 4-8. Gauge Elements**

The objects in the figure are described here.

- **Attribute.** The counter for which the gauge is measuring activity.
- **Current Reading.** The current level that the activity of the attribute has reached.
- **Highest Reading Indicator.** The interior region of the gauge that indicates the highest reading the attribute has reached in the current session. Note that the current reading of the Gauge Needle and the High Watermark Indicator may be different (the High Watermark Indicator maybe higher). Once you leave the screen, the High Watermark Indicator returns to 0.
- **Gauge Needle.** The black pointer in the center of the gauge that points to different values on the gauge, indicating levels of activity for the attribute.
- **Normal Activity Region.** The lower region of the gauge, always shown in green, indicating a healthy level of attribute activity.
- **Warning Severity Region.** The middle region of the gauge, always shown in yellow, indicating an increasingly severe level of attribute activity.
- **Critical Severity Region.** The higher region of the gauge, always shown in red, indicating a problem with the level of attribute activity and that action needs to be taken.

After the web browser interface displays the Overview Window, the Attribute Reading fields for all four attributes display the **Measuring...** indicator, meaning that the application is collecting current data from the hub to represent in the gauges. After a few seconds, the Attribute Reading fields display values, frequently 0, but sometimes high values. The Gauge needle moves to a position reflecting the current level for the attribute displayed. Note the three colored regions in the gauge. These colors appear in three distinct *Gauge Severity Regions*. They also map to specific Status Indicator shapes that are displayed in two places:

- The Status column in the Alert Log
- The Status Bar above and to the left of the Gauges area

See Table 4-3 (page 4-24) for details on Status Indicator shapes.

The range of each Gauge Severity Region differs for each attribute. For example, the upper limit of the range for the Normal Activity Region for Utilization is about 40 (percent). The upper limit of the range for the Normal Activity Region for Collisions is just over 25 (percent). The thresholds for warning and critical levels are as follows:









**Table 4-2. Attribute Values Range**

Attribute	Warning Threshold	Critical Threshold
Utilization%	40	75
Collisions	30	50
Broadcasts*	600	2000
Errors*	2	3
Multicasts*	1500	4000

\* Available by clicking on the Performance Button to display data for individual ports or segments.

## The Alert Log

The Alert Log, shown in the lower half of the Status | Overview screen (figure 4-6 on page 4-12), shows a list of network occurrences, or *alerts*, that were retrieved from the hub. Typical alerts are **Loss of Link**, indicating a severed connection between a hub port and multiple nodes, **Broadcast Storm**, indicating an excessive number of broadcasts received on a port, and **Problem Cable**, indicating a faulty cable. A full list of alerts are shown in Table 4-3.

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.
	Auto Fastrxn	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/ Repeater Hops	15-Sep-97 1:46:03 PM	Far-end loss detected, which could be due to excessive cable length or repeater hops on port 1.
	Problem Cable	15-Sep-97 1:46:03 PM	Problem cable detected on port 1.
	Problem Driver or NIC	15-Sep-97 1:46:02 PM	Problem driver or NIC detected on port 1.

**Figure 4-9. The Alert Log**

Each alert contains the following fields of information:

**Status.** The level of severity of the event generated. Severity levels can be Informational, Warning, and Critical.

**Alert.** The specific event name being sent.

**Date/Time.** The date and time the event was received by the web browser interface. This value is shown in the format: *DD-MM-YY HH:MM:SS AM/PM*, for example, **12-Sep-99 3:57:20 PM**.

**Description.** A short narrative statement that details the nature of the event. For example, **Lost connection to multiple devices on port 1**.

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.

You can sort by other columns if you want. 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. To change the sort criteria, click on the column heading for the type of sorting you want. To change the sort order in the selected column, click on the column heading again.

## Alert Types

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

Alert Message	Alert Description
First Time Install	Important installation information for your hub.
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. Packet loss detected, which could be due to excessive number of repeater hops to traverse.
Over Bandwidth	Excessive network traffic on port.
Broadcast Storm	Excessive broadcasts detected on port.
Auto Partition	The port is repeatedly auto-partitioning itself. (The hub automatically partitions a port if a collision condition exists for an excessive duration or occurs during an excessive number of consecutive attempts to transmit. The hub monitors the partitioned port and automatically re-enables the port when it no longer detects the conditions causing the collisions.)
Network Loop	Network loop detected by hub. Network loop detected on port.
Backup link transition	A the primary link to another device has failed and the hub has transitioned to a port configured as a backup link to that device.
Security Violation	A port security violation has occurred.
Loss of Link	Lost connection to multiple devices on port.

## Working with Detail Views

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

- An Acknowledge Event Button that removes the New symbol from the entry.
- A Delete Event Button which removes the alert from the Alert Log

- A Retest Button that polls the hub again to determine whether or not the error can be regenerated.

A sample Detail View describing a Loss of Link alert is shown here.

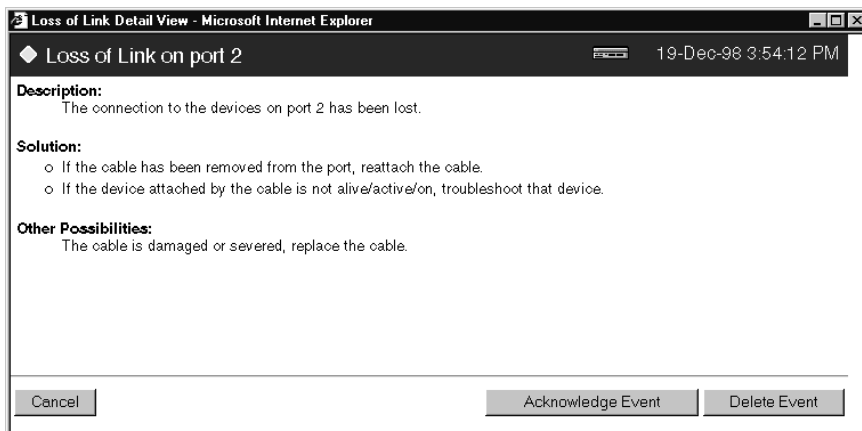


Figure 4-10. Example of a Detail View

## The Alert Control Bar

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



Figure 4-11. The Alert Control Bar

- **Refresh Button.** Displays new alerts that have occurred since you opened this window. Note new faults are automatically retrieved every 15 seconds.
- **Open Event Button.** Displays the selected alert.
- **Acknowledge Selected Events Button.** Removes the **New** symbol from the entry. This feature is useful if you have more than one system administrator working on problems. It shows that someone has looked at it. The Status Bar will no longer consider it a fault needing to be displayed.

If an alert has not been acknowledged, the **New** symbol appears in the Status column to the left of the Status Indicator. Once the alert has been acknowledged, the label is removed.

- **Delete Selected Events Button.** Removes an alert from the Alert Log.

## Understanding The Tab Bar

The web browser interface Tab Bar contains six tabs, four of which launch button bars that 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 topical areas of the web browser interface, click on the appropriate tab in the Tab Bar. The tabs are as follows.

### Identity

This tab displays the Identity Window which is a source of quick information about the device you have selected. The editable information (System Name, Location, and Contact) are maintained in the System Information window (under the Configuration tab).

### Status

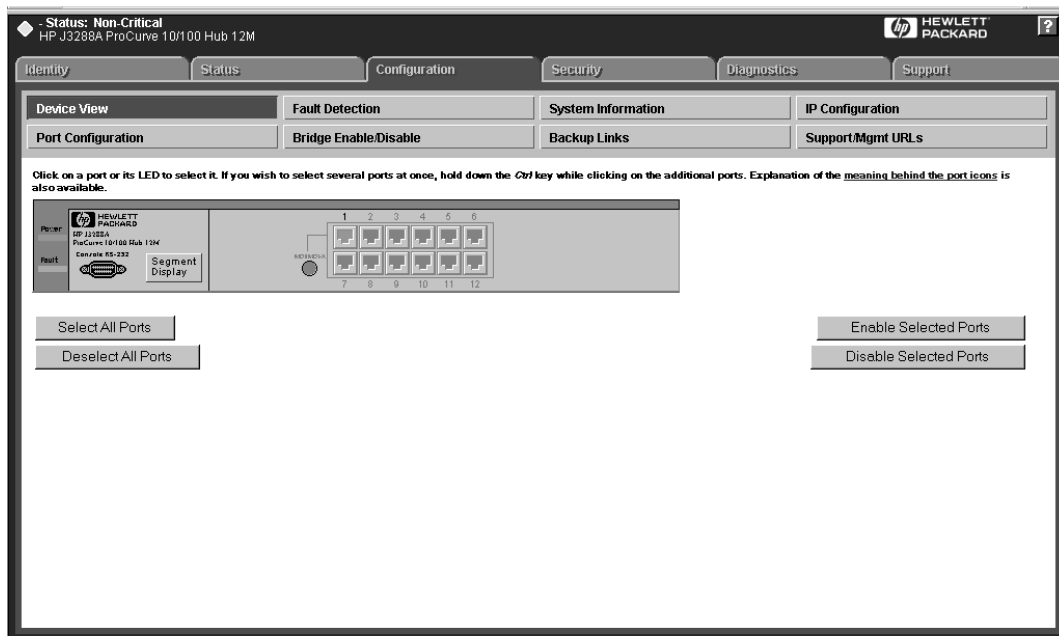


Figure 4-12. The Status Tab Bar

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

- **Overview.** The home position for the web browser interface. Displays a window that contains both the Gauges Area and the Alert Log.
- **Performance Gauges.** An exploded view of the Gauges Area on the home page that enables you to set counters for ports.
- **Global Counters.** Displays hub-level statistics for various activity types.
- **Port Counters.** Displays port-level statistics for various activity types.

## Configuration



**Figure 4-13. The Configuration Tab Bar**

This tab displays the Configuration button bar, which contains buttons that launch windows enabling you to set or change values in various configuration areas on your hub. 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, port speed-reducing, and port disabling.
- **System Information.** Provides for viewing and setting system information for a selected device.
- **IP Configuration.** Provides for changing existing values for an IP address, subnet mask, default gateway address, and time to live parameters.
- **Port Configuration.** Provides for enabling and disabling ports in addition to viewing the security and source address information.

- **Bridge Enable/Disable.** Provides for enabling (the default) or disabling the internal bridge between the 10 Mbps and 100 Mbps segments in the hub.

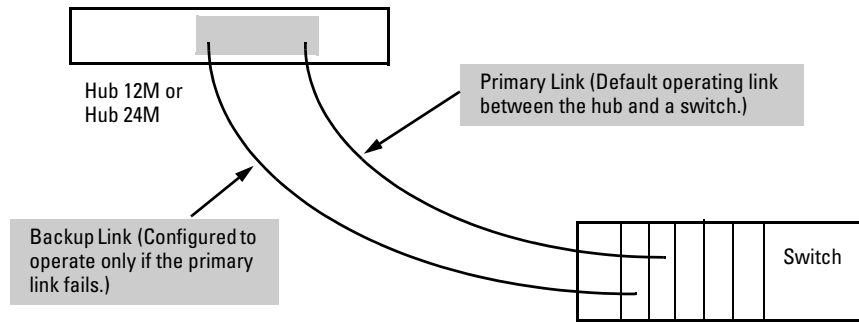
---

**Bridge  
Performance  
Note**

---

In most cases it is recommended that this setting remain enabled for optimum connectivity. Cases where you may want to disable the bridge include a topology where you want to connect the segments via an external switch or where you want to simplify the network for troubleshooting purposes.

- **Backup Links.** Enables you to configure a primary and a redundant communication link between two devices in a cascaded topology, using two separate cables and two ports on the hub and on the connected device.



**Figure 4-14. Example of Backup Link Operation**

---

**Note**

---

When using the Backup Link feature, configure the primary and backup ports *before you connect the cables*. Otherwise, plugging in the cables as shown above creates a network loop that could cause a broadcast storm that will slow down or halt the network.

- **Support/Mgmt URLs:**
  - **Support URL:** Specifies the URL of the web site that will be automatically accessed when you open the Support tab. If you have an internal support structure, you may wish to change this.
  - **Management (MGMT) URL:** Specifies the URL of the source for web browser interface Online Help. See "Online Help for the Web Browser Interface" on page 4-10.



## Security



**Figure 4-15. The Security Tab Bar**

This tab displays the Security button bar that contains buttons that enable you to view and set access restrictions for your hub. The buttons are:

- **Device Passwords.** Provides for setting operator and manager-level passwords for the hub.
- **Port Security.** Provides for setting an authorized station (MAC) address and other security parameters for each port.
- **Intrusion Log.** Lists ports that have learned of unauthorized devices attempting to connect to them.

## Diagnostics



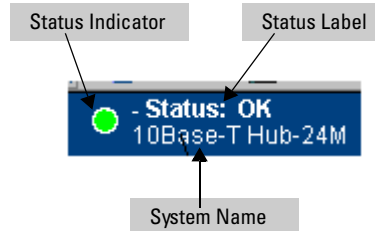
**Figure 4-16. The Diagnostics Tab Bar**

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

- **Ping/Link Test.** Provides for sending 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 Reboot.** Causes the hub to reset its state as though it were powered on and off.
- **Factory Reset.** Restores factory default configuration and reboots the hub. (The web browser interface connection to the hub may be lost, because the IP addressing configuration will be defaulted to Bootp/DHCP.)
- **Configuration Report.** Displays a master list of various settings for the hub, including information about port status, authorized managers, community names, backup links, IP addresses, security configuration, and general system information.

## Understanding the Status Bar

The Status Bar is the area between the Tab Bar and the top portion of your browser's frame.







**Figure 4-17. 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 object can be one of four shapes and one of four colors. The mapping of color to Gauge Severity Regions and Status Indicator shapes is shown in the following table.

**Table 4-3. Status Indicator Key**

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

- **System Name.** Indicates the product name of the hub to which you have connected your current web browser interface session.
- **Status Label and Most Critical Alert Description.** A short narrative description of the earliest, unacknowledged alert with the current highest severity in the Alert Log, appearing in the right portion of the Status Bar. In instances where multiple critical alerts have the same severity level, only the earliest unacknowledged alert is deployed in the Status Bar.

## Setting Fault Detection Policy

One of the powerful features in the web browser interface is the Fault Detection feature. It works to identify performance-degrading error conditions on the network and enables you to deal with cable problems and other problems with marginal connections by performing two types of fault management:

- Control the types of alerts reported to the Alert Log based on their level of severity
- Provide for either disabling or speed-reducing a problem port based on the sensitivity level specified for this option.

---

### Note

---

It is strongly recommended that all ports on the hub be configured to Auto-negotiate (the default configuration mode setting) to take full advantage of the Fault Detection feature and to avoid network problems that can result from misconfiguring a hub port for the device to which it is connected.)

**Operation.** Fault detection internally monitors the hub's port counters and port states, looking for error conditions such as a large number of CRC errors, partitions, and port isolations that indicate cabling or noise problems that can be reduced or eliminated by slowing a connection from 100T to 10T. Initially, warning messages concerning potential problems are sent to the Alert log. If the condition persists and the end node causing the problem can be reduced to 10T operation, the hub will change the operating speed on that port to 10T. If the problem persists after the change to 10T operation, additional warnings will be sent to the Alert log. In a few cases, such as a persistent auto-partitioning of the port, the hub will actually disable the port.

**Recovery.** After a port has been speed-reduced or disabled, you can return it to Auto-negotiated 100T in either of the following ways:

- In the Alert Log (Status | Overview window), double-click on the Alert message indicating the speed reduction or port disable to view the Detail View of the event. In the Detail View, click on the button to re-enable the port or restore the port speed to Auto-negotiation.
- In the hub's Console interface, select

#### 3. Hub Configuration . . .

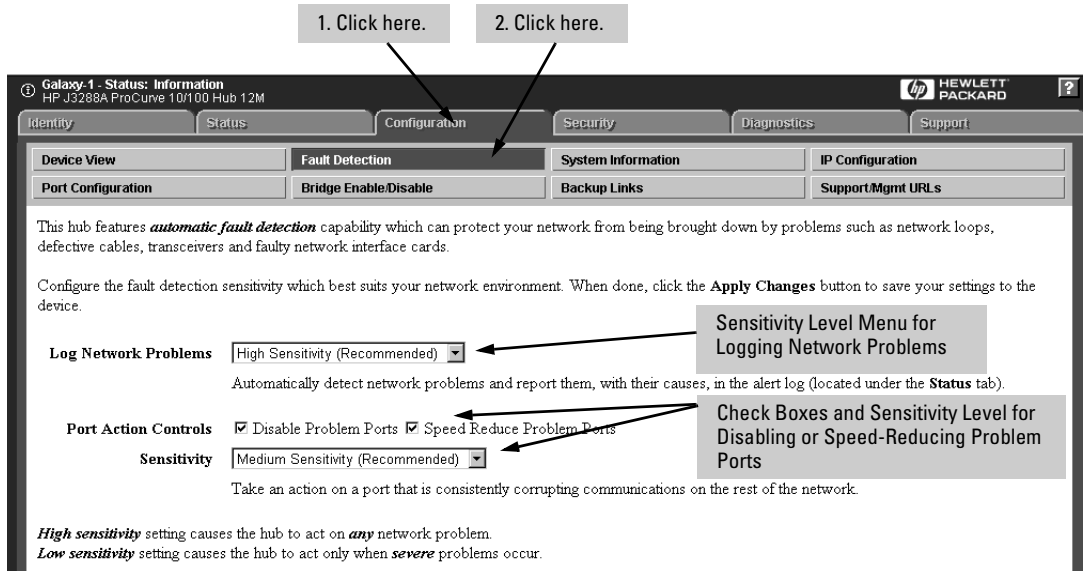
#### 6. Advanced Configuration Menu

#### 1. Port Speed Configuration

Set the speed for the affected port to **A** (for Auto-negotiation).

- Disconnect the link to the affected port, then reconnect it.

**Default Setting.** In the factory default configuration, the Log Network Problems field is set to **Medium Sensitivity**. The Port Action Controls are disabled and the sensitivity level is set to **Never**.



**Figure 4-18. Example for Setting the Fault Detection Window**

The Fault Detection Area contains two list boxes that control fault detection and response policy. The list boxes are:

- **Log Network Problems.** Provides sensitivity threshold levels that determine when a network problem should generate an alert and send it to the Alert Log.
- **Disable or Speed-Reduce Problem Ports.** Provides options and sensitivity threshold levels that determine when a network problem on a port is critical enough to either reduce speed on a port or to disable the port.

The sensitivity levels for both list boxes are:

- Never
- Low Sensitivity
- Medium Sensitivity
- High Sensitivity

Note that the **Disable Problem Ports** and **Speed-Reduce Problem Ports** settings cannot have a higher sensitivity than the one selected in the **Log Network Problems** list box. The mapping between the two settings is shown in the following table:

**Table 4-4. Recommended Settings**

Detection Policy	Log Network Problems Setting	Disable or Speed-Reduce Problem Ports
Most Automated	High Sensitivity	High Sensitivity
High Automation	High Sensitivity	Medium Sensitivity
Medium Automation	Medium Sensitivity	Medium Sensitivity
Medium Automation	Medium Sensitivity	Low Sensitivity
Low Automation	Low Sensitivity	Low Sensitivity
Low Automation	Low Sensitivity	Never
Manual	Never	Never

The recommended sensitivity level for **Log Network Problems** is High Sensitivity. The recommended sensitivity level for **Disable Problem Ports** or **Speed-Reduce Problem Ports** is Medium Sensitivity. The Fault Detection Area settings are described here.

**High Automation.** The most sensitive of the settings, this policy directs the hub to send all alerts to the Alert Log and, optionally, to disable or speed-reduce the offending port in instances of severe network disruption.

<b>Sample Scenario</b>	You have a network with no or very few problems. You can use high automation Fault Detection settings to take action on any detrimental network event.
------------------------	--

**Medium Automation.** The middle sensitivity of the settings, this policy directs the hub to send alerts related to network problems to the Alert Log and to disable ports in instances of extreme network disruption. If you want to be notified of problems which cause a noticeable slowdown on the network, use this setting. Ports affecting the network are disabled or speed-reduced.

<b>Sample Scenario</b>	You have a network with no or very few problems. You can use medium automation Fault Detection settings to take action on only the most severe problems.
------------------------	--

**Low Automation.** The least sensitive of the settings, this policy directs the hub to send only the most severe alerts to the Alert Log and to rarely or never disable or speed-reduce a port generating the alert.

<b>Sample Scenario</b>	You do not want the device taking any actions on its own, but you still want it to let you know about network problems. You can use low automation Fault Detection settings to initiate problem reporting.
------------------------	--

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 web browser interface until you decide to change them.
- **Clear Changes.** 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 settings for both list boxes to Medium Sensitivity for Log Network Problems and Never for Disable Problem Ports or Speed-Reduce Problem Ports.

# Using HP TopTools or Other SNMP Tools to Monitor and Manage the Hub

---

This chapter provides an overview of SNMP management for the hub and provides an overview of the configuration process for supporting SNMP management of the hub. For the configuration procedures for specific features, see "Community Name" (page 6-28) and "Authorized Managers" (page 6-30).

You can manage the hub via SNMP from a network management station. (The hub supports SNMP v1 and SNMP v2c, except as noted below for SNMP v2 Notifications.)

Before using SNMP management, you must first configure the hub with the appropriate IP address. You can do this manually (see chapter 2, "Configuring an IP Address on the Hub) or, if you are using Bootp/DHCP to configure IP addresses on devices in your network, ensure that the Bootp/DHCP process provides the IP address.

Included with the hub is a CD-ROM containing a copy of HP TopTools for Hubs & Switches, an easy-to-install-and-use network management application that runs on your Windows NT- or Windows 95-based PC. HP TopTools provides control of your hub through its graphical interface. Also, it makes use of the RMON agent and Extended RMON that is included in the hub to provide powerful, but easy-to-use traffic monitoring and network activity analysis tools.

SNMP management features on the hub include:

- Security via configuration of SNMP communities
- Event reporting via SNMP traps and RMON (SNMP v2 Notifications are not supported at this time.)
- Managing the hub with a network management tool such as HP TopTools for Hubs & Switches.
- Monitoring data normally associated with the SNMP agent ("Get" operations). Supported *Standard* MIBs include:
  - MAU MIB (RFC 2239)
  - Interface MIB (RFC 2233)
  - RMON MIB (RFC 1757)— groups 1, 2, 3, and 9

- SNMP MIB-II (RFC 1213)
- RPTR MIB (RFC 2108)
- Entity MIB (RFC 2037)
- SNMPv2 MIB (RFC 1907)

*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 10Base-T Hubs configuration (config.mib)
- HP EASE MIB version 4 to allow extended RMON sampling
- HP Linktest MIB for basic device management (linktest.mib)
- HP ICF Linktest MIB for link test features (icfbasic.mib)

The hub SNMP agent also uses certain variables that are included in a Hewlett-Packard proprietary MIB file you can add to the SNMP database in your network management tool. You can copy the MIB file from the compact disk (CD) shipped with the hub, or from the following World Wide Web site:

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

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

### Use of Authorized Managers

In many networks, manager addresses are not used. In this case, all management stations using the correct community name may access this device with the View and Access levels that have been set for that community. If you want to restrict access to one or more specific nodes, you can enter up to 10 IP addresses of such nodes. *Configuring one or more IP addresses means that only the network management stations at those addresses are authorized to use the community name to access the hub.*

---

#### **Caution**

---

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



## SNMP Configuration Process

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

1. If you have not already configured IP addressing, including any necessary gateways, do so now. From the console Main menu select:

- 2. Management Access Configuration . . .**

- 1. IP Configuration**

- (For more information, see chapter 2, "Configuring an IP Address on the Hub".)

2. Configure the appropriate SNMP communities. From the console Main menu select:

- 2. Management Access Configuration . . .**

- 2. Community Name**

- (For more information, see "Community Name" on page 6-28. (The "public" community exists by default and is used by HP's network management applications.)

3. Configure authorized managers, if used in your network. From the console Main menu select:

- 2. Management Access Configuration . . .**

- 3. Authorized Managers**

- (For more information, see "Authorized Managers" on page 6-30.)



# Configuration Reference

---

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

- Chapter 3, "Using the Hub Console Interface"
- Chapter 4, "Using the HP Web Browser Interface"

**Why Reconfigure?** In its factory default configuration, the hub is configured to operate as an unmanaged repeater. However, to enable management features and to "fine tune" the hub for the specific performance and security needs in your network, you will most likely want to reconfigure at least some individual hub parameters. (To be a managed device in your network, the hub must be configured with a valid IP address. See chapter 2, "Configuring an IP Address on the Hub".)

Each configuration topic is described as follows:

- Overview
- Example Hub Console screen and parameter descriptions
- Example web browser interface window

## Online Help

For more information on status and configuration topics in the web browser interface, see the online help provided for the web browser interface. (See also "Management and Support URLs" on page 6-75.)

**How To Find a Configuration Topic.** See Table 6-1, "Configurable Feature Comparison" on page 6-2.

Configuration topics are covered in this chapter in the order they appear in the *console*. That is, if you view console screens starting with the top screen in the Main Menu and work your way down through the environment, you will follow the presentation sequence in this chapter. A web browser interface window appears in the same section with each console screen that provides similar functionality.

Refer to the following table for a master list of the order of all console screens and web browser interface Windows to determine where they will be presented in the reference. Note that menu names are bolded.

**Table 6-1. Console Screen/Web Browser Interface Map**

<b>Feature</b>	<b>Hub Console</b>	<b>Web Browser Interface</b>	<b>Page</b>
Main Menu	Yes	—	6-3
General System Information	Yes	Yes	6-6
Port Status	Yes	Yes	6-8
Port, Bridge, and Global Counters	Yes	Yes	6-11
Security Intruder Log	Yes	Yes	6-17
Clear Security Security Flashing LEDs	Yes	Yes	6-20
IP Configuration	Yes	Yes	6-23
Community Name	Yes	—	6-28
Authorized Managers	Yes	—	6-30
User Name and Password	Yes	Yes	6-32
Telnet Enable/Disable	Yes	—	6-35
Web Browser Enable/Disable	Yes	—	6-36
Serial Timeout	Yes	—	6-37
Hub System Information	Yes	Yes	6-40
Bridge Enable/Disable	Yes	Yes	6-45
Port Enable/Disable	Yes	Yes	6-42
Device View	—	Yes	6-43
Port Security	Yes	Yes	6-47
Port Security Configuration	—	Yes	6-48
Backup Links	Yes	Yes	6-52
Port Speed	Yes	Yes	6-56
Reset Hub to Factory Default	Yes	Yes	6-58
Ping Test	Yes	Yes	6-61
Link Test	Yes	Yes	6-63
Browse Hub Configuration	Yes	Yes	6-65
Reboot the Hub	Yes	Yes	6-68
Download OS	Yes	—	6-70
Management Support URLs	—	Yes	6-75
Support	—	Yes	6-77

## Console Main Menu

To access the Main Menu, begin a console interface session and enter **MENU** at the command line prompt. (For more on using the console, see chapter 3, "Using the Hub Console Interface".)

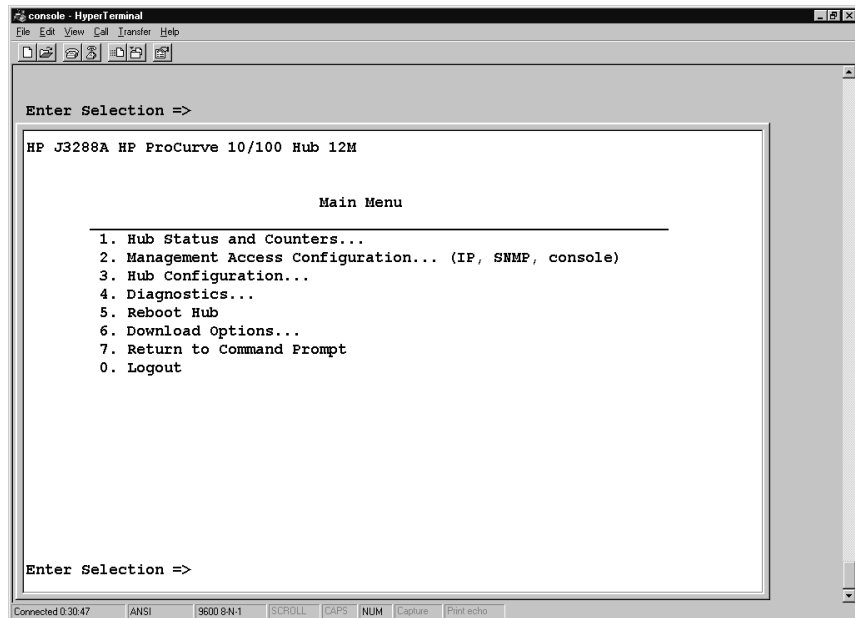


Figure 6-1. The Main Menu Screen

- **Hub Status and Counters.** Provides options that detail hub identification and state information including system attributes, port states, port-level statistics for various activity types, hub-level statistics for various activity types, a record of unauthorized end-node and device entry (intruders) to the hub and a clear function to stop LED flashing associated with intruders.
- **Management Access Configuration.** Provides options that enable you to configure an IP Address, assign community names, assign exclusive management stations, allow access to the device via Telnet sessions, and assign passwords to the console.
- **Hub Configuration.** Provides options that enable you to configure hub system attributes to turn on or off a port, enable or disable the 10/100 bridge, to create backup paths, change port speed configuration, and to reset the hub to the factory default configuration.

- **Diagnostics.** Provides options that enable you to initiate network layer (Ping) and data link layer (Link) tests between the hub and other devices on the network, and to browse the hub configuration.
- **Reboot Hub.** Performs a reset on the hub to clear port and segment counters and begin a new console session (page 6-68).
- **Download Options.** Provides XMODEM and TFTP OS (operating system, or firmware) download options (page 6-70).

## Hub Console Status and Counters Menu

The Hub Status and Counters Menu displays a list of menus and options that describe hub identification and state information.

### Hub Console

From the Main Menu, select

#### 1. Hub Status and Counters

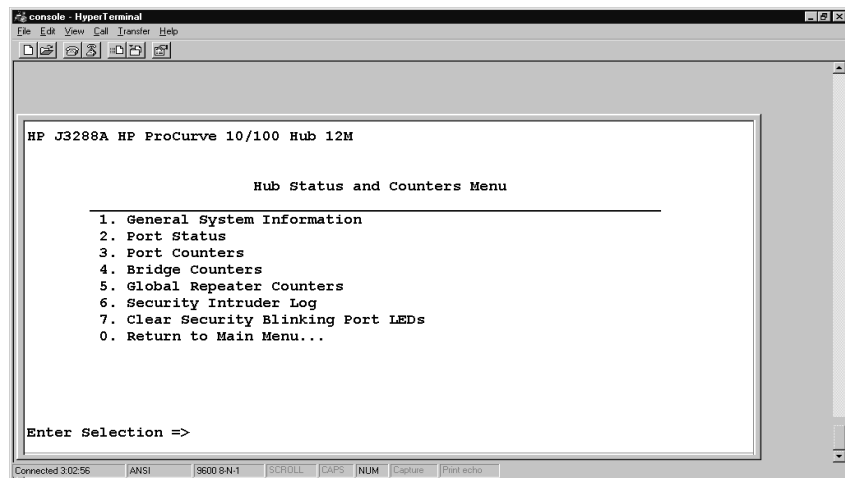


Figure 6-2. The Hub Status and Counters Menu Screen

- **General System Information.** Displays identification and attributes.
- **Port Status.** Displays port state information.
- **Port Counters.** Displays port-level statistics for various activity types.
- **Bridge Counters.** These counters display a summary of traffic in the hub's two segments (100T and 10T). These statistics are calculated only on a per-segment basis for traffic within the respective segments. **Rx** means "Received"; **Tx** means "Transmitted".
- **Global Repeater Counters.** Displays various hub-level statistics.
- **Security Intruder Log.** Displays a record of unauthorized end nodes and devices (intruders) gaining entry to ports on the hub.
- **Clear Security Blinking Port LEDs.** Clears blinking port LEDs associated with intruders.

## General System Information

The General System Information screen displays hub system identification information retrieved from the System Group in MIB II for the user-configurable System Name, System Contact, and System Location fields.

### Hub Console

From the Console Main Menu, select

#### 1. Hub and Status Counters . . .

##### 1. General System Information

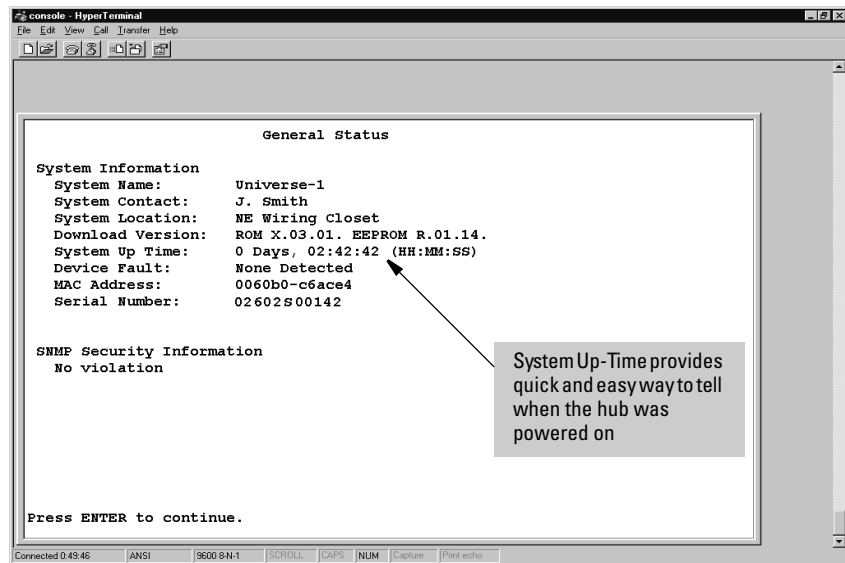


Figure 6-3. The General Status Screen

- **System Name.** Enables you to associate a common name to identify the device. For example, **My Hub**. The console allows only 80 characters to be set; the web browser interface allows 255.
- **System Contact.** The name of the person responsible for the device.
- **System Location.** Provides a description of where the device will be located. This can be up to 80 characters, including spaces. For example, **Wiring Closet -- East**.
- **Download Version.** Provides the versions of ROM, firmware, and hardware of the device.



- **System Up Time.** Provides the amount of time elapsed since the device was powered on.
- **Device Fault.** Indicates errors discovered during the device self test.
- **MAC Address.** Provides the MAC address of the device. For example, **080009-495925**.
- **Serial Number.** Provides the serial number of the device. For example, **SG63401386**.
- **SNMP Module Security Information.** Indicates whether the hub has experienced a violation, generally a packet from a management station that is not authorized to manage the hub.
- **Management Server.** Specifies the source of online Help for the web browser interface (page 6-75).

## General System Information in the Web Browser Interface

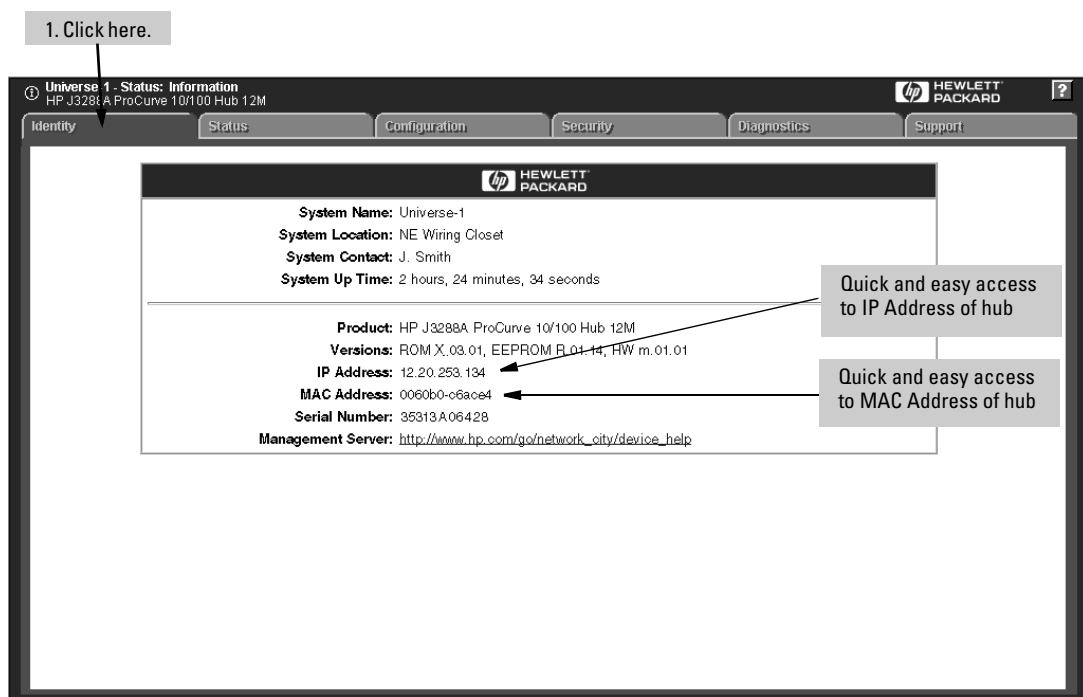


Figure 6-4. The Identity Window

## Port Status

The Port Status screen displays a port list that provides information about the state of all ports on the hub.

### Hub Console

From the console Main Menu, select

1. Hub Status and Counters . . .
2. Port Status

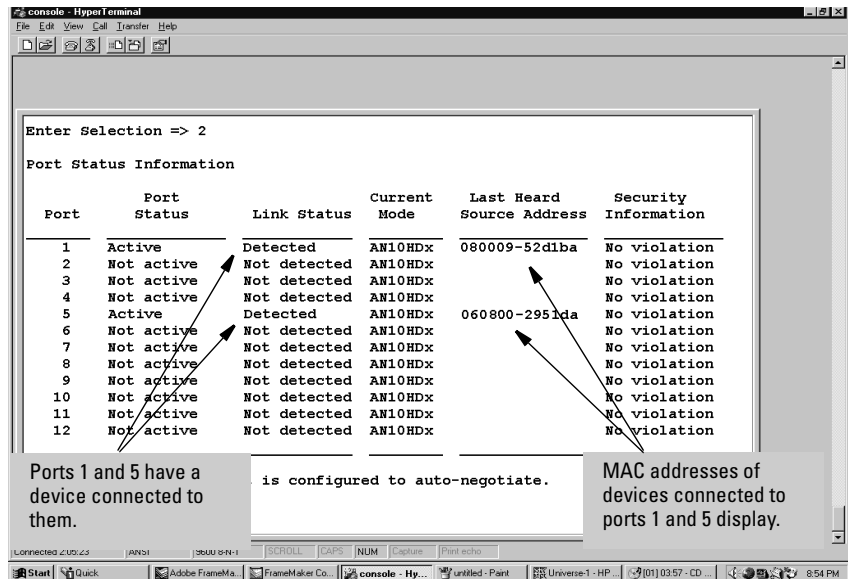


Figure 6-5. Example of the Port Status Screen

In the above example, ports 1 and 5 are active and link status has been detected, indicating a valid connection has been made for both. MAC addresses for devices connected to both ports are listed in the Last Heard Source Address column and no security violation has been recorded for either port.

- **Port number.** Indicates the port label on the hub.
- **Port status.** Indicates whether the port is active or inactive. Settings can be:
  - **Active.** Indicates the port is enabled and ready to receive and transmit packets.

- **Not Active.** Indicates the port is not available to receive and transmit packets.
- **Link status.** Indicates whether link signalling has been detected on the hub. Settings can be:
  - **Detected .** Indicates the port has sensed a connected device.
  - **Not Detected .** Indicates the port has not sensed a connected device.
- **Current Mode.** Indicates current port speed setting. Options include:
  - **AN10HDX:** The port is configured to auto-negotiate the port speed (the default setting) and is currently operating at 10 Mbps, half-duplex.
  - **AN100HDX:** The port is configured to auto-negotiate the port speed (the default setting) and is currently operating at 100 Mbps, half-duplex.
  - **10HDX (forced 10T):** The port has been configured to operate at 10 Mbps, half-duplex.
  - **100HDX (forced 100T):** The port has been configured to operate at 100 Mbps, half-duplex.

---

**Caution**

---

Setting a port to a speed for which the device at the other end of the link is not already configured may cause loss of link and other network problems. For this reason it is recommended that you keep each hub port configured to **Auto-neg (Auto-negotiation)** unless the device connected to the port requires forced 10T or forced 100T to operate.

- **Last Heard Source Address.** Shows the MAC address of the device that sent the last packet to the port. Addresses are shown only for active ports.
- **Security Information (Listed as a "violation" on the web browser interface).** Indicates whether the port's security rules have been violated. Settings can be:
  - **No violation .** Indicates no unauthorized address has attempted to connect to the port.
  - **Violation .** Indicates a port intrusion has occurred on the port.

## Port and Segment Status Information in the Web Browser Interface

The screenshot displays the HP ProCurve 107100 Hub 12M web browser interface. The top navigation bar includes tabs for Identity, Status, Configuration, Security, Diagnostics, and Support. The main content area is divided into four sections: Overview, Performance Gauges, Global Counters, and Port Counters. Each section contains a gauge for Utilization % and Collisions %.

Below the gauges is a table with the following columns: Status, Alert, Date / Time, and Description.

Status	Alert	Date / Time	Description
New	First Time Install	06-Dec-98 4:55:52 PM	Important installation information for your hub.

At the bottom of the interface are buttons for Refresh, Open Event, Acknowledge Selected Events, and Delete Selected Events.

Four callout boxes provide the following information:

- Overview:** This button displays status for the 100T and 10T segments.
- Performance Gauges:** This button displays status for either individual ports, all 10T ports, or all 100T ports.
- Global Counters:** This button displays global counters for the 100T and 10T segments.
- Port Counters:** This button displays counters for either individual ports or for the traffic that crosses the bridge between the 100T and 10T segments.

Configuration Reference

## Counters

The hub offers counters for:

- Individual ports
- The internal 100T/10T bridge
- The 100T and 10T segments (global)

The port, bridge, and global counter outputs in the Console are updated each time you display the particular counter screen. These counter outputs are updated every 30 seconds in the web browser interface .

### Hub Console Port Counters

Port counters give you a snapshot of the hub's effectiveness. Especially note the Collisions and CRC Errors. If certain ports show high numbers for these events, you may want to investigate their end nodes. Both of these counters are dependent upon time for collisions. Collisions are normal occurrences. However, you should watch for *spikes*, indicating sudden changes.

From the console Main Menu, select

#### 1. Hub Status and Counters . . .

#### 2. Port Counters

```

Enter Selection => 3

Port Counter Information

Port      Valid Packets  Collisions  CRC Errors  Late Col-  Very Long  Broadcast
          Packets      sions      Errors     lisions   Events     Packets
-----
 1      284622         28          0           0           0          30593
 2           0          0           0           0           0           0
 3           0          0           0           0           0           0
 4           0          0           0           0           0           0
 5           0          0           0           0           0           0
 6           0          0           0           0           0           0
 7           0          0           0           0           0           0
 8           0          0           0           0           0           0
 9           0          0           0           0           0           0
10          0          0           0           0           0           0
11          0          0           0           0           0           0
12          0          0           0           0           0           0

Press ENTER to continue.
  
```

Figure 6-6. Example of the Port Counters Screen

The Hub Port Counters screen displays activity recorded on each hub port for six management variables. The values shown for the variables for each port are cumulative since the hub was last powered on or reset. The Hub Port Counters screen enables you to determine the traffic patterns for each port. The default variables are:

- **Valid Packets.** Provides the total number of good packets (packets with no errors) received by the port.
- **Collisions.** Provides the total number of collisions on the port. A collision is generated when two or more devices attempt to transmit a message on the same network segment at the same time; they corrupt each other's transmissions. The number of collisions should be proportional to the number of packets transmitted over time and the number of nodes on the network. Collisions are a normal occurrence on a CSMA/CD network collision domain.
- **CRC Errors.** Provides the total number of errors associated with a Cyclic Redundancy Check code which is typically placed at the end of the frame or packet to ensure the integrity of the data within the frame.
- **Late Collisions.** Gives the total number of late collisions on the port. A late collision is a packet reporting a collision after the first 64 bytes of the packet have been successfully transmitted. A late collision is generally indicative of one of the transmitting nodes not detecting an existing transmission at the onset of transmission. This condition can be caused by the packet having to pass through too many repeaters on the network or too much distance over a cable. In both cases, the transmitting node initially will detect a clear wire, but because too much time goes by because of the delays of distance or repeater changes, another packet has had the opportunity to enter the wire, creating a collision.
- **Very Long Events.** Long, unbroken transmissions from an end node.
- **Broadcast Packets.** Provides the total number of broadcasts received by this port. A broadcast is a message sent to all users on the network.

## Hub Console Bridge Counters

From the console Main Menu, select

1. **Hub Status and Counters . . .**

2. **Bridge Counters**

console - HyperTerminal

File Edit View Call Transfer Help

Bridge Counters

Counter	100 Segment	10 Segment
Packets Rx	0	22243
Packets Tx	1221	1179
Broadcast Rx	0	2861
Broadcast Tx	2864	2
Multicast Rx	0	1193
Multicast Tx	1193	0
Errors	0	0

Press ENTER to continue.

Connected 35446 ANSI 9600 8-N-1 SCROLL CAPS NUM [Capture] [Print echo]

**Figure 6-7. Example of the Bridge Counter Screen**

These counters display a summary of traffic in the hub's two segments (100T and 10T). These statistics are calculated only on a per-segment basis for traffic within the respective segments.

"**Rx**" means "Received";

"**Tx**" means "Transmitted".

**Segments** means the 10T or 100T segment for which the corresponding data is displayed.

- **Packets Rx.** The total number of packets received on the indicated segment.
- **Packets Tx.** The total number of packets transmitted on the indicated segment.
- **Broadcast Rx.** The total number of broadcast packets received on the indicated segment.
- **Broadcast Tx.** The total number of broadcast packets transmitted on the indicated segment.
- **Multicast Rx.** The total number of multicast packets received on the indicated segment.

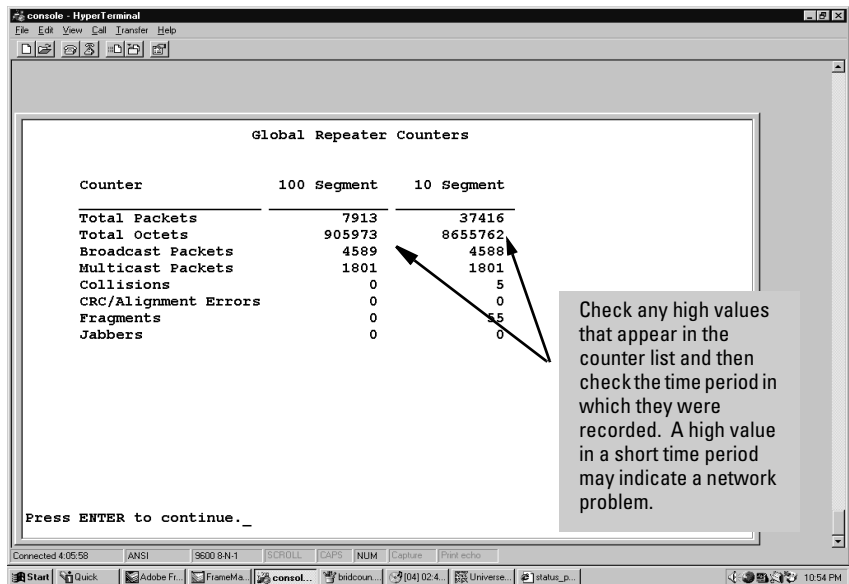
- **Multicast Tx.** The total number of multicast packets transmitted on the indicated segment.
- **Errors Rx.** The total number of errors received from the ports on the indicated segment.

## Hub Console Global Counters

From the console Main Menu, select

### 1. Hub Status and Counters . . .

### 2. Global Repeater Counters



**Figure 6-8. Example of the Global Repeater Counters Screen**

The Global Repeater Counters screen displays aggregate activity recorded for the hub's 100T and 10T segments (and not for specific ports). The values shown are cumulative since the hub was powered on or reset. The Global Repeater Counters screen enables you to determine the traffic patterns for the hub. The default variables are:

- **Total Packets.** Displays the total number of all packets, both valid and error packets, seen on the hub.
- **Total Octets.** Displays the total number of octets (both valid and invalid) seen on the hub.



- **Broadcast Packets.** Displays the total number of broadcasts seen by the hub. A broadcast is a message sent to all users on the network.
- **Multicast Packets.** Displays the total number of multicasts seen by the hub. A multicast is a form of broadcast where the packet is delivered to a subset of the group within a network as opposed to a true broadcast which forwards the packet to all users on the network.
- **Collisions.** Displays the total number of collisions on a network segment. A collision is generated when two or more devices attempt to transmit a message on a cable at the same time; they corrupt each other's transmission. The number of collisions should be proportional to the number of packets transmitted over time and the number of nodes on the network. Collisions are a normal occurrence on a CSMA/CD network collision domain.
- **CRC/Alignment Errors.** Displays the number of instances where the Cyclic Redundancy Check (CRC) method detected a corrupted packet. The CRC is a code typically placed at the end of the frame or packet to ensure the integrity of the data within the frame.
- **Fragments.** Displays the number of illegally short packets, usually caused by collisions.
- **Jabbers.** Displays the number of instances where a packet had both of the following problems associated with it:
  - The packet was too big in its byte count (more than 1518 bytes).
  - The packet had a corrupted bit in it for any of a variety of reasons. This corrupt bit was detected during the packet checksum process executed on the hub when it received the packet. Commonly known as a *Cyclic Redundancy Check* or *Frame Check Sequence* error.

## Global, Port, and Bridge Counters in the Web Browser Interface

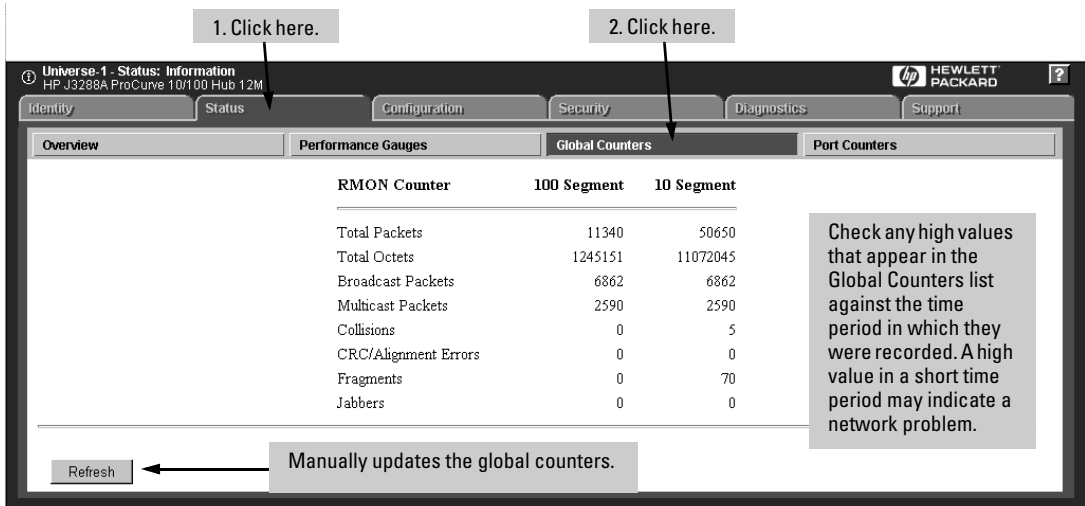


Figure 6-9. Example of Global Counters Window

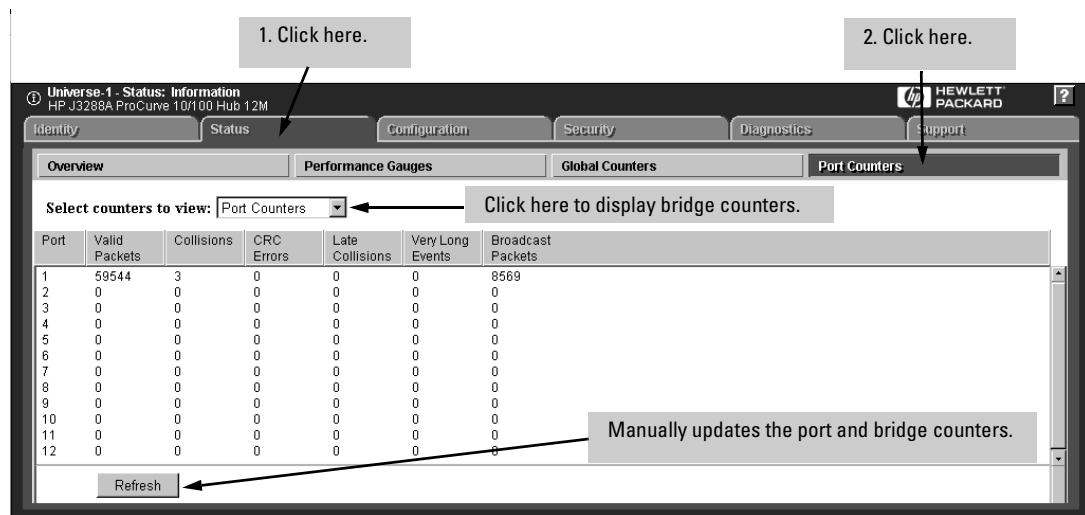


Figure 6-10. Example of Port Counters Window with Bridge Counters Option

For more on these windows, including a description of the bridge counters, see the online Help provided with the web browser interface.

## Security Intruder Log

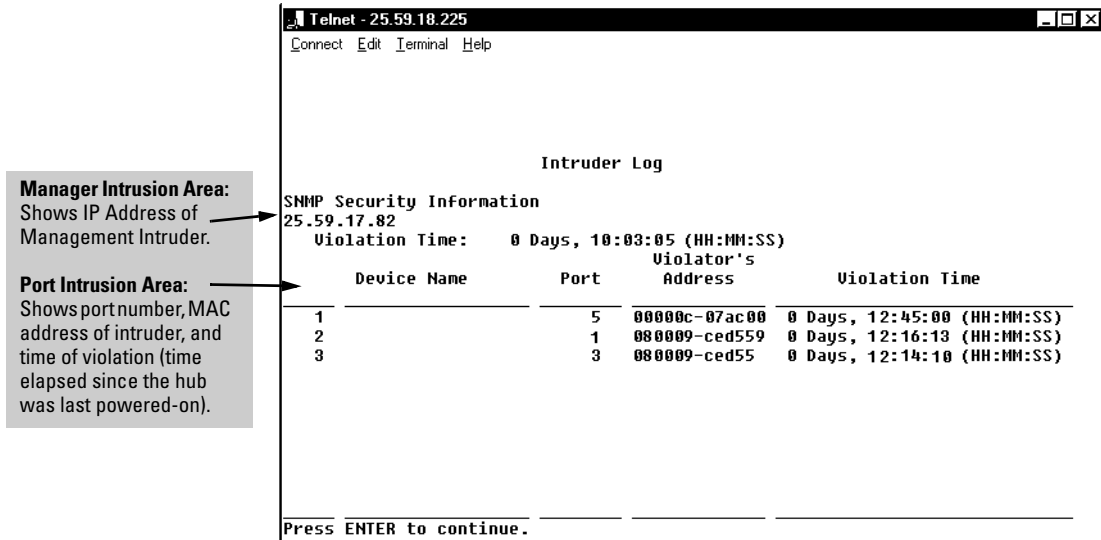
This section describes security intrusions.

- To configure port security, see "Port Security" on page 6-47.
- To turn off blinking port LEDs indicating a security violation, see "Clear Security Blinking Port LEDs" on page 6-20.

### Hub Console

From the console Main Menu, select

1. Hub Status and Counters . . .
2. Security Intruder Log



**Figure 6-11. Example of Intruder Log Screen in the Console**

The Security Intruder Log displays the following access violations:

- Intrusions by unauthorized management stations (lists the IP address of intruding stations)
- Network devices attempting to connect to the ports without proper authorization (lists the MAC addresses of such devices). The hub disables the corresponding ports and you must use the Console or the web browser interface to re-enable them.

**Severity of Intrusions.** When tracking intrusions, give special attention to repeat intrusions by the same MAC address. If you feel the intrusions are not significant, you may want to change the Address Selection settings in the Port Security screen (page 6-47) to be less restrictive.

**Manager Intrusion.** Occurs when an unauthorized manager, generally a management station, attempts to access the hub without being on the authorized manager list (page 6-30) or without using the correct Community Name (page 6-28). Manager intrusion policy is controlled by the entries you make in the Authorized Managers window in HP TopTools or the Authorized Managers screen (page 6-30) in the hub console interface. For any detected management intruders:

- The console Intruder Log screen lists the intruder IP address under the heading **SNMP Security Information**. (See figure 6-17, above.)
- The web browser interface displays **SNMP Agent** in the port column and the intruder IP address in the Intruder Address column.

**Port Intrusion.** Occurs when a MAC address detected from an incoming packet on a port does not match the authorized MAC address for the port. Port intrusion policy is controlled by the entries you make in the Port Security window in HP TopTools or in the web browser interface (page 6-47). For any detected port intruders:

- The console Intruder Log screen lists the port on which the unauthorized device was connected and the MAC address of the unauthorized device. (See figure 6-17, above.)
- The web browser interface lists the number of the port on which the intruder attempted to connect, and displays the intruder MAC address in the Intruder Address column.

**The Intruder Log:** This log displays the single most recent manager (SNMP agent) intrusion, if any, and the 20 most recent port intrusion entries. (Note that you cannot clear Intruder Log entries.)

Intruder Log information includes:

- **Violation Time** (Console only). Indicates how long the hub had been powered-on ("up time") when the intrusion occurred, in the format *DD, HH:MM:SS*.
- **Port (source)**. The port number that is reporting attempted access by an unauthorized device.
- **Intruder Address (Violator's Address in Console)**. The MAC address of the unauthorized device.
- **Time** (Violation Time in Console). The date and time of the intrusion in the format *DD:MM:YY HH:MM:SS*.

To clear flashing port intrusion LEDs, see "Clear Security Blinking Port LEDs" on page 6-20.

### Security Intruder Log in the Web Browser Interface

1. Click here.

2. Click here.

Manager Intrusion

Port Intrusions

Clear Port Intrusion LEDs

Note that an IP Address is reported here and NOT a MAC address. This indicates that the violation was a manager intrusion. (Only the last such intrusion is displayed.)

To clear the blinking security violation LEDs:  
 1. Click on an Intrusion Log entry.  
 2. Click on the Clear Port Intrusion LEDs button.  
 3. Click on the resulting OK button.

Figure 6-12. Example of Intruder Log Screen in the Web Browser Interface

## Clear Security-Flashing Port LEDs

When a port recognizes a packet as being sent from an unauthorized device, its LED flashes rapidly to indicate that the port was disabled because an intruder has been detected on the port. A rapidly flashing port LED indicates that automatic port disabling has occurred, due either to a port security violation or because of a proactive action taken by the hub's management features as the result of a fault-finder event. (For more on LED behavior, refer to the *Installation Guide* you received with the hub.) You can use either the console or the web browser interface to clear a security-blinking port LED and to re-enable the port, if desired.

This section describes how to turn off the flashing port LED indication for a security violation. For information on:

- The Security Intruder Log, turn to page 6-17.
- Configuring port security, turn to page 6-47.

### Hub Console

From the console Main Menu, select

**1. Hub Status and Counters . . .**

**2. Clear Security Blinking Port LEDs**

**Executing this command will clear all security violations on the hub.  
Continue (Y/N)**

Enter **Y** at the prompt

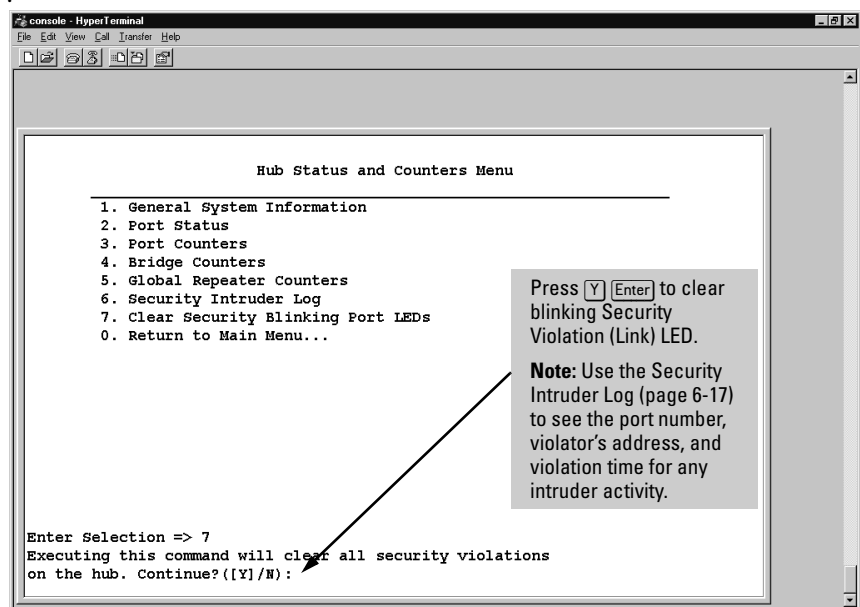


Figure 6-13. The Clear Security Blinking LEDs Option

### Clear Port Intrusion LEDs in the Web Browser Interface

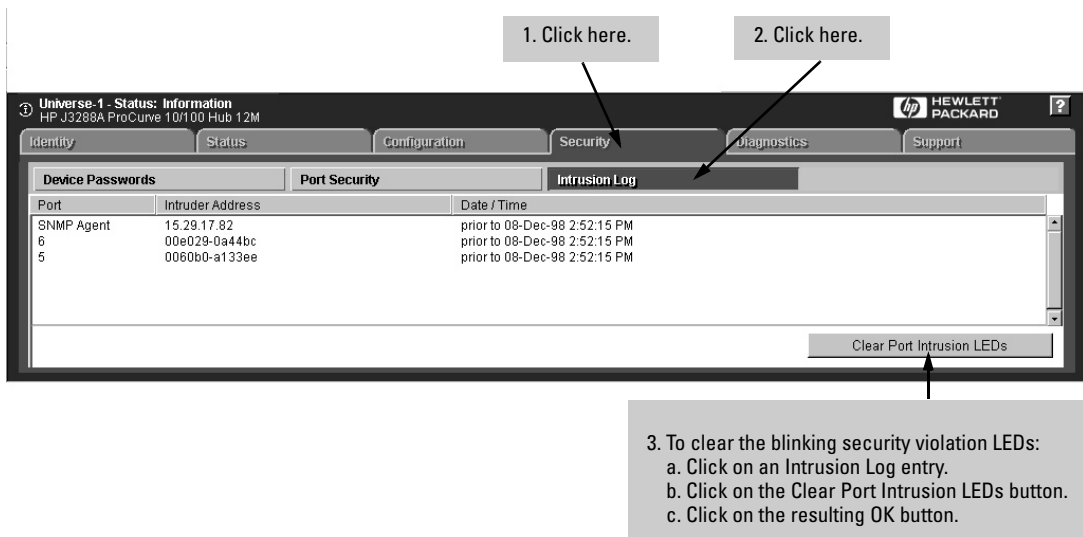


Figure 6-14. Example of Intruder Log Screen in the Web Browser Interface

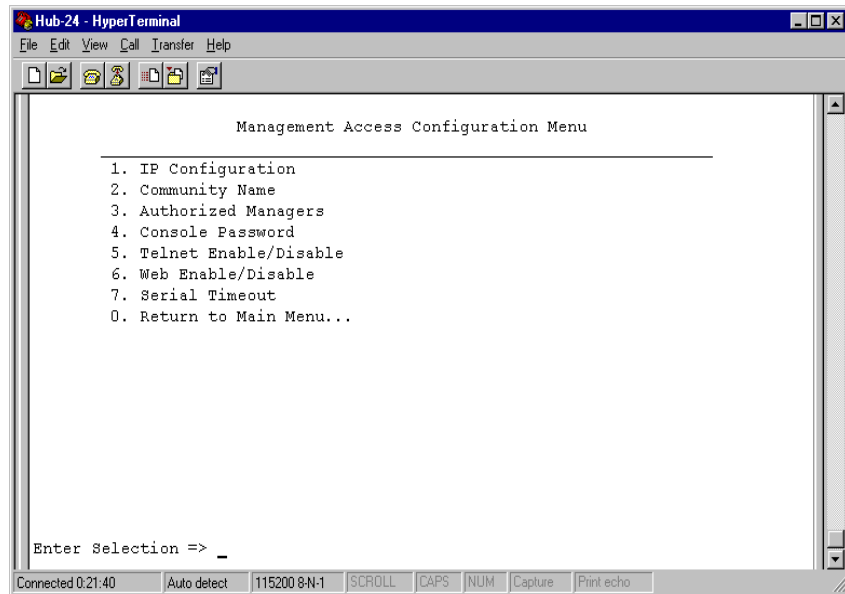
## Management Access Configuration Menu

The Management Access Configuration Menu displays a list of menus and options that enable you to perform management access tasks.

### Hub Console

From the console Main Menu, select

#### 1. Management Access Configuration . . . (IP, SNMP, Console)



**Figure 6-15. The Management Access Configuration Menu**

- **IP Configuration.** Enables you to configure an IP Address, subnet mask, and the gateway address for the hub so that it can be managed in an IP network.
- **Community Name.** Enables you to add, edit, or delete SNMP community names for the hub.
- **Authorized Managers.** Enables you to specify the management stations that can manage this device. You can configure a list of up to 10 network management stations.
- **Telnet Enable/Disable.** Allows configure the hub for Telnet access.
- **Console Password.** Enables you to set or change the password you use to access the Hub Console.



## IP Configuration

The IP Configuration screen enables you to change existing values for an IP Address, a subnet mask, and (optionally) the gateway address for the hub so that it can be managed in an IP network. It also enables you to access the hub via HP TopTools for Hubs & Switches and the web browser interface.

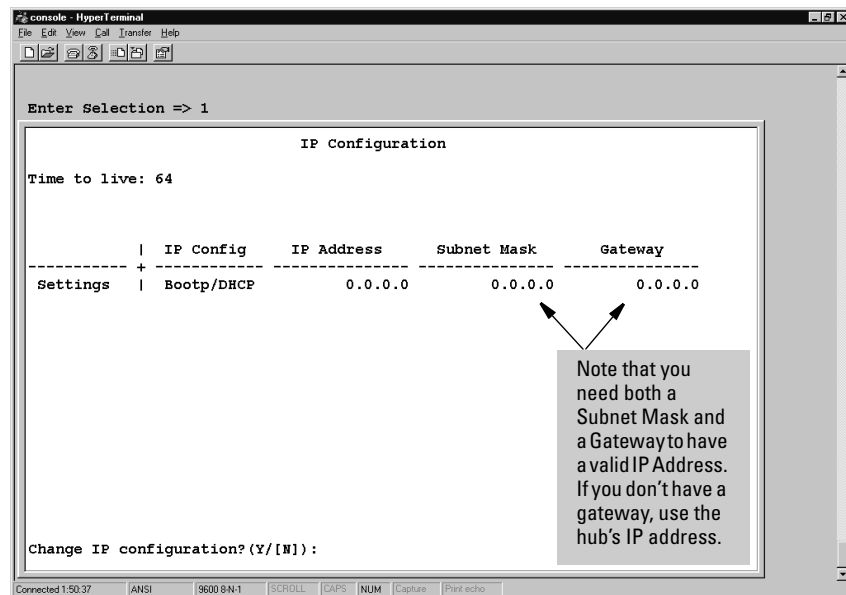
You can configure the IP Address manually or direct the agent on the hub to retrieve an available address, using the BOOTP/DHCP (factory default) option.

### Hub Console

1. From the console Main Menu, select

#### 1. Management Access Configuration . . . (IP, SNMP, Console)

#### 1. IP Configuration



**Figure 6-16. The Default IP Configuration Screen**

2. At the **Change IP Configuration** prompt, enter **Y**. The console interface prompts you to select the method by which you want to assign an IP Address to your hub. The three address assignment options are:

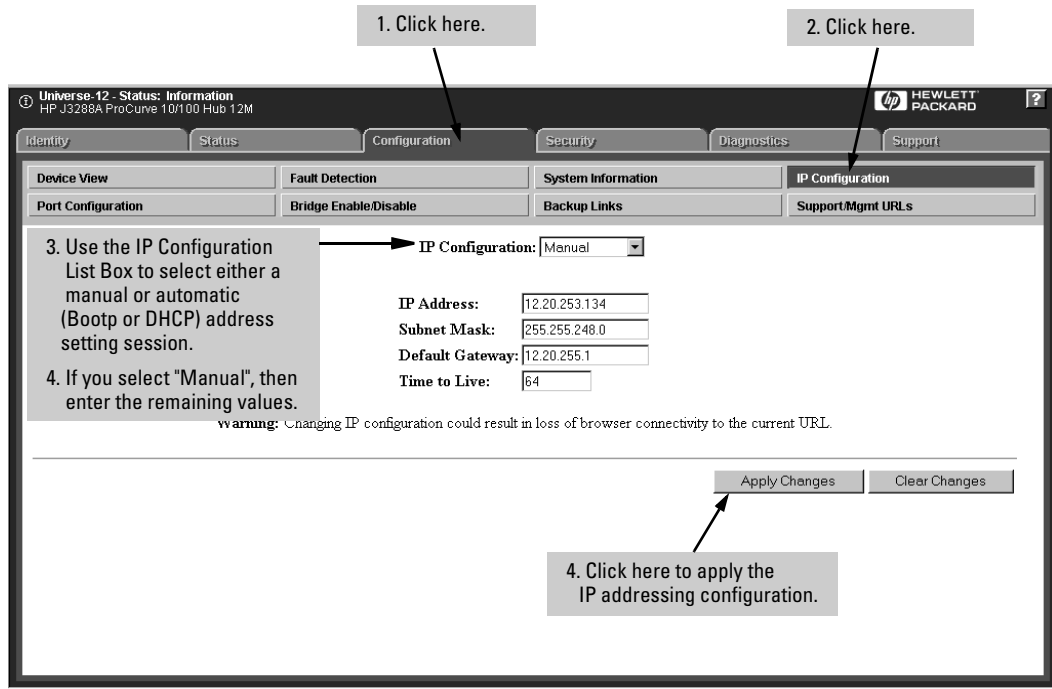
- **(B)ootp/DHCP**

- **(M)anual Config**
  - **(D)isable** (disables IP addressing; not recommended)
3. Enter **M** to manually assign an IP Address to the hub. The console interface prompts you to type an IP Address.
  4. At the **Enter IP Address** prompt, enter an available IP Address. Continue to supply values for the subnet mask, default router, and Time to Live values when prompted.
  5. At the **Change and save to new IP configuration** prompt, enter **Y** to store all values you have set.

The IP Configuration screen contains the following columns that indicate information about IP configuration for your hub.

- **IP Config.** Indicates whether the IP Address is configured manually or automatically. The settings are:
  - **Manual:** Selects the manual hub IP configuration process.
  - **Bootp/DHCP:** Selects the automatic BOOTP or DHCP method of IP configuration.
- **IP Address.** Indicates the IP Address assigned to the hub. The IP Address, or Internet Protocol address, is the network layer address of a device assigned by the administrator of an IP network. A sample IP Address is 16.39.2.140. Each of the fields in the address can be 1 through 32 in binary or 1 through 254 decimal.
- **Subnet Mask.** Indicates the subnet mask assigned to the hub. The subnet mask is a bit mask defining the subnet portion of the IP Address in the same format as the IP Address. (All devices on the same subnet should have the same subnet mask.)
- **Gateway.** Indicates the IP Address of the nearest router in the network. If there are no routers, use the hub's IP address or the address of a network management station.
- **Time to Live.** Indicates the number of IP routers a packet is allowed to cross before the packet is discarded. The default value is 64. Increase this value if the hub is managed from a network management station that is more than 64 routers away. The maximum allowable value is 255.

## Configuring IP Addressing in the Web Browser Interface



**Figure 6-17. The IP Settings Window**

For more on the above parameters, see the preceding page.

### Automatically Acquiring an IP Address Using Bootp/DHCP

BOOTP (Bootstrap Protocol) is used to download network configuration data from a server (the Bootp/DHCP server) to the hub. The configuration data the hub retrieves from the Bootp/DHCP server is:

- The IP address for the hub
- The subnet mask for the subnet on which the hub is installed
- The default router

If you have configured the hub's IP parameters on a Bootp/DHCP server, you do not need to use the IP Configuration screen in the hub console. As shipped from the factory, the hub is configured to use Bootp/DHCP to retrieve the IP configuration information.

**The Bootp/DHCP Process.** When the hub is powered on, it broadcasts Bootp/DHCP requests that contain the hub's MAC address. The Bootp/DHCP server receives the request and searches its Bootp/DHCP table file for an entry that matches the hub's MAC address. If a match is found, the configuration data in the associated file entry is returned to the hub as a Bootp/DHCP reply.

For most UNIX systems, the Bootp table is contained in the **/etc/bootptab** file.

**BOOTP Table File Entries.** An entry in the BOOTP table file **/etc/bootptab** for an HP 10/100 Hub-24M would be similar to the following:

```
hphub12M:\
  ht=ether:\
  ha=080009123456:\
  ip=190.40.101.22:\
  sm=255.255.255.0:\
  gw=190.40.101.1:\
  vm=rfc1048
```

#### Definitions of the table entry fields:

---

<b>hphub12M</b>	is a user-defined symbolic name to help you find the correct section of the bootptab file. If you have multiple hubs that will be using BOOTP to get their IP configuration, you should use a unique symbolic name for each hub.
<b>ht</b>	is the "hardware type" tag. For the HP 10Base-T hubs, set this to <b>ether</b> (for Ethernet). <i>This tag must precede the ha tag.</i>
<b>ha</b>	is the "hardware address" tag. Use the hub's 12-digit MAC address.
<b>ip</b>	is the IP address to be assigned to the hub. Enter the address in the dotted-decimal format as shown in the example on the previous page.
<b>sm</b>	is the subnet mask of the subnet in which the hub is installed.
<b>gw</b>	is the IP address of the default router (or gateway) that allows the hub to communicate with systems that are not on the local network segment. If there is no default router, do not include this tag.
<b>vm</b>	is a required entry that specifies the BOOTP report format. <i>For the HP 10/100 hubs, you must set this parameter to <b>rfc1048</b>.</i>

---

#### Notes for the bootptab file:

- Blank lines and lines beginning with the pound sign (#) are ignored.
- Spaces are not allowed between the characters on a line.
- Names, such as **hphub12M** must begin with a letter and can only contain letters, numbers, periods, or hyphens.

- Include a colon (:) and a backslash (\) as a continuation indication at the end of each line except the last one. Each record is a single line. The colon (:) separates fields in the record. The backslash (\) indicates the current record continues on the next line as if there were no carriage return and linefeed characters.

**Notes on Using DHCP.** The Dynamic Host Configuration Protocol (DHCP) manages the allocation of TCP/IP configuration information by automatically assigning IP addresses. When a device connects to the network, it requests an address from the DHCP server. In dynamic mode, the address is used by the device for a specified period of time. The time period depends on the situation; one device may need the address for an hour, while another device may use the same address for several days.

### 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 addressing that has 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).

## Community Name

The Community Names screen enables you to set community names which are used as strings that enable varying levels of access to devices. Typically, you create community names to perform two tasks:

- to set access levels for different user types
- to enable traps to be sent to named groups of users, known as *communities*.

A Community Name is similar to a password, although passwords tend to have one access level while Community Names have many access levels. The access levels used in HP 10/100 Hubs are described here.

If you are using HP TopTools for Hubs & Switches or an SNMP tool to manage your HP hubs, you can assign a Community Name for both the Read and Write privileges for a user attempting to access a device.

### Hub Console

From the console Main Menu, select

1. Management Access Configuration . . . (IP, SNMP, Console)
2. Community Name

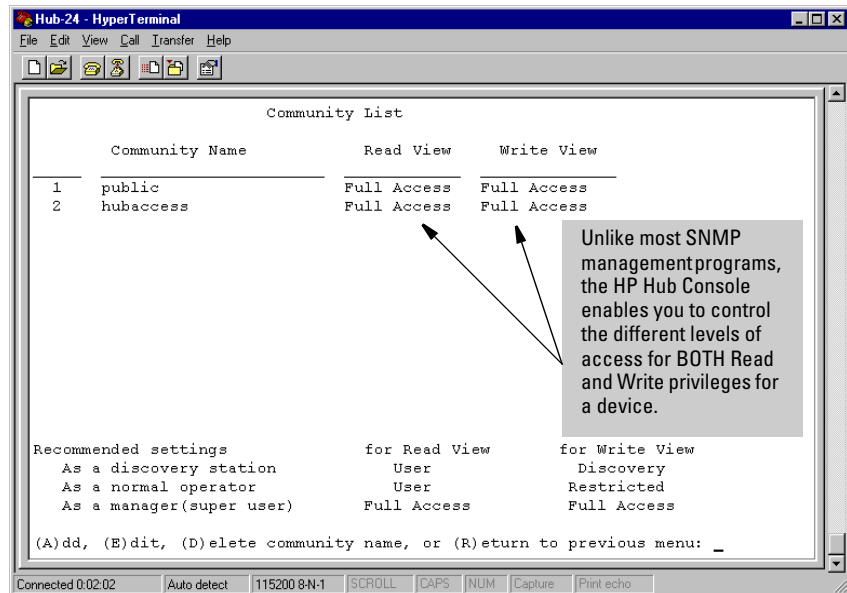


Figure 6-18. The Community List Screen

The different access levels are:

- **Full.** Provides you with complete access to all features in the management environment. Typical use is to provide access levels to network operators by a network administrator.
- **User.** Provides you with near-complete access to features in the management environment, except for Authorized Manager assignment and Community Name configuration. Typical use is for general management of a device by a network operator.
- **Restricted.** Provides you with partial access to features in the management environment. Typical use is for restricted management of a device by a network operator.
- **Discovery.** Enables a device to be discovered by HP TopTools for Hubs & Switches for mapping in a Topology View or a similar SNMP tool. The only tasks that are allowed are Link Test and Discovery (AnnounceAddress function). Typical use for these applications are running on management stations to locate a device for mapping purposes.
- **None.** Provides access to no tasks within the management environment.

Note that the Community Names screen comes with a default Community Name of Public that has Read and Write privileges for all areas of the device.

The following table indicates the recommended combination of Read and Write settings for different levels of access to HP 10/100 Hubs.

**Table 6-2. Community Names Read-Write Settings**

User Level	Read Setting	Write Setting	Description
Discovery	User	Discovery	Enables you to discover and perform a Link Test (MAC address test) for a hub. For use by first-level network operators.
Normal	User	Restricted	Enables you to perform all management tasks for a hub except for Authorized Manager and Community Name setting. For use by second-level network operators.
Manager	Full	Full	Enables you to perform all management tasks for a hub, including all security setting tasks. For use by network administrators.

## Authorized Managers

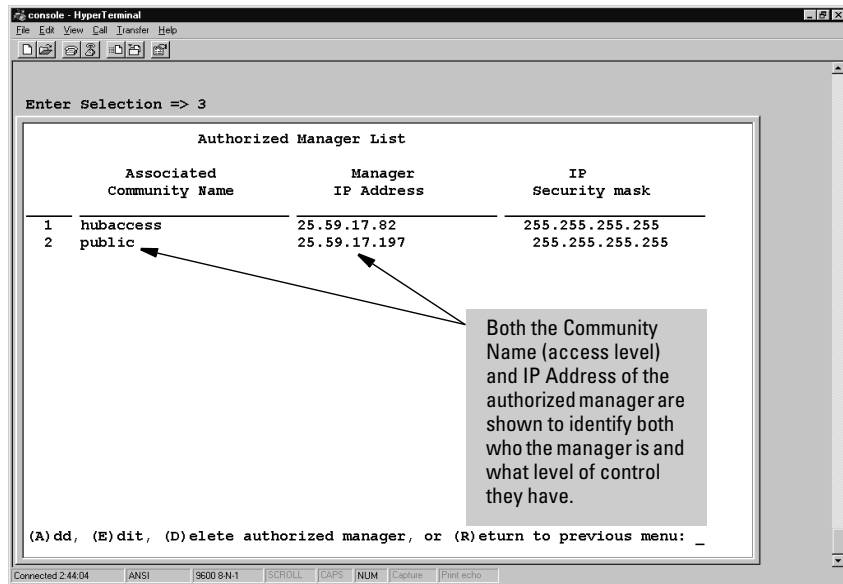
The Authorized Managers screen enables you to specify the management stations that can manage the hub. You can configure a list of up to 10 network management stations.

Authorized managers are configured using existing community names. Also, you must configure Authorized Managers before you can receive trap packets from the hub. Once set on the hub, an Authorized Manager does not have to be set again unless you perform a Factory Reset.

### Hub Console

From the console Main Menu, select

1. Management Access Configuration . . . (IP, SNMP, Console)
3. Authorized Managers



**Figure 6-19. The Authorized Managers Screen**

- **Associated Community Name.** Indicates the Community Name of the hub for which you are creating an authorized manager.
- **Manager IP Address.** Indicates the network address of the management station you want to assign to be the authorized manager for the hub.



- **IP Security Mask.** Indicates the security mask of the hub for which you are creating an authorized manager. The security mask is a value that reveals the extent to which the address of the authorized manager needs to be explicit for manager entry to the hub. For example, a security mask of 255.255.255.252 applied to an address of 15.47.66.40 allows for addresses of
  - 15.47.66.40
  - 15.47.66.41
  - 15.47.66.42
  - 15.47.66.43and disallows all other addresses. HP recommends that you use a security mask value of 255.255.255.255.

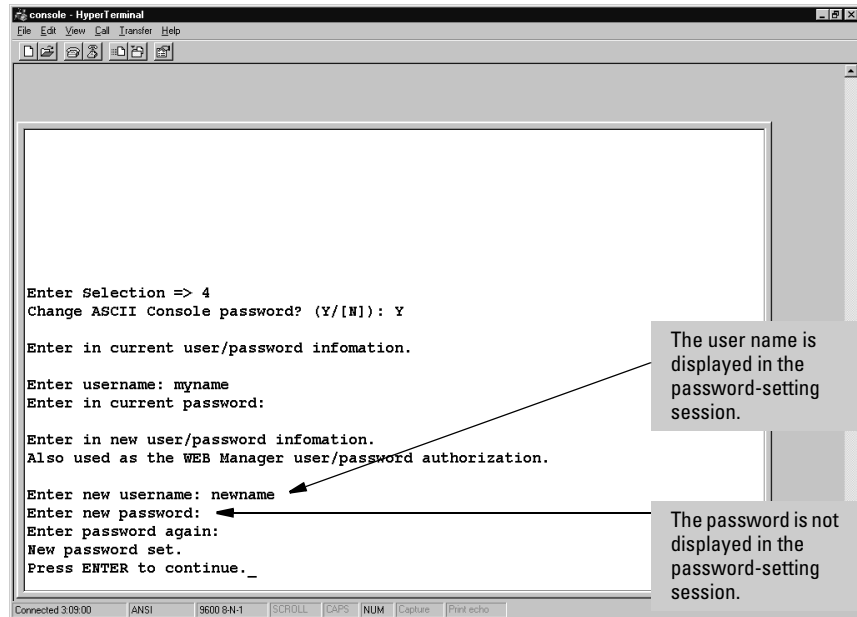
## User Names and Passwords

You may want to create both a user name and password for access security for your hub. The Console Password screen enables you to set or change a Manager user name and password for entry to the console and the web browser interface for device management. Note that passwords and user names you set in the hub Console are set for the web browser interface, and vice-versa.

### Hub Console

From the console Main Menu, select

1. Management Access Configuration . . . (IP, SNMP, Console)
4. Console Password



**Figure 6-20. The Device Password Option**

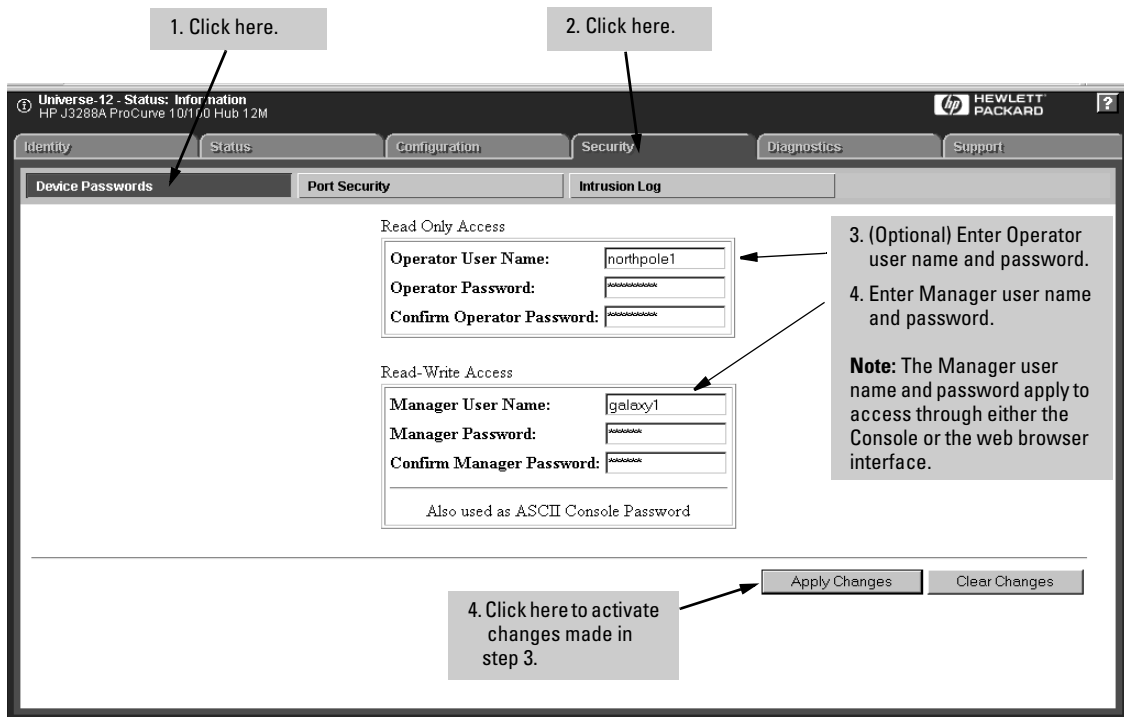
Note that, while the console uses only a Manager user name and password, the web browser interface allows both Operator and Manager user names and passwords:

- **Operator.** This type allows read-only privileges via the web browser interface; that is, to read all environments in the web browser interface except for ones relating to Security. Note that the Operator user name

and password are used only for the web browser interface and *do not* overwrite any earlier, Manager user name and password assigned in the hub Console interface.

- Manager.** This type allows read-write privileges and is assigned in either the Console interface or the web browser interface, and used for access to both interfaces. Values assigned in the Manager fields using either the hub Console or the web browser interface will overwrite previous Manager values assigned in either interface.

### User Name and Password in the Web Browser Interface



**Figure 6-21. The Device Passwords Window**

- Operator User Name.** Enables you to enter a user name value that provides read-only privileges. May have up to 14 (ASCII) characters, including spaces.
- Operator Password.** Enables you to enter a password providing read-only privileges. May have up to 15 (ASCII) characters. Spaces are not allowed.

- **Confirm Operator Password.** Enables you to verify the read-only password that you entered by retyping it. The password characters appear as a series of asterisks (\*) to prevent them from being read from the screen by unauthorized persons.
- **Manager User Name.** Enables you to enter a user name providing read-write privileges. May have up to 14 (ASCII) characters, including spaces.
- **Manager Password.** Enables you to enter a password providing read-write privileges. May have up to 15 (ASCII) characters. Spaces are not allowed.
- **Confirm Manager Password.** Enables you to verify the read-write password that you entered by retyping it. The password characters appear as a series of asterisks (\*) to prevent them from being read from the screen by unauthorized persons.

## Telnet Enable/Disable

The Telnet Enable/Disable screen enables and disables the ability to access the hub Console interface using a Telnet connection. (The factory default setting is *Telnet enabled*.) Note that this feature does not initiate a Telnet session. Instead, it lets you control whether a user on your network can get access to the hub Console by establishing a Telnet session.

From the console Main Menu, select

### 1. Management Access Configuration . . . (IP, SNMP, Console)

### 5. Telnet Enable/Disable

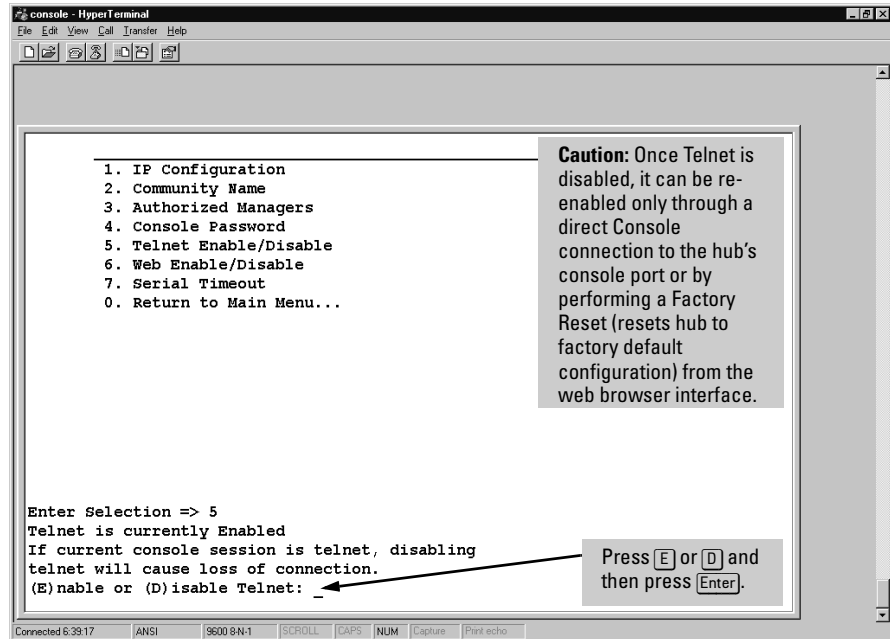


Figure 6-22. The Telnet Enable/Disable Option

## Web Enable/Disable

The Web Enable/Disable screen:

- Tells you whether access to the hub's web browser interface is enabled or disabled
- Enables and disables the hub's web browser interface. (The factory default setting is *web enabled*.)

This feature lets you control whether a user on your network can get access to the hub via a web browser.

From the console Main Menu, select

### 2. Management Access Configuration . . . (IP, SNMP, Console)

#### 6. Web Enable/Disable

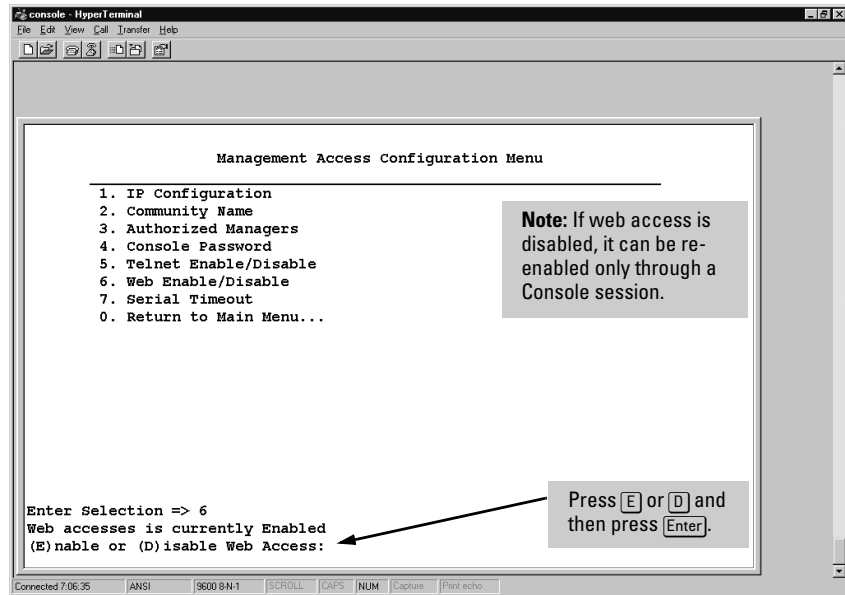


Figure 6-23. The Web Enable/Disable Option

## Serial Timeout

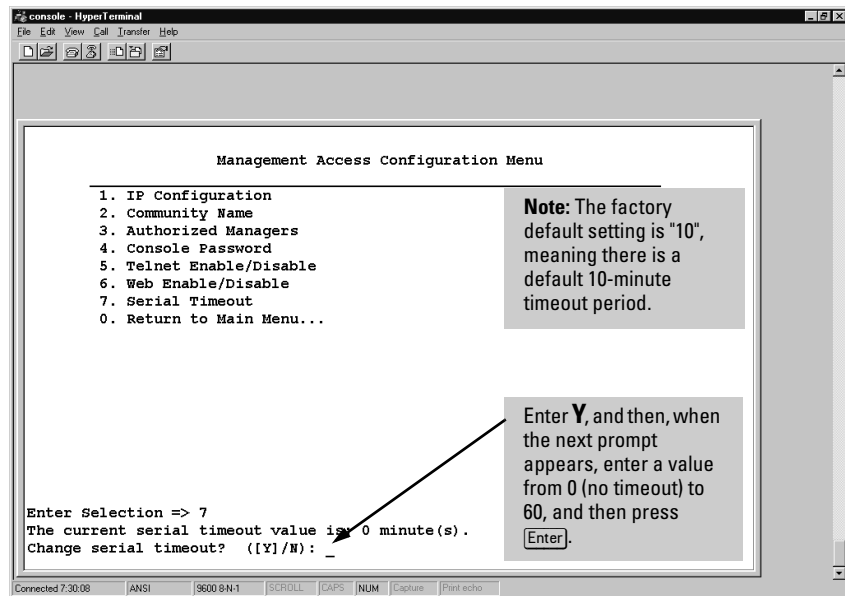
A lack of console activity indicates that the management station may have been left unattended and that hub activity, status, and settings could be viewed or manipulated by an unauthorized user. The Serial Timeout screen:

- Displays the current timeout setting (the number of minutes of Console inactivity before the Console screen times out; **0** = no timeout)
- Enables you to set the amount of minutes allowed to lapse before the hub Console interface shuts down (times out)

From the console Main Menu, select

### 2. Management Access Configuration . . . (IP, SNMP, Console)

#### 7. Serial Timeout



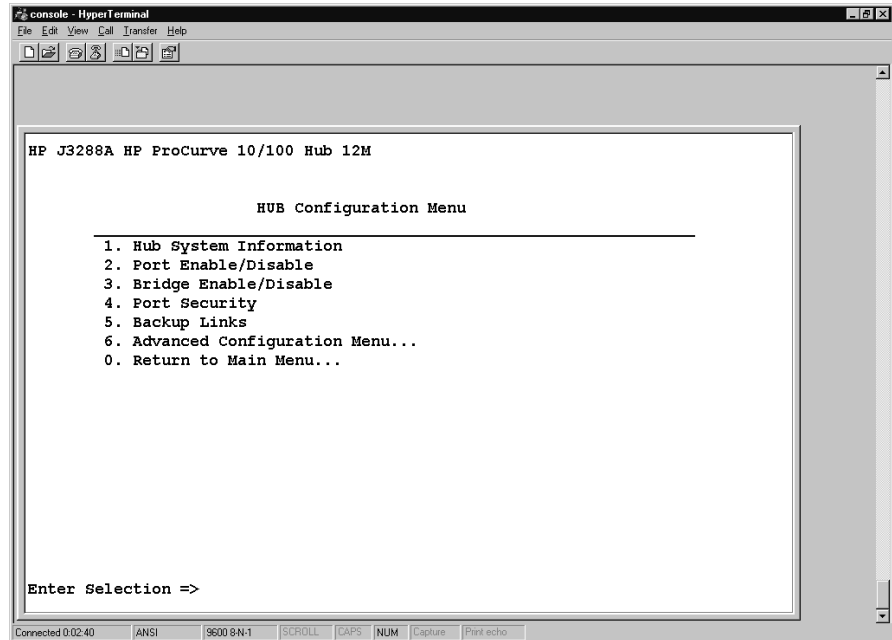
This feature is useful for security reasons in instances when the hub Console interface has detected no activity during a defined period of time. By having timeout control, you can minimize unauthorized user access by directing the console to be inactive after the interface has been left unattended for a set amount of time. The longer the timeout value, the less secure the Console interface is. The shorter the timeout value, the more secure it is, as it will become inaccessible more quickly. This feature is also useful for disconnecting from a modem if a call is interrupted.

## Hub Configuration Menu

The Hub Configuration Menu displays a list of menus and options that enable you to perform hub and port configuration tasks.

From the console Main Menu, select

### 3. Hub Configuration



**Figure 6-24. The Hub Configuration Menu**

- **Hub System Information.** Displays hub identification information and system attributes. Allows you to edit the hub's system name, contact, and location data.
- **Port Enable/Disable.** Enables you to turn ports on and off. A port that is "on" can receive and transmit packets. A port that is "off" does not send or receive traffic.
- **Port Security.** Displays security information about all ports on the hub, showing the address learning method, authorized station (MAC) address for the hub, whether Eavesdrop Prevention has been enabled, and whether an alarm is to be sent in the event of an unauthorized packet. The console allows Port Security to be disabled.



- **Backup Links.** Enables you to configure a primary and a redundant communication link between multiple devices in a cascaded topology, using two separate cables and two ports on each device. One port is defined as the primary port and the other the backup port. The backup port becomes active only if the primary port becomes inactive, and will automatically deactivate if the primary port becomes active again. Any of the network ports can be used as either the primary or backup port.
- **Advanced Configuration Menu.** Provides access to the following port speed and hub reset to factory default features:

---

**Caution**

Setting a port to a speed for which the device at the other end of the link is not already configured may cause loss of link and other network problems

Resetting the hub to its factory default settings clears the hub's IP addressing and resets it to Bootp/DHCP, as well as all port configurations. If your network is not set up to provide IP addressing to the hub via Bootp or DHCP, then the hub will operate in an unmanaged state. In this case, to restore management functionality, it will be necessary to connect a Console device via the hub's Console port.

- **Port Speed Configuration.** Enables you to force a port's speed setting to Auto-negotiation (the default), 100 Half-Duplex, or 10 Half-Duplex.
- **Reset Hub to Factory Default.** Clears all configuration parameters to their factory default settings, including any IP address configuration, and then reboots the hub. By resetting these parameters, you can often correct the performance of a failing device if its configuration is the source of the problem.

## System Information

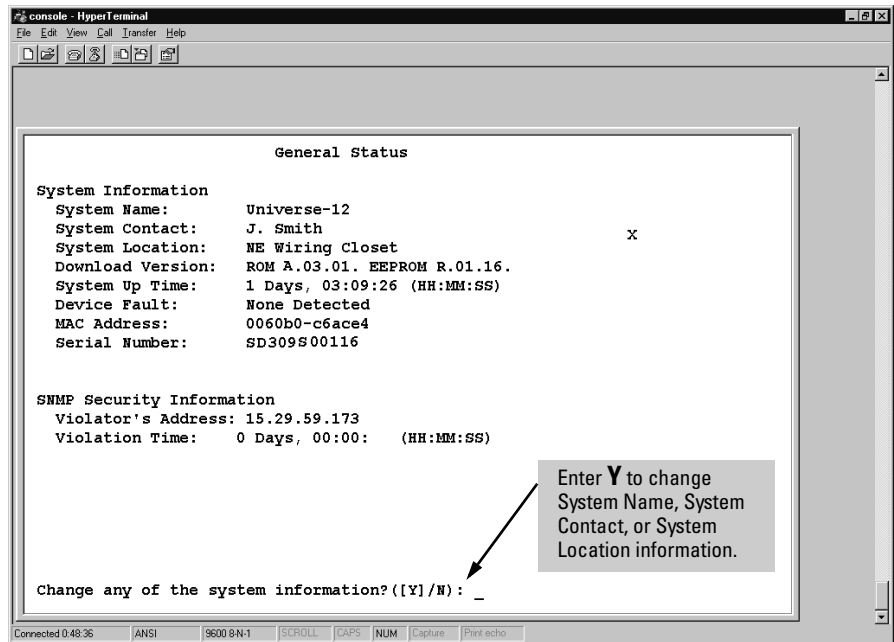
The General System Information screen displays hub system identification information retrieved from the System Group in the MIB II. It also enables you to change System Name, System Contact, and System Location strings.

### Hub Console

From the console Main Menu, select

#### 3. Hub Configuration . . .

##### 1. Hub System Information

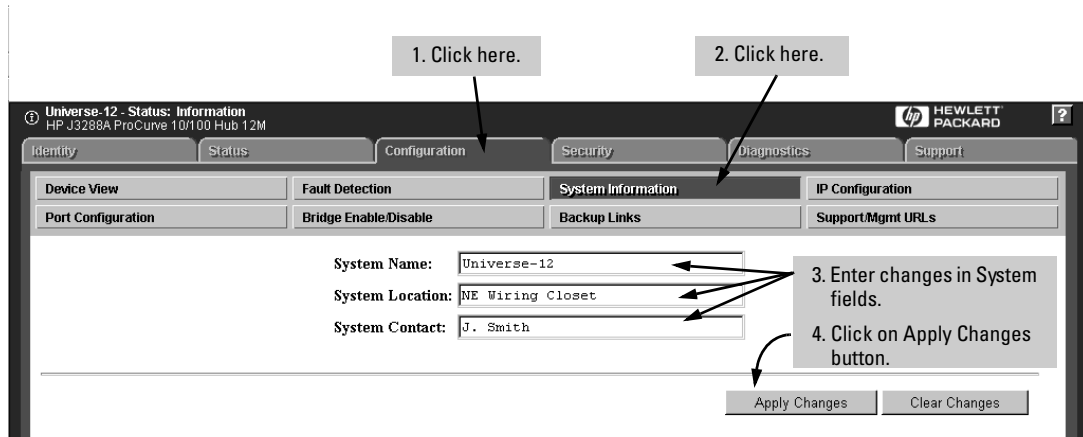


**Figure 6-25. Example of the Hub System Information Screen**

- **System Name.** A label used to associate a common name to identify the device.
- **System Contact.** The name of the person responsible for or who administers the device.
- **System Location.** A description of where the device will be located. This can be up to 255 characters, including spaces.

- **Download Version (read-only).** The versions of ROM and firmware of the device. A sample ROM version is **A.01.00**. A sample firmware version is **A.01.01**.
- **System Up Time (read-only).** The amount of time elapsed since the device was powered on. Displayed in the format *DD:HH:MM:SS* where *D* is days, *H* is hours, *M* is minutes, and *S* is seconds. For example, **21:43:50:14**.
- **Device Fault (read-only).** Indicates any errors discovered during the device self test. Only shown in the Console.
- **MAC Address (read-only).** The MAC address of the device. For example, **06007b-52d1ba**.
- **Serial Number (read-only).** The serial number of the device. For example, **SD300BT00386**.
- **SNMP Security Information (read-only).** Indicates whether the hub has experienced a management violation, generally, a packet from a device or management station that has not been authorized to manage the hub in a particular (or any) way. For more on this topic, see "Security Intruder Log" on page 6-17.

## System Information in the Web Browser Interface



**Figure 6-26. Configurable System Information in the Web Browser Interface**

## Port Enable/Disable

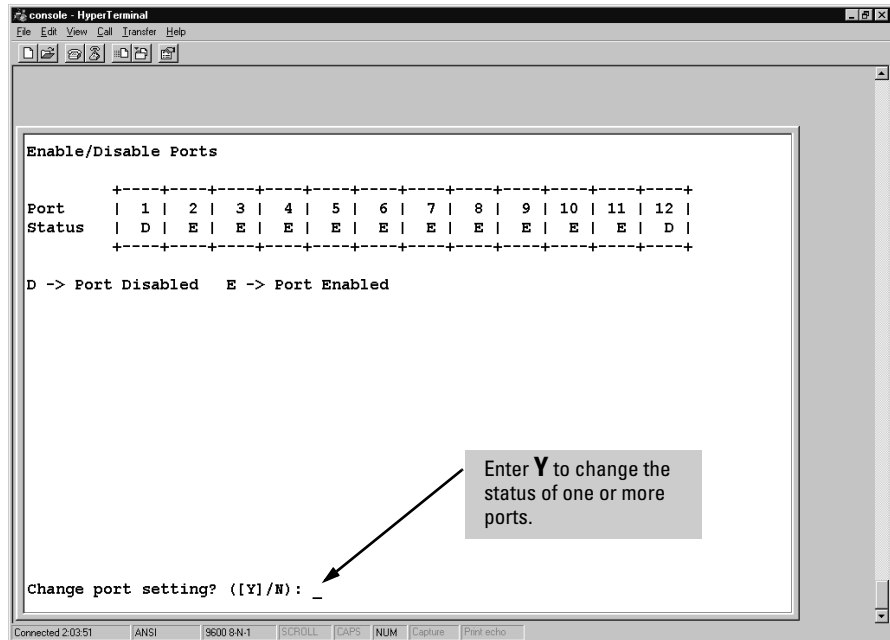
The Port Enable/Disable screen in the Console and the Device View Window in the web browser interface are both used to turn ports on and off so that they can connect to other devices or be inactive. The default port setting is Enabled.

### Hub Console

From the console Main Menu, select

**3. Hub Configuration . . .**

**2. Port Enable/Disable**



**Figure 6-27. The Port Enable/Disable Screen**

- **Port Status.** Displays a series of numbered squares, each representing a corresponding port on the hub, and indicating whether the port is enabled or disabled. Each square contains one of the following letters, indicating the status of the port:
  - **E:** Indicates the port is enabled and can send or receive packets to or from another device if connected to the port.

- **D**: Indicates the port is disabled and cannot send or receive packets to or from another device connected to the port.

## Enabling and Disabling Ports in the Web Browser Interface

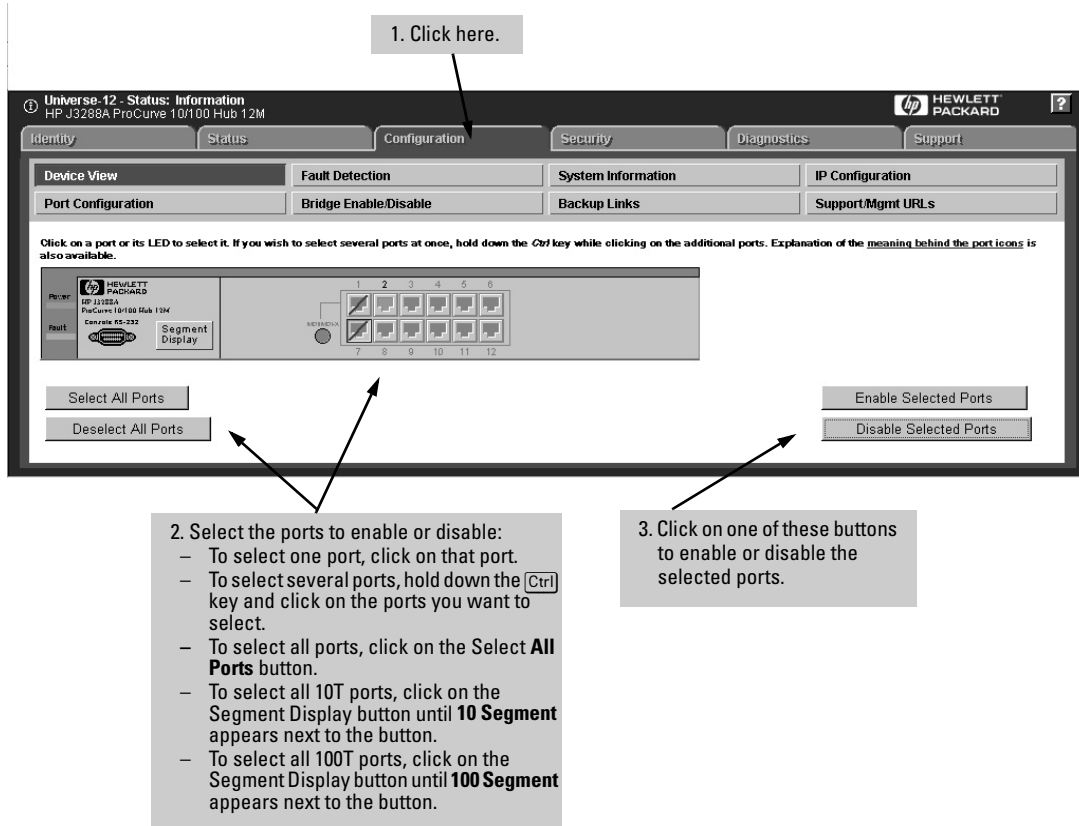






Figure 6-28. Example of the Device View Window

In the port region of the Device View, port states are indicated as follows:

**Table 6-3. Port State Color Key**

Port State	Color	Description
	Green (not actual)	The port is enabled and detects Link Signalling on a device connected to the port.
	Gray	The port is enabled, but does not detect Link Signalling.
	Gray with a blue diagonal slash	The port is disabled.
	Red (not actual)	This port has been autopartitioned or if there has been a security violation on a port that is still active. (See "Security Intruder Log" on page 6-17.)

## Bridge Enable/Disable

---

### Note

---

In most cases it is recommended that this setting remain enabled for optimum connectivity. Cases where you may want to disable the bridge include a topology where you want to connect the segments via an external switch or where you want to simplify the network for troubleshooting purposes.

This feature enables (the default) or disables the internal bridge between the hub's 10 Mbps and 100 Mbps segments.

### Hub Console

From the console Main Menu, select

#### 3. Hub Configuration . . .

#### 3. Bridge Enable/Disable

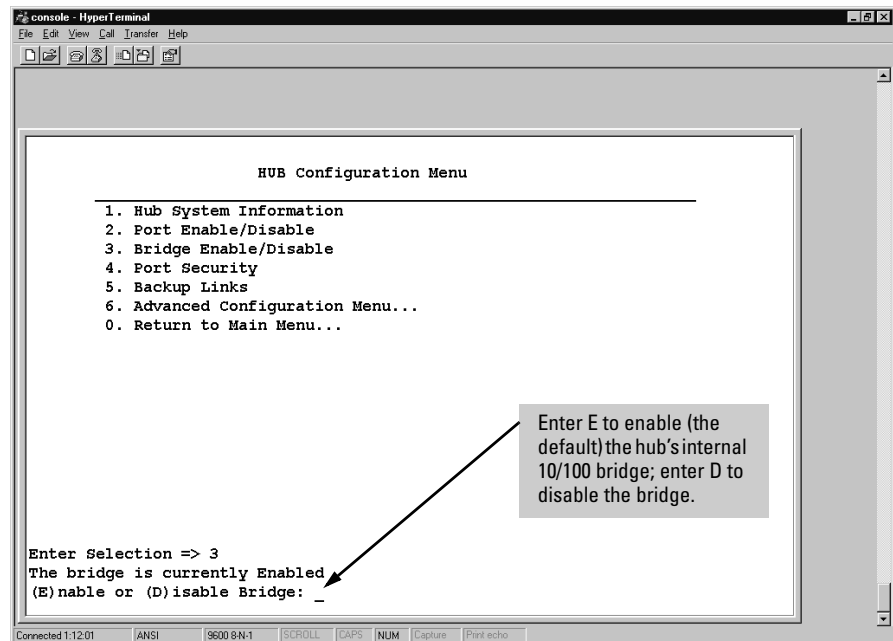
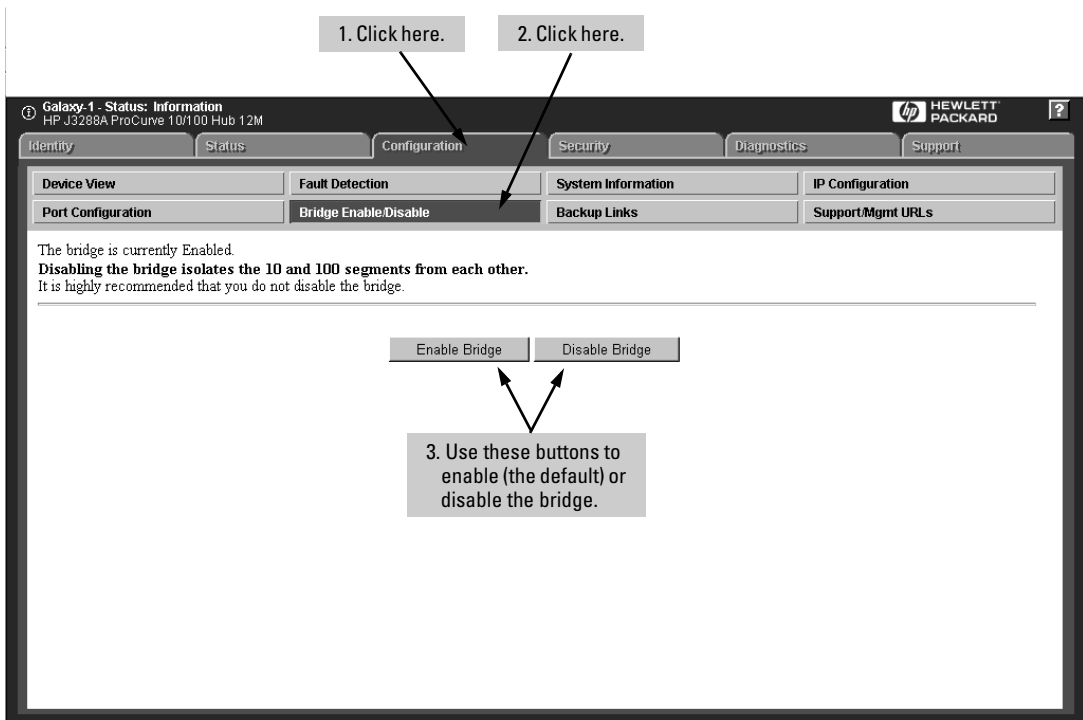


Figure 6-29. The Bridge Enable/Disable Screen

## Bridge Enable/Disable in the Web Browser Interface

### Note

In most cases it is recommended that this setting remain enabled for optimum connectivity. Cases where you may want to disable the bridge include a topology where you want to connect the segments via an external switch or where you want to simplify the network for troubleshooting purposes.





## Port Security

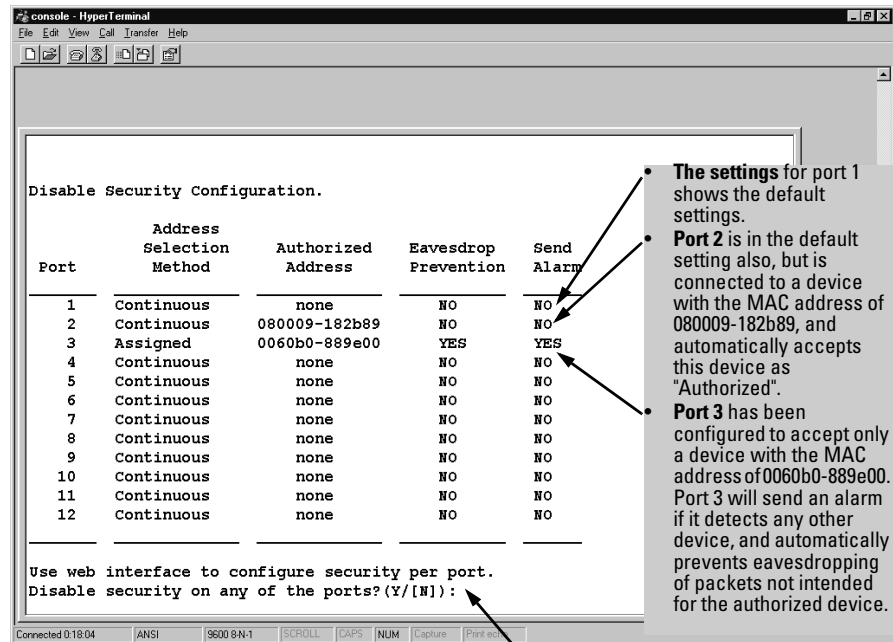
The default port security setting is "off". That is, any device can access a port without causing any type of security reaction. However, on a per-port basis, you can configure security measures to block unauthorized connections to the hub or listening on the hub, and to notify you if such connections are made.

- Use the Console interface to view and disable port security.
- Use the web browser interface to view, set, and modify port security.

## Hub Console

From the console Main Menu, select

### 3. Hub Configuration . . . 2. Port Security



The settings for port 1 shows the default settings.

Port 2 is in the default setting also, but is connected to a device with the MAC address of 080009-182b89, and automatically accepts this device as "Authorized".

Port 3 has been configured to accept only a device with the MAC address of 0060b0-889e00. Port 3 will send an alarm if it detects any other device, and automatically prevents eavesdropping of packets not intended for the authorized device.

To disable security for a port that has been previously configured for security in the web browser interface, enter **Y**.

**Figure 6-30. Example of the Port Security Screen**

- Use the Console's Port Security screen (above) to disable port security.
- Use the web browser interface to enable port security.

## Configuring Port Security

To configure port security, you must use the web browser interface.

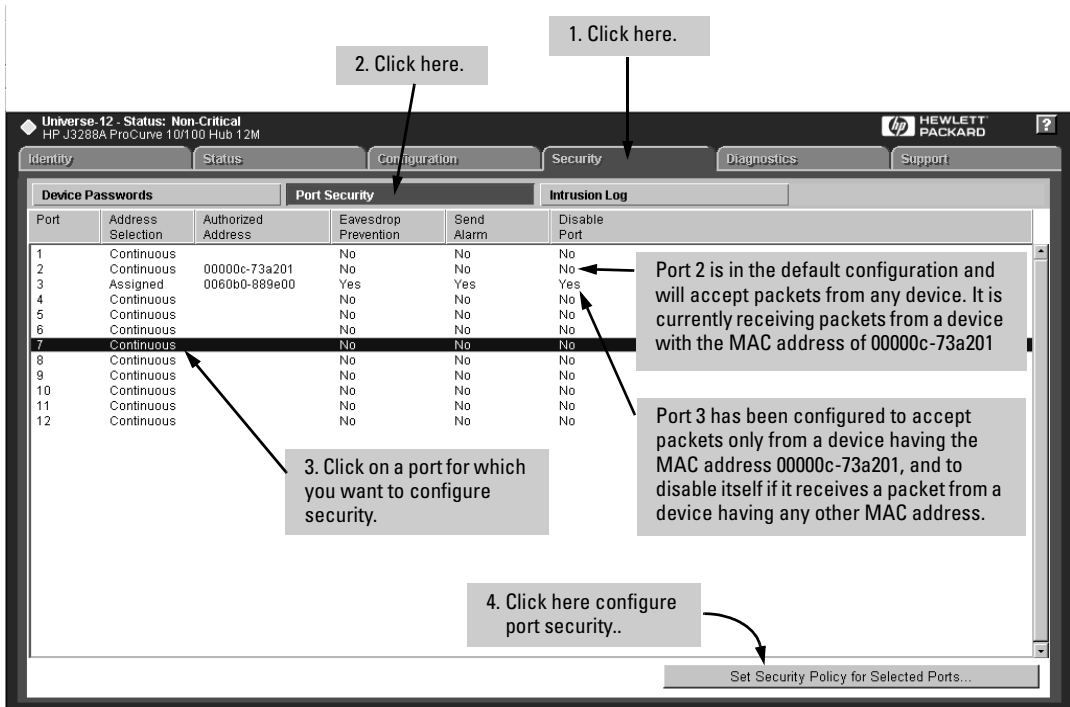


Figure 6-31. Example of the Port Security Window

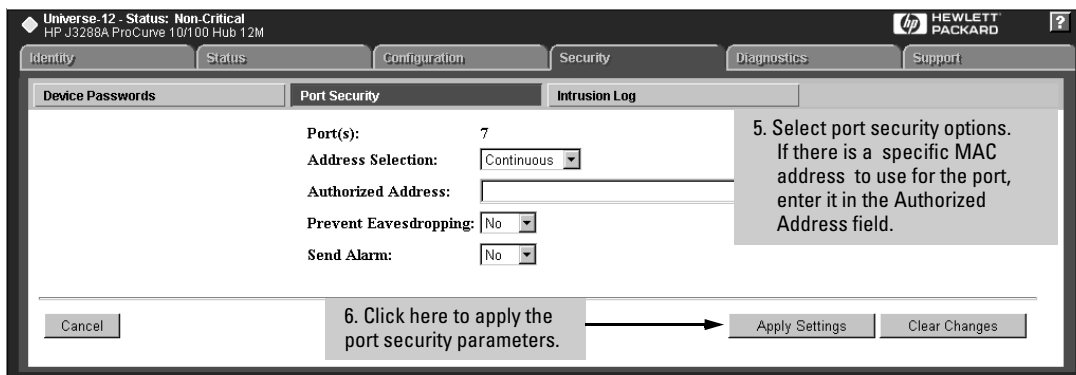


Figure 6-32. The Default Port Security Configuration Window

The port security parameters are:

- **Port.** Indicates the port label on the hub.
  - 1-12** on the Hub 12M
  - 1-24** on the Hub-24M
- **Address Selection Method.** Indicates the Address Selection method used on the port. The settings can be:
  - **Continuous** (the default). The hub learns the address of the device currently attached to the port and makes it the authorized address. This allows any device attached to the port to be selected. This is the method to use on cascaded ports.
  - **First Heard**. The hub learns the address of the first device attached to the port and makes it the authorized address.
  - **Assigned**. You enter the address of the device that is authorized to be attached to the port.
- **Authorized Address.** Indicates the authorized MAC Address for a device connected to the port.
- **Eavesdrop Prevention.** Indicates whether packets not intended for the port will be scrambled. The settings can be:
  - **On**. Indicates that a packet not intended for the port will be scrambled.
  - **Off**. Indicates that all packets will be received by the port.

---

**Caution**

---

*Do not turn on Eavesdrop Prevention for a cascaded port. (See "I Can't Communicate with My Hub" in chapter 7, "Troubleshooting".)*

- **Send Alarm.** Indicates whether an alarm will be sent to a network management application (such as HP TopTools for Hubs & Switches) when an incoming packet from the connected node does not match the authorized address. (See "Alarm Destinations for Unauthorized Packet Events" on page 6-51.) The settings can be:
  - **On**. Indicates that an alarm will be sent to a log when an incoming packet from the connected node does not match the authorized address.
  - **Off**. Indicates that no alarm will be sent to a log when an incoming packet from the connected node does not match the authorized address.
- **Disable Port.** Indicates whether the port will be disabled when an incoming packet from the connected node does not match the authorized address. The settings can be:

- **On**. Indicates the port will be disabled in response to it receiving an incoming packet from the connected node that does not match the authorized address. This configuration occurs automatically if either the **First Heard** or the **Assigned** address selection method is used.
- **Off**. Indicates the port will not be disabled in response to it receiving an incoming packet from the connected node that does not match the authorized address.
- **Set Security Policy for Selected Ports Button** (web browser interface only). Stores the security settings you have configured for ports on the hub.

---

**Note**

---

You can disable port security from the hub Console interface. However, you must use the web browser interface to set security parameters.

## Intruder Prevention

This feature stops an unauthorized computer from gaining access to the network. The manner in which this action occurs is through the address selection method, a technique that sets addresses for which devices the port is allowed to connect. The three address selection methods are:

- **First Heard**
- **Continuous**
- **Assigned**

See “Address Selection Methods” to learn about each method. When a port is configured for Intruder Prevention, the hub examines the source address of each packet coming through the port and compares it with the address permitted by the address selection method. If the addresses are not the same, the hub concludes that an intruder, or unauthorized device is attempting to gain access to the network and takes the appropriate action. Actions can be either sending an alarm to a log, disabling the port or both.

## Address Selection Methods

The technique used to control which devices are permitted to communicate with a port is known as *Address Selection*. Address Selection is the process by which the port sets policy for receiving packets from attached devices. The port performs this task by comparing addresses in the source header of a packet with a preset, acceptable source address. One address per port is allowed (except **Continuous** mode, which *does not* compare addresses):

- **Continuous**. Any device is permitted to transmit to this hub port.

- **First Heard.** The hub learns the address of the device attached to the port and makes it the authorized address. If a different device is later attached to the port, the new address is registered as an intruder address. This indicates a security violation has occurred and the port is automatically disabled.
- **Assigned.** You enter the address of the device that is authorized to be attached to the port. If a different device is later attached to the port, the new address is registered as an intruder address. This indicates that a security violation has occurred and the port is disabled. If you choose Assigned, you need to go to the Authorized Address box and type in a specific MAC address of a device authorized to be attached to that port.

## Eavesdrop Detection

A feature that stops a device connected to a port on the hub from receiving network packets not intended for that device. The hub performs this task by comparing the port's authorized address with the destination address of packets being repeated through the hub. If the addresses do not match, the packet's bit pattern is scrambled, rendering it unreadable by any device on that port.

## Alarm Destinations for Unauthorized Packet Events

When the Send Alarm parameter is enabled for a port, the port will send an alarm to a network management application such as HP TopTools for Hubs & Switches.

HP TopTools receives events sent by devices that may signal trouble or require action on your part. When a new event arrives, TopTools processes it into an alert (TopTools uses the term *alert* to denote either an SNMP trap or DMI alert) and notifies you of its presence by updating the alert icon on the Alerts button in the TopTools navigation frame. In addition, the alert is added to the Alert page, to the database of alerts, and to the device description in the Devices page. For more information, see the online Help provided with HP TopTools for Hubs & Switches.

## Backup Links

The Backup Links screen is used to configure a primary and a redundant communication link or path between the hub and any other device. One port on the hub is defined as the connection to the primary path to the other device and another port on the hub is defined as the connection to the secondary or backup path to the other device.

The backup port becomes active only if the primary port can no longer connect to the specified other device. Any of the hub ports can be used as either the primary or backup port. A maximum of four backup links can be created.

### Hub Console

From the console Main Menu, select

#### 3. Hub Configuration . . .

#### 5. Backup Links

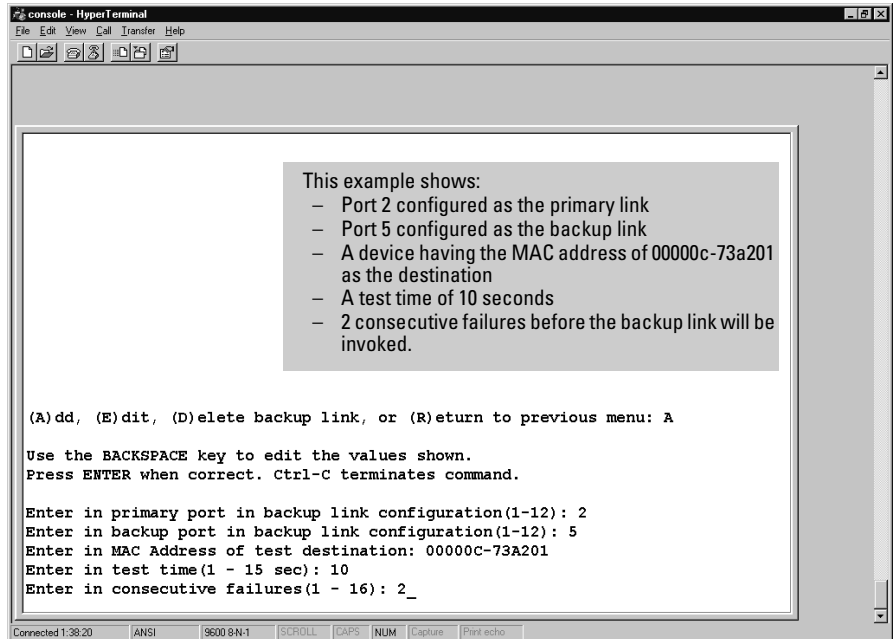


Figure 6-33. Example of the Backup Links Configuration Screen

- **Backup Port.** The port assigned as a backup in case the primary port fails. If the primary port is active, the backup port is inactive.
- **MAC Address.** The station (MAC) address of the device to which you have a backup (redundant) path; that is, the recipient of the 802.2 test packets, which will be used to verify the primary path.
- **Status.** Indicates the current status of which port in the backup link port pair that is being used. The screen can display one of two settings:
  - **Using Primary.** Indicates the hub is using the primary port.
  - **Using Backup.** Indicates the hub is using the backup port.
- **Primary Port.** The port to be used as the primary connection to another device.
- **Backup Port.** A port you have assigned as the backup port to a primary port; that is, the specific port that will be used in the event of a failure on the primary port.
- **Test Time (Seconds).** Indicates the number of seconds allowed for the primary port to wait for a response from its target device before timing out and attempting a retry. The number can be between 1 and 15.

As a general rule, for connections of greater distances, slower media throughput, and higher hop counts, the test time value should be higher so more time can be allowed for a response.

- **Number of Failures till switching to backup.** ("Retries" on the web browser interface) The maximum number of times the test packets from the primary port fail to return from the other device before the backup port is implemented as the active port.
- **Add New Backup Link (Web Browser Interface Only).** The button on the Backup Links window in the web browser interface that begins a session to add a backup link.
- **Delete Selected Items (Web Browser Interface Only).** Deletes the selected backup link configuration. (Removes a configured backup link, thus removing backup support for the indicated primary link.)

## Configuring Backup Links in the Web Browser Interface

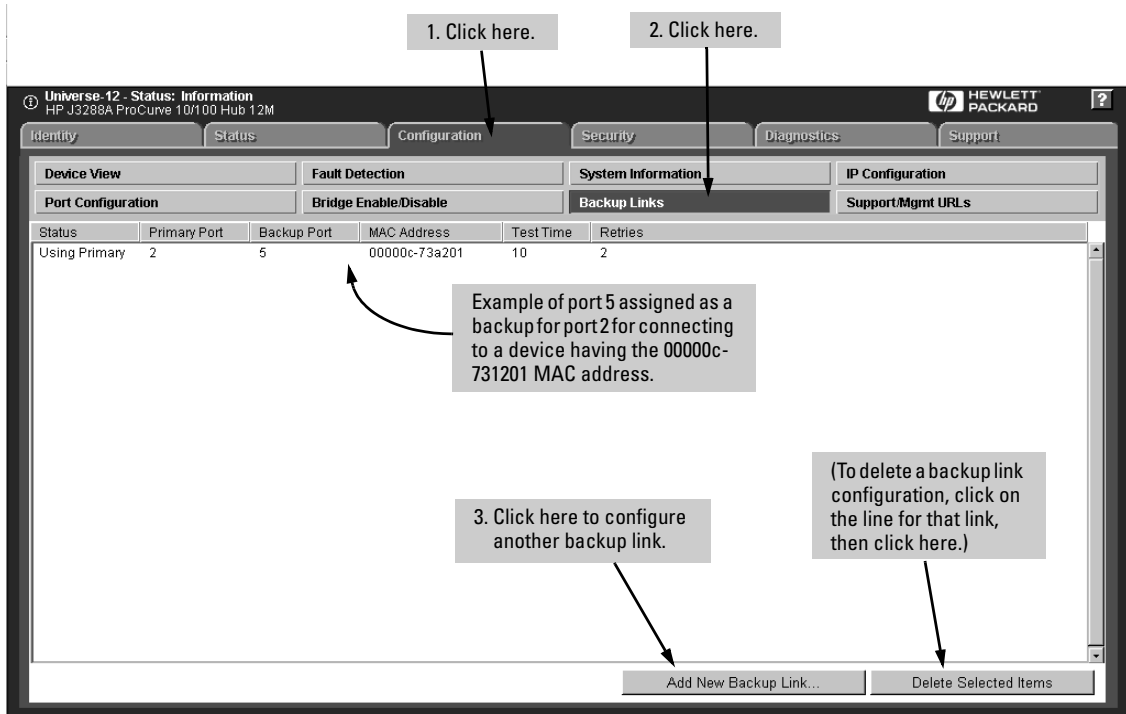


Figure 6-34. The Backup Links Window

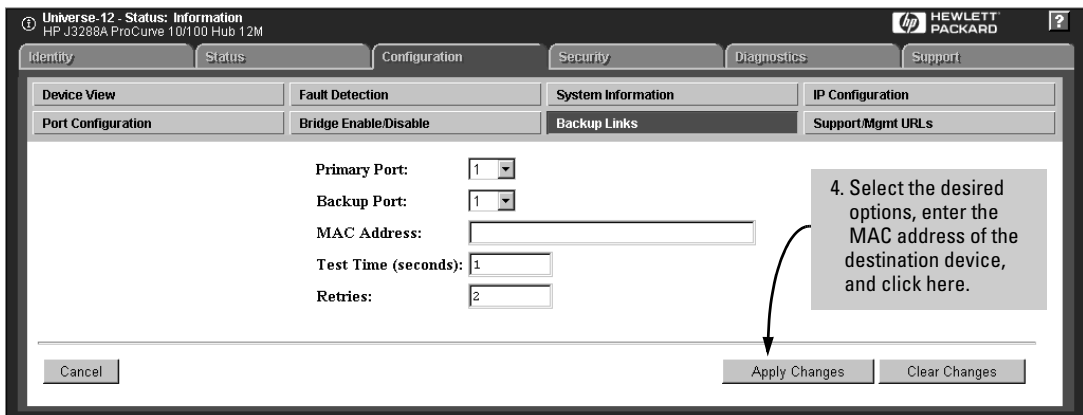
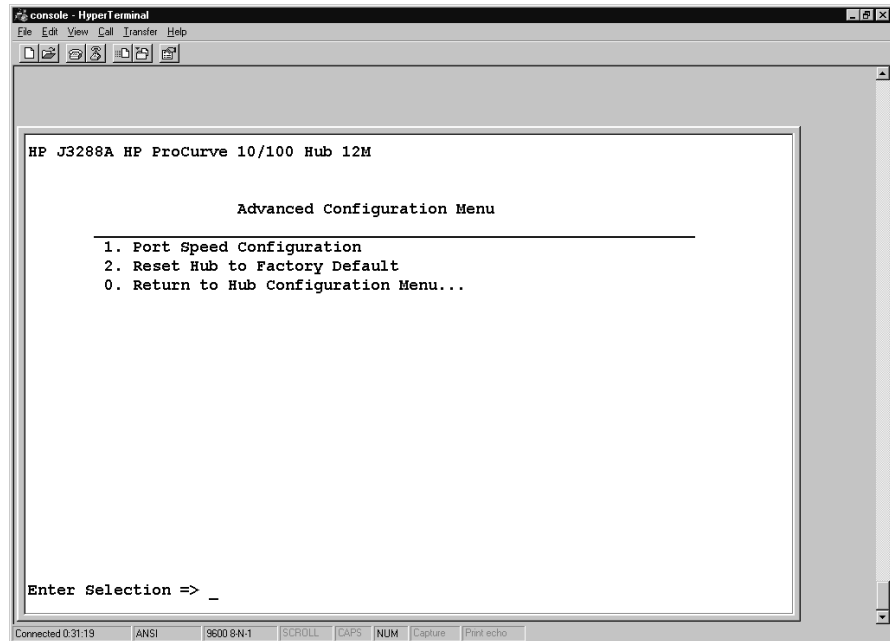


Figure 6-35. Adding a Backup Link



## Advanced Configuration Menu



**Figure 6-36. The Advanced Configuration Access Menu**

From the console Main Menu, select

**3. Hub Configuration . . .**

**6. Advanced Configuration Menu . . .**

The Advanced Configuration menu displays hub features that enable you to perform actions that can have a severe impact on hub operation:

- **Force a port speed configuration.** The default port speed setting is Auto-negotiation. This screen enables you to specify 10 half-duplex or 100 half-duplex, or to reset to Auto-negotiation.
- **Reset the hub to the factory default configuration.** This feature returns the hub to the factory-default, plug-and-play configuration. In this state the hub operates as an unmanaged device unless either your network supports IP addressing for the hub through Bootp or DHCP, or you later configure IP addressing using the Console.

## Port Speed Configuration

### Caution

Setting a port to a speed for which the device at the other end of the link is not already configured may cause loss of link and other network problems. For this reason, it is recommended that, for each port, you leave this parameter at (the default) **Auto-negotiate** setting.

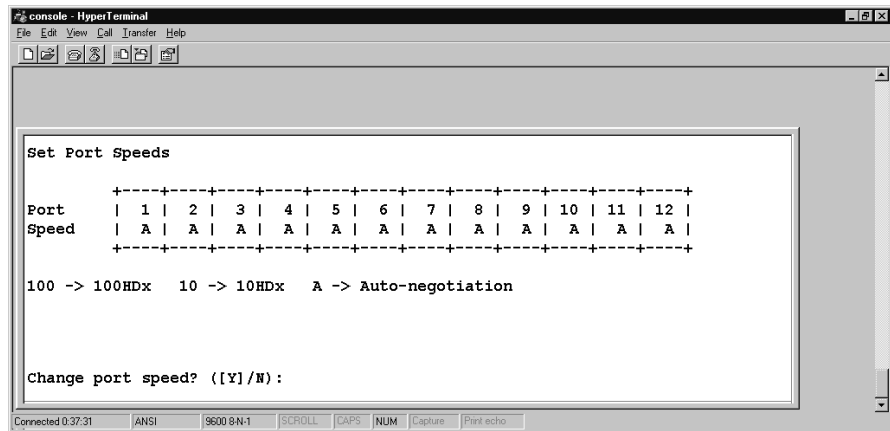
### Hub Console

From the console Main Menu, select

#### 3. Hub Configuration . . .

#### 6. Advanced Configuration Menu . . .

#### 1. Port Speed Configuration



Port speeds include the following:

- **Auto-negotiation (the default).** This is the recommended setting. It allows the hub to determine the speed of a device connected to a port, and then automatically configure that port to operate at the same speed setting as the connected device. That is, the port auto-senses, or negotiates, a speed (10 Mbs half-duplex or 100 Mbps half-duplex) with the device to which it is connected.
- **100 half-duplex.** This setting forces the port to operate at 100HDx.
- **10 half-duplex.** This setting forces the port to operate at 10HDx.

**Caution**

Forcing a port to a speed for which the device at the other end of the link is not already configured may cause loss of link and other network problems. HP recommends leaving the hub's port speeds set to **Auto-neg** (Auto-negotiation).

Port Speed Configuration in the Web Browser Interface

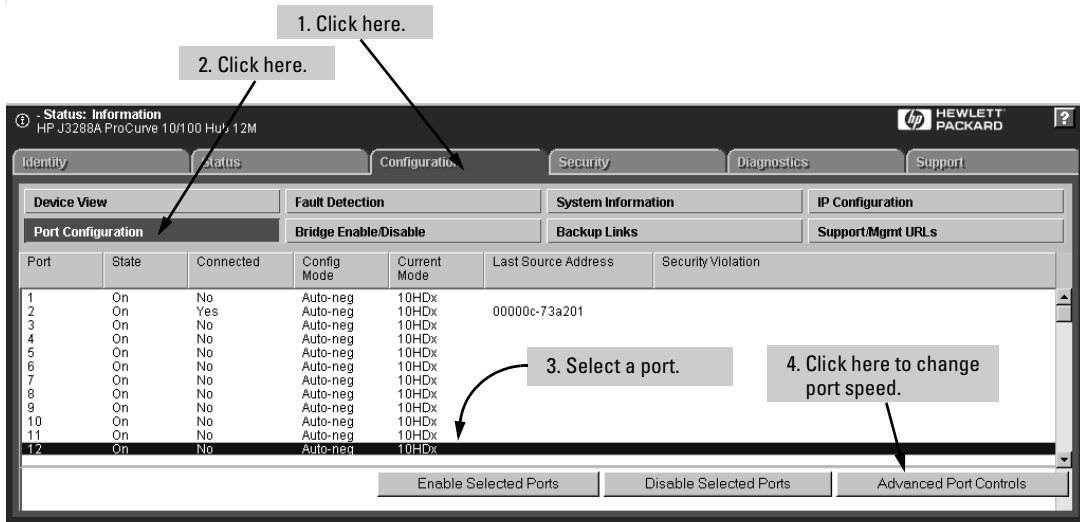


Figure 6-37. The Port Configuration Window

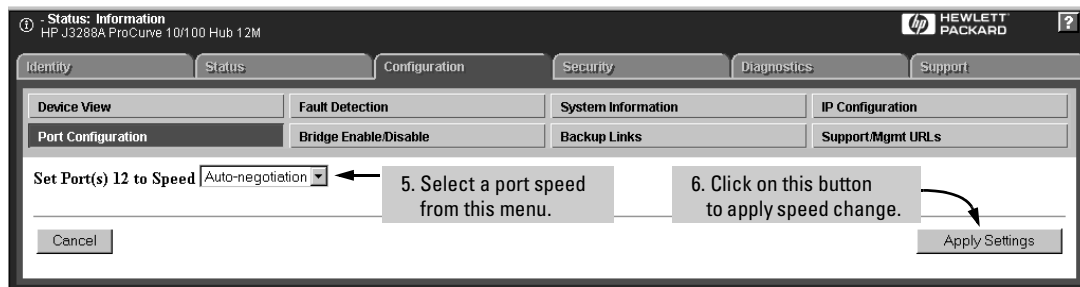


Figure 6-38. The Port Speed Change Window

## Reset the Hub to Its Factory Default Configuration

---

### Caution

---

If backup links are configured on the hub, returning the hub to its factory default configuration eliminates the backup function on redundant links. This results in network loops, which can cause broadcast storms that will slow down the network or, in some cases, bring it to a halt due to oversubscribed bandwidth.

Resetting the hub to its factory default configuration removes any configuration changes performed on the hub after removal from its original packaging. This includes all IP addressing. In the factory default configuration, the hub's management functions will be reachable only if you have configured the device via Bootp or DHCP servers. (You can also access some management features by using a console device connected directly to the hub.)

### Hub Console

From the console Main Menu, select

- 3. Hub Configuration . . .**
- 6. Advanced Configuration Menu . . .**
- 2. Reset Hub to Factory Default**

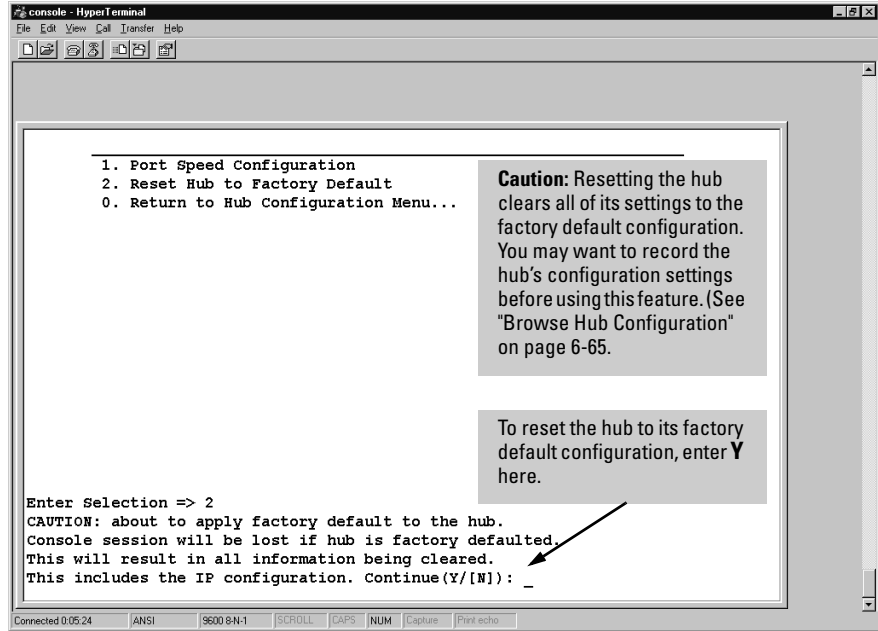


Figure 6-39. The Factory Reset Window

### Factory Reset in the Web Browser Interface

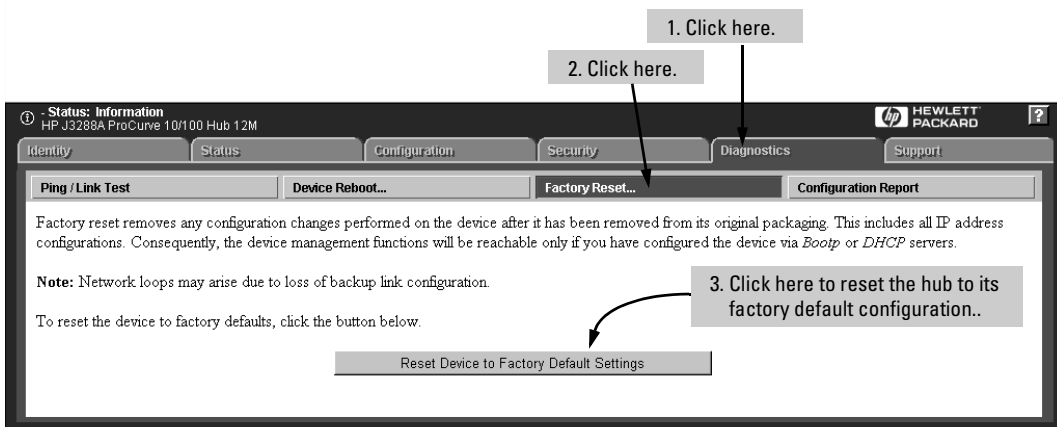


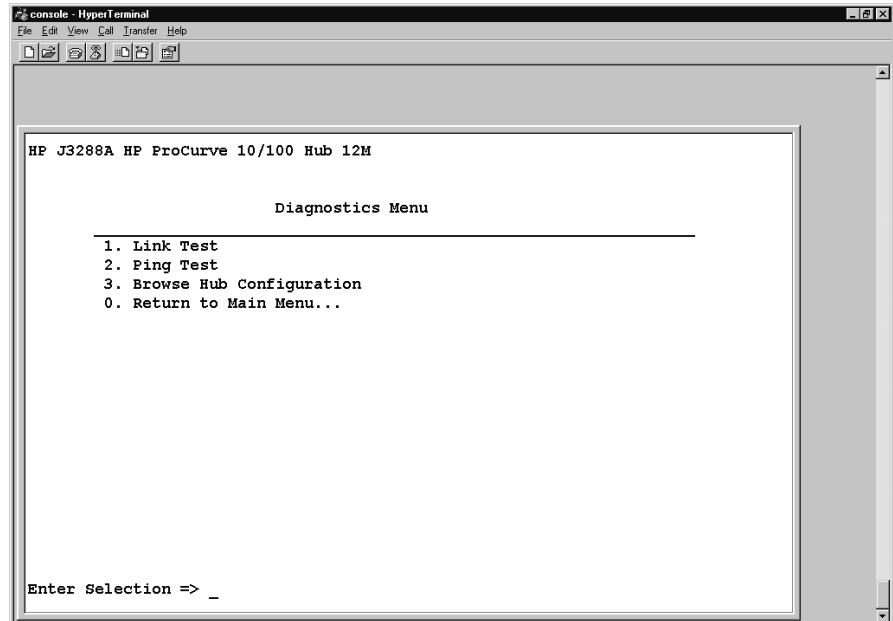
Figure 6-40. The Factory Reset Window

## Diagnostics Menu

The Diagnostics Menu contains several options used for network device troubleshooting.

From the console Main Menu, select

### 4. Diagnostics



**Figure 6-41. The Diagnostics Menu**

- **Link Test.** Runs a test of the connection between the hub (the “local” device) and a designated remote device.
- **Ping Test.** Runs a test of the path between the hub and another device on an IP network that responds to IP (Internet Protocol) packets.
- **Browse Hub Configuration.** Provides a listing of the hub’s current configuration settings.

## Ping Test

Ping tests the network layer (IP Address) path between the hub and another device on an IP network that responds to IP packets. During a Ping test, the managed device sends ICMP (Internet Control Message Protocol) echo request packets to another node with the specified IP Address and waits for echo response packets to return. The node must be capable of receiving and responding to ICMP packets. A failure means that either device at the destination address did not respond within the time range specified or the data returned from the device indicated an error. The Ping test is useful because it can tell you whether the hub is communicating properly with another device on the network.

### Hub Console

From the console Main Menu, select

#### 4. Diagnostics ...

#### 2. Ping Test

```

console - HyperTerminal
File Edit View Call Transfer Help
[Icons]

Enter Selection => 2

Use the BACKSPACE key to edit the values shown.
Press ENTER when correct. Ctrl-C terminates command.

Enter destination IP address: 25.52.252.197
Enter number of packets to send (1-10000): 5
Enter per-packet timeout in seconds (1-30): 5

Press CTRL-C to abort.

PING RESULTS
Passes Left   Errors
-----
0             0
Test completed.

Test Attempts: 5
Test Successes: 5
Min Response Time (ms): 50
Max Response Time (ms): 200
Total Response Time (ms): 500

Press ENTER to continue.

Connected 4:11:57  ANSI  9600 8-N-1  SCROLL  CAPS  NUM  Capture  Print echo
  
```

Figure 6-42. Example of Ping Test in the Console

Test results in the console include:

- **Min Response Time (ms):** Milliseconds used by the shortest test attempt.
- **Max Response Time (ms):** Milliseconds used by the longest test attempt.
- **Total Response Time (ms):** Milliseconds used to complete the overall test.

### Ping Test Using the Web Browser Interface

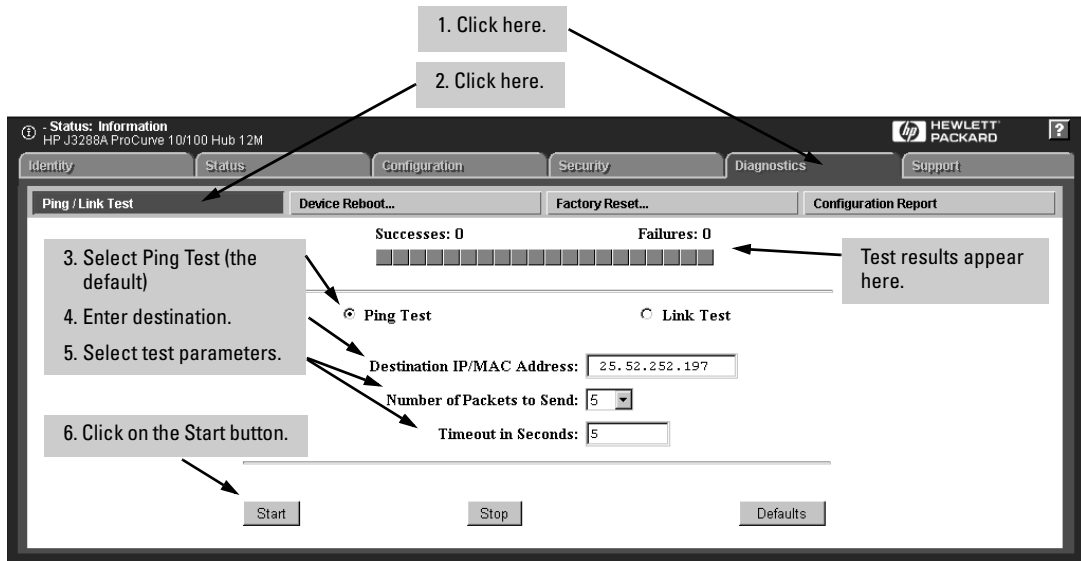


Figure 6-43. Example of a Ping Test in the Web Browser Interface



## Link Test

The Link test is a test of the link layer (MAC Address) connection between a local device and a designated remote device, and tells you whether the hub is communicating properly with the remote device. ( For this test to be meaningful, the remote device must be able to respond to an IEEE 802.2 test packet.) During the Link test, IEEE 802.2 test packets are sent from the hub to the designated remote device. The remote device returns the data to the hub, where it is compared to the data transmitted. If the received data matches the transmitted data, the test passes. A failure means that either the device at the destination address did not respond within the time range specified or the data returned from the destination device indicated an error.

## Hub Console

From the console Main Menu, select

### 4. Diagnostics ...

#### 1. Link Test

```

Enter Selection => 1

Use the BACKSPACE key to edit the values shown.
Press ENTER when correct. Ctrl-C terminates command.

Enter destination MAC address: 0060b0-e24280
Enter number of packets to send (1-10000): 5
Enter per-packet timeout in seconds (1-30): 5
Press CTRL-C to abort.

TESTLINK RESULTS

Passes Left  Errors
-----
           0      0
Test completed.

Test Attempts: 5
Test Successes: 5
Min Response Time (ms): 50
Max Response Time (ms): 150
Total Response Time (ms): 450

Press ENTER to continue.
  
```

1. Enter the destination MAC address.

2. Enter the number of packets (tests).

3. Enter the timeout per packet (that is, the maximum time between packet transmissions).

Test progress appears here.

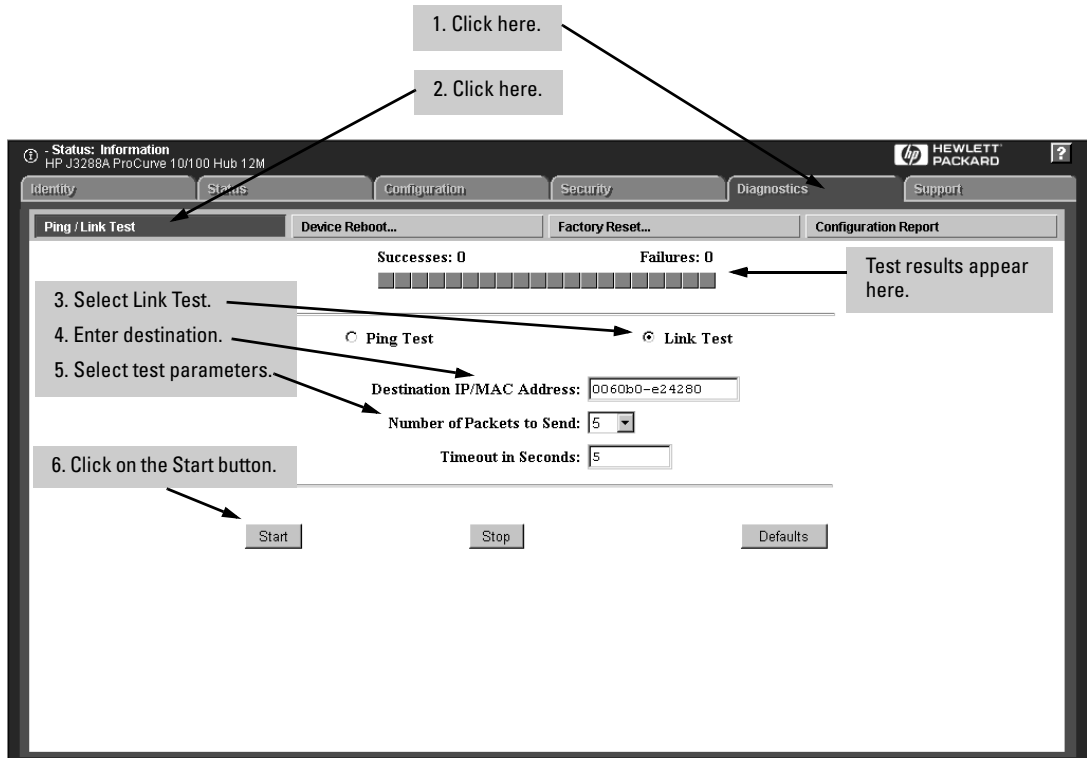
Test results appear here.

Figure 6-44. Example of Link Test in the Console

Test results in the console include:

- **Min Response Time (ms):** Milliseconds used by the shortest test attempt.
- **Max Response Time (ms):** Milliseconds used by the longest test attempt.
- **Total Response Time (ms):** Milliseconds used to complete the overall test.

### Link Test Using the Web Browser Interface



## Browse Hub Configuration

The Browse Hub Configuration screen provides a status readout of the following areas available from the hub Console interface:

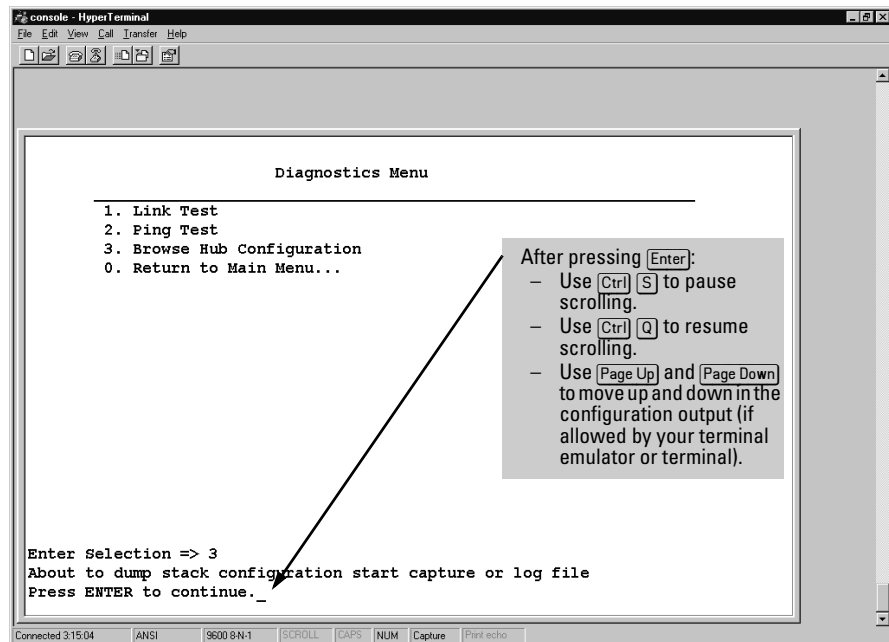
- General Status
- IP Configuration
- Web Accesses Status
- Current Timeout Value
- 10/100 Internal Bridge Status
- Backup Links Configuration
- Community List
- Authorized Manager List
- Port Status Information
- Security Configuration

### Hub Console

From the console Main Menu, select

#### 4. Diagnostics ...

#### 3. Browse Hub Configuration



**Figure 6-45. Using the Browse Hub Configuration Option in the Console**

You can do one or both of the following with the output of the **Browse Hub Configuration** feature:

- If your terminal emulator or terminal allows, you can use **Page Up** to page back through the configuration output. (For example, Hyperterminal—developed for MicroSoft by Hilgraeve, Inc.—allows you to page back through several consecutive screens.)
- Copy data into a text file for later viewing.

## Copying the Hub Configuration Output to a File

This procedure assumes you are using Hyperterminal in a Windows environment. You can use either an output file that you create or a default output file automatically created by Hyperterminal (step 1, below).

1. (Optional.) Create an empty text file in a directory that is accessible from the console.
2. Do the following start-up tasks:
  - a. Start Hyperterminal.
  - b. Start the Console interface and select

### 4. Diagnostics

#### 3. Browse Hub Configuration

3. In the Hyperterminal menu bar, click on **Transfer**. Hyperterminal displays a series of menu options.
4. In the resulting menu, click on **Capture Text**. Hyperterminal displays the Capture Text dialog box. The box contains a file box that provides the default filename C:\WINDOWS\CAPTURE.TXT. The Hyperterminal text capture program will send the contents of the Browse Hub Configuration execution to this file unless you use the Browse button to find another text file to use, such as the option file mentioned in step 1.
5. When you are satisfied with your target filename, click on the Start button in the Capture Text dialog box. The Hyperterminal program is now in text capture mode, meaning that the contents of all screens will be redirected to the file you have specified.
6. Press **Enter** to run the **Browse Hub Configuration** option.
7. Turn off the automatic redirection to the text file:
  - a. In the Hyperterminal menu bar, click on **Transfer**.
  - b. Click on **Capture Text**.
  - c. Click on **Stop**.

**Caution**

Be sure to turn off the redirection action, as described in step 7, above. Otherwise, each new screen displayed in the Console will be appended to the text file selected in step 4, above, which could result in a large file of mostly unwanted data.

- Using a standard DOS or Windows text editor, open the file to review the configuration data.

**Browse Hub Configuration in the Web Browser Interface**



**Figure 6-46. The Configuration Report Window**

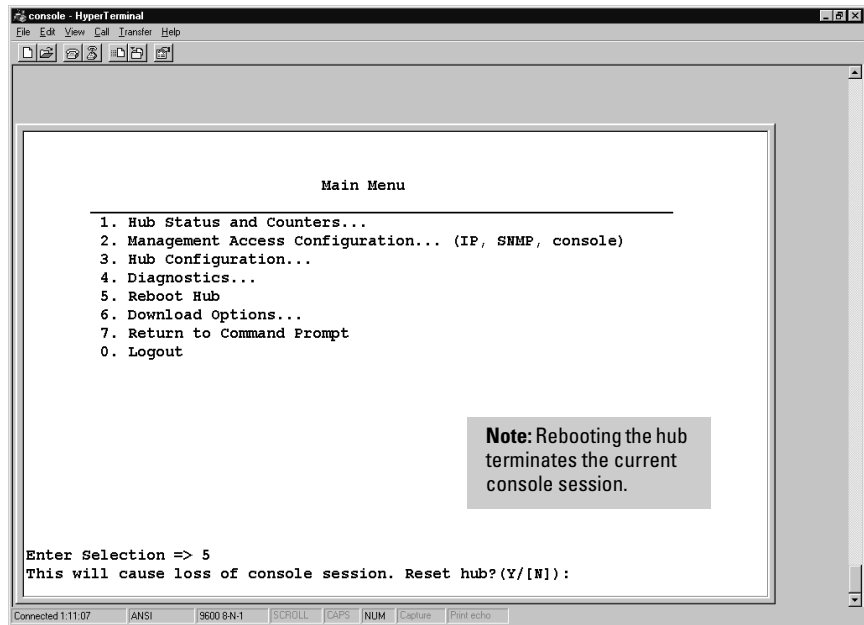
## Reboot the Hub

The Reboot Hub option enables you to reset the hub to clear any temporary error condition that may have occurred. This option clears the hub's port, bridge, global repeater, and system uptime counters, restarts the hub, and executes the hub self-test. This action has the same effect as unplugging, then replugging the hub's power cord.

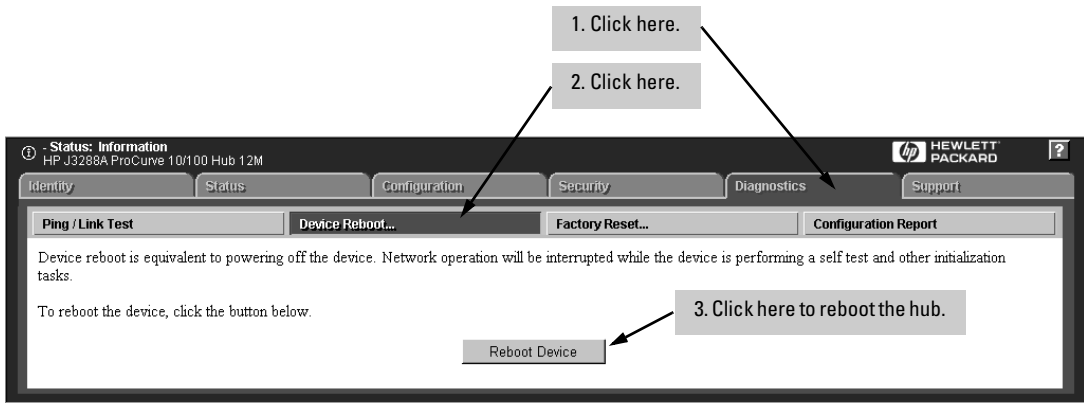
### Hub Console

From the Main Menu:

#### 5. Reboot Hub



## Rebooting the Hub in the Web Browser Interface



**Figure 6-47. Rebooting the Hub in the Web Browser Interface**

## Download OS

HP periodically provides operating system (OS) updates through the ProCurve website (<http://www.hp.com/go/procurve>) and the HP FTP Library Service. For more information, see the support and warranty booklet shipped with the hub. After you acquire a new hub OS file, you can use either of the following methods to download it into the hub:

- The TFTP method
- The XMODEM method

---

**Note**

---

Downloading a new OS does not change the current hub configuration.

### Using TFTP To Download the OS File

This procedure assumes that:

- The hub is properly connected to your network and has been configured with a valid IP address, subnet mask, and gateway IP address (page 6-23).
- An OS file for the hub has been stored on a TFTP server accessible to the hub. (The OS file is typically available from HP's electronic services—see the support and warranty booklet shipped with the hub.)

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 hub (for example, "j3289105.bin").

---

**Note**

---

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

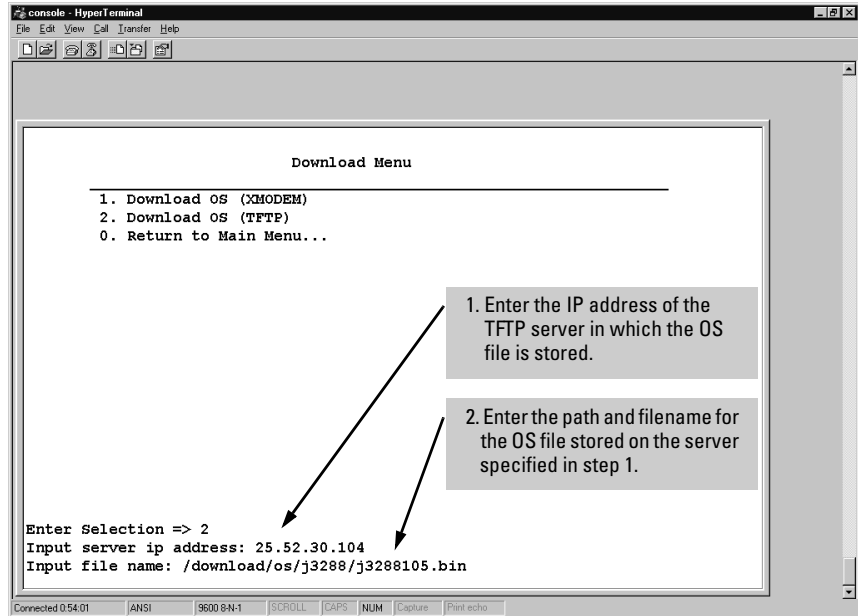
After a download, the Console session closes and the hub reboots itself.

---

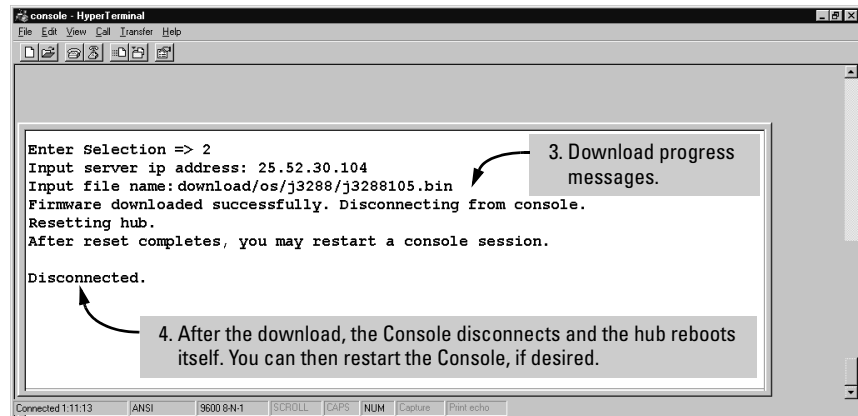


From the Main Menu, select:

**6. Download Options . . .**



**Figure 6-48. Example of TFTP Download Screen**



**Figure 6-49. Example of Download Progress and Messages**

## Using XMODEM To Download an OS File

This procedure assumes that:

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

**How To Perform the XMODEM OS Download.** This example uses the Hyperterminal program included in Windows NT.

---

### Note

---

Depending on the time it takes to move through these steps, the hub may time-out and stop the download. If this occurs, begin the procedure again from step 1.

1. From the console Main Menu, select:

#### 6. Download Options

##### 1. Download OS (XMODEM)

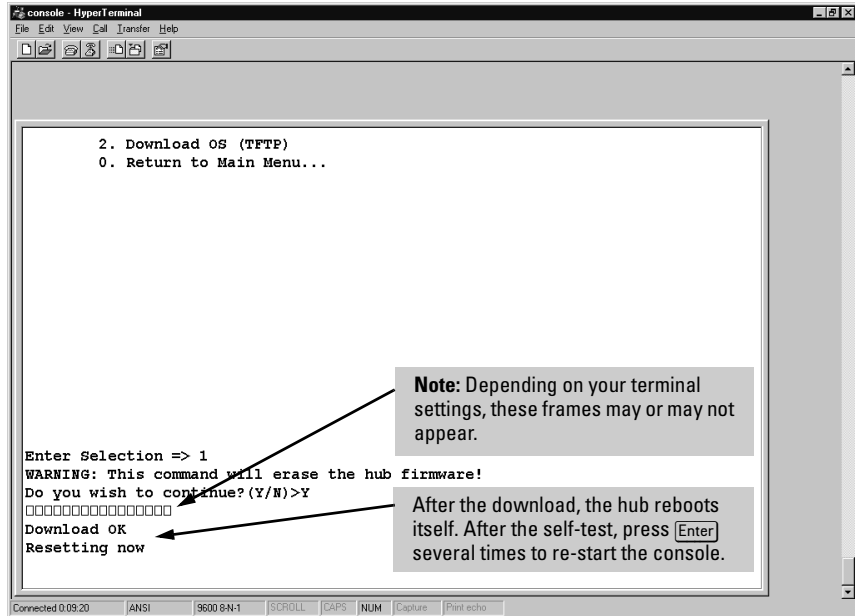
You will then see this prompt:

**WARNING: This command will erase the hub firmware!  
Do you wish to continue? (Y/N)**

2. Enter **Y** at the above prompt to prepare the hub to receive the download.
3. In the Hyperterminal menu bar, click on **Transfer**.
4. In the dropdown menu, select **Send File . . .**
5. In the Send File dialog box:
  - a. Use the **Browse . . .** button to select the OS file to download into the hub.
  - b. Use the Protocols dropdown menu to select **Xmodem**.
  - c. Click on the **Open** button.

- d. Click on the **Send** button to begin the download. You will then see the "Xmodem file send for console" box, which displays the progress of the download.

The download can take several minutes, depending on the baud rate used for the transfer. (Typically, this is the baud rate in use by the Console.)



**Figure 6-50. Example of XMODEM OS Download Progress**

- 6. When the download finishes, the hub 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 **Download Version** line. It should show the version number of the OS you just downloaded. For example, if you downloaded OS version A.01.05, you should see a line similar to the following:

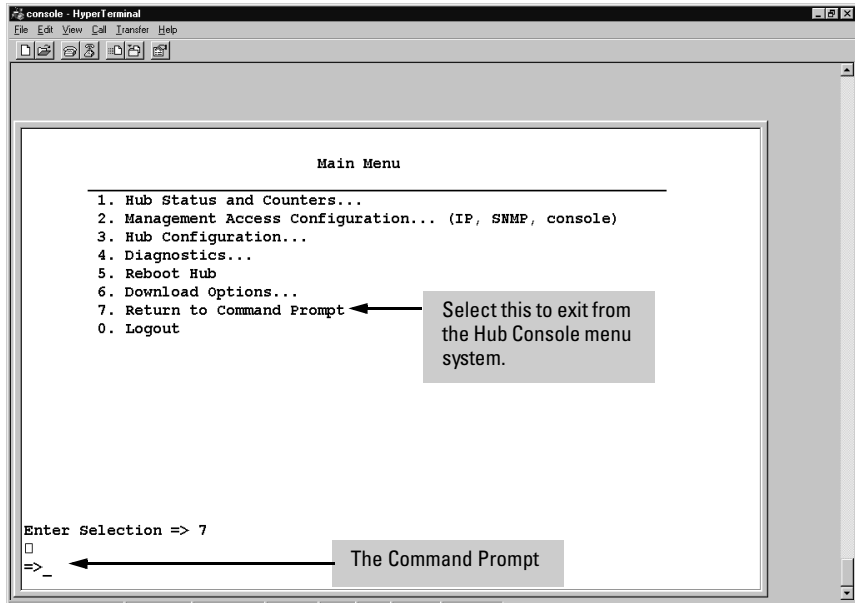
**Download Version:           ROM A.01.00   EEPROM A.01.05.**

## Return to the Command Prompt

Return to the Command Prompt takes you out of the Hub Console Interface menu system.

From the Main Menu, select:

### 7. Return to Command Prompt

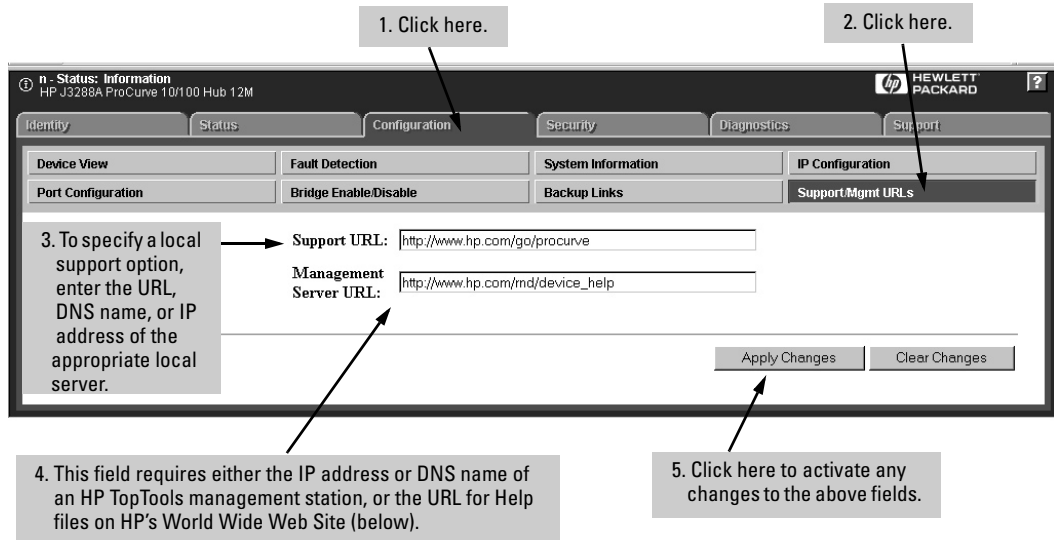


**Figure 6-51. Return to the Command Prompt**

## Management and Support URLs

The Support/MGMT URLs window specifies:

- The URL (Universal Resource Locator) of the web site that will be automatically accessed when you select the Support tab
- The URL for the source of online Help for the web browser interface



**Figure 6-52. The Support/Mgmt URLs Window**

**The Support URL.** This is configured to automatically access HP's ProCurve website on the World Wide Web. However, if you have an internal support structure, you may want to change the Support URL to access that structure.

**The Management Server URL.** Online Help is automatically available if you install HP TopTools for Hubs & Switches on your network or if you already have Internet access to the World Wide Web. Retrieval of the Help files is controlled by automatic entries to the Management Server URL field. That is, the hub is shipped from the factory with the following URL, which is needed to retrieve online Help through the World Wide Web:

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

However, if HP TopTools is installed on your network and discovers the hub, the Management Server URL is automatically changed to retrieve the Help from your TopTools management station.

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

## Support

This window automatically displays the support site specified in the Support URL field of the Support/Mgmt URLs window (page 6-75) in the web browser interface. By default, the URL is set to HP's ProCurve website. However, you can change it to the URL for another location, such as an internal support site. (See "Management and Support URLs" on page 6-75.)

2. Click here for HP support information and OS downloads.

1. Click here.



Figure 6-53. The Support Window

Configuration Reference





# Troubleshooting

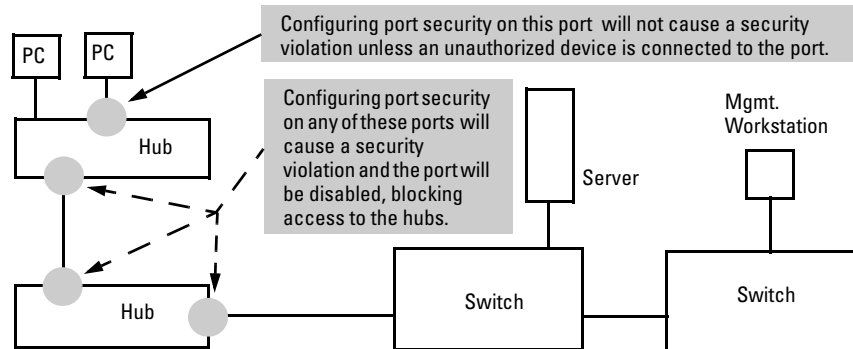
The hub's proactive features are designed to find common network problems, to notify you, and to fix or limit them. To monitor this activity, you should periodically view the Alert Log in the Status | Overview window of the hub's web browser interface. For more information, see chapter 4.

**Problem: "I forgot the hub's password."**

**Solution:** Clear the user name and password by pressing and holding the hub's Clear button for 10 seconds.

**Problem: "I can't communicate with the hub."**

**Solution:** Begin by looking for the closest and furthest instances of the failure. If the ping test and link test both fail, try using HP TopTools maps to find the devices that can't be reached. Check the closest device for configuration problems such as port security configured on a port that has multiple devices connected. (Such a port has multiple addresses connected, and will immediately create security violations if security is configured, resulting in the port being disabled. See figure 7-1 on the next page.) Also, check the Alert logs on any devices that have them, and for device failure. It may be that another HP ProCurve device has disabled the connection to your hub due to excessive errors that impacted the rest of the network. If the closest device is operating properly, then check devices further away.



**Figure 7-1. Example of Correct and Incorrect Hub Port Security Configurations**

**Problem: "My network is really slow."**

**Solution A:** Ensure that a fixed, full-duplex device has not been attached to any of your hubs. (Hub ports are half-duplex—HDx—only.)

**Solution B:** Ensure that you do not have any loops in your network (more than one active path between two nodes). The Spanning Tree Protocol (STP—which is available on switches and other devices that support it) and HP ProCurve's "Find, Fix, and Inform" capabilities can help detect and, if you choose, resolve network loops.

**Solution C:** For all 100T connections, ensure that you are using Category 5 cabling that passes cable testing requirements.

**Solution D:** If you are using 100T connectors, ensure that you are not exceeding 100T topology limitations. They are a maximum of:

- 100 meters from end node to hub.
- 5 meters from hub to hub.
- 205 meters end-to-end distance.
- One level (two hubs) of cascading between any two end nodes.

**Problem: "My 10T nodes can't communicate."**

**Solution:** If no devices on your 10T segment can communicate, this may be due a hub port being configured (forced) into a 10Mbps-only mode (instead of the default Auto-negotiation mode), and then mistakenly connected to a 100T-only port on another device.

To verify, look for a hub that has the Activity and Collision LED on solid. Slowly unplug and replug each connection on the hub until you find a connection that, when unplugged, causes the LEDs to return to their normal (flickering) state. This indicates the mismatched connection. To remedy the situation, plug the connection into a port that supports the 100Mbps mode.

**Problem: "The hub's fault LED is on."**

**Solution:** Attach a console session to check for any display which might identify the error. If the error is that the hub's operating system (OS) has been corrupted, try downloading the OS again. (The hub will typically recover fully after the new OS has been downloaded and the hub rebooted.) If this does not

solve the problem, or if you cannot start a console session even after resetting the hub, contact your HP reseller for assistance or see the Support/Warranty booklet shipped with the hub.

**For More Troubleshooting Information.** See the *Installation Manual* you received with your hub for LED indications of problem conditions, and other troubleshooting information.



---

# Index

## Symbols

=> prompt ... 3-6, 3-10

## Numerics

100T hub segment ... 6-45, 6-46

10T hub segment ... 6-45, 6-46

## A

access level configuration tasks ... 1-3

access levels

device ... 6-28

different ... 6-28

Active button ... 4-13

Active tab ... 4-13

address selection ... 6-18

assigned ... 6-50, 6-51

continuous ... 6-50

first heard ... 6-50

methods ... 6-50

address, network manager ... 5-2

Advanced Configuration menu ... 6-39

alarm, destinations ... 6-51

alarm, send ... 6-49

Alert log ... 4-6, 4-13, 4-16, 4-25, 7-1

AnnounceAddress function ... 6-29

ASCII Console Interface

accessing ... 3-10

command prompt ... 3-7, 3-11

ASCII terminal ... 2-2

assigned address selection ... 6-50, 6-51

Gauges area, attributes ... 4-15

authorized manager ... 5-2

authorized manager list ... 6-18

limit ... 6-30

Authorized Managers screen ... 6-22

about ... 6-30

IP security mask ... 6-31

Manager IP Address column ... 6-30

Auto neg

See *Auto-negotiate*.

auto-discovery ... 5-2

Auto-negotiate ... 4-25, 6-9, 6-56

auto-partition ... 4-18

## B

backup link ... 4-22, 6-39

about ... 6-52

caution ... 6-58

field ... 6-53

link, add ... 6-53

link, delete ... 6-53

link, transition ... 4-18

MAC Address field ... 6-53

number of failures before backup ... 6-53

primary and secondary links ... 6-52

Primary Port field ... 6-53

screen ... 6-52, 6-53

Status field ... 6-53

Test Time field ... 6-53

window ... 6-54

Bootp ... 2-1–2-2, 4-23, 5-1, 6-23–6-25

configuration, automatic ... 2-2

example table entry ... 6-26

obtaining an IP Address ... 6-23

bootstrap protocol ... 6-25

bridge counters ... 6-5

bridge, enable/disable ... 4-22, 6-45

broadcast packets ... 6-15

Broadcast Packets counter ... 6-12

broadcast, thresholds ... 4-16

Browse Hub Configuration ... 6-65

Browse Hub Configuration option ... 6-60

Browse Hub Configuration screen ... 6-65

web browser interface

Active button ... 4-13

Active tab ... 4-13

elements ... 4-12

Gauges area ... 4-13

Status bar ... 4-13, 4-16

status indicator ... 4-16

system requirements ... 4-2

understanding ... 4-12

where to run ... 4-2

## C

- Clear button ... 3-7, 4-9-4-10, 7-1
- Clear Security Intruder Log screen ... 6-5
- Collisions ...
  - collisions ... 4-14, 6-1, 6-15
  - Collisions counter ... 6-12
  - collisions, thresholds ... 4-16
- command prompt ... 6-74
- community names ... 6-28
  - Authorized Manager assignment ... 6-29
  - compared to a password ... 6-28
  - definition ... 6-28
  - different access levels ... 6-29
  - different combinations ... 6-29
  - Discovery ... 6-29
  - Discovery Write Settings mapped to user level ... 6-29
  - full write setting mapped to user level ... 6-29
  - Manager level ... 6-29
  - none ... 6-29
  - normal level ... 6-29
  - read privileges ... 6-28
  - reasons for setting ... 6-28
  - Restricted Write setting mapped to user level ... 6-29
  - screen ... 6-22
  - table of Read-Write combinations ... 6-29
  - user levels ... 6-29
  - User Read setting mapped to user level ... 6-29
  - write privileges ... 6-28
- Community Names screen ... 6-28
- Community Names settings ... 6-29
- configuration
  - backup links ... 6-54
  - browse hub configuration ... 6-67
  - DHCP/Bootp ... 2-2
  - download ... 6-70
  - factory default ... 2-1, 3-1, 6-39, 6-55
  - factory default, caution ... 6-58
  - IP options ... 6-23
  - IP, disable ... 6-24
  - IP, manual ... 6-24
  - port security ... 6-48
  - port speed ... 6-39
  - report ... 4-23
- Configuration Report window ... 6-67
- configure SNMP ... 5-3
- Console Password screen ... 6-22, 6-32

- console port ... 2-2, 3-3
- console, timeout ... 6-37
- continuous address selection method ... 6-50
- counters ... 6-5, 6-11
- counters, global ... 6-14
- CRC Alignment Errors counter ... 6-12
- CRC/Alignment Errors ... 6-11, 6-15
- Critical Severity Region, Gauges area ... 4-15

## D

- default router ... 2-3
- default, factory
  - See *configuration*.
- device fault ... 6-7, 6-41
- Device Passwords window ... 4-7
- Device View window ... 6-42
- DHCP ... 2-1-2-2, 4-23, 6-23, 6-25
  - using ... 6-27
- Diagnostics menu ... 6-60
- Diagnostics screen ... 6-4
- disable bridge ... 4-22, 6-45
- discovery ... 6-29
- DNS ... 4-3, 6-75
- download version ... 6-6, 6-41
- download, TFTP ... 6-70
- download, XMODEM ... 6-72

## E

- eavesdrop detection ... 6-51
- eavesdrop prevention ... 6-49
- eavesdrop prevention caution ... 6-49
- enable bridge ... 4-22
- enter user name prompt ... 3-10
- errors, threshold ... 4-16
- events, very long ... 6-12

## F

- factory default configuration ... 4-23, 6-39
  - See also *configuration*.
- factory reset ... 4-23
- Factory Reset window ... 6-59
- fault detection ... 4-7
- fault-detection policy ... 4-7, 4-25, 4-26
- fault-detection window ... 4-26
- fault-detection, settings ... 4-27

- fault-finder ... 6-20
- fault LED ... 7-2
- FCS ... 6-15
- first heard, address selection ... 6-50, 6-51
- fragments ... 6-15

## G

- gateway ... 6-23, 6-24
- gateway router ... 2-6
- gauge needle, Gauges area ... 4-15
- gauge, color ... 4-24
- gauge, value range ... 4-16
- Gauges area
  - attributes ... 4-15
  - Critical Severity region ... 4-15
  - high watermark indicator ... 4-15
  - needle ... 4-15
  - normal activity region ... 4-15
  - severity regions ... 4-16
  - warning severity region ... 4-15
  - web browser interface ... 4-13
- Gauges area elements ... 4-15
- General System Information screen ... 6-5, 6-40
- global counters ... 6-5, 6-14

## H

- help, online ... 4-11, 6-75
- help, online inoperable ... 4-11
- help, online, not available ... 6-76
- High Watermark Indicator
  - Gauges Area ... 4-15
- HP FTP Library Service ... 6-70
- HP proprietary MIB ... 5-2
- HP TopTools for Hubs & Switches
  - See *TopTools*.
- HP web browser interface
  - See *web browser interface*.
- hub configuration ... 6-3

- hub console
  - advantages ... 1-3
  - baud rate ... 3-3
  - command prompt region ... 3-6
  - communication parameters ... 3-3
  - connecting with a serial cable ... 3-3
  - Console port ... 3-3
  - flow control ... 3-3
  - menu system ... 3-6
  - parity ... 3-3
  - running through Telnet ... 3-5
  - stop bit ... 3-3
  - terminal configuration, bits per character ... 3-3
  - terminal emulation ... 3-3
- Hub Port Counters screen, about ... 6-12
- Hub Status and Counters screen ... 6-3

## I

- ICMP packets ... 6-61
- Identity window
  - about ... 6-7, 6-54
  - viewing ... 6-7, 6-54
- IEEE 802.2 test packets ... 6-63
- in-band ... 2-1, 3-2
- Internet Control Message Protocol ... 6-61
- intruder address ... 6-18
- intruder log ... 6-18
- intruder prevention ... 6-50
- intrusions, insignificant ... 6-18
- IP address ... 2-1, 2-3, 4-23, 6-23
  - configuration screen ... 2-6, 6-22–6-23
  - default router ... 2-3
  - format ... 2-3
  - global assignments ... 6-25
  - globally assigned addressing ... 6-27
  - needed for Telnet access to hub console ... 3-2
  - requirement for Telnet ... 3-5

See also *Bootp* and *DHCP*.  
setting manually ... 6-23  
SNMP ... 5-1  
subnet mask ... 2-3  
time to live ... 2-3  
using Bootp ... 6-25  
using DHCP ... 6-27  
using for web browser interface ... 4-3  
gateway column ... 6-24  
subnet mask column ... 6-24  
IP packets  
testing ... 6-61  
IP security mask ... 6-31

## J

Jabbers ... 6-15  
Java ... 4-3-4-4  
JavaScript ... 4-3

## L

last heard source address ... 6-9  
Late Collisions counter ... 6-12  
LED, clear flashing ... 6-20  
link beat ... 6-44  
link status ... 6-9  
link test ... 6-60  
about ... 6-60, 6-63  
link test ... 4-23, 6-63  
links, primary and secondary ... 6-52  
log file, configuration information ... 6-66  
loop ...  
loop, network ... 4-18, 7-2  
loss of link ... 6-56  
lost password ... 4-9

## M

MAC Address ... 6-7, 6-41  
Main Menu ... 2-4, 6-3  
launching ... 3-10  
management server URL default ... 4-11  
Management Access Configuration menu ... 6-22  
Management Access Configuration screen ... 6-3  
Management URL window ... 6-75  
Manager Address field ... 5-2  
manager intrusions ... 6-18

manager password ... 4-7, 4-9  
manager, authorized ... 5-2  
ME command ... 3-10  
MIB II ... 6-40  
MIB, HP proprietary ... 5-1  
MIB, standard ... 5-1  
Microsoft Internet Explorer ... 4-3  
modem ... 3-4  
multicast packets ... 6-15  
multicast, threshold ... 4-16  
multiple configuration information  
sending to a log file ... 6-66

## N

Netscape ... 4-3  
network loop ... 4-18, 7-2  
network management functions ... 5-2  
network manager address ... 5-2  
Number of Failures, Backup Links screen ... 6-53

## O

online help ... 4-11, 6-75  
online help, not available ... 6-76  
operator password ... 4-7, 4-9  
OS version ... 6-73  
OS download, TFTP ... 6-70  
OS download, XMODEM ... 6-72  
OS updates ... 6-70  
out-of-band ... 1-3, 3-2  
overwrite password or user name ... 4-8

## P

packets, very long ... 6-12  
password ... 4-7, 4-9  
creating ... 4-7  
creating from the web browser interface ... 6-32  
delete ... 4-9  
entering at the command prompt ... 3-6, 3-11  
if you lose the password ... 4-9  
lost ... 3-7, 4-9,  
manager ... 4-7, 6-32, 6-33  
operator ... 4-7, 6-32  
overwrite ... 4-8  
setting ... 4-8  
using to access browser and console ... 4-9



- ping test ... 4-23, 6-60, 6-61
- Ping/Link Test window ... 6-62
- policy, security ... 6-50
- Port Enable/Disable screen ... 6-42
- port intrusions ... 6-18
- Port Number ... 6-8
- port security
  - eavesdrop detection ... 6-51
  - intruder prevention ... 6-50
- Port Security screen ... 6-18, 6-47
  - address selection ... 6-18
- port security, configuring ... 6-48
- port speed ... 6-9
- port speed configuration ... 6-39
- port speed, caution ... 6-56–6-57
- port state color key ... 6-44
- port status ... 6-8, 6-10, 6-42 6-44
- Port Status screen, about ... 6-8
- port, disabled ... 4-25, 4-26, 6-49
- port, speed-reduced ... 4-25, 4-26
- primary port, Backup Links screen ... 6-53
- problems ... 7-1
- Procurve web site ... 6-70
- proprietary MIB ... 5-2
- public ... 6-29
- public SNMP community ... 5-2

## R

- read-only privileges ... 6-28, 6-32
- read-write privileges ... 6-33
- reboot ... 4-23
- Reboot Hub option ... 6-68
- redundant link ... 6-39
- reinitializing hub counters ... 6-58
- reset hub to Factory Default ... 6-58
- resetting the hub from the web browser
  - interface ... 6-58, 6-59
- RFC 1213 ... 5-2
- RFC 1515 ... 5-1
- RFC 1573 ... 5-1
- RFC 1757 ... 5-1
- RFC 1907 ... 5-2
- RFC 2037 ... 5-2
- RFC 2108 ... 5-2
- RMON ... 5-1
- router, default ... 6-25
- router, gateway ... 2-6

- router,default ... 2-3
- RS-232 ... 1-3, 2-2

## S

- security ... 1-2, 4-10, 6-37, 6-47
- security information ... 6-9
- Security Intruder log
  - about ... 6-17
  - intruder address ... 6-18
  - manager intrusions ... 6-18
  - number of violations displayed ... 6-18
  - port information ... 6-18
  - port intrusions ... 6-18
  - SNMP security information ... 6-18
  - violation time ... 6-18
  - violator address ... 6-18
- Security Intruder Log screen ... 6-5
- security policy ... 6-50
- security-flashing LED, clear ... 6-20
- segment status ... 6-10
- segments, external connection ... 6-45
- serial number ... 6-7, 6-41
- Serial Timeout screen ... 6-37
- severity of intrusions ... 6-18
- SNMP ... 2-1, 5-1, 6-29
  - configure ... 5-3
  - IP address ... 5-1
  - traps ... 5-1
  - v1 agent ... 5-1
- SNMP agent ... 6-18
- SNMP communities ... 5-3
- SNMP management ... 5-1
- SNMP public community ... 5-2
- SNMP v2 Notifications ... 5-1
- SNMP, configuration ... 5-3
- spikes ... 6-11
- standard MIB ... 5-1
- status bar ... 4-24
- Subnet Mask ... 6-24
- subnet mask ... 2-1, 6-23
- Support URL window ... 6-75
- system contact ... 6-6, 6-40
- system location ... 6-6, 6-40
- system name ... 6-6, 6-40
- system requirements,
  - web browser interface ... 4-2
- system up time ... 6-7, 6-41

## T

- Telnet Enable/Disable screen ... 6-35
- Telnet ... 1-3, 3-5, 3-7
  - accessing the hub console ... 3-2
- Telnet console session
  - establishing ... 3-5
- Telnet Enable/Disable screen ... 6-22
- terminal emulator,
  - configuration ... 3-3
- TFTP OS download ... 6-70
- threshold setting ... 5-2
- thresholds ... 4-16
- time to live ... 2-3, 6-24
- topology limitations ... 7-2
- TopTools system requirements ... 1-1
- TopTools access ... 4-3
- Total Octets ... 6-14
- Total Packets ... 6-14
- traffic monitoring ... 5-2
- troubleshooting ... 4-18, 6-45–6-46, 7-1
  - using the Diagnostics options ... 6-60

## U

- unauthorized access ... 3-7
- unauthorized device ... 6-18
- unauthorized manager ... 6-18
- URL ... 4-10
- URL, management and support ... 6-75
- user name
  - creating from the web browser interface ... 6-32
  - manager ... 6-32
  - operator ... 6-32
  - overwrite ... 4-8
  - using for browser or console access ... 4-7
- using the passwords ... 4-9
- usnames
- utilization, thresholds ... 4-16
- Utilization attribute, Gauges area ... 4-13

## V

- Valid Packets counter ... 6-12
- version, OS ... 6-73
- very long events ... 6-12
- very long packets ... 6-12
- violation time, Security Intruder log ... 6-18

- violator address

- Security Intruder log ... 6-18

## W

- warranty ... ii
- web agent, advantages ... 1-2
- web agent enabled ... 4-1
- web browser interface ... 2-1
  - access parameters ... 4-7
  - advantages ... 1-2
  - backup links, configuring ... 6-54
  - bridge enable/disable ... 6-46
  - browse hub configuration ... 6-67
  - clear port intrusion LED ... 6-21
  - configuration, support URL ... 4-10
  - disable access ... 4-1
  - enabling ... 4-3
  - first-time install ... 4-6
  - first-time tasks ... 4-6
  - help via TopTools ... 4-10
  - IP addressing ... 6-25
  - management server URL ... 4-10
  - online help ... 4-10
  - online help, inoperable ... 4-11
  - password ... 4-8
  - password lost ... 4-9
  - password, setting ... 4-8
  - port security, configuring ... 6-48
  - port state color key ... 6-44
  - port status ... 6-10
  - ports, enable/disable ... 6-43
  - security ... 4-1
  - security intruder log ... 6-19
  - segment status ... 6-10
  - URL default ... 4-11
  - user name ... 4-8
- Web enable/disable screen ... 6-36
- web site, HP ... 5-2
- Windows 95 ... 2-2
- Windows NT ... 2-2
- world wide web site ... 5-2
- Write privileges ... 6-28

## X

- Xon/Xoff ... 3-3





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 01/99

Manual Part Number  
5967-9933

