HEWLETT® PACKARD

HP ProCurve 10Base-T Hubs

Management and Configuration Guide

HP 10Base-T Hub 12M
HP 10Base-T Hub 24M

HP Networking

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

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

Less Work, More Network

HP ProCurve 10Base-T Hubs

Management and Configuration Guide

Publication Number

5967-6862
June 1998

Applicable Product

HP ProCurve 10Base-T Hub 12M (J3301A)

HP ProCurve 10Base-T Hub 24M (J3303A)

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 warranty booklet and the registration form included with the product.

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

Hewlett-Packard Company
8000 Foothills Boulevard, m/s 5552
Roseville, California 95747-5552
http://www.hp.com/go/procurve

Contents

About Hub Management Interfaces

This chapter describes the following topics:

- understanding hub management interfaces for manageable HP ProCurve 10Base-T Hubs
- advantages of using each interface

Understanding Hub Management Interfaces

The interfaces enable you to reconfigure the hub and to monitor hub status and performance.

Manageable HP ProCurve 10Base-T Hubs provide the following interfaces:

- the Web Browser Interface --an interface that can be accessed using a standard Web browser (Netscape Navigator or Microsoft Internet Explorer)
- the hub console--an ASCII console interface
- HP Top Tools for Hubs and Switches--a Microsoft Windows and Unix SNMP graphical user interface

Note

The interfaces only apply to the manageable HP ProCurve 10Base-T Hubs:

- HP J3301A 10Base-T Hub 12M
- HP J3303A 10Base-T Hub 24M

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

See chapter 2 for information on connecting up and using the hub console. Chapter 4 tells you how to use the Browser Interface. Chapter 6 is a management screen reference for both the Browser Interface and the hub console.

For coverage of HP Top Tools for Hubs and Switches, see the *HP Top Tools for Hubs and Switches User's Guide* or the online help available with that product. HP HP Top Tools for Hubs and Switches comes on a separate CD-ROM with the HP ProCurve 10Base-T Hubs that have built-in SNMP management capabilities.

Advantages of Using the Browser Interface

The following are advantages of using the Browser Interface:

- **easy access** of the hub from anywhere on the network, if you know the device IP address
- **familiar browser interface**–locations of window objects consistent with known standard
- **faster configuration**, avoiding cycling through a series of prompts—enables less keystrokes, using mouse clicking for navigation; no terminal setup and console menu access necessary
- **many features have all their fields in one scree**n so you can view all values at once (the console scrolls through a series of prompts)
- **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

Advantages of Using the Hub Console Interface

The following are advantages of using the hub console:

- **more comprehensive set of features** to work with than the Browser Interface
- **out-of-band access** (through RS-232 connection) to hub, so is not affected by network bottlenecks, crashes, and downtime
- **management access configuration**, for example, creating an IP address, and setting Community Names and Authorized Managers
- **several environment access variables available** for setting, for example Web and Telnet access
- **rebooting the hub** is available
- **faster navigation**, avoiding having to wait for slower display of graphical objects over a browser interface

HP Top Tools for Hubs and Switches

The manageable HP ProCurve 10Base-T Hubs enable you to use HP Top Tools for Hubs and Switches. Operate HP Top Tools for Hubs and Switches from a PC on the network to monitor traffic and manager your hubs and switches. Easy to install and use, HP Top Tools for Hubs and Switches (formerly HP ASA) is the answer to your management challenges.

Network Devices:

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

Network Traffic:

- Shows traffic and “top talker” nodes right on screen.
- Traffic monitor diagrams make bottlenecks easy to see.
- Real-time fault isolation improves network reliability.
- See your entire network without having to put RMON probes on every segment (up to 50 segments).

Network Growth:

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

Running the Hub Console

This chapter describes the following topics:

- overview of the hub console
- starting a hub console session
  - through a direct out-of-band serial connection
  - through a modem out-of-band serial connection
  - through an in-band Telnet connection
- using the hub console
  - the two console regions
  - the command prompt region
  - the menu system

Overview of the Hub Console

The hub console interface enables you use a PC, running a terminal emulator, or a standard ASCII terminal to do the following:

- modify the hub's configuration
- configure the hub with an IP address that enables the hub to be managed from an SNMP-based network management station, through the hub's Browser Interface, described in chapter 4, "Running the Browser Interface", or through Telnet access to the console interface.
- control console security by configuring passwords
- monitor the hub and its port status
- monitor the network activity through a set of counters
- download new software to the hub

Note

The 10Base-T hubs are "plug-and-go" network devices. They are shipped with a factory default configuration that will work for most network situations. All the hub ports are enabled, and the DHCP/BOOTP is enabled so the hub can 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, but you can use the console for the uses listed above.

Starting a Hub Console Session

The hub console interface can be run on a PC that has a terminal emulator program, or on a standard ASCII or ANSI terminal. You can connect the console to the hub in the following ways:

- directly, through an out-of-band RS-232 serial connection (using a serial cable)
- remotely, using an out-of-band modem connection
- over the network (in-band) through a Telnet session (requires that the hub have an IP address)

Starting a Session Through a Direct Serial Connection

To serially connect a console to a hub, follow these steps:

1. Connect an 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 10Base-T 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 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 some hub version information followed by the message:

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

   and the => prompt is displayed. 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 username 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" at the end of this chapter.

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

For more information on the commands, see "The Command Prompt Region" on page 2-7. For information on the console menus, go to the section, "The Console Menu System" on page 2-9.

Starting a Session Through a Modem Connection

To establish a remote session, using a pair of modems and terminal, follow these steps:

1. Use full-duplex, asynchronous (character-mode) modems only. For the list of supported modems and their initialization strings, go to the HP networking products web page, **http://www.hp.com/go/procurve**. Then, select Support and from the Support page, select 10Base-T hubs. On the 10Base-T hubs page, select Modem Configuration.
2. Initialize both modems according to the initialization strings found on the web page.
3. 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 10Base-T Hubs Installation Guide*.
4. At the remote site, connect the modem for the console end to the serial port on the PC or terminal.
5. 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.
6. Press [Enter] a few times until the console displays some hub version information followed by the message:

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

   and the => prompt is displayed. 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 username 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" at the end of this chapter.

You are now in the command prompt region of the console interface. You can enter `HE` 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

The HP ProCurve 10Base-T Hubs support accessing the hub console over Telnet.

Note

Running a Telnet session with the hub requires that the hub first be configured with an IP address. If you have not set an IP address for your hub, go to one of the previous two procedures to first start an out-of-band console session through which you can set an IP address on the hub. The hub ships with DHCP/BOOTP enabled, though, so if you have a properly configured server on your network, the hub will automatically acquire an IP address from the server.

To establish a Telnet session, follow these steps:

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 the hub accessibility.) Go to the IP Address reference page in chapter 6 for details on setting an IP address.
2. 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 name resolution system such as Domain Name Server--DNS.)

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

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

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

For more information on the commands, see “The Command Prompt Region” on page 2-7. For information on the console menus, go to the section, “The Console Menu System” on page 2-9.

To end the Telnet session, select `Logout` from the console Main menu to terminate the console session, and then use your Telnet application’s command to close or quit the Telnet session.

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. The hub console consists of two regions as described in the next section.

The Console's Two Regions

The hub console interface has two regions:

- **the Command Prompt region** which you enter at first. This region enables you to perform tasks by issuing commands. For details on using commands in this region, see Table 2-1.
- **the Menu System region** which you access by entering `ME` from the command prompt. The menus enable you to configure hub, port, and network settings through screens that contain fields and prompts. See "The Console Menu System" later in this chapter, and for details on each of the menus in this region, see chapter 6.

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. These commands are detailed by entering `HE` at the command prompt. Figure 2-1 shows a sample Command Prompt screen where the hub's product number and firmware information is displayed by the ID command.

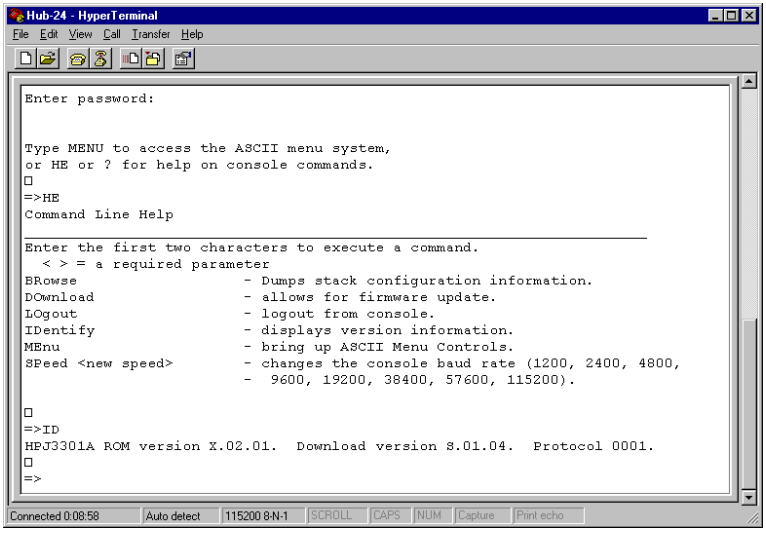


Figure 2-1. Command Prompt Screen Displaying Help and ID Commands

Commands Available

The available commands in the Command Prompt region are shown in the following table.

Table 2-1. Commands Issued from the Console Command Prompt.

Command	Command Name	Description
DO	Download	Downloads new versions of hub firmware from a firmware server.
HE	Help	Displays some basic help on all console commands.
ID	Identify	Displays firmware revision number, for example, `X.02.01`.
LO	Logout	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 firmware.
SP	Speed	Enables you to set the Baud Rate for an out-of-band connection with the hub.

The Console Menu System

The hub console menu system starts at the Main Menu, which contains access to the top level menus for the program. The top level menus contain all the necessary options, grouped by common topic. These menus 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 get into the hub console's menu system, enter `ME` at the command prompt. The Main Menu will be displayed as shown in figure 2-2.

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

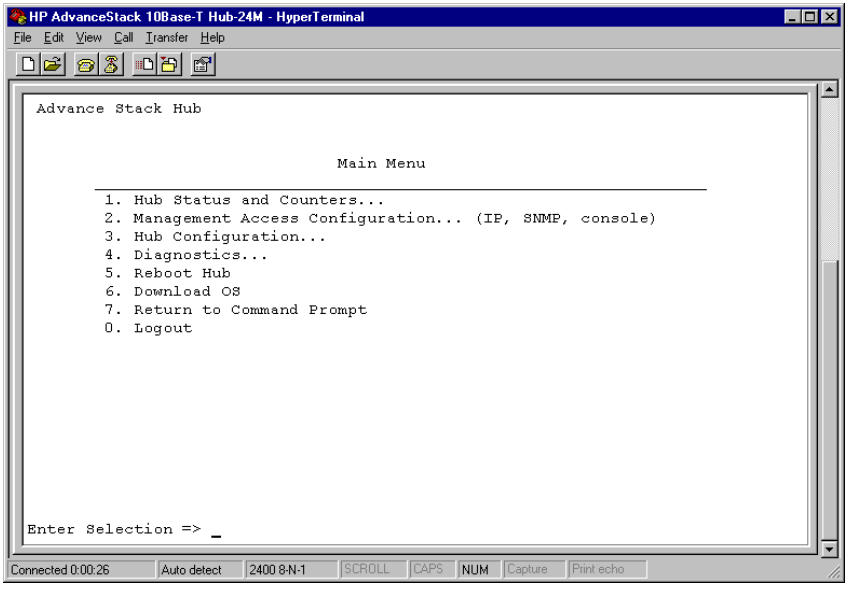


Figure 2-2. The Hub Console Main Menu.

Responding to an `Enter username` Prompt

If the interface displays an Enter username prompt, you need to provide proper device access strings to reach the Command Prompt (=>). To reach the Command Prompt, perform the following steps:

1. Type in the string required at the `Enter username` prompt and press Enter. The console displays a `Password` prompt. If you typed the wrong user name, the interface displays the following message:

   ```
   Username incorrect
   ```

   Check to see if you have typed the username incorrectly. If you have typed it correctly, check with your network administrator to see if you are using the proper username. The interface allows for three retries before disconnecting.

2. Type in the password string required at the `Password` prompt. Note that, when entered, the password string is not displayed on the screen for security reasons. If you typed the wrong password string, the interface displays the following message:

   ```
   Password incorrect
   ```

   Check to see if you have typed the username and password incorrectly.

   - If you have typed these strings incorrectly, check with your network administrator to see if you are using the proper password. The interface allows three retries before disconnecting.
   - If you typed these strings correctly, the interface displays a => prompt as shown in figure 2-3.

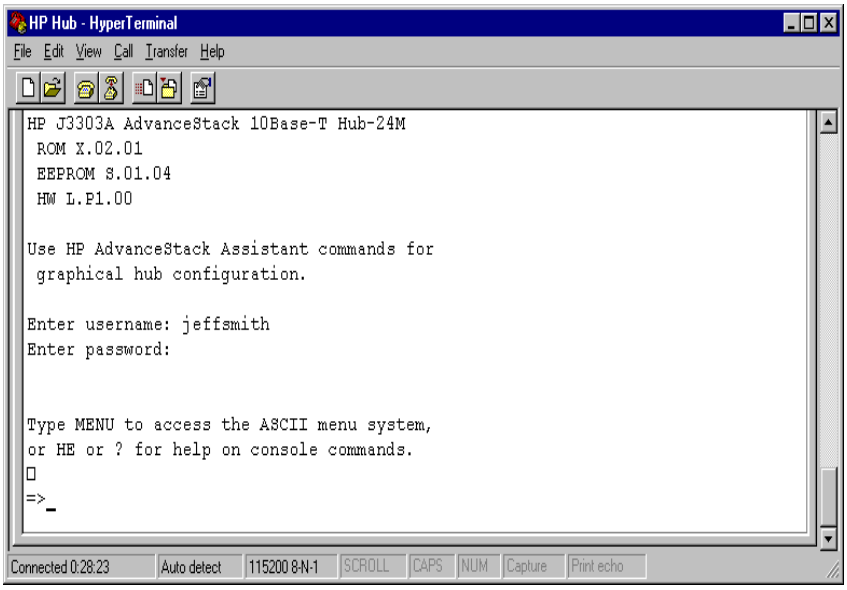


Figure 2-3. A Password Issuing Session

Note

If you cannot retrieve either the hub's username or password, you can remove it 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.

If you want to change your password and username, go to the Password option under the Management Access Configuration Menu. For details on process, see the reference page in Chapter 6 of this guide for Passwords.

Setting an IP Address for the Hub

This chapter explains the following topics:

- communication between the hub and network management
- globally assigned IP network addresses
- IP configuration parameters
- ways of setting an IP address
  - setting an IP address from the Hub Console Interface
  - setting an IP address using BOOTP/DHCP

Communication Between the Hub and Network Management Station

The manageable HP ProCurve 10Base-T Hubs can be managed over the network by both a World Wide Web browser application and a network management software application that complies with the Simple Network Management Protocol (SNMP) standard and has standard SNMP MIB-browser functionality.

The communication between the SNMP network management station and the hub takes place using the network layer protocols. (IP for TCP/IP networks).

The network layer communications require that the hub have a network layer address. This chapter provides some background information on IP addressing and the procedures for assigning an IP address to the hub.

Globally Assigned IP Network Addresses

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

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

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

IP Configuration Parameters

List all the manageable devices on your network and their IP configuration. Make sure that every manageable device has a unique IP address. Make sure that all manageable devices on the network have the same subnet mask.

The IP configuration parameters are as follows:

IP Address: The IP address of the hub is written in the format X.X.X.X, where each X is a decimal number between 1 and 254. Every IP address on a network must be unique.

Subnet Mask: The bit mask defines which portion of the IP address is the subnet address and is written in the format X.X.X.X. The default value is automatically generated and depends on the class of IP address that you entered. See your network administrator for the subnet mask address. All devices on your IP network must use the same subnet mask address.

Default Router: The routing IP address of the nearest router in your network. The default is 0.0.0.0. If no routers are in your network, enter the IP address of your hub.

Time To Live: 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.

Ways of Setting an IP Address

To manage the hub using the Browser Interface or from an SNMP network management station, your hub needs an IP address. Some configuration items in the Hub Console Interface are also not affective unless the hub has an IP address, for example, setting a Community Name and an Authorized Manager list for the hub.

Note

You can manage the hub using the console without having to set an IP address.

The hub can be configured with its assigned IP address in two ways:

- manually through a series of screen prompts in the hub console
- automatically through a BOOTP or DHCP server (console not required)

Once you have set the IP address in the console, you can change it either in the console, Browser Interface, or HP Top Tools for Hubs and Switches. For the Browser Interface, see the reference pages for IP Configuration in chapter 6. For the For HP Top Tools for Hubs and Switches, see the online help in that product.

Manually Setting an IP Address from the Hub Console

To configure the hub with an IP address:.

1. Start a hub console session and at the prompt, enter `ME` to access the menu system region.
2. From the Main Menu, enter `2` to display the Management Access Configuration screen.
3. From the Management Access Management screen, enter `1` to display the IP Configuration Screen shown in figure 3-1.

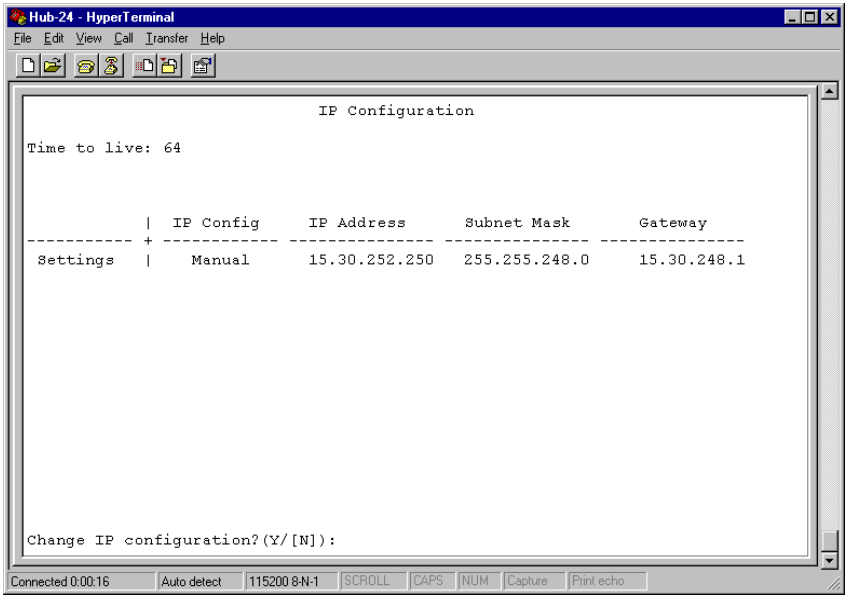


Figure 3-1. The IP Configuration Screen.

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` or `(M)anual Config`.

   DHCP and Bootp are automatic network address selection protocols. See "Automatically Acquiring an IP Address Using Bootp/DHCP" later in this chapter.

5. Enter `M` to manually assign the IP address information. The interface prompts you to enter an IP address, subnet mask, default router address, and time to live. These parameters are defined under "IP Configuration Parameters" earlier in this chapter.

   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.

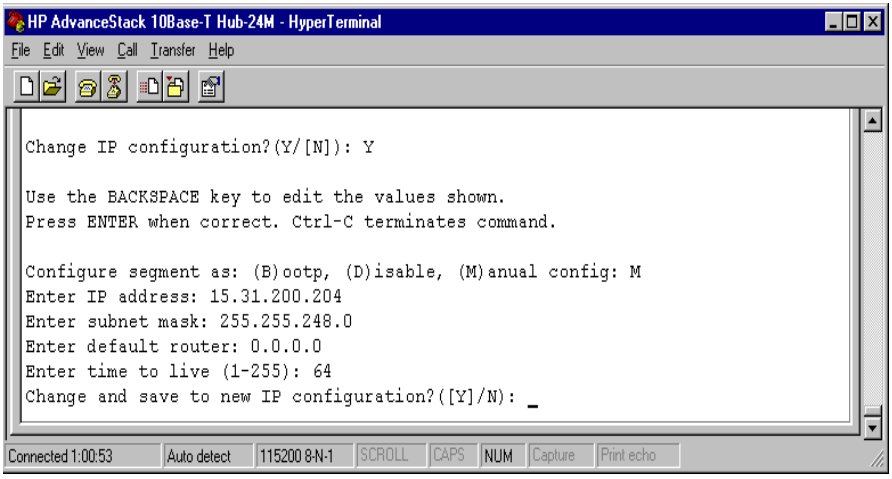


Figure 3-2. Setting an IP Address in the Hub Console.

6. After entering 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.

Your hub is now ready to be managed as a network device through the Browser Interface, or through HP Top Tools for Hubs and 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 Top Tools for Hubs and Switches or HP OpenView, see the online help in those applications.

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 ProCurve 10Base-T Hub-24M would be similar to the following:

```
hphub24M:\
  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:

hphub12M	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.
ht	is the "hardware type" tag. For the HP ProCurve 10Base-T Hubs, set this to **ether** (for Ethernet). *This tag must precede the* **ha** *tag.*
ha	is the "hardware address" tag. Use the hub's 12-digit MAC address.
ip	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.
sm	is the subnet mask of the subnet in which the hub is installed.
gw	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.
vm	is a required entry that specifies the BOOTP report format. *For the HP 10Base-T hubs, you must set this parameter to* **rfc1048**.

Notes for the bootptab file:

- Blank lines and lines beginning with the pound sign (#) are ignored.
- Make sure you 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.
- 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.

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.

Microsoft NT server includes DHCP server software. Consult the NT server online help for information on activating and configuring the DHCP server.

Running the Browser Interface

This chapter details use of the Browser Interface. The following areas are covered:

- system requirements to run the Browser Interface
- places where you can run the Browser Interface
- establishing a Browser Interface session
- working with your first Browser Interface session
- creating usernames and passwords in the Browser Interface
- understanding the Browser Interface environment
- understanding the Gauges Area
- understanding the Alert Log
- understanding the Tab Bar
- setting Fault Detection policy on the Browser Interface

System Requirements to Run the Browser Interface

To run the Browser Interface, you need the following system requirements.

Table 4-1. System Requirements

Platform Entity	Minimum Requirement	Desired Requirement
PC Platform	90 MHz Pentium	120 MHz Pentium
Unix Platform	100 MHz	120 MHz
RAM	16 Mbytes	32 Mbytes
Pixel Count	800 X 600	1,024 x 760
Color Count	256	65,000
Internet Browser	Netscape Navigator 3.0 Microsoft Explorer 4.0	Netscape Navigator 4.0 Microsoft Explorer 4.0
PC Operating System	Microsoft Windows 95 Microsoft Windows NT	Same
Unix Operating System	Standard Unix OS	Same
Internet Application	Javascript 2.0	Same

Places Where You Can Run the Browser Interface

The Browser Interface resides in your Flash RAM. However, unlike the Hub Console Interface, it can be run using less connection types. You can begin a Browser Interface session in the hub in the following ways:

- directly, using an in-band network connection
- directly, using either a network cable or serial cable, running HP Top Tools for Hubs and Switches on a management station

Establishing a Browser Interface Session

To establish a Browser Interface session, perform the following steps:

1. Launch your Web Browser.
2. Enable Javascript/Applets.
   - In Netscape 4.0, click on the Java/Javascript option found under the Security Menu.
   - In Microsoft Internet Explorer 4.0, click on the Settings menu.

   See the online help in your browser for more specific information on how to enable Javascript.
3. Type the IP address of the hub you want to access in the Location field and press Enter. If you are using a Domain Name Server (DNS), your hub may have a friendly name associated with it (for example, Hub20) that you can type in the Location field. See your network administrator for the friendly name associated with the hub.

The Browser Interface first displays the Overview Window under the Status Tab as shown in Figure 4-1. This location is the home window for the Browser Interface or the window you arrive at when you run the Browser Interface. This window has two sections: a Gauges Area, across the top portion of the window, and an Alert Log, in the bottom portion.

Working with Your First Browser Interface Session

Upon accessing the Browser Interface for the first time, the Alert Log will contain one event called `First Time Install`. By clicking on this event, the Browser Interface displays the First Time Install window that provides information about first-time installations. Upon the first session with the Browser Interface, the Alert Log always displays the First Time Install alert as shown in the following figure.

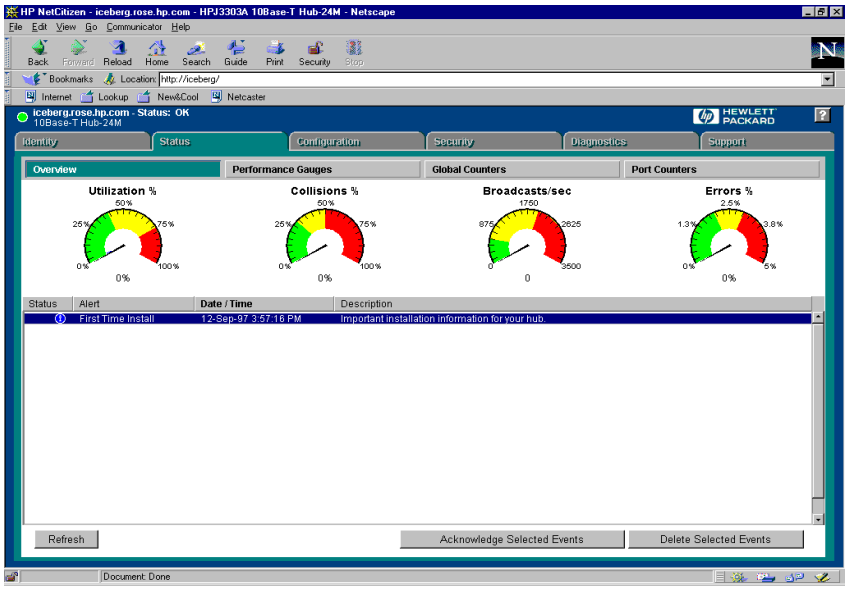


Figure 4-1. The Overview Window during a First Time Install.

Click on the First Time Install alert. The Browser Interface displays the First-Time Install Window.

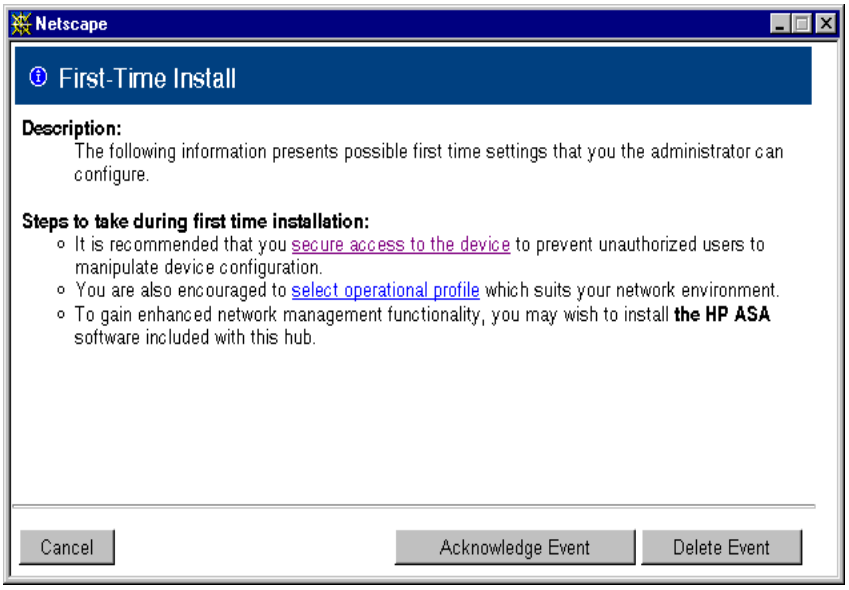


Figure 4-2. The First Time Install Window

This window is the launching point for the basic configuration you need to perform to set Browser Interface access parameters and Fault Detection policy for future use with the Browser Interface. To set Fault Detection policy, click on the jump string `select fault detection` in the second bullet in the window and go to the section, "Setting Fault Detection Policy" later in this chapter. To set Browser Interface access parameters, click on the jump string `secure access to the device` to display the Device Passwords Window and go to the next section.

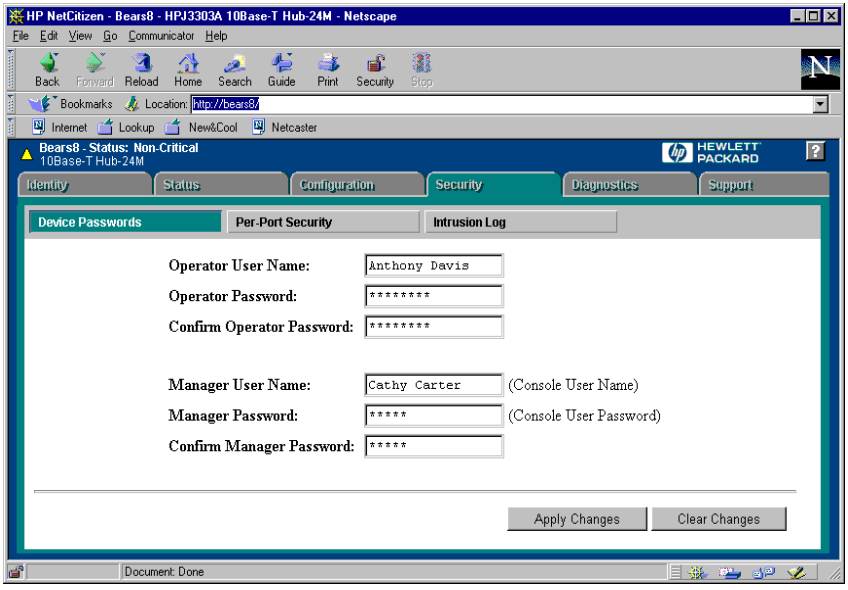


Figure 4-3. The Device Passwords Window

Creating Usernames and Passwords in the Browser Interface

You may want to create both a username and password to create access security for your hub. Note that both a username and password are not required to use the Browser Interface. You can create two types of usernames and passwords:

operator. These strings assign you read privileges for the Browser Interface.

manager. These strings assign you read-write privileges. The manager strings are used as your defaults for Hub Console Interface access. Strings you assign in the manager fields will overwrite previous access strings assigned for both the Browser Interface and the Hub Console Interface.

Creating Operator Usernames and Password

To create an operator username and password, perform the following steps:

1. Click in the Operator User Name box and type a string. The string may be separated by spaces and may include any ASCII character in it. The string may be no longer than 16 characters, including spaces. Spaces are allowed in the string.
2. Click in the Operator Password box and type a string. The string should not have spaces, but may include any ASCII character in it. The string may be no longer than 16 characters. To represent spaces, use the underscore (_) character. The string is not echoed in the window.
3. Click in the Confirm Operator Password box and retype the string to validate your entry.
4. Click on the Apply Changes Button. The Browser Interface stores the username and password information and returns you to the Overview Window.

Creating Manager Usernames and Passwords

To create a manager username and password, perform the following steps:

1. Click in the Manager User Name box and type a string. The string may be separated by spaces and may include any ASCII character in it. The string may be no longer than 15 characters, including spaces. To represent spaces, use the underscore (_) character.
2. Click in the Manager Password box and type a string. The string should not have spaces, but may include any ASCII character in it. The string may be no longer than 16 characters. To represent spaces, use the underscore (_) character. The string is not echoed in the window.
3. Click in the Confirm Manager Password box and retype the string to validate your entry.
4. Click on the Apply Changes Button. The Browser Interface stores the username and password information and returns you to the Overview Window.

Understanding the Browser Interface Environment

Now that you have successfully run the Browser Interface and created a password and username, become comfortable with the environment. The 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 Browser Interface Overview Window is the home environment for any entry into the Browser Interface. The following figure details the different pieces to it.

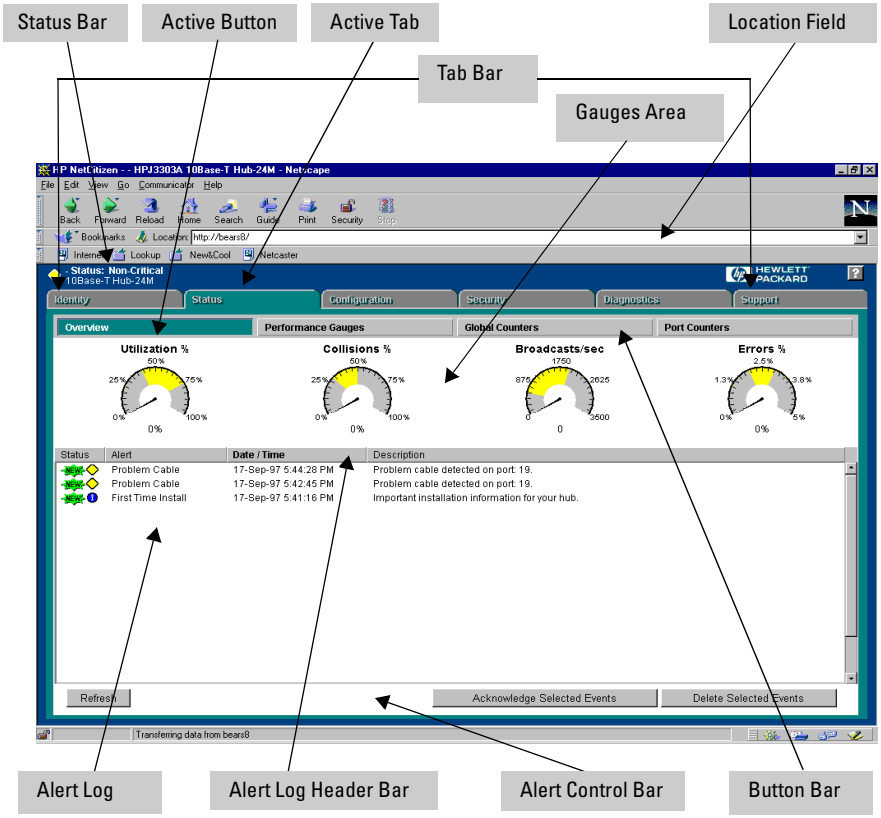


Figure 4-4. The Overview Window

The areas and fields in the Browser Interface Overview Window are detailed here.

Tab Bar. The row of tabs displaying all the Browser Interface Top Level menus.

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

Status Bar. The region above the Tab Bar that displays status and device name information.

Gauges Area. The region containing gauge graphics that indicate performance trends.

Button Bar. The row of buttons that are contained within the Active Button.

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 Log Header Bar. The row of column heads running across the top of the Alert Log.

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 Gauges Area

The Gauges Area contains four separate graphical meters or *gauges* which display values associated with four separate attributes. The Gauges Area, shown across the top of the screen, details performance for the hub based on four attributes. The following figure shows a sample reading of the Gauges Area.

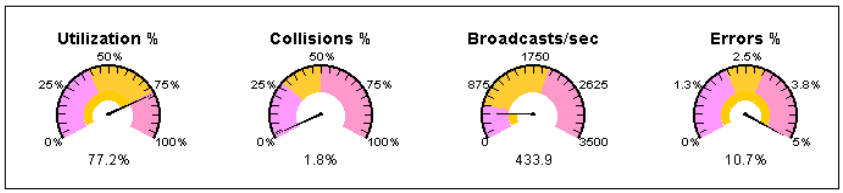


Figure 4-5. The Gauges Area

The attributes are:

Utilization. The amount of network capacity used on the hub, expressed as a percent.

Collisions. The number of Collisions, expressed as a percent of all packets received on the hub.

Broadcasts. The number of Broadcast packets, expressed as an amount per second, collected over a fixed number of seconds.

Errors. The number of Error packets, expressed as a percent of all packets received on the hub.

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

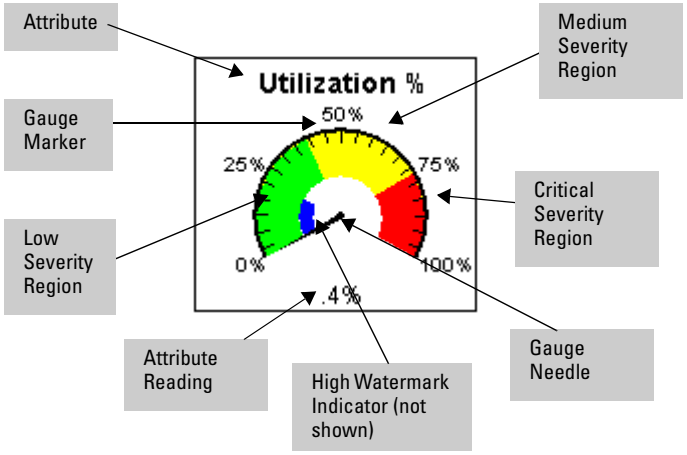


Figure 4-6. Gauge Elements

The objects in the figure are described here.

Attribute. The counter for which the gauge is measuring activity.

Gauge Marker. Refers to the values (0, 25, 60, 75, and 100) that appear around the edge of the gauge. The markers help you get a numerical sense of what percent your activity lies.

Attribute Reading. The current level that the activity of the attribute has reached.

High Watermark 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 Browser Interface displays the Overview Window, the Attribute Reading fields for all four attributes display the string Measuring..., indicating 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 point to a Gauge Marker that reflects the Attribute Reading displayed. Note the three colored regions in the gauge. Note that the three 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 left of the Gauges Area

See Table 4-4 for details on Status Indicator shapes.

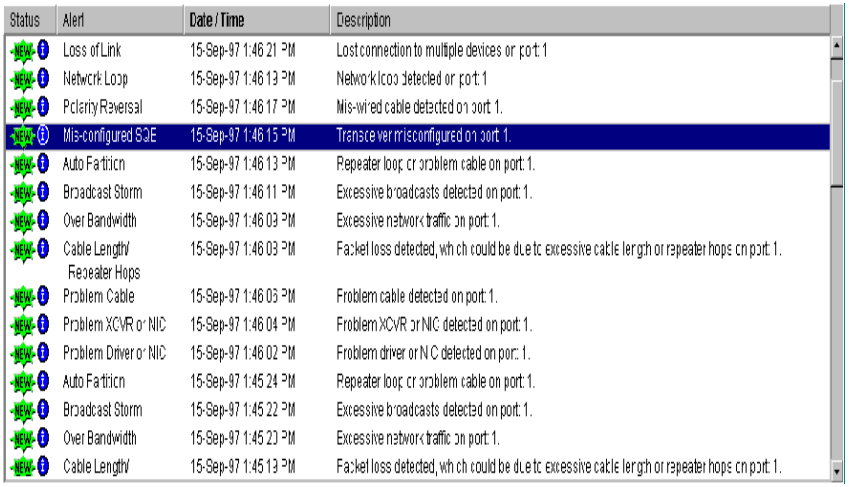
The range of each Gauge Severity Region differs for each attribute. For example, the upper limit of the range for the Normal Activity Region for Utilization is about 40 (percent). The upper limit of the range for the Normal Activity Region for Collisions is just a bit more than 25 (percent). The thresholds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

Table 4-2. Attribute Range Values

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

The Alert Log

The Alert Log, shown in the lower half of the screen, shows a list of network occurrences, or *alerts*, that were retrieved from the hub's MIB. Typical alerts are `Loss of Link`, indicating a severed connection between a hub port and the management station, `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
NEW	Loss of Link	15-Sep-97 1:46:21 PM	Lost connection to multiple devices or port 1
NEW	Network Loop	15-Sep-97 1:46:13 PM	Network loop detected on port 1
NEW	Polarity Reversal	15-Sep-97 1:46:17 PM	Mis-wired cable detected on port 1.
NEW	Mis-configured SQE	15-Sep-97 1:46:15 PM	Transceiver misconfigured on port 1.
NEW	Auto Partition	15-Sep-97 1:46:13 PM	Repeater loop or problem cable on port 1.
NEW	Broadcast Storm	15-Sep-97 1:46:11 PM	Excessive broadcasts detected on port 1.
NEW	Over Bandwidth	15-Sep-97 1:46:09 PM	Excessive network traffic on port 1.
NEW	Cable Length/ Repeater Hops	15-Sep-97 1:46:09 PM	Packet loss detected, which could be due to excessive cable length or repeater hops on port 1.
NEW	Problem Cable	15-Sep-97 1:46:09 PM	Problem cable detected on port 1.
NEW	Problem XCVR or NIC	15-Sep-97 1:46:04 PM	Problem XCVR or NIC detected on port 1.
NEW	Problem Driver or NIC	15-Sep-97 1:46:02 PM	Problem driver or NIC detected on port 1.
NEW	Auto Partition	15-Sep-97 1:45:24 PM	Repeater loop or problem cable on port 1.
NEW	Broadcast Storm	15-Sep-97 1:45:22 PM	Excessive broadcasts detected on port 1.
NEW	Over Bandwidth	15-Sep-97 1:45:21 PM	Excessive network traffic on port 1.
NEW	Cable Length/	15-Sep-97 1:45:13 PM	Packet loss detected, which could be due to excessive cable length or repeater hops on port 1.

Figure 4-7. The Alert Log

Each alert contains the following fields of information:

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

Alert. The specific event name being sent.

Date/Time. The date and time the event was received by the Browser Interface. This value is shown in the format: *`DD-MM-YY HH:MM:SS`* `AM/PM`, for example, `12-Sep-97 3:57:20 PM`.

Description. A short narrative statement that 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.

Alert Types

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

Table 4-3. Alert Strings and Descriptions

Alert String	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 on port. Packet loss detected, which could be due to excessive number of gateways to traverse.
Over Bandwidth	Excessive network traffic on port.
Broadcast Storm	Excessive broadcasts detected on port.
Auto Partition	Port has shut down because it detected a collision on 32 consecutive transmission tries.
Misconfigured SQE	Transceiver misconfigured on port.
Polarity Reversal	Miswired cable detected on port.
Network Loop	Network loop detected by hub. Network loop detected on port.
Loss of Link	Lost connection to multiple devices on port.

Working with Detail Views

By clicking on Alert Entries, the Browser Interface displays a Detail View or separate window detailing information about the events. The Detail View contains a description of the problem and a possible solution. It also provides 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 which polls the hub again to determine whether or not the error can be regenerated.

A sample Detail View describing a Polarity Reversal alert is shown here.

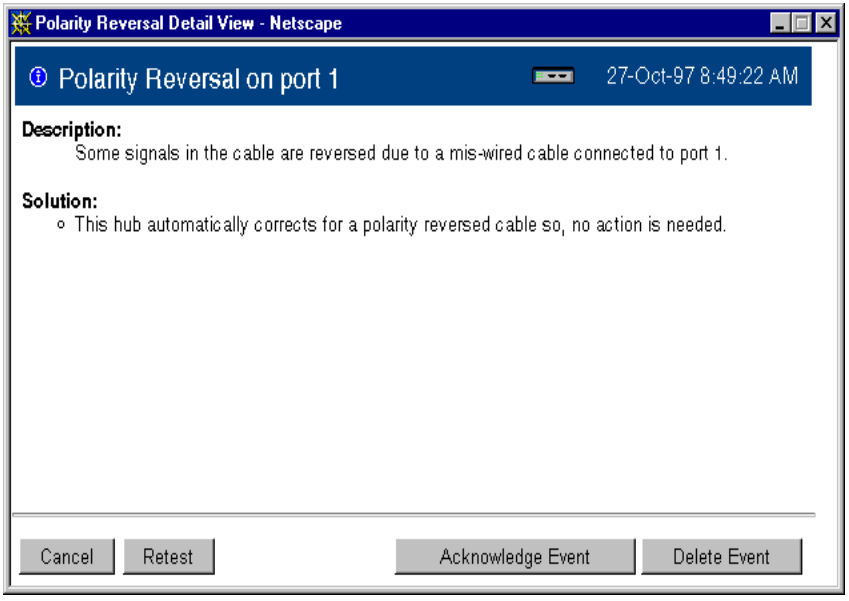


Figure 4-8. Detail View

The Alert Control Bar

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

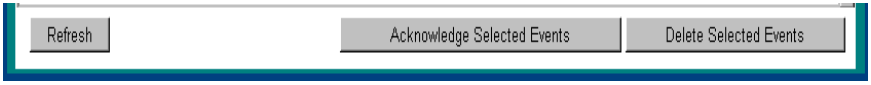


Figure 4-9. The Alert Control Bar

The buttons are detailed here.

Refresh Button. Displays new alerts that have occurred since you opened this window. Note new faults are automatically clocked to every 15 seconds.

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` label 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 Browser Interface Tab Bar contains six tabs, four of which launch button bars which launch specific functional windows. One tab, Identity, launches a dedicated functional window with no buttons. Another tab, Support, launches a separate web page with support information.

To navigate through the different topical areas of the 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 Administration dialog box.

Status

Figure 4-10. 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 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

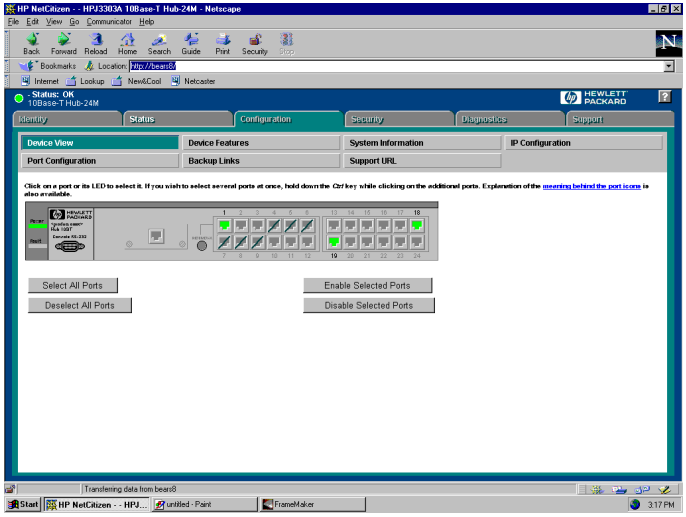


Figure 4-11. The Configuration Tab Bar

This tab displays the Configuration Button bar which contains buttons that launch sessions 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 enable and disable ports on the device by clicking on port graphics and an enable or disable port button.

Fault Detection. Controls the alert log sensitivity, and port disabling.

System Information. Enables you to view and set system information for a selected device.

IP Configuration. Enables you to change existing value for an IP address, subnet mask, and the gateway address for the hub.

Port Configuration. Enables you to enable and disable ports in addition to viewing the security and source address information.

Backup Links. Enables you to configure a primary and a redundant communication link between two hubs in a cascaded topology, using two separate cables and two ports on each hub.

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.

Security

Figure 4-12. The Security Tab Bar

This tab displays the Security Button Bar which contains buttons that enable you view and set access restrictions for your hub. The buttons are:

Device Passwords. Enables you to set operator and manager-level passwords for the hub.

Port Security. Enables you to set 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 4-13. 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. Enables you to send test packets to devices connected to a port, using both the IP address (Ping) and the MAC address (Link) as criteria for a valid connection.

Device Reboot. Causes the hub to reset its state as though it were powered on and off.

Factory Reset. Restores out of the box configuration.

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.

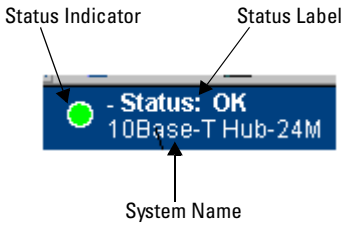


Figure 4-14. The Status Bar

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 five colors. The mapping of color to Gauge Severity Regions and Status Indicator shapes is shown in the following table.

Table 4-4. Status Indicator Key

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

System Name. Indicates the name of product name of the hub for which you have created your current Browser Interface session.

Status Label. Indicates, by test string, the severity of the most critical alert in the current display of the Alert Log.

Most Critical Alert Description. A short narrative description of the earliest, unacknowledged alert with the current highest severity in the Alert Log, appearing in the right portion of the Status Bar. In instances where multiple critical alerts have the same severity level, only the earliest unacknowledged alert is deployed in the Status Bar.

Setting Fault Detection Policy

One of the powerful features in the Browser Interface is the Fault Detection facility. This feature enables you to perform two types of fault management tasks:

- controls the types of alerts reported to the Alert Log based on their level of severity
- controls the sensitivity level required by a port before the port is disabled.

You perform these tasks in the Fault Detection Window. The Fault Detection Window is shown below.

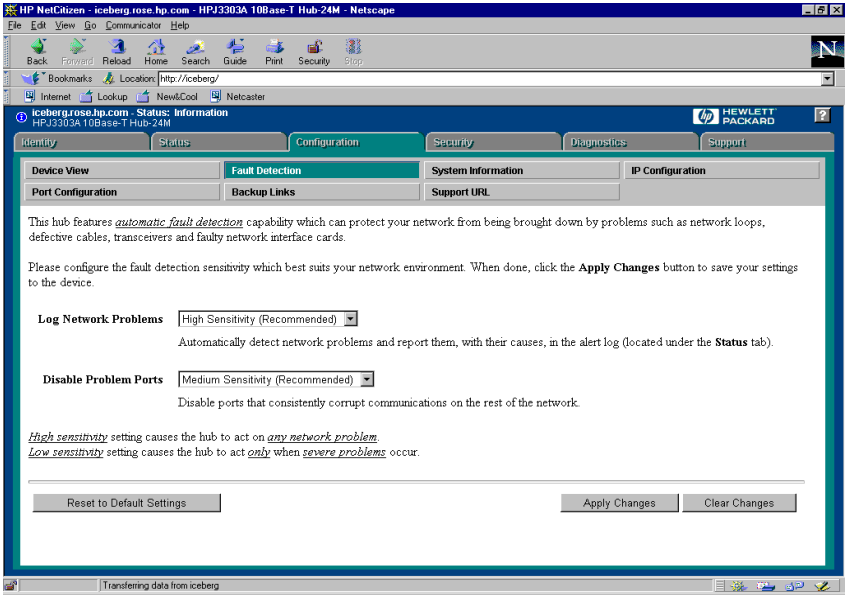


Figure 4-15. The Fault Detection Window

Working With Fault Detection

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 Problem Ports. Provides sensitivity threshold levels that determine when a network problem is critical enough to direct a port to be disabled.

The sensitivity levels for both list boxes are:

- Never
- Low Sensitivity
- Medium Sensitivity
- High Sensitivity

Note that the Disable Port setting 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 4-5. Recommended Settings

Detection Sensitivity	Log Network Problems Setting	Disable 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 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 to disable the offending port in instances of severe network disruption.

Sample Scenario	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 sensitive 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 which are affecting the network are disabled.

Sample Scenario	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 a port generating the alert.

Sample Scenario	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 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.

Using SNMP To Monitor and Manage the Hub

You can manage the hub via SNMP from a network management station using a tool such as HP TopTools for Hubs and Switches. (The hub supports SNMP v1 and SNMP v2c, except as noted below for SNMP v2 Notifications.) You must either configure the hub with the appropriate IP address or, if you are using Bootp/DHCP to configure the hub, ensure that the Bootp/DHCP process provides the IP address.

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 Top Tools for Hubs and Switches
- Monitoring data normally associated with the SNMP agent ("Get" operations). Supported *Standard* MIBs include:
  - Bridge MIB (RFC 1493)
  - Etherlike MIB (RFC 1650)
  - Ethernet MAU MIB (RFC 1515)
  - Interfaces Evolution MIB (RFC 1573)
  - Novell Standard IPX MIB (ipx.mib)
  - RMON MIB (RFC 1757)— all nine groups
  - SNMP MIB-II (RFC 1213)
  - RPTR MIB (RFC 2108)

HP Proprietary MIBs include:

- Statistics for message and packet buffers, tcp, telnet, and timep (netswtst.mib)
- Port counters, forwarding table, and CPU statistics (stat.mib)
- tftp download (downld.mib)
- 802.12 (100VG) information (vg.mib)
- Integrated Communications Facility Authentication Manager and SNMP communities (icf.mib)
- HP 10Base-T Hubs configuration (config.mib)
- HP VLAN configuration information (vlan.mib) supporting hpVlanGeneralGroup
- HP EASE MIB version 4 to allow EASE sampling
- HP Linktest MIB for basic device management (linktest.mib)
- HP ICF Linktest MIB for link test features (icfbasic.mib)

The 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 following World Wide Web site:

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

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

SNMP Configuration Process

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

1. From the Main menu, select Hub Configuration.
2. Enable and configure an IP address for the hub, including any necessary gateways.
3. Configure the appropriate SNMP communities.

See Community Name and IP Configuration reference pages in chapter 6 for details.

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".

Configuration Reference

This chapter provides reference descriptions for screens in the Hub Console Interface and windows in the Browser Interface. The reference pages each contain the following:

- Quick Lookup Table
- Screen/Window Purpose Description
- Field and Column Descriptions
- Sample Views of Browser Interface Windows and Hub Console Screens
- Procedures on how to use features in both the Browser Interface and the Hub Console

The way the screens and windows are ordered in this chapter are by the order the environment appears in the *console*. In other words, if you view console screens starting with the top screen in the top menu in the Main Menu and work your way down through the environment, you will be following the presentation sequence in the reference. A Browser Interface Window will be presented in this reference alongside each console screen that provides similar functionality.

Remember, if you are trying to find a Browser Interface Window, you need to know the order in which the like Hub Console Screen appears in the application. For example, to find the Browser Interface Intrusion Log Window, you need to know that the Hub Console Interface Intruder Log Screen appears under the Hub Status and Counters Menu, the first functional menu in the console, even though the Intrusion Log Window appears under the Security Tab, the last functional area in the Browser Interface. This means the Intrusion Log Window reference page appears relatively early on in the reference.

Refer to the following table for a master list of the order of all console screens and Browser Interface Windows to determine where they will be presented in the reference. Note that menu names are in bold print.

Table 6-1. Console Screen/Browser Interface Map

Hub Console Menu/Screen	Browser Interface Window
Main Menu	
Hub Status and Counters Menu	
General System Information	Hub System Information
Port Status	Port Settings
Port Counters	Port Counters
Global Counters	Global Counters
Security Intruder Log	Intrusion Log
Clear Security Intruder Log	Clear Port Intrusion LEDs Button in the Intrusion Log Window
Management Access Configuration Menu	
IP Configuration	IP Settings
Community Name	--
Authorized Managers	--
Console Password	Device Passwords
Telnet Enable/Disable	--
Browser Interface Password	--
Serial Timeout	--
Hub Configuration Menu	
Hub System Information	Hub System Information
Port Enable/Disable	Device View
Port Security	Port Security
	Port Security Configuration
Backup Links	Backup Links
	Backup Links Configuration
Reset Hub to Factory Default	Factory Reset
Diagnostics Menu	
Ping Test	Ping/Link Test
Link Test	Ping/Link Test
Browse Hub Configuration	Configuration Report
Web Support	
	Overview
	Fault Detection
	First Time Install

Main Menu

Attribute	Description
Screen Name	Main Menu
Menu	--
Function	The home menu upon first entry into the Hub Console Interface's menu system. Displays a list of all menus and top-level options available from the console.
Common Use	Launching any top-level menu available from the console.
Browser Interface Window	The Overview Window

The Main Menu displays a list of all menus and top level options available from the console. The menus are listed here.

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 to hubs, assign exclusive management stations to set parameters for the hub, 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, to configure activities that occur upon port security violations, to create backup paths and to revert hub settings to factory default levels.

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.

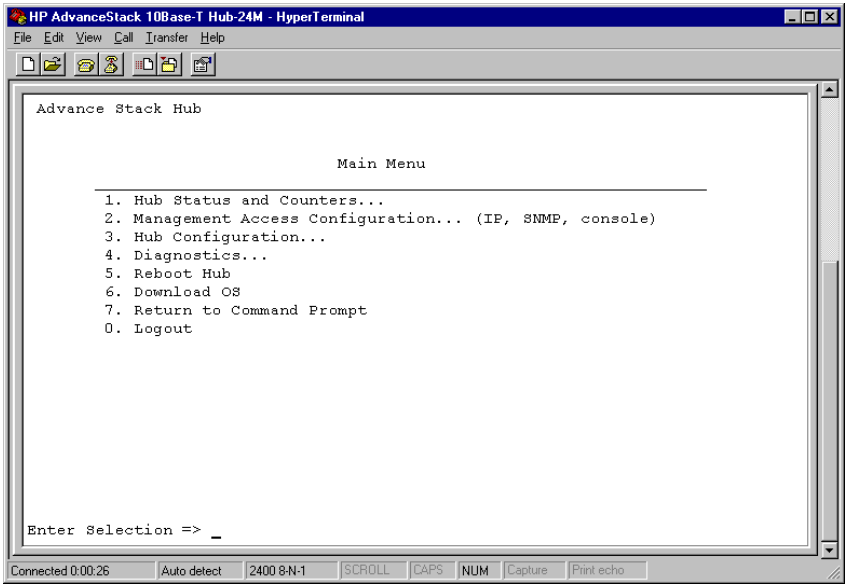


Figure 6-1. The Main Menu Screen

Hub Status and Counters

Attribute	Description
Screen Name	Hub Status and Counters
Menu	Main Menu
Function	Displays a list of options that detail hub identification and state information.
Common Use	Launching options that detail hub identification and state information.
Browser Interface Window	--
Browser Interface Tab	Status

The Hub Status and Counters Menu displays a list of menus and options that detail hub identification and state information. The options are listed here.

General System Information. Displays hub identification information and system attributes.

Hub Port Status. Displays port state information.

Hub Port Counters. Displays port-level statistics for various activity types.

Global Repeater Counters. Displays hub-level statistics for various activity types.

Security Intruder Log. Displays a record of unauthorized end nodes and devices (intruders) gaining entry to a port on the hub.

Clear Security Blinking Port LEDs. Clears blinking port LEDs associated with intruders.

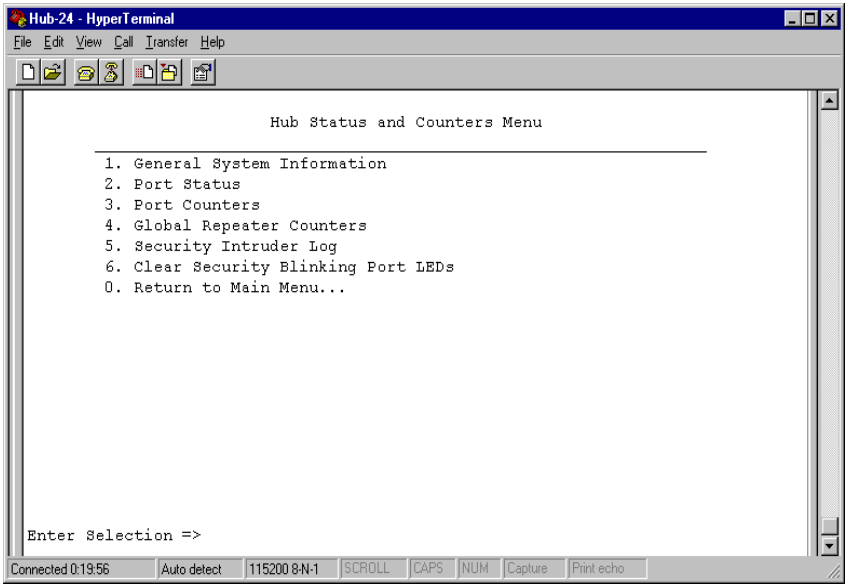


Figure 6-2. The Hub Status and Counters Menu Screen

General System Information

Attribute	Description
Screen Name	General System Information
Menu	Hub Status and Counters
Function	Displays a list of information about the hub.
Common Use	• Obtaining the hub's MAC address. • Obtaining the hub's IP Address. • Obtaining the hub's serial number. • Obtaining system up time.
Browser Interface Window	Identity
Browser Interface Tab	Identity
Default Setting	• MAC Address, MAC Address of hub. • IP Address, None • Download Version • System Up Time: 0 Days 00:00:00 (HH:MM:SS) • All other fields are empty

The General System Information Screen displays hub system identification information retrieved from the System Group in the MIB II. The information shown is detailed here.

System Name. Enables you to associate a common name to identify the device. For example, `My Hub`. The console only allows 80 characters to be set and the Browser Interface allows 255.

System Contact. Provides the name of the person responsible for or who administers the device. The console only allows 80 characters to be set and the Browser Interface allows 255.

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`. The console only allows 80 characters to be set and the Browser Interface allows 255.

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 to the hub.

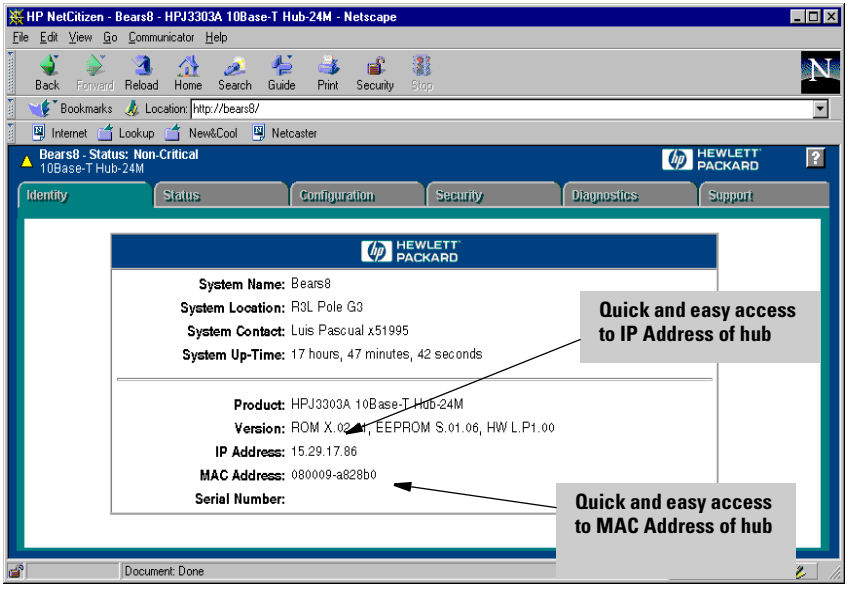


Figure 6-3. The Identity Window

Viewing Hub System Information in the Browser Interface

To view information in the Identity Window in the Browser Interface, click on the Identity Tab. The Browser Interface displays the Identity Window. The Identity Window is an easy and quick way to determine the IP Address and MAC address of your hub.

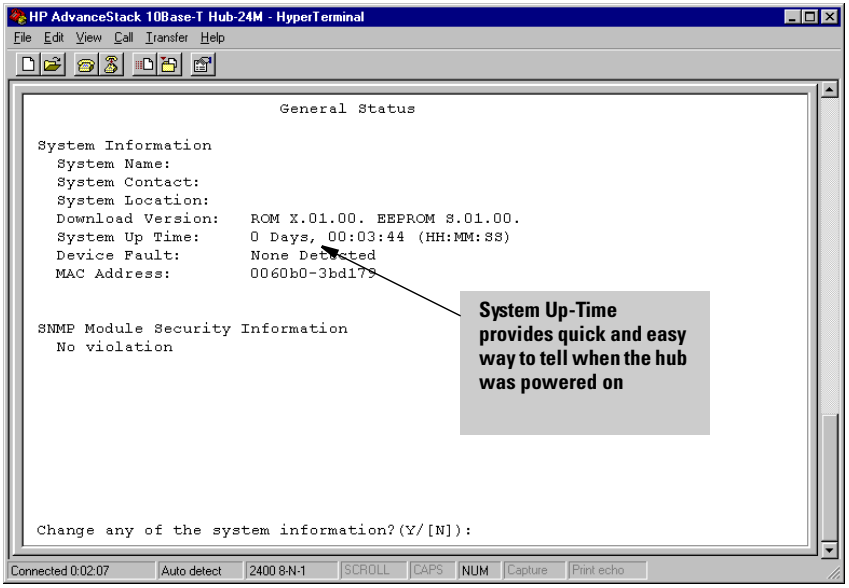


Figure 6-4. The General Status Screen

Viewing Hub System Information in the Console

To view information in the General Status Screen in the Hub Console Interface, perform the following steps:

1. From the Main Menu, type 1 and press Enter. The Hub Console Interface displays the Hub Status and Counters Menu.
2. From the Hub Status and Counters Screen, type 1 and press Enter. The Hub Console Interface displays the General Status Screen.

Port Status

Attribute	Description
Screen Name	Port Status
Menu in Hub Console	Statistics and Counters
Function	Displays port list that provides information about the state of all ports on the hub.
Common Use	Determining whether the hub is receiving packets from a connected device Identifying which devices are connected to the hub; identifying MAC addresses of connected hubs Determining if a security violation is present.
Browser Interface Window	Port Configuration
Browser Interface Tab	Configuration
Default Setting	• Port Status: Not active • Link Status: Not detected • Last Heard Source Address: None • Security Information: No violation

The Port Status Screen displays a port list that provides several columns of information about the state of all ports on the hub. The columns of information are:

Port number. Indicates the port label on the hub. Settings can be:

`1-12` and `XCVR` on the Hub 12M

`1-24` and `XCVR` on the Hub 24M

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 the Link Beat signal has been detected on the hub. Settings can be:

`Detected.` Indicates the port has sensed a device that supports link beat.

`Not Detected.` Indicates the port has not sensed a device that supports link beat.

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 (Violation on the 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.

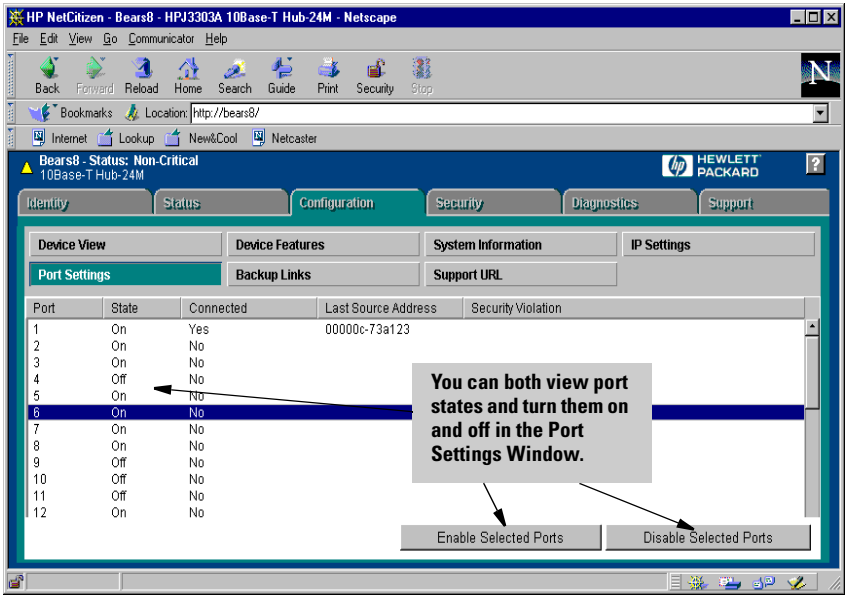


Figure 6-5. The Port Settings Window

Viewing Port Settings in the Browser Interface

To view information in the Port Settings Window in the Browser Interface, perform the following steps:

1. From the Tab Bar, select the Configuration Tab. The Browser Interface displays the Configuration Button Bar.
2. From the Configuration Button Bar, select the Port Settings Button. The Browser Interface displays the Port Settings dialog box. This dialog box contains a port list with the associated status of each port on the hub.

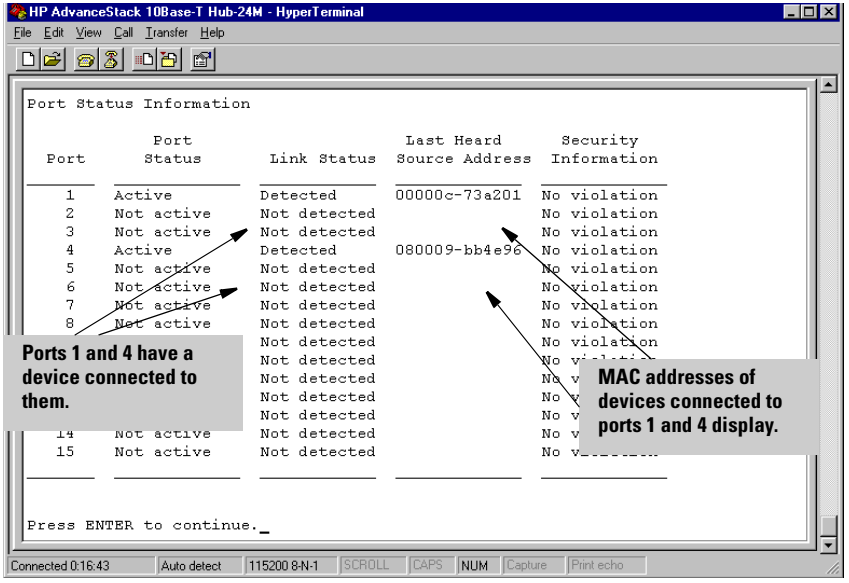


Figure 6-6. The Port Status Screen

Viewing the Port Settings in the Console

To view settings in the Port Status Screen in the Hub Console Interface, perform the following steps:

1. From the Main Menu, type 1 and press Enter. The Hub Console Interface displays the Hub Status and Counters Menu.
2. From the Hub Status and Counters Menu, type 2 and press Enter. The Hub Console Interface displays the Port Status Screen.

In the example shown, ports 1 and 4 are active and the Link Beat signal has been detected, indicating a valid 10Base-T 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.

Hub Port Counters

Attribute	Description
Screen Name	Hub Port Counters
Menu	Hub Status and Counters
Function	Displays activity recorded on each hub port for six MIB variables.
Common Use	Determining which ports may be experiencing problems.
Browser Interface Window	Port Counters
Browser Interface Tab	Status
Default Setting	All counters are 0.

The Hub Port Counters Screen displays activity recorded on each hub port for six MIB variables. The variables are retrieved from the hub's firmware. The values shown for the variables for each port are cumulative since the hub was powered on. The Hub Port Counters Screen enables you to determine the traffic patterns for each port. The default variables shown are:

Valid Packets. Provides the total number of good packets (packets with no errors) seen 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 a cable at the same time; they are capable of degrading 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. 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. Provides 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 packets not detecting the other 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 10Base-5 coaxial cable. In both cases, the packet 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.

Giant Packets. Provides the total number of packets seen by this port that contain oversize frames.

Broadcast Packets. Provides the total number of broadcasts seen by this port. A broadcast is a message sent to all users on the network.

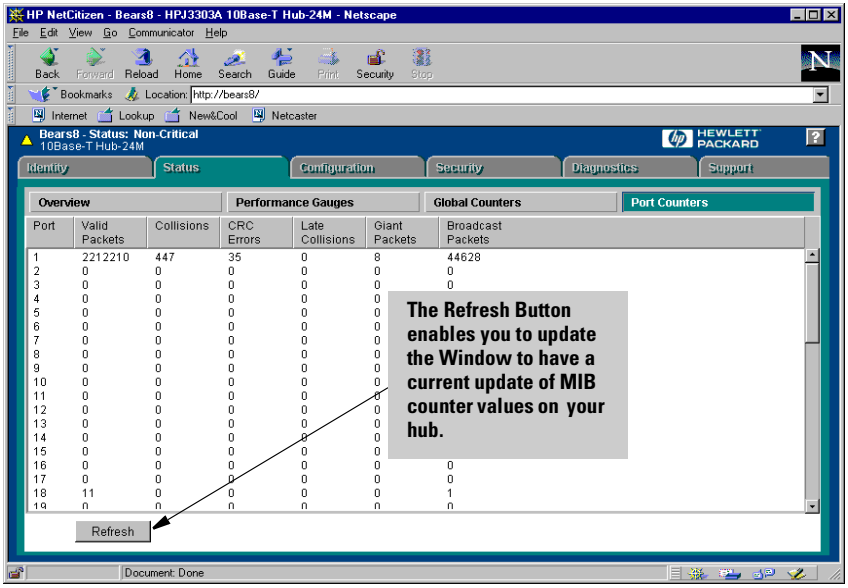


Figure 6-7. The Port Counters Window

Viewing Port Counter Statistics in the Browser Interface

To view port counter values in the Port Counters Window in the Browser Interface, perform the following steps:

1. From the Tab Bar, click on the Status Tab. The Browser Interface displays the Status Button Bar.
2. From the Status Button Bar, click on the Port Counters Button. The Browser Interface displays the Port Counters Window.

This dialog box can give you a snapshot of the hub's effectiveness. Especially note the Collisions and CRC Errors columns. If certain ports show high number in these columns, you may want to investigate your end nodes. Both of these counters are dependent upon time for collisions. Collisions are normal occurrences on the network. High values can occur for them. You should watch for *spikes*, indicating sudden changes.

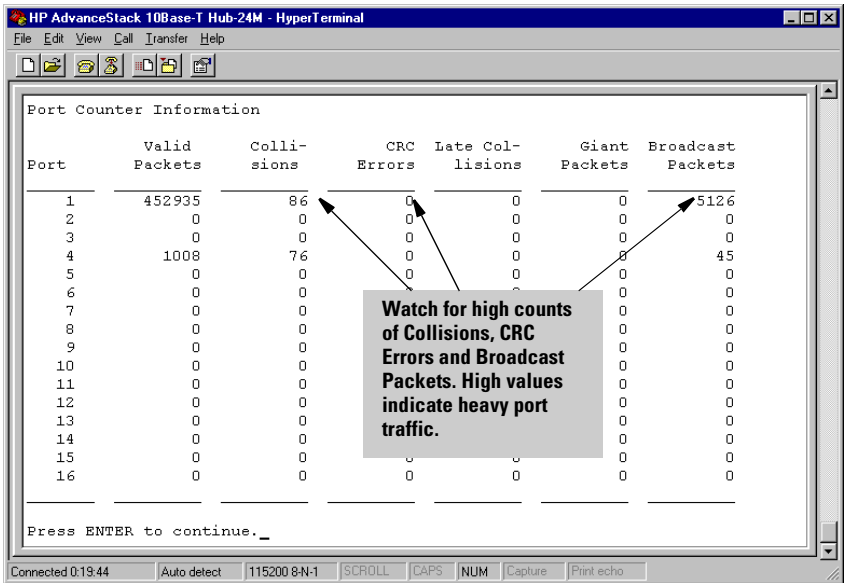


Figure 6-8. The Hub Port Counters Screen.

Viewing Port Counter Statistics in the Console

To view port counter values in the Port Counters Screen in the Hub Console Interface, perform the following steps:

1. From the Main Menu, type 1 and press Enter. The Hub Console Interface displays the Hub Status and Counters Menu.
2. From the Hub Status and Counters Menu, type 3 and press Enter. The Hub Console Interface displays the Port Counters Screen.

Global Counters

Attribute	Description
Screen Name	Global Counters
Menu	Hub Status and Counters
Function	Displays a list of MIB variables that show activity recorded on the hub.
Common Use	To determine traffic patterns on the hub to help make decisions about ways to optimize hub performance.
Browser Interface Window	Global Counters
Browser Interface Tab	Status
Default Setting	All counters are 0.

The Global Repeater Counters Screen displays aggregate activity recorded for the entire hub (not specific ports) for eight variables from the Remote Monitoring (RMON) MIB. The values shown for the variables for the hub are cumulative since the hub was powered on. The Global Repeater Counters Screen enables you to determine the traffic patterns for the hub. The default variables shown 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 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 the hub. A collision is generated when two or more devices attempt to transmit a message on a cable at the same time; they are capable of degrading 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 was used to detect a packet whose bits were misaligned because of timing errors. CRC is a method for detecting timing errors on a frame or 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 instances where remaindered portions of large frames from one network have been recorded. Fragmentation is the process in which large frames from one network are broken up into smaller frames compatible with the network to which they'll be forwarded.

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) and caused timing delay in processing of it because of its oversized state. Commonly known as *oversize*.
- the packet had a corrupted bit in it where one of the digits was transposed for any of a variety of reasons, including timing and alignment errors. 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.

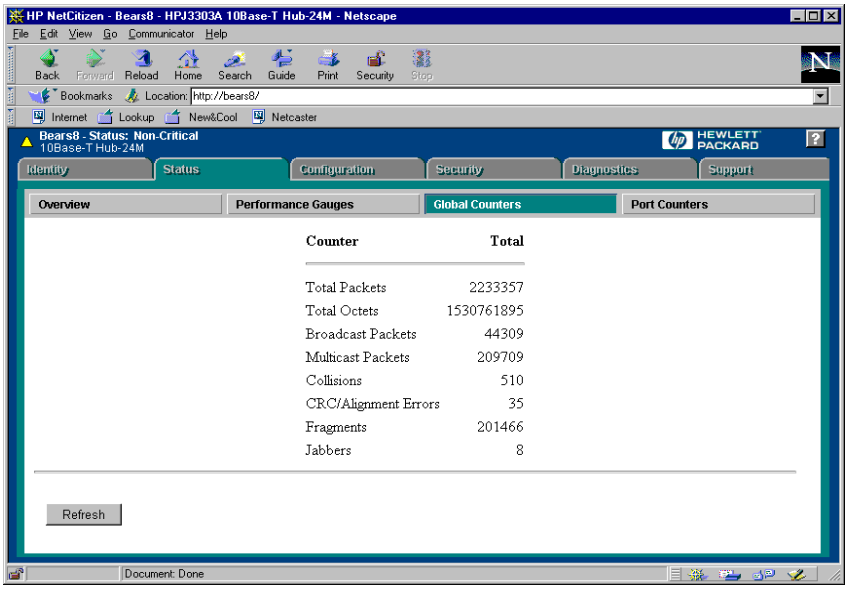


Figure 6-9. The Global Counters Window

Viewing Hub Counter Statistics in the Browser Interface

To view hub counter values in the Global Counters Window in the Browser Interface, perform the following tasks:

1. From the Tab Bar, click on the Status Tab. The Browser Interface displays the Status Button Bar.
2. From the Status Button Bar, click on the Global Counters Button. The Browser Interface displays the Global Counters window.

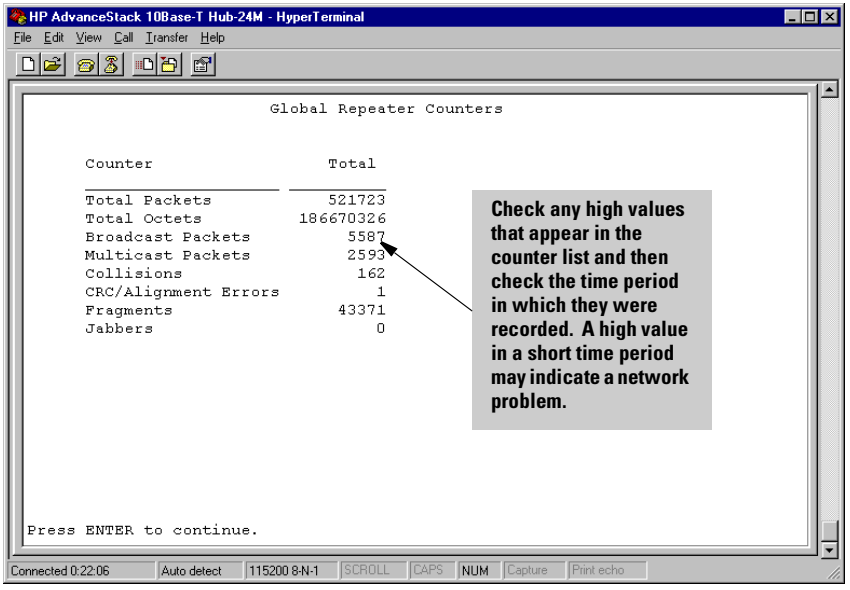


Figure 6-10. The Global Repeater Counters Screen

Viewing Hub Counter Statistics in the Console

To view hub counter values in the Global Counters Screen in the Hub Console Interface, perform the following steps:

1. From the Main Menu, type 1 and press Enter. The Hub Console Interface displays the Hub Status and Counters Menu.
2. From the Hub Status and Counters Menu, type 4 and press Enter. The Hub Console Interface displays the Global Counters Screen.

Watch for high levels of Collisions and Broadcast Packets. These counters indicate potential overloads on your hub and your network.

Security Intruder Log

Attribute	Description
Screen Name	Security Intruder Log
Menu	Hub Status and Counters
Function	Displays a listing of ports that have learned of MAC addresses of devices attempting to connect to the ports without proper authorization.
Common Use	To detect port intruders.
Browser Interface Window	Intruder Log
Browser Interface Tab	Security
Default Setting	None

The Security Intruder Log is a facility that displays a listing of ports that have learned of MAC addresses of devices attempting to connect to the ports without proper authorization. Authorization is an access scheme set on ports of devices. Violations of unauthorized devices are of two types:

Manager Intrusions. Occurs when an unauthorized manager, generally a management station, attempts to access the hub without being on the authorized manager list or without using the correct Community Name. Manager intrusions are controlled by the entries you make in the Authorized Managers dialog box in HP Top Tools for Hubs and Switches or the Authorized Managers Screen in the Hub Console Interface. Manager intrusions are shown at the top of the Hub Console Interface screen in non-tabular form under the heading `SNMP Security Information`. Manager intrusions are indicated in the Browser Interface Window in two ways

- the string SNMP Agent is displayed in the Port column.
- an IP Address of the unauthorized management station is displayed in the Intruder Address column.

Port Intrusions. Occurs when a MAC address detected from an incoming packet on a port does not match the authorized MAC address for the port. Port intrusions are controlled by the entries you make in the Port Security dialog box in HP Top Tools for Hubs and Switches or the Browser Interface. Port intrusions are shown at the bottom of the Hub Console Interface screen in tabular form. Port intrusions are differentiated from manager intrusions in the Browser Interface in two ways.

- the number of the port to which the unauthorized manager attempted to connect is displayed in the Port column.
- a MAC address is displayed in the Intruder Address column.

Note that you cannot clear the log of entries. The Intruder Log can display up to 20 entries. Entries are displayed in the log for the life of the hub until more than 20 are recorded. When new entries are received after 20 have been recorded, existing entries are removed to maintain a maximum entry count of 20. Entries are removed on the basis of age, the oldest entry being removed first, the second oldest entry removed next, and so on.

The information shown in the Intruder Log is as follows.

Violation Time (Console only). Indicates the amount of time that has elapsed since the hub was powered on in the format DD, HH:MM:SS.

Port. The port number that is reporting attempted access by an unauthorized device. Settings can be:

- Port number for a port intrusion
- `SNMP Agent` for a manager intrusion

Intruder Address (**Violator's Address** in Console). The address of the unauthorized device.

- IP Address for a manager intrusion
- MAC address for a port intrusion

Time (Violation Time in Console). The date and time in the format DD:MM:YY HH:MM:SS. The console also contains the violation time in the number of days. This value is the system up time when an intruder was detected.

Clear Intrusion Log Fault LED. (Browser Interface only). Stops LEDs of ports reporting port intrusions from flashing.

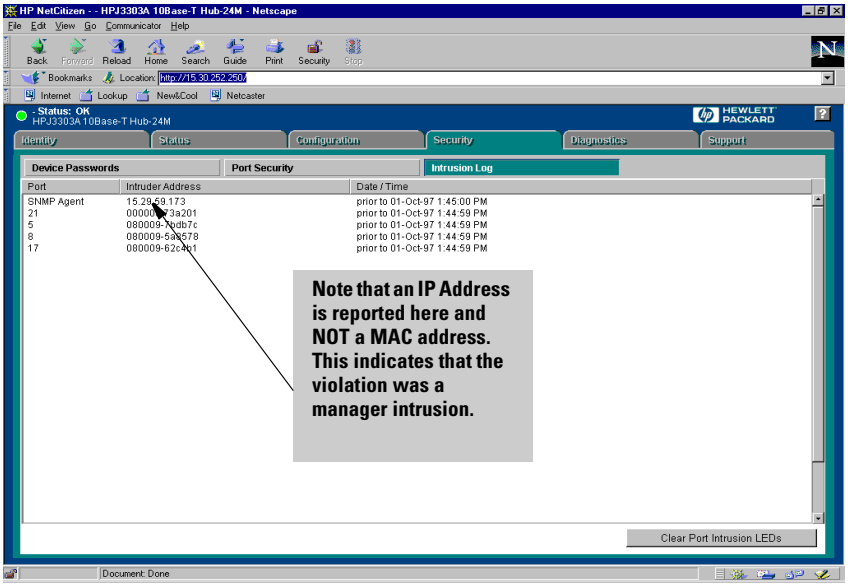


Figure 6-11. The Intrusion Log Window

Viewing the Intruder Information in the Browser Interface

To view unauthorized addresses in the Intruder Log from the Browser Interface, perform the following tasks:

1. From the Tab Bar, click on the Security Tab. The Browser Interface displays the Security Button Bar.
2. From the Security Button Bar, click on the Intruder Log Button. The Browser Interface displays the Intruder Log Window.

3. View each column to learn about unauthorized access activity occurring on the hub.
   - Pay special attention to repeat intrusions by the same address.
   - If you feel the intrusions are not significant, you may want to change the Address Selection settings in the Port Security Window to be less restrictive.
   - Note any entries that have the string SNMP Agent in the Port column. These entries are manager intrusions, indicating that an unauthorized manager attempted to connect to the hub. Note the address for these entries is an IP Address.
   - Note entries that display a port number in the Port column. These entries are port intrusions, indicating that the Address Selection method selected in the Port Security Window would not permit the address of the hub attempting to communicate with the port to be admitted.

Stopping Intruder Flashing LEDs in the Browser Interface

When a port recognizes a packet as being sent from an unauthorized hub, its LED flashes to indicate that an intruder has been recorded for the port. To stop LEDs from flashing in response to port intruders, perform the following steps on the Browser Interface.

1. Click on an Intruder entry in the Intrusion Log to highlight it. The entry is selected.
2. Click on the Clear Port Intrusion LEDs Button. The Browser Interface removes the Clear Port Intrusion LEDs Button and displays an OK Button. The Browser Interface also displays the following message

   ```
   The intrusion fault LEDs have been cleared.
   ```

3. Click on the OK Button. All LEDs of ports that have registered intruder entries will stop flashing.

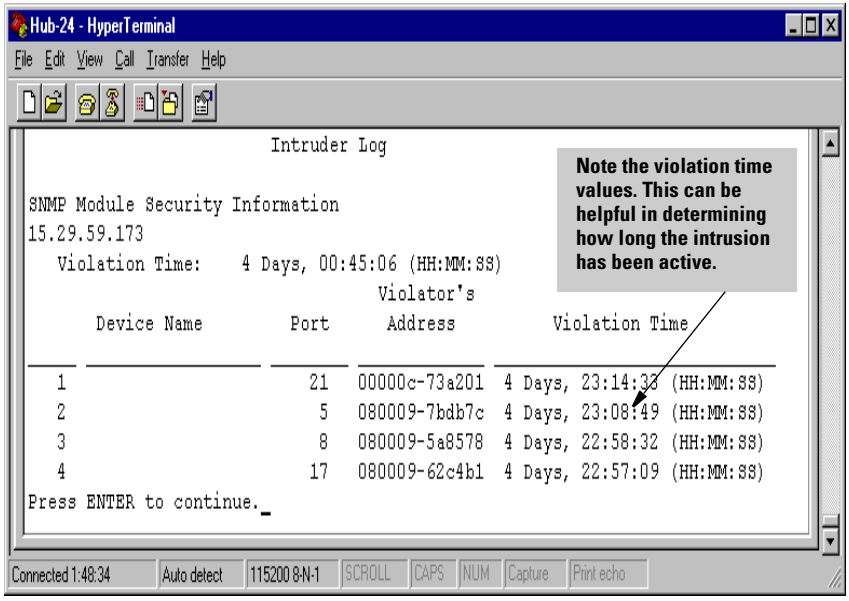


Figure 6-12. The Intruder Log Screen

Viewing Intruder Information in the Console

To view unauthorized addresses in the Intruder Log from the Hub Console Interface, perform the following tasks:

1. From the Main Menu, type 1 and press Enter. The Hub Console Interface displays the Hub Status and Counters Menu.
2. From the Hub Status and Counters Menu, type 5 and press Enter. The Hub Console Interface displays the Security Intruder Log.
3. Note the difference between the manager intrusion area and the port intrusion area. The manager intrusion area is at the top of the screen under the heading SNMP Security Information. Note that the address of an intruder displayed in this area is an IP Address. The port intrusion area is at the bottom of the screen in the table. Note that the address of an intruder displayed in this area is a MAC address.
4. View all the information to learn about unauthorized access activity occurring on the hub. Pay 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 to be less restrictive.

Clear Security Blinking Port LEDs

Attribute	Description
Screen Name	Clear Security Blinking Port LEDs
Menu	Hub Status and Counters
Function	Enables you to stop port intruder-related flashing on LEDs for ports that have recorded intruders.
Common Use	Clearing LEDs flashing on the hub to create a less confusing LED panel.
Browser Interface Window	Intruder Log (Button within the Window)
Browser Interface Tab	Security
Default Setting	Flashing LEDs associated with unauthorized device are allowed.

When a port recognizes a packet as being sent from an unauthorized device, its LED flashes to indicate that an intruder has been recorded for the port. If you are working in the Hub Console Interface, a dedicated option in the Hub Status and Counters Menu enables you to stop port intruder-related flashing on LEDs for ports that have recorded intruders.

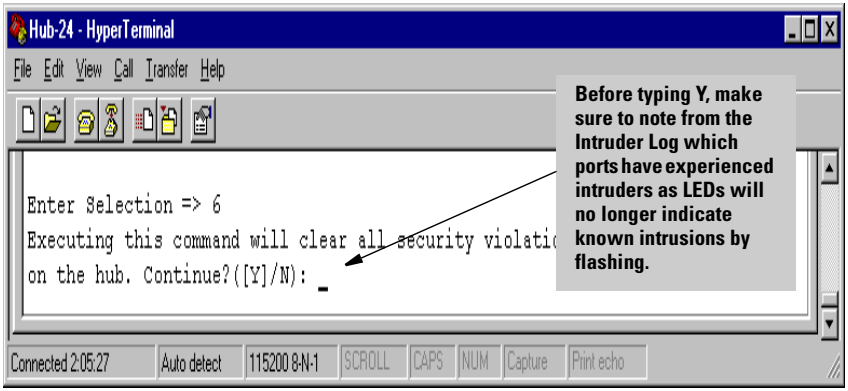


Figure 6-13. The Clear Security Blinking Port LEDs Option

Stopping Intruder Flashing LEDs in the Console

To stop LEDs from flashing in response to port intruders, using the Browser Interface, perform the following steps:

1. From the Main Menu, type 1 and press Enter. The Hub Console Interface displays the Hub Status and Counters Menu.
2. From the Hub Status and Counters Menu, type 6 and press Enter. The Hub Console Interface displays the following prompt:

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

3. Type Y and press Enter. All LEDs of ports that have registered intruder entries will stop flashing.

Management Access Configuration Menu

Attribute	Description
Screen Name	Management Access Configuration Menu
Menu	--
Function	Displays a list of all menus and options that enable you to configure agent access methods.
Common Use	Launching screens to perform device access tasks.
Browser Interface Window	--
Browser Interface Tab	Configuration

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

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 you to configure the hub to allow Telnet access.

Console Password. Enables you to set or change the password you use to access the Hub Console.

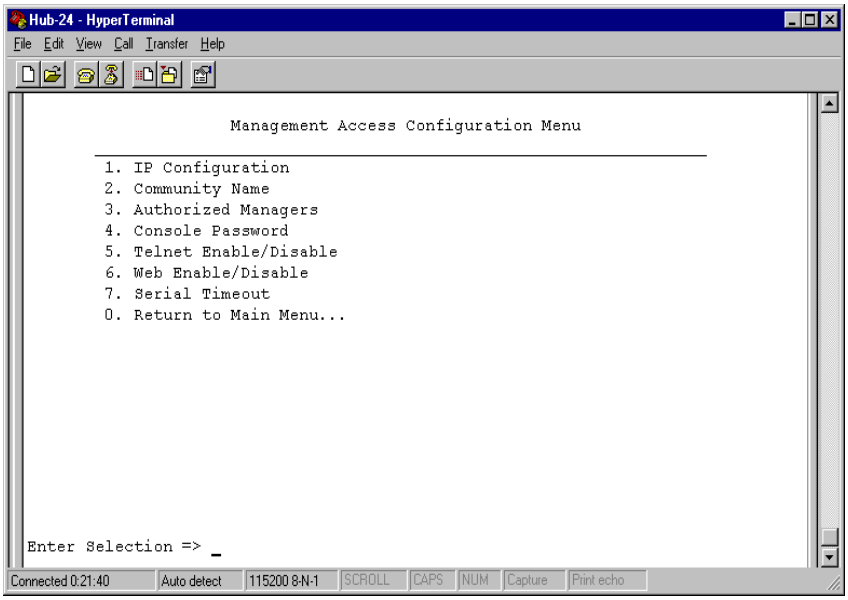


Figure 6-14. The Management Access Configuration Menu

IP Configuration

Attribute	Description
Screen Name	IP Configuration
Menu	--
Function	Enables you to configure an IP Address, a subnet mask, and the gateway address for the hub so that it can be managed in an IP network.
Common Use	Creating an IP Address for the hub.
Browser Interface Window	IP Configuration
Browser Interface Tab	Configuration
Default Setting	Bootp/DHCP

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 Top Tools for Hubs and Switches and the 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 facility. The IP Configuration Screen contains the following columns of information 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`. Indicates you have set the hub's IP configuration manually.

`Bootp/DHCP`. Indicates the hub's IP configuration was set automatically using BOOTP or DHCP.

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 0 through 255 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.

Gateway. Indicates the IP Address of the nearest router in the network. If there are no routers, the address of the network management station is commonly used.

Time to Live. Indicates the number of IP routers a packet is allowed to cross before the packet is discarded. The default value is 32. Increase this value if the hub is managed from a network management station that is more than 32 routers away. The maximum allowable value is 255.

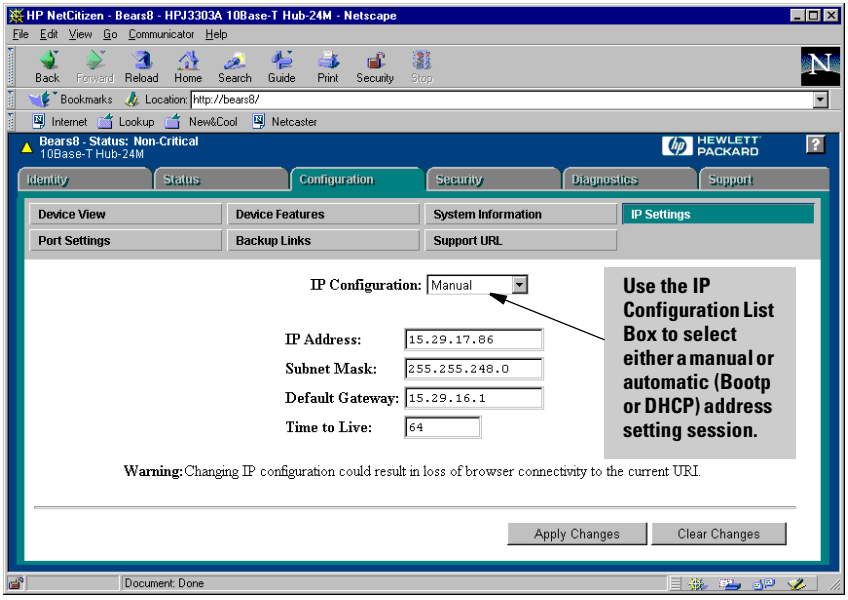


Figure 6-15. The IP Settings Window

Setting an IP Address in the Browser Interface

To set an IP Address on the hub using the Browser Interface, perform the following steps:

1. From the Tab Bar, click on the Configuration tab. The Browser Interface displays the Configuration Button Bar.
2. From the Configuration Button Bar, click on the IP Configuration Button. The Browser Interface displays the IP Configuration Window.
3. To manually configure network values, make sure the IP Configuration list box is set to Manual.
4. Type IP Address, Subnet Mask, Default Gateway and Time to Live values in the appropriate fields and click on the Apply Changes button.

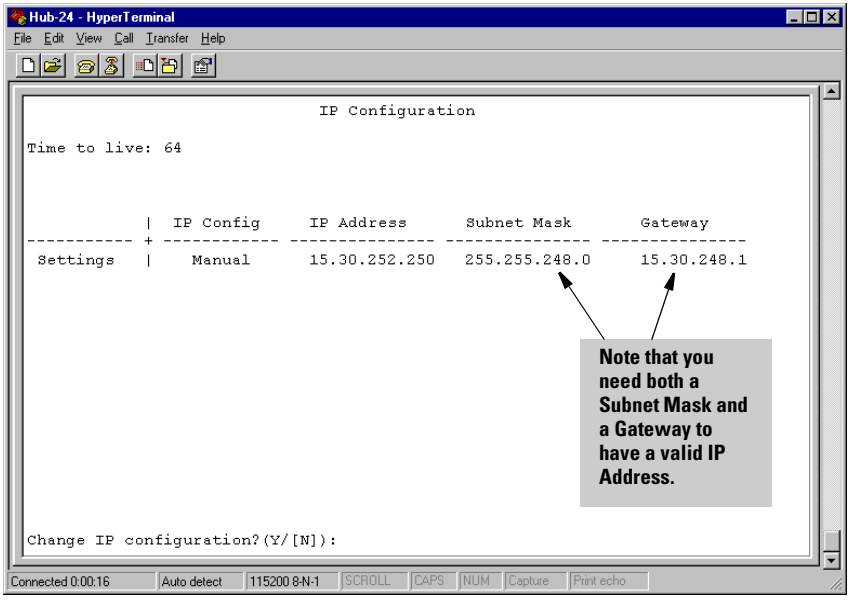


Figure 6-16. The IP Configuration Screen

Setting an IP Address in the Console

To set an IP Address on the hub, using the Hub Console, perform the following tasks:

1. From the Main Menu, type 2 and press Enter. The Hub Console Interface displays the Management Access Configuration Menu.
2. Type 1 and press Enter. The Hub Console Interface displays the IP Configuration Screen.
3. At the Change IP Configuration prompt, type Y and press Enter. The console interface prompts you to select the method by which you want to assign an IP Address to your hub. The two address assignment options are (B)ootp/DHCP or (M)anual Config.
4. Type M and press Enter to manually assign an IP Address to the hub. The console interface prompts you to type an IP Address.
5. At the Enter IP Address prompt, type an available IP Address and press Enter. Continue to supply values for the subnet mask, default router, and Time to Live values when prompted.
6. At the Change and save to new IP configuration prompt, type Y and press Enter to store all values you have set.

Community Name

Attribute	Description
Screen Name	Community List
Menu	Management Access Configuration
Function	Enables you to gain various levels of read and write access to devices.
Common Use	Creating device security for various levels of users and management stations.
Browser Interface Window	None
Browser Interface Tab	None
Default Settings	• Community Name: Public • Write View: Full Access • Read View: Full Access

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 ProCurve 10Base-T Hubs are described here.

If you are using HP Top Tools for Hubs and 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. 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 Top Tools for Hubs and 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 is for locating 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 ProCurve 10Base-T 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.

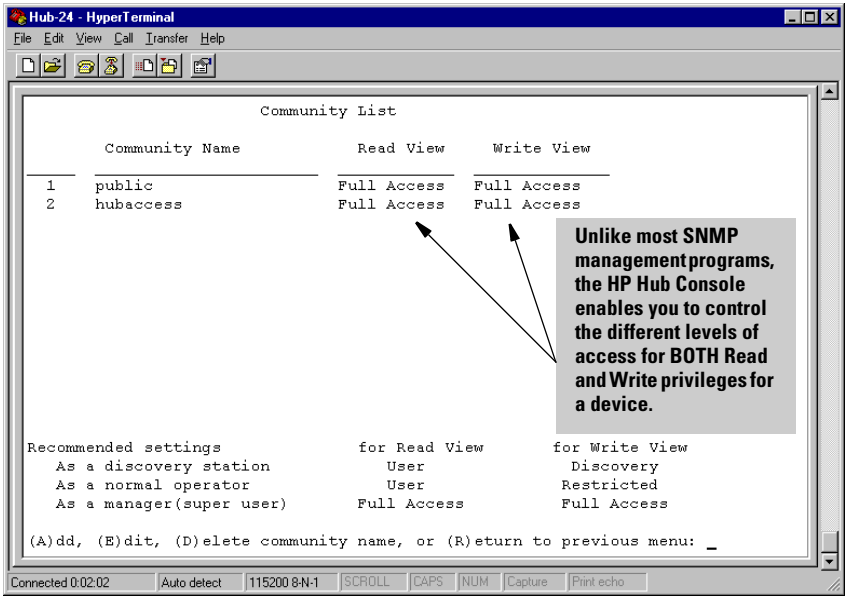


Figure 6-17. The Community List Screen

Setting Community Names in the Console

To set Community Names for the hub, using the Hub Console, perform the following tasks:

1. From the Main Menu, type 2 and press Enter. The Hub Console Interface displays the Management Access Configuration Menu.
2. From the Management Access Configuration Menu, type 2 and press Enter. The Hub Console Interface displays the Community List Screen. The Community List comes with a preset Community Name, Public that provides manager level access.

To add a Community Name, perform the following steps:

1. Type A and press Enter. The Community List Screen displays the following prompt:

   ```
   Enter in community name:
   ```

2. Type the name of the Community Name you want to use and press Enter. The Community LIst Screen displays the following prompt and information:

```
Enter in Read View as (N)one, (R)estricted, (U)ser,
(F)ull:
```

3. Type the Read-level access you want this Community Name to provide (either N, R, U, or F) and press Enter. The Community List Screen displays some basic Read-Write mapping information. It also displays the following prompt:

```
Enter in Write View as (N)one, (D)iscovery, (R),
(U)ser, (F)ull
```

4. Type the Write-level access you want this Community Name to provide (either N, D, R, U, or F) and press Enter. The Community List Screen redisplays the home Screen and displays the new Community Name in the Community Name List. A sample session is shown below.

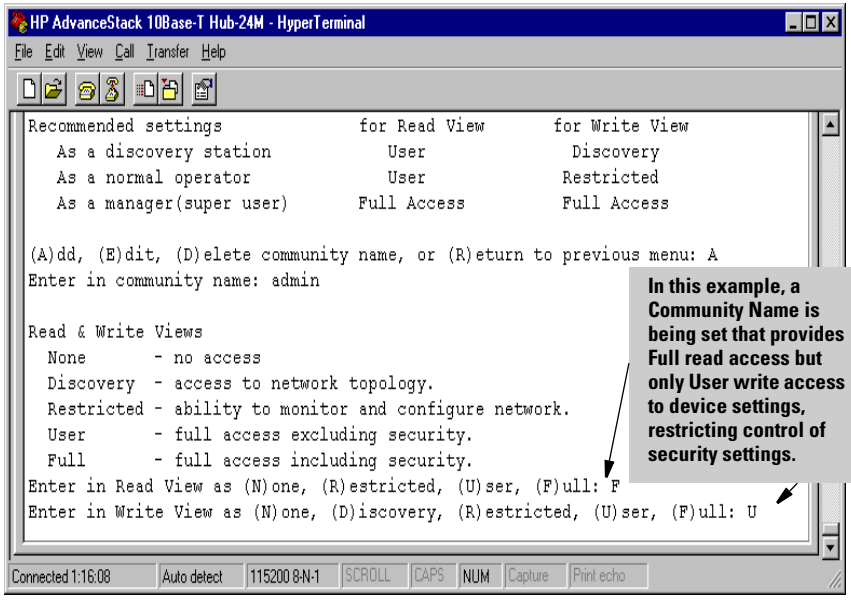


Figure 6-18. Adding a Community Name

To edit a Community Name:

1. From the Community List Screen, type E and press Enter. The Community List Screen displays the following prompt:

   ```
   Select community name to edit (1 – #) and press Enter.
   ```

2. Type the number of the Community Name in the Community Name List that you want to edit and press Enter. The Community List Screen displays the following prompt:

   ```
   Enter in community name: community name
   ```

   Note that the name appearing in the Community Name List associated with the number you typed is displayed in the screen. If you want to continue to use that name, press Enter. If you would like to use a different name, backspace over the name, type a new name of up to 256 characters and press Enter. The Community List Screen displays the following prompt:

   ```
   Enter in Read View as (N)one (R)estricted (U)ser (F)ull
   ```

3. Type the Read-level access you want this Community Name to provide (either N, R, U, or F) and press Enter. The Community List Screen displays some basic Read-Write mapping information. It also displays the following prompt.

   ```
   Enter in Write View as (N)one, (D)iscovery, (R),
   (U)ser, (F)ull
   ```

4. Type the Write-level access you want this Community Name to provide (either N, D, R, U, or F) and press Enter. The Community List Screen redisplays the Community List Screen and displays the new Community Name in the Community Name List.

To delete a Community Name, perform the following steps:

1. Type D at the Community List Screen and press Enter. The Community List Screen displays the following prompt.

   ```
   Select community name to delete (1 – #)
   ```

2. Type the number of the Community Name in the Community Name List that you want to delete and press Enter. The Community List Screen displays the following message and verification prompt:

   ```
   Deleting this community will also remove authorized
   managers associated with this community.

   Continue with community deletion? ([Y]/N):
   ```

3. Type Y and press Enter to continue deleting the community name. The Community List Screen redisplays the Community List Screen and displays the Community Name List without the Community Name you just deleted.

Authorized Managers

Attribute	Description
Screen Name	Authorized Managers
Menu	Management Access Configuration
Function	Enables you to specify the management stations that can manage the hub or all devices in your network.
Common Use	Launching any second-level menu available from the console.
Browser Interface Window	None
Browser Interface Tab	None
Default Setting	• Management Station: The IP Address of the management station you are currently using to access the Hub Console Interface. • Community Name: Public

The Authorized Managers Screen enables you to specify the management stations that can manage the hub or all devices in your network. You can configure a list of up to 10 network management stations.

You must configure the Authorized Managers first before you can receive any traps. Once set, it does not have to be set again unless you perform a Factory Reset.

The columns of information in the Authorized Managers Screen are shown here.

Associated Community Name. Indicates the Community Name of the hub for which you are creating an authorized manager.

Manager IP or IPX 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 255.255.255.251 applied to an address of 15.47.66.40 to disallow values of 15.47.66.46, 15.47.66.47, 15.47.66.48, and 15.47.66.49. HP recommends you use a security mask value of 255.255.255.255.

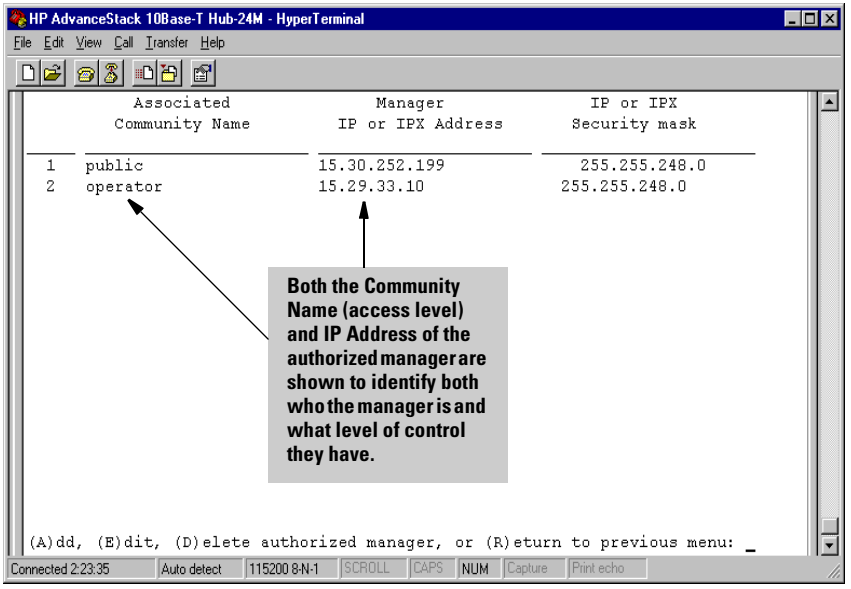


Figure 6-19. The Authorized Managers Screen

Setting Authorized Managers in the Console

To set authorized managers for the hub, perform the following tasks:

1. From the Main Menu, type 2. The Hub Console Interface displays the Management Configuration Access Menu.
2. From the Management Configuration Access Menu, type 3. The Hub Console Interface displays the Authorized Managers Screen.

To Add an Authorized Manager, perform the following tasks:

1. Type A and press Enter. The Hub Console Interface displays a numbered list of all available Community Names and the following prompt:

   ```
   Select community for manager (1-#)
   ```

2. Type the number of the Community Name you want to assign the authorized manager and press Enter. The Hub Console Interface displays the following prompt:

   ```
   Enter in Manager IP Address
   ```

3. Type in the IP Address of the device that you want to act as a manager for the hub and press Enter. The Hub Console Interface displays the following prompt:

```
Enter in manager IP mask:
```

4. Type the security mask for the device that you want to act as a manager for the hub and press Enter. HP recommends you use a security mask value of 255.255.255.255.

   The Hub Console Interface displays the authorized manager list with the authorized manager you just created at the bottom of the list. Note that the authorized manager is identified first by its community name (far left column) and then by network addressing information associated with the management station.

To Remove an Authorized Manager, perform the following steps:

1. Type D and press Enter. The Hub Console Interface displays the following prompt:

   ```
   Select manager to delete (1-#):
   ```

2. Type the number of the authorized manager that you want to remove from the Authorized Managers List and press Enter.

   The Hub Console Interface displays the authorized manager list. Note that the authorized manager you just removed no longer is displayed in the Authorized Manager List.

To Edit an Authorized Manager, perform the following tasks:

1. Type E and press Enter. The Hub Console Interface displays the following prompt:

   ```
   Select manager to edit (1-#):
   ```

2. Type the number of the authorized manager that you want to edit and press Enter. The Hub Console Interface displays a numbered list of all available Community Names and the following prompt:

   ```
   Select community for manager (1-#):
   ```

3. Type the number of the Community Name you want to assign the authorized manager and press Enter. The Hub Console Interface displays the following prompt:

   ```
   Enter in Manager IP Address
   ```

4. Type in the IP Address of the device that you want to act as a manager for the hub and press Enter. The Hub Console Interface displays the following prompt:

   ```
   Enter in manager IP mask:
   ```

5. Type the subnet mask for the device that you want to act as a manager for the hub and press Enter.

   The Hub Console Interface displays the authorized manager list with the authorized manager you just changed at the bottom of the list. Note that the authorized manager is identified first by its community name (far left column) and then by network addressing information associated with the management station.

Console Passwords

Attribute	Description
Screen Name	Console Password
Menu	Management Access Configuration
Function	Enables you to set or change both a password and username for entry to the console and Browser Interface for device management.
Common Use	Block use of the console or Browser Interface by unauthorized users.
Browser Interface Window	Device Passwords
Browser Interface Tab	Security
Default Setting	• No Password • No Username

The Console Password Screen enables you to set or change both a password and username for entry to the console and Browser Interface for device management. You may want to create both a username and password to create access security for your hub. Note that both a username and password are not required to use the Browser Interface. Also, passwords and usernames you set in the Hub Console are set for the Browser Interface. Note that in the Browser Interface, you can create two types of usernames and passwords:

operator. These strings assign you the following read-only privileges. These strings enable you to read all environments in the Browser Interface except for ones relating to Security. Note that these passwords will only be set for the Browser Interface and not overwrite previous access strings assigned for the Hub Console Interface.

manager. These strings assign you the following read-write privileges. The manager strings are used as your defaults for Hub Console Interface access. Strings you assign in the manager fields will overwrite previous access strings assigned for the Hub Console Interface.

The Device Passwords Window in the Browser Interface contains the following boxes and buttons:

Operator User Name. Enables you to enter a string that will be a username providing read-only privileges.

Operator Password. Enables you to enter a string that will be a password providing read privileges.

Confirm Operator Password. Enables you to verify the read-only password string that you entered by retyping it. The string is not echoed (displayed) in this box when you type it.

Manager User Name. Enables you to enter a string that will be a username providing read-write privileges.

Manager Password. Enables you to enter a string that will be a password providing read-write privileges.

Confirm Manager Password. Enables you to verify the read-write password by retyping it. The string is not echoed (displayed) in this box when you type it.

Apply Changes Button. Stores all password and username strings you have set in the current session.

Clear Changes Button. Removes all password and username strings you have set in the current session.

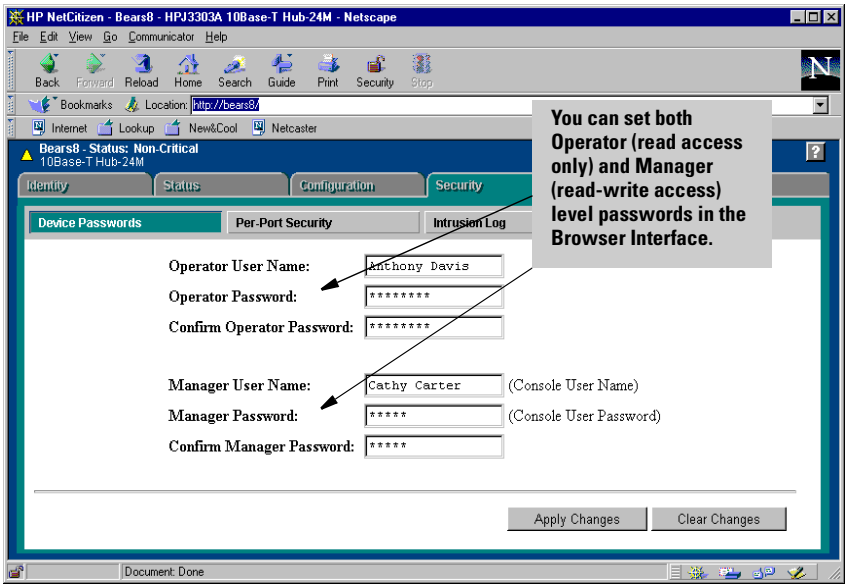


Figure 6-20. The Device Passwords Window

Setting Operator Usernames and Passwords in the Browser Interface

To create an operator username and password, perform the following steps:

1. From the Tab Bar, click on the Security Tab. The Browser Interface displays the Security Button Bar.
2. From the Security Button Bar, click on the Device Passwords Button. The Browser Interface displays the Device Passwords Window.
3. Click in the Operator User Name box and type a string. The string may be separated by spaces and may include any ASCII character in it. The string may be no longer than 15 characters, including spaces.
4. Click in the Operator Password box and type a string. The string should not have spaces, but may include any ASCII character in it. The string may be no longer than 16 characters.

   Note that spaces are allowed in the string (for example, `Jeff Smith`). The string is not echoed in the window.
5. Click in the Confirm Operator Password box and retype the string to validate your entry.

6. Click on the Apply Changes Button. The Browser Interface stores the username and password information and returns you to the Overview Window.

Creating Manager Usernames and Passwords

To create a manager username and password, perform the following steps:

1. From the Tab Bar, click on the Security Tab. The Browser Interface displays the Security Button Bar.
2. From the Security Button Bar, click on the Device Passwords Button. The Browser Interface displays the Device Passwords Window.
3. Click in the Manager User Name box and type a string. The string may be separated by spaces and may include any ASCII character in it. The string may be no longer than 16 characters, including spaces.
4. Click in the Manager Password box and type a string. The string should not have spaces, but may include any ASCII character in it. The string may be no longer than 16 characters. To represent spaces, use the underscore (_) character. The string is not echoed in the window.
5. Click in the Confirm Manager Password box and retype the string to validate your entry.
6. Click on the Apply Changes Button. The Browser Interface stores the username and password information and returns you to the Overview Window.

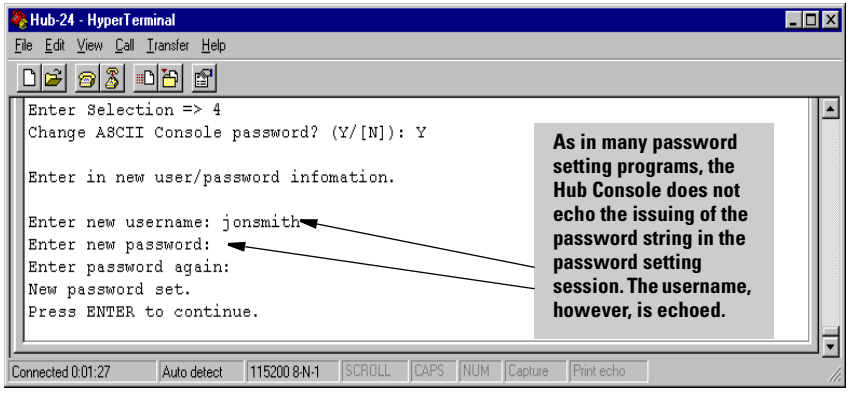


Figure 6-21. The Device Password Option

Setting Usernames and Passwords in the Console

To initially set or change both a username and a password in the Hub Console, perform the following steps:

1. From the Main Menu, type 2 and press Enter. The Hub Console Interface displays the Management Access Configuration Menu.
2. From the Management Access Configuration Menu, type 4 and press Enter. The Hub Console Interface displays the following prompt:

   ```
   Change Hub Console password (Y/[N])?
   ```

3. Type Y and press Enter. The Hub Console Interface displays the following prompt

   ```
   Enter new username:
   ```

4. If you have an existing username, the current string is displayed at the prompt. Type a new username and press Enter. The Hub Console Interface displays the following prompt:

   ```
   Enter new password:
   ```

5. If you have an existing password, the current string is displayed at the prompt. Type a new password and press Enter. The Hub Console Interface displays the following prompt:

   ```
   Enter password again:
   ```

6. Type the password again and press Enter. You have now successfully set or changed both a password and a username.

Telnet Enable/Disable

Attribute	Description
Screen Name	Telnet Enable/Disable
Menu	Management Access Configuration
Function	Enables and disables the ability to access the Hub Console Interface using a Telnet connection.
Common Use	Allowing Telnet session to be run.
Browser Interface Window	None
Browser Interface Tab Bar	None
Default Setting	Enabled

The Telnet Enable/Disable Screen enables and disables the ability to access the Hub Console Interface using a Telnet connection. Note that this feature does not initiate a Telnet session, rather, it provides you the ability to permit users connected to the hub to establish or not establish a Telnet session.

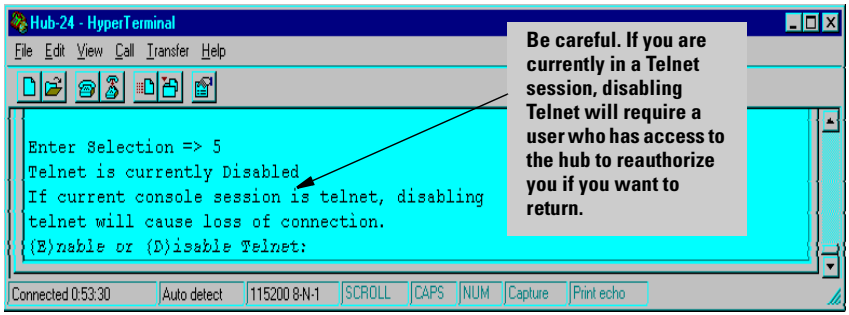


Figure 6-22. The Telnet Enable/Disable Option

Setting Telnet Access on the Hub in the Console

To control Telnet access capability on the hub, perform the following steps:

1. From the Main Menu, type 2. The Hub Console Interface displays the Management Access Configuration Screen.
2. From the Management Access Configuration Screen, type 5 and press Enter. The Hub Console Interface will respond in one of two ways, depending on what state your Telnet control feature has been set.
   - If this is your first session with this feature, the Hub Console Interface displays the following prompt:

     ```
     Telnet is currently Enabled.

     If current console session is telnet, disabling
     telnet will cause loss of connection.

     (E)nable or (D)isable Telnet:
     ```

     Type E and press Enter to enable the Telnet feature. You may now establish a Telnet session with the hub. See chapter 2 for more information on running Telnet with the hub.
   - If you have already enabled the Telnet feature, the Hub Console Interface will display the following prompt:

     ```
     Telnet is current enabled
     ```
   - If you want to disable it, type D and press Enter. You may not establish a Telnet session with the hub now.

Web Enable/Disable

Attribute	Description
Screen Name	Web Enable/Disable
Menu	Management Access Configuration
Function	Turns on and off the ability to manage the hub using the Browser Interface.
Common Use	To keep unauthorized operators from using the Browser Interface.
Browser Interface Window	None
Browser Interface Tab Bar	None
Default Setting	Browser Interface is enabled.

The Web Enable/Disable Screen enables and disables the ability to access the Browser Interface to manage the hub.

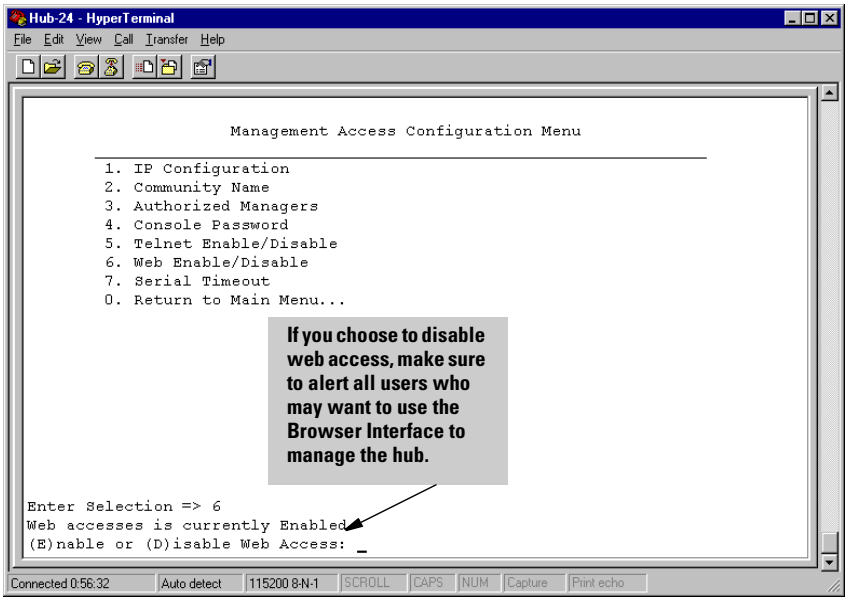


Figure 6-23. The Web Enable/Disable Option

Setting Browser Interface Access on the Hub in the Console

To control Browser Interface access capability on the hub, perform the following steps:

1. From the Main Menu, type 2 and press Enter. The Hub Console Interface displays the Management Access Configuration Screen.
2. From the Management Access Configuration Screen, type 5 and press Enter. The Hub Console Interface will respond in one of two ways, depending on what state your Telnet control feature has been set.
   - If the Browser Interface is current disabled, the Hub Console Interface displays the following prompt:

     ```
     Web accesses is currently Disabled.
     (E)nable or (D)isable Telnet:
     ```

     Type E and press Enter to enable the Browser Interface feature. You may now establish a Browser Interface session with the hub. See chapter 2 for more information on running a Browser Interface session with the hub.
   - If you have already enabled the Browser Interface feature, the Hub Console Interface will display the following prompt:

     ```
     Web accesses is current enabled
     ```
   - If you want to disable it, type D and press Enter. You may not establish a Browser Interface session with the hub now.

Serial Timeout

Attribute	Description
Screen Name	Serial Timeout
Menu	Management Access Configuration
Function	Sets the amount of minutes allowed to lapse before the Hub Console Interface becomes inactive.
Common Use	Launching any second-level menu available from the console.
Browser Interface Window	None
Browser Interface Tab Bar	None
Default	0 minutes

The Serial Timeout Screen enables you to set the amount of minutes allowed to lapse before the Hub Console Interface shuts down (times out). This is useful for security reasons in instances when the Hub Console Interface has detected no activity during a set period of time.

This lack of 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. 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 higher the value, the less secure the Hub Console Interface is. The lower the value, the more secure it is as it will become inaccessible more quickly. The values can be between 0 and 60 minutes. A value of 0 means no timeout.

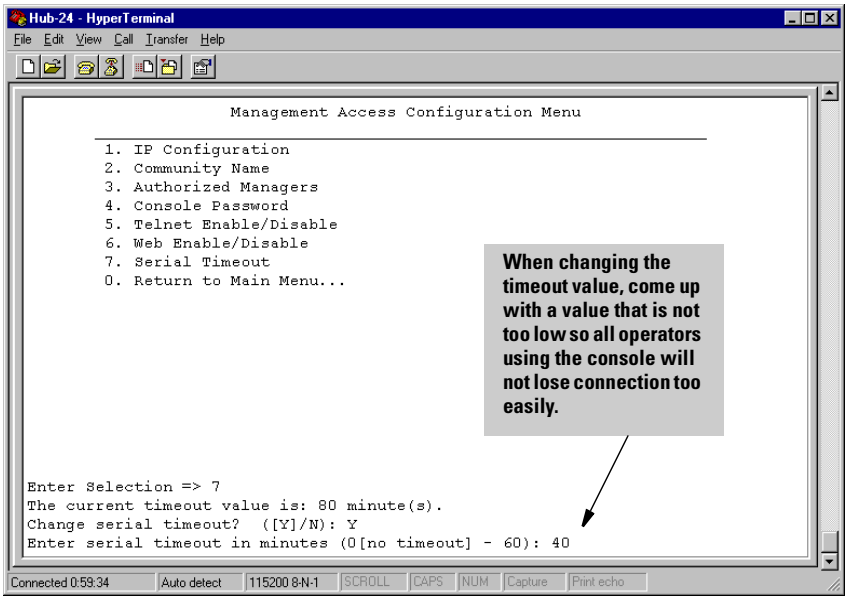


Figure 6-24. The Serial Timeout Option

Setting a Console Serial Timeout Value

To set an Hub Console serial timeout default value, perform the following steps:

1. From the Main Menu, type 2 and press Enter. The Hub Console Interface displays the Management Access Configuration Menu.
2. From the Management Access Configuration Menu, type 7 and press Enter. The Hub Console Interface displays the following prompt:

   ```
   The current timeout value is 0 minutes.

   Change serial timeout: [Y/N]:
   ```

3. Type Y and press Enter to indicate that you want to change the timeout value. The Hub Console Interface displays the following prompt:

   ```
   Enter serial timeout in minutes (0[no timeout] - 60:
   ```

4. Type the number of minutes you want to allow to lapse with no activity on the Hub Console Interface before it becomes inactive. Press Enter.

   The Hub Console Interface timeout value has been changed to the value you have set.

Hub Configuration Menu

Attribute	Description
Screen Name	Hub Configuration Menu
Menu	--
Function	Displays a list of options that enable you to perform hub and port configuration tasks.
Common Use	Launches options that enable you to perform hub and port configuration tasks.
Browser Interface Window	--
Browser Interface Tab	Configuration

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

Hub System Information. Displays hub identification information and system attributes.

Port Enable/Disable. Enables you to turn ports on and off, allowing them to receive and transmit packets.

Port Security. Displays security information about all ports on the hub, showing the address learning method, authorized manager 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 hubs in a cascaded topology, using two separate cables and two ports on each hub. 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 (twisted-pair or AUI/Xcvr) can be used as either the primary or backup port.

Reset Hub to Factory Defaults. Enables you to reinitialize the hub's counters in the event that the device is performing incorrectly. All devices are shipped with various counters, byte addresses and other variables set to specific values. By resetting these parameters, you can correct the performance of a failing device.

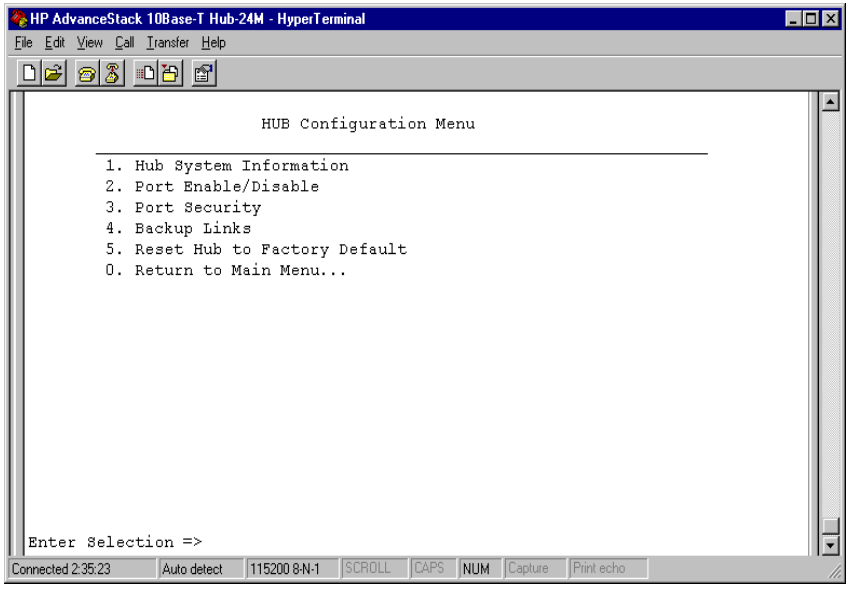


Figure 6-25. The Hub Configuration Menu

Hub System Information

Attribute	Description
Screen Name	Hub System Information
Menu	Hub Configuration
Function	Displays a list of all menus and top-level options available from the console.
Common Use	Launching any second-level menu available from the console.
Browser Interface Window	Identity
Browser Interface Tab	Identity
Defaults	• Port Status: Not active • Link Status: Not detected • Last Heard Source Address: None • Security Information: No violation

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. The information shown in the General System Information Screen is detailed here.

System Name. A label used to associate a common name to identify the device. This can be up to 255 characters, including spaces. For example, `My Hub`.

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. For example, `Wiring Closet -- East`.

Download Version. The versions of ROM and firmware of the device. A sample ROM version is `X.P1.00`. A sample firmware version is `A.0.02`.

System Up Time. 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, `73:43:50`.

Device Fault. Indicates errors discovered during the device self test. Only shown in the console.

MAC Address. The MAC address of the device. For example, `080009-495925`.

Serial Number. The serial number of the device. For example, `SG63401386.`

SNMP Module Security Information. Indicates whether the hub has experienced a violation, generally, an packet from a device or management station that has not been authorized to transmit to the hub.

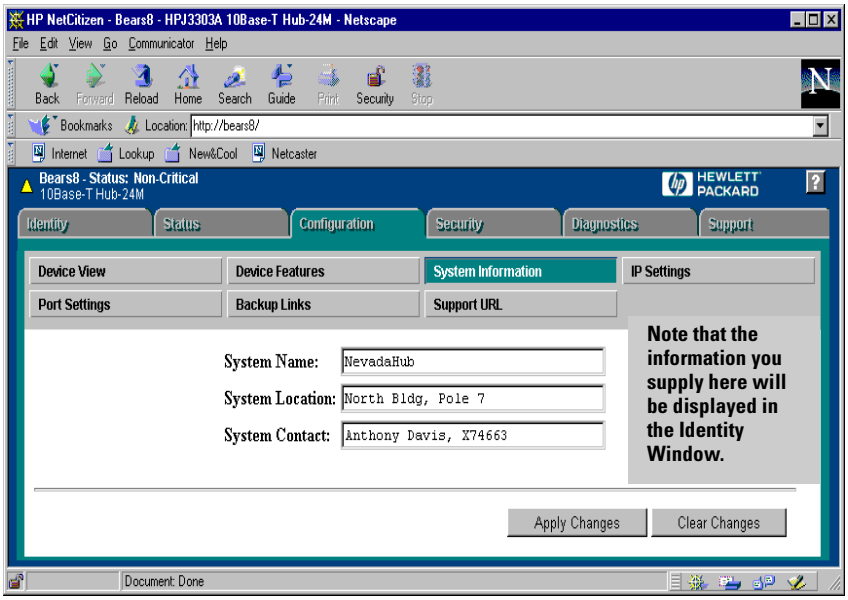


Figure 6-26. The Identity Window

Changing Hub System Information in the Browser Interface

To change hub system information from the Browser Interface, perform the following steps:

1. From the Tab Bar, click on the Configuration Tab. The Browser Interface displays the Configuration Button Bar.
2. From the Configuration Button Bar, click on the System Information Button. The Browser Interface displays the System Information Window.
3. In the System Name box, type in a string that will help you identify the hub.
4. In the System Location box, type in a string that will help you identify where the hub has been placed.
5. In the System Contact box, type in the name of the key person managing the hub.
6. Click on the Apply Changes button.

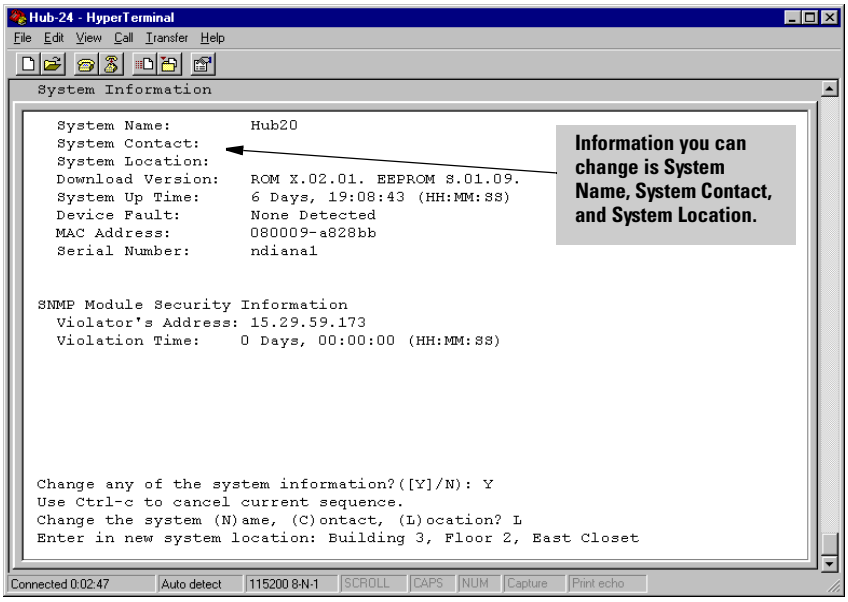


Figure 6-27. The Hub System Information Screen

Changing Hub System Information in the Console

To change hub system information from the Hub Console, perform the following steps:

1. From the Main Menu, type 3 and press Enter. The Hub Console Interface displays the Hub Configuration Menu.
2. From the Hub Configuration Menu, type 1 and press Enter. The Hub Console Interface displays the Hub System Information Screen.
3. From the Hub System Information Screen, type Y and press Enter to enter or change system parameters. The Hub Console Interface displays the following prompt:

   ```
   Change the system (N)ame, (C)ontact, (L)ocation?
   ```

4. To begin entering or changing one or all of these strings, perform the appropriate step:
   - To enter a new system name, type N and press Enter.
   - To enter a new system contact, type C and press Enter.
   - To enter a new system location, type L and press Enter.
   - Using system name as an example, the Hub Console Interface displays the following prompt:

   ```
   Enter in new system location:
   ```

5. Type in any string and press Enter. The string can include spaces and any ASCII character. It can be as long as 255 characters. You have now created a new system parameter.

Port Enable/Disable

Attribute	Description
Screen Name	Port Enable/Disable
Menu	Hub Configuration
Function	Displays a list of all menus and top-level options available from the console.
Common Use	Launching any second-level menu available from the console.
Browser Interface Window	Device View
Browser Interface Tab	Configuration
Default	All ports enabled

The Port Enable/Disable Screen and Device View Window are both used to turn ports on and off so that they can connect to other devices or be inactive. The settings displayed in the Port Enable/Disable Screen are shown here.

The Hub Console Port Enable/Disable Screen

Port Status. Displays a series of squares, each representing each port on the hub, indicating whether the port is enabled or disabled. Each square is labeled with either a number that represents the port number on the hub or the string XCVR which represents the Transceiver Port. Also, each square contains one of the following letters, indicating the status of the port:

E. Indicates the port is on and can receive packets from another device when connected.

D. Indicates the port is off and cannot receive packets from another device when connected.

The Browser Interface Device View Window

Select All Ports Button. Selects all ports on the hub graphic. Selection is indicated by the ports being highlighted or darkened.

Deselect All Ports Button. Removes all ports from selected state.

Enable/Disable Button. Activates or renders inactive any selected port on the hub graphic. This button acts as a toggle. If the port is inactive, pressing this button will enable the port. If the port is active, pressing this button will render the port inactive.

Enable Selected Ports Button. Activates any selected port.

Disable Selected Ports Button. Renders inactive any selected port.

The Device View graphic for HP ProCurve 10Base-T Hubs contains the following graphical objects:

Power LED. Always illuminates green to indicate that power is on. If power is not on, you will not be able to display the Device View.

Fault LED. Illuminates orange in the event of a fault.

Port Region. A view of all RJ-45 ports on your hub. The ports can be in one of three states, represented by one of three colors, detailed in the following table.

Table 6-3. Port State Color Key

Port State	Color	Description
	Green (not actual)	The port is enabled and detects Link Beat on a device connected to the port.
	Gray	The port is enabled, but does not detect Link Beat.
	Gray with a blue diagonal slash	The port is disabled.
	Red (not actual)	This port has been autopartitioned or the port has a security violation.

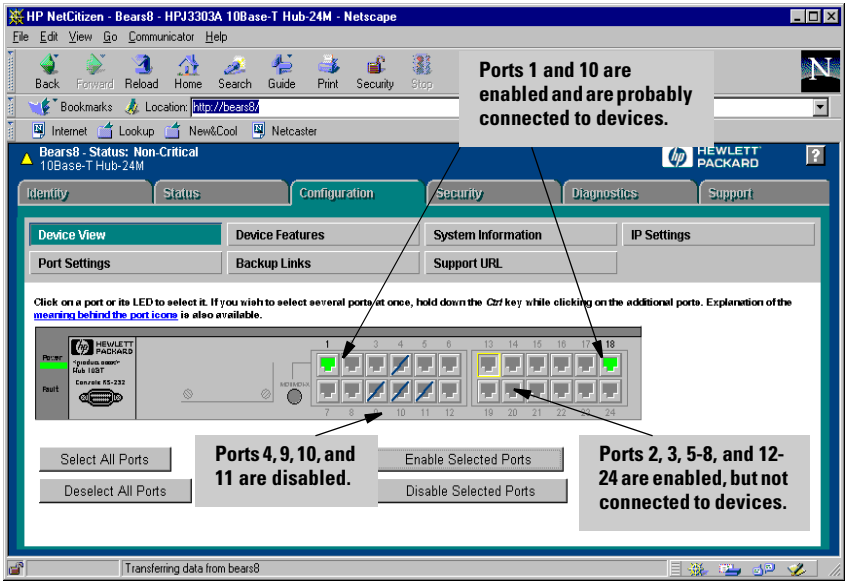


Figure 6-28. The Device View Window

Enabling and Disabling Ports in the Browser Interface

To enable and disable ports using the Device View, perform the following tasks:

1. From the Tab Bar, click on the Configuration Tab. The Browser Interface displays the Configuration Button Bar.
2. From the Configuration Button Bar, click on the Device View Button. The Browser Interface displays the Device View Window which contains a panel graphic of your hub. The window initially shows the following message laid over the panel graphic.

   `Retrieving Port Status`

   This message indicates that the Browser Interface application is retrieving port state information from your HP ProCurve 10Base-T Hub for all the ports on the hub.
3. Take a moment to review the panel graphic. It is a representation of what you see on the front of your device.

4. To enable a port that is disabled, click the left mouse button on a gray-colored port. The Browser Interface highlights the port a blue border, indicating the port has been selected. The port can display one of two states:
   - green, indicating the port is enabled and detects Link Beat from another device connected to port. This state means the port is functioning properly.
   - gray with a blue diagonal slash through it, indicating the port is enabled, but does not detect Link Beat from another device. This state means the port either does not have a cable from another device plugged in to it, or the connecting device is faulty.
   - red, indicating the port has been autopartitioned or the port has a security violation.
5. To disable a port that is enabled, click the left mouse button a green-colored port or a gray-colored port with a diagonal slash through it. The port color turns to gray, indicating it can no longer connect to another device.

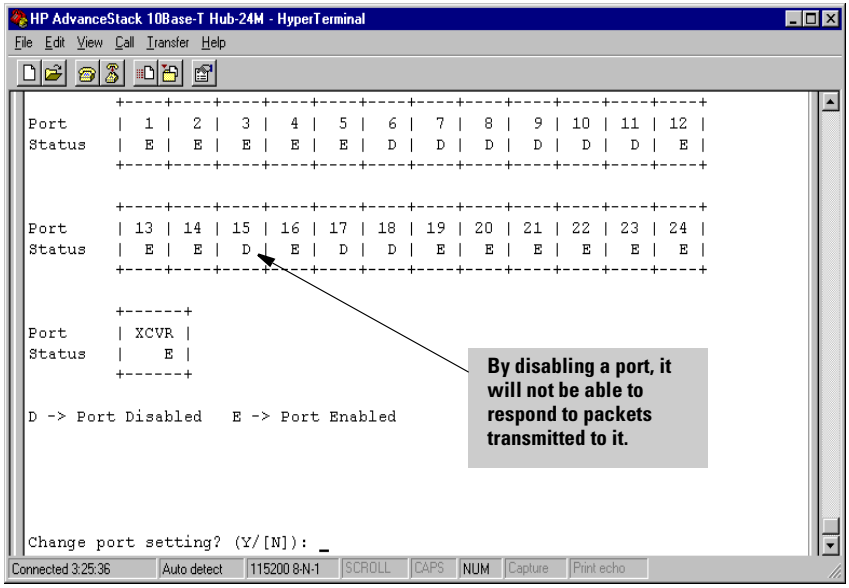


Figure 6-29. The Port Enable/Disable Screen

Enabling and Disabling Ports in the Console

To enable and disable ports using the Port Enable/Disable Screen in the Hub Console Interface, perform the following tasks:

1. From the Main Menu, type 3 and press Enter. The Hub Console Interface displays the Hub Configuration Menu.
2. From the Hub Configuration Menu, type 2 and press Enter. The Hub Console Interface displays the Port Enable/Disable Screen. Note two aspects of the screen:
   - it displays a representation of ports on the hub shown in the series of boxes containing port numbers. If you have a 24-port hub, you will see 25 boxes (24 boxes for RJ-45 ports 1-24 and one box for the XCVR port).
   - each box contains one of two settings, a `D`, indicating the port is disabled or an `E`, indicating the port is enabled.
3. To change a port setting, type `Y` at the `Change port setting?` prompt and press Enter. The screen displays the following prompt:

   ```
   Enter range of ports to disable or enable, Examples:
   1-3,6, XCVR

   (range 1-#, XCVR, ALL)
   ```

4. Type a number and press Enter. You can enter port numbers in the following fashion:
   - a discrete number, for example, 5
   - multiple discrete numbers, separating each with a comma, for example, 3, 11, 19
   - a range of port numbers, using a dash, for example, 3-6
   - both a discrete number and a range of numbers separated by a comma, for example, 3-6, 9
   - multiple ranges of numbers separated by a comma, for example, 3-6, 19-21
   - X or XCVR can be inserted in any of the above conventions to indicate the XCVR port.

   The console displays the following prompt:

   ```
   Configure Port as (D)isabled or (E)nabled:
   ```

5. Type E to enable the port or D to disable it and press Enter.

   The console displays the hub graphic with the new port status.

Port Security

Attribute	Description
Screen Name	Port Security
Menu	Hub Configuration
Function	Sets security parameters on the hub, providing address selection for intruder prevention and eavesdrop detection.
Common Use	Learning of unauthorized ports that attempt to communicate with the hub.
Browser Interface Window	Port Security
Browser Interface Tab	Security
Default	• Address Selection: Continuous • Eavesdrop Prevention: No • Send Alarm: No • Disable Port: No

The Port Security Screen displays a port list that provides several columns of information about the state of all ports on the hub. The columns of information are:

Port. Indicates the port label on the hub.

`1-12` and `XCVR` on the Hub 12

`1-24` and `XCVR` on the Hub-24

Address Selection. Indicates the Address Selection method used on the port. The settings can be:

`Continuous`. The hub learns the address of the device attached to the port and makes it the authorized address.

`First Heard`. The hub learns the address of the 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 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 a packet not intended for the port will be received by the port.

Send Alarm. Indicates whether an alarm will be sent to a log when an incoming packet from the connected node does not match the authorized address. 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 and Eavesdrop Prevention is enabled.

`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 when Eavesdrop Prevention is enabled.

`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 (Browser Interface only). Stores the security settings you have configured for ports on the hub.

Note that you cannot control Port Security settings from the Hub Console Interface. You need to use the Browser Interface or HP Top Tools for Hubs and Switches to set security parameters. You can only disable security from a port, using the Hub Console Interface.

Take a moment to review the settings in the Port Security environment. Additionally, you may want to become comfortable with several concepts before continuing. Network security comprises several features that are commonly used for protecting your device from potential problems.

The features used are described below.

Intruder Prevention

A feature that 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 the port is allowed to connect. The three address selection methods are:

- First Heard
- Continuous
- Assigned

See the section, “About 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.

Eavesdrop Detection

A feature that stops a device connected to a port on the hub from seeing 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.

Understanding Address Selections 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. The port performs this task by comparing addresses in the source header of a packet with preset address tables that compile lists of acceptable source addresses. The address tables can be very restrictive in allowing for packet reception or less restrictive. Address tables are determined by the Address Selection method you set for the port. The three address selection methods are:

Continuous. 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 learned and becomes the authorized address.

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.

Table 6-4. Alarm Destinations for Unauthorized Packet Events

Environment	Logging Facility
HP Browser Interface	Browser Interface Security Intruder Log
HP Hub Console Interface	Hub Console Interface Security Intruder Log (alarms are automatically logged in the console whether traps are set or not.)
HP Top Tools for Hubs and Switches	HP Top Tools for Hubs and Switches Notification Manager
Third Party SNMP Managers	Logs of other SNMP managers you may have running in tandem with the Browser Interface.

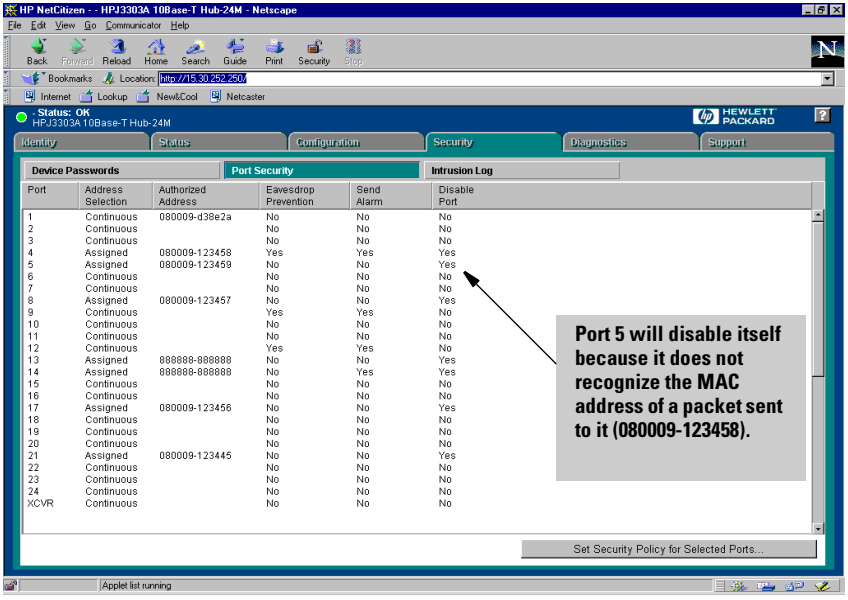


Figure 6-30. The Port Security Window

Setting Security on Ports in the Browser Interface

To set security parameters on a port on the hub, perform the following steps:

1. From the Tab Bar, click on the Security Tab. The Browser Interface displays the Security Button Bar.
2. From the Security Button Bar, click on the Port Security Button. The Browser Interface displays the Port Security Window. Note the window contains a Port List with columns of security information corresponding to it.
3. Launch the Port Security Configuration Window. You can do this in one of two ways:
   - Double click on the port.
   - Click on a port to highlight it (the port number and all corresponding fields of information are darkened). Then click on the Set Security Policy for Selected Ports Button.

   The Browser Interface displays the Port Configuration Window. Take a moment to review this window. It contains several fields and list boxes that enable you to set security parameters. Also, note the current port selected is displayed at the top of the Window.

4. From the Address Selection list box, select the Address Selection method you want to use. The options are:
   - continuous
   - first heard
   - assigned

   For more detail on these address selection methods, see the discussion on address selection methods at the beginning of this section.

5. If you selected the Assigned address selection method, in the Authorized Address box, type the MAC address of the device you want to permit to communicate with the current port.

6. From the Prevent Eavesdropping list box, select the appropriate setting for this feature. The settings are:

   `Yes.` Directs the hub to block transmission of packets not directed to the device connected on that port.

   `No.` Directs the hub to transmit packets to all devices.

7. From the Send Alarm list box, select the appropriate setting for this feature. The settings are:

   `Yes.` Directs the hub to send an alarm to one of the logs detailed in the table earlier in the section:

   `No.` Directs the hub to not generate an alarm.

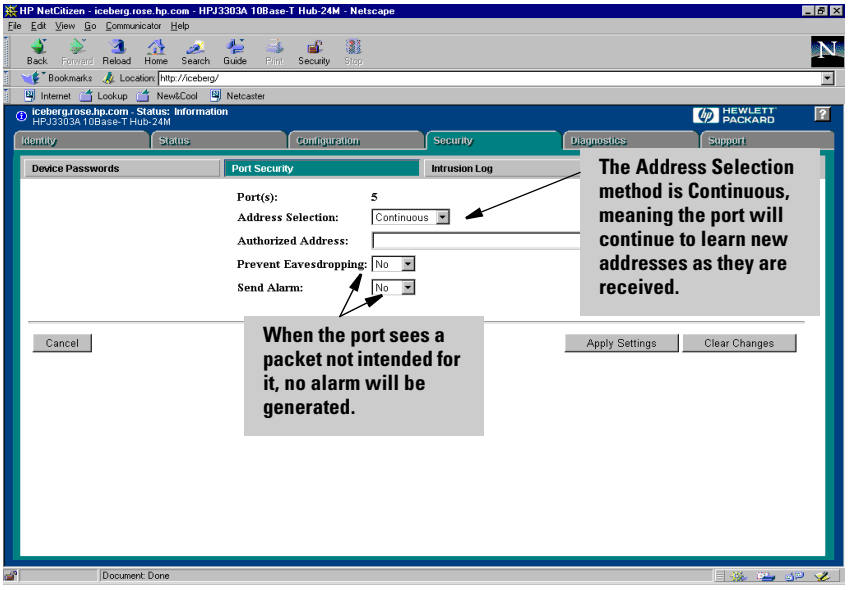


Figure 6-31. The Port Security Configuration Window

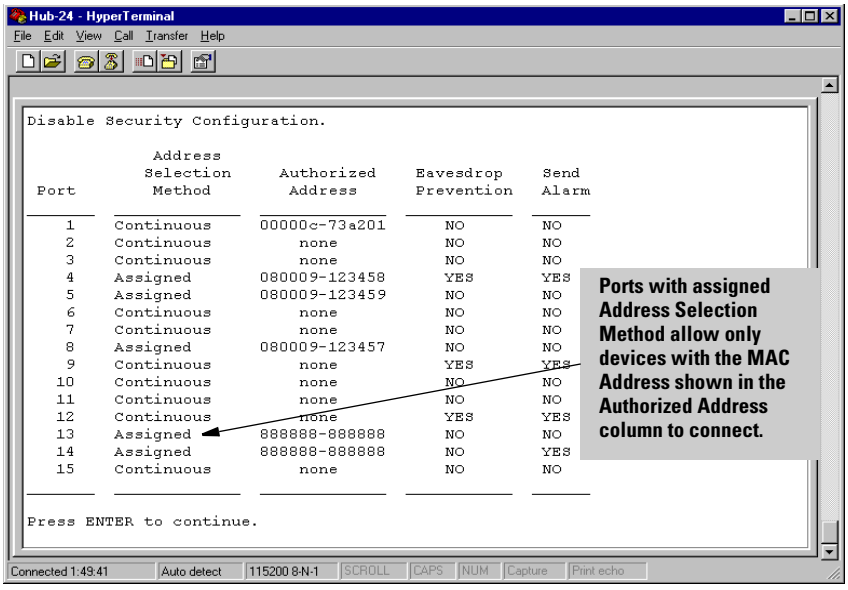


Figure 6-32. The Port Security Screen

Disabling Security from Ports in the Console

You can disable security from ports. To disable security on a port, perform the following steps:

1. Type Y at the prompt `Disable Security from the Ports` and press Enter. The screen displays the following prompt:

   `Apply the disabled security to which ports`

2. Type the port number for which you want security disabled and press Enter. You have several different methods for entering port numbers.
   - For a single port, simply type the port number.
   - For consecutive ports, you can type a range value in, using a dash. For example 3-7 indicates you want to disable security for ports 3, 4, 5, 6, and 7.
   - For a mix of consecutive and non-consecutive ports, you can use both dashes and commas. For example, 3-7, 12, 19 indicates you want to disable security for ports 3, 4, 5, 6, 7, 12, and 19.

After you have typed the port number(s), press Enter. The screen displays the following prompt:

`Continue with security disable`

3. Type Y and press Enter. The port list is redistilled, indicating disabled security for the ports you selected. Disabled security is indicated by the following settings:

   None in the Authorized Address column

   No in the Eavesdrop Prevention column

   No in the Send Alarm column

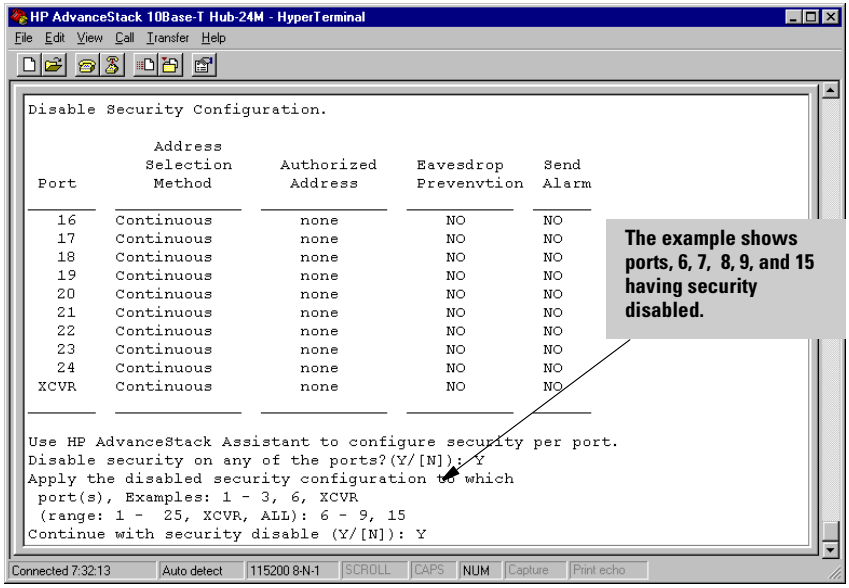


Figure 6-33. Disabling Port Security from the Port Security Screen

Backup Links

Attribute	Description
Screen Name	Backup Links
Menu	Hub Configuration
Function	Configure a primary and a redundant communication link or path between the hub and any other device.
Common Use	Creating a redundant communication link between the hub and any other device.
Browser Interface Window	Backup Links
Browser Interface Tab	Configuration
Default Settings	• Test Time: 1 Second • Retries: 2

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 current or local HP ProCurve 10Base-T Hub is defined as the connection to the primary path to the other device and another port on the current 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 network ports (twisted-pair or AUI/Xcvr) can be used as either the primary or backup port. A maximum of four backup links can be created.

The Backup Links Screen has the following fields

Backup Link. Provides the number or name of the backup link as it appears in the list of entries in the Backup Links Screen. When no backup link is configured, this column displays nothing.

MAC Address. Provides the MAC address of the alternate hub that will become the backup hub in the event of a failure by the primary hub.

Status. Indicates the current use 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 on the primary port.

Using Backup. Indicates the hub is using the backup port.

Primary Port. Indicates the number of the port on the hub. This port is used during a standard connection of a hub and the connected device.

Backup Port. Indicates the number of the backup port on the hub.

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 Browser Interface) Indicates the limit of the number of times the hub does not receive a response from test packets sent to its target device before the hub disables the primary port and activates the backup link. The number can be between 1 and 16.

Add New Backup Link Button. Begins a backup link add session.

Delete Selected Items Button. Restores all settings to values present during the last session when settings were stored.

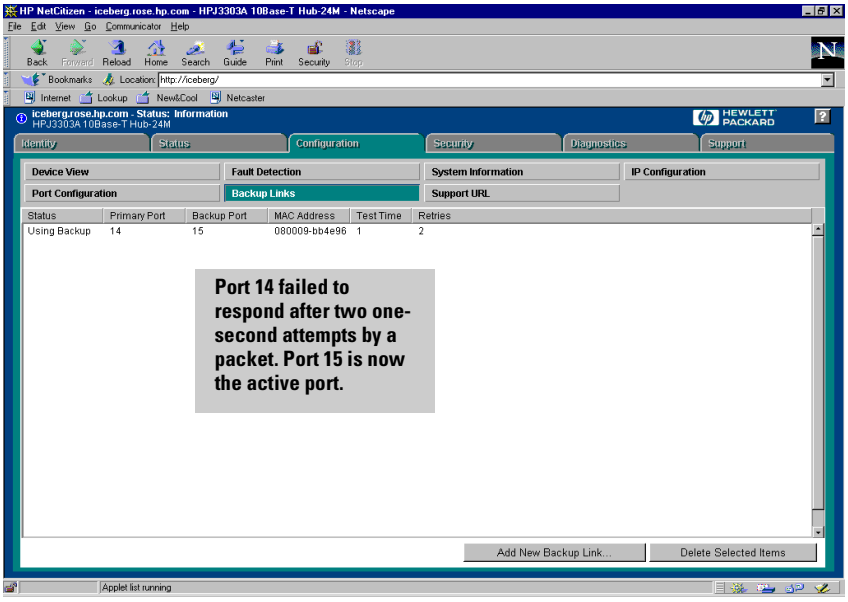


Figure 6-34. The Backup Links Window

Setting Backup Links in the Browser Interface

To set backup links from the Browser Interface, perform the following steps:

1. From the Tab Bar, click on the Configuration Tab. The Browser Interface displays the Configuration Button Bar.
2. From the Configuration Button Bar, click on the Backup Links Button.The Browser Interface displays the Backup Links Window.
3. Click on the Add New Backup Link Button. The Browser Interface displays the Backup Links Configuration Window.
4. From the Primary Port list box, select the number of the port on the hub for which you want to assign a backup port.
5. From the Backup Port list box, select the number of the port on the hub that will act as the backup port when the primary port fails.
6. From the MAC Address box, type the MAC address of the remote device to which primary and backup ports connected.
7. From the Test Time box, type the number of seconds to lapse between packets transmitted on the primary port to verify that it continues to operate correctly.

8. From the Retries box, type the number of times you will allow the port to time out during test packet transmissions because of no response from the remote device before being disabled.

9. Press the Apply Changes Button.

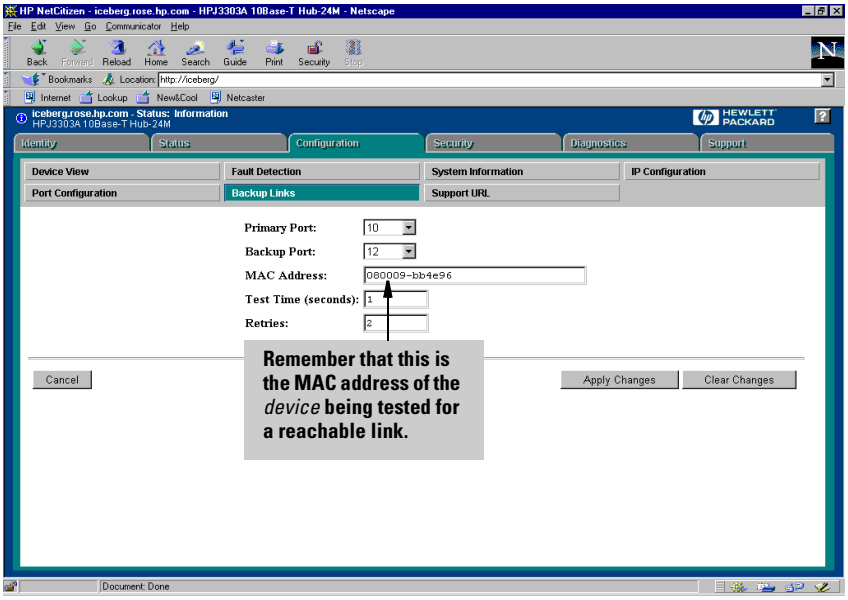


Figure 6-35. The Backup Links Configuration Window

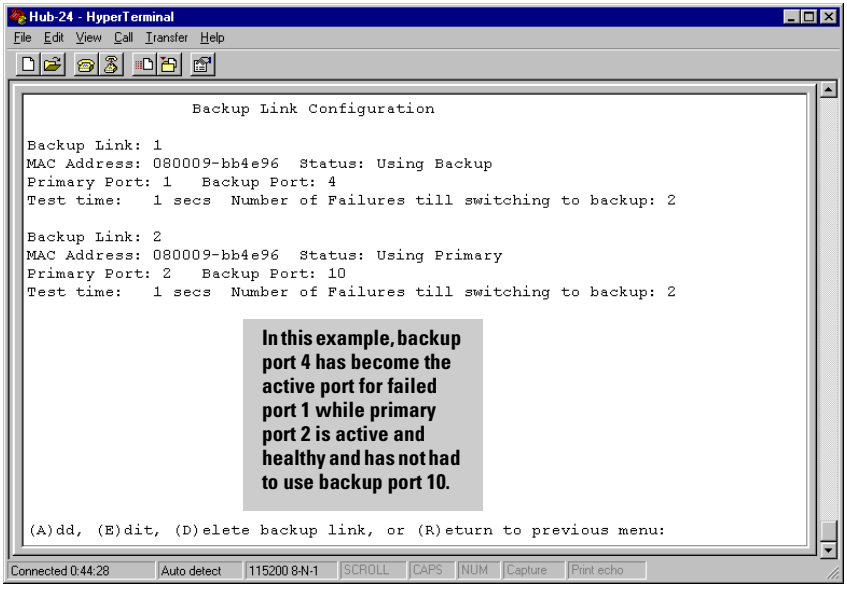


Figure 6-36. The Backup Links Screen

Setting Backup Links in the Hub Console

To set Backup Links from the Hub Console Interface, perform the following steps:

1. From the Main Menu, type 3 and press Enter. The Hub Console Interface displays the Hub Configuration Menu.
2. From the Hub Configuration Menu, type 4 and press Enter. The Hub Console Interface displays the Backup Links Configuration Screen.

To Add a Backup Link, perform the following

1. Type A and press Enter. The Hub Console Interface displays the following prompt:

   ```
   Enter in primary port in backup link configuration
   (1-24, XCVR):
   ```

2. Type the number of the port for which you want to assign a backup port. Press Enter. The Hub Console Interface displays the following prompt:

   ```
   Enter in backup port in backup link configuration (1-
   24, XCVR):
   ```

3. Type the number of the port that will act as the backup port when the primary port fails. Press Enter. The Hub Console Interface displays the following prompt:

   ```
   Enter in MAC Address of test destination.
   ```

4. Type the MAC address of the remote device you are trying to reach. Press Enter. The Hub Console Interface displays the following prompt:

   ```
   Enter in test time (1 - 15 sec#)
   ```

5. Type the number of seconds that you want to lapse between test packets transmitted on the primary link to verify that it continues to operate correctly. Press Enter. The Hub Console Interface displays the following prompt:

   ```
   Enter in consecutive failures (1-16):
   ```

6. Type the number of times you allow the port to time out during test packet transmissions before being disabled. Press Enter. The Backup Links dialog box displays the information shown in the screen on the previous page.

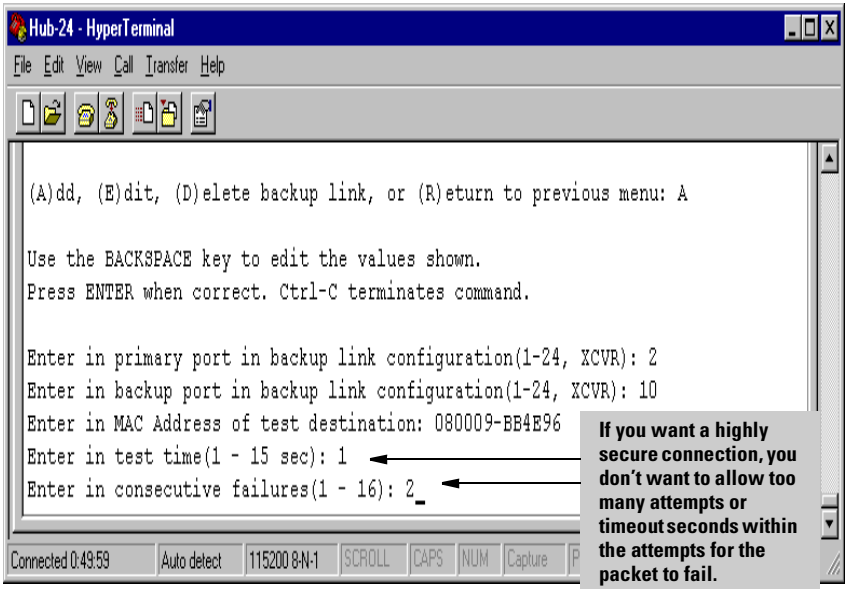


Figure 6-37. Adding a Backup Link

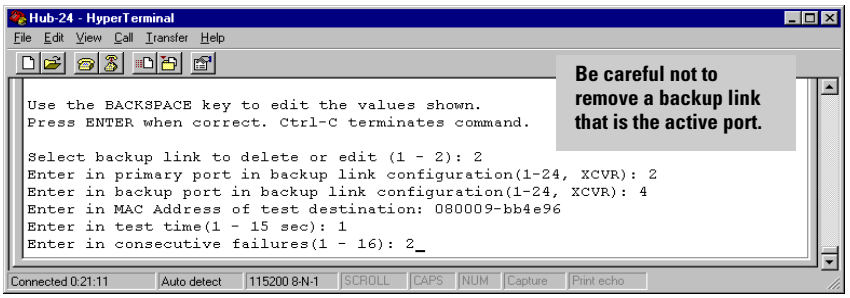


Figure 6-38. Editing a Backup Link

To edit or delete a Backup Link

1. Type E to edit a backup link or D to delete a backup link and press Enter. The Hub Console Interface displays the following prompt:

   ```
   Select backup link to delete or edit (1-#):
   ```

2. Type the number of the backup link that you want to modify and press Enter.

   ```
   Enter in primary port in backup link configuration (1-24, XCVR):
   ```

3. Type the number of the port on the local hub for which you want to reassign a backup port or delete a backup link assignment. Press Enter. The Hub Console Interface displays the following prompt:

   ```
   Enter in backup port on Backup Link Configuration (1-24):
   ```

4. Type the number of the port that will act as the backup port when the primary port fails. Press Enter. The Hub Console Interface displays the following prompt:

   ```
   MAC Address of test destination.
   ```

5. Type the MAC address of the remote device that you are trying to reach. Press Enter. The Hub Console Interface displays the following prompt:

   ```
   Enter in test time (1 - 15 sec):
   ```

6. Type the number of seconds that you want to lapse between test packets transmitted on the primary link to verify that it continues to operate correctly. Press Enter. The Hub Console Interface displays the following prompt:

   ```
   Enter in consecutive failures (1-16):
   ```

7. Type the number of times you will allow the port to time out during the text packet transmissions before being disabled. Press Enter. The Backup Links Screen displays the information shown in the sample screen.

Reset Hub to Factory Default

Attribute	Description
Screen Name	Reset Hub to Factory Default
Menu	Hub Configuration
Function	Reinitializes the hub's configuration.
Common Use	Correcting a corrupted hub that was altered by a computer virus, network bottlenecking, a power failure, and other irregular activities.
Browser Interface Window	Factory Reset
Browser Interface Tab	Diagnostics
Default Setting	None

Factory resets remove any configuration changes performed on the device after it has been removed from its original packaging. This includes all IP address configurations. Consequently, the device management functions will be reachable only if you have configured the device via Bootp or DHCP servers.

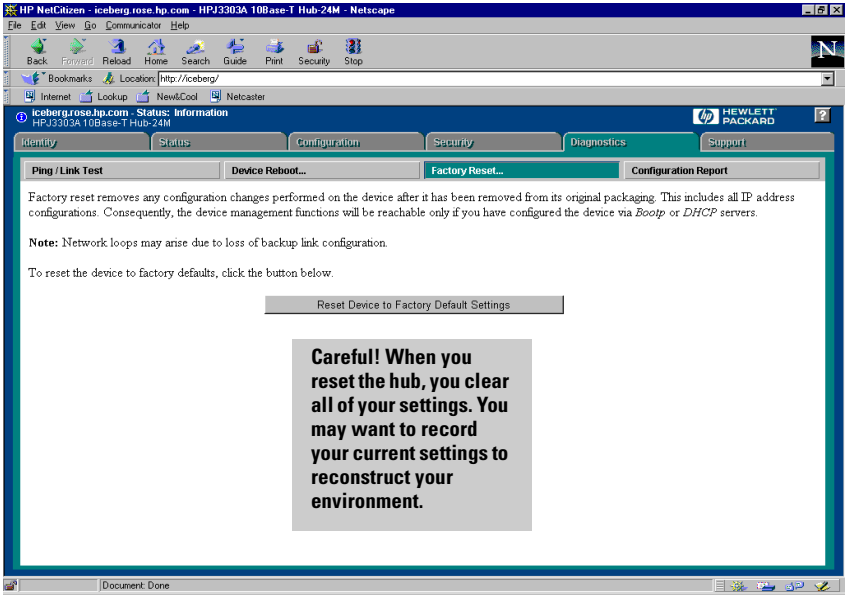


Figure 6-39. The Factory Reset Window

Resetting the Hub in the Browser Interface

To reset the hub from the Browser Interface, perform the following tasks:

1. From the Tab Bar, click on the Diagnostics Tab. The Browser Interface displays the Diagnostics Button Bar.
2. From the Diagnostics Button Bar, click on the Factory Reset Button. The Browser Interface displays the Factory Reset Window.
3. Click on the Reset Device to Factory Defaults Button.

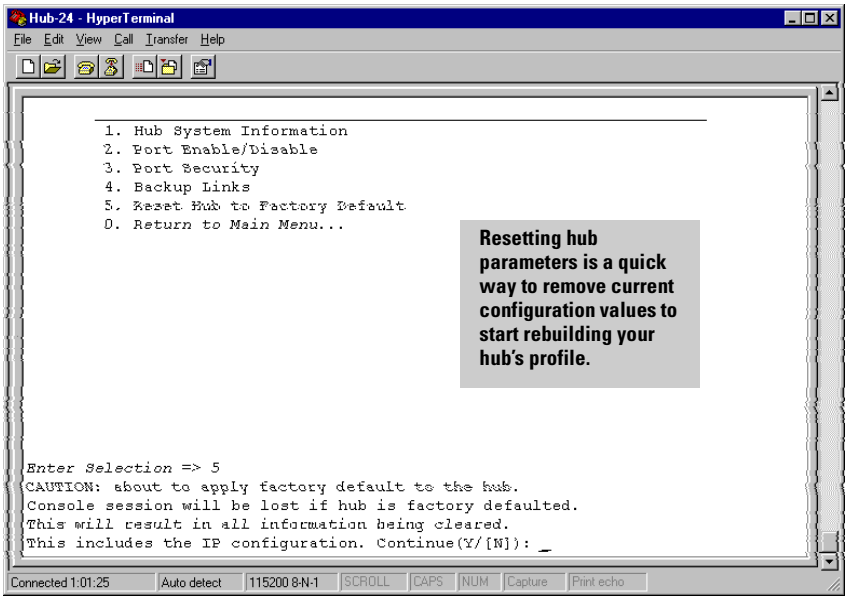


Figure 6-40. The Reset Hub to Factory Default Option

Resetting the Hub to Factory Defaults in the Console

To reset the hub to factory defaults from the Hub Console Interface, perform the following steps:

1. From the Main Menu, type 3 and press Enter. The Hub Console Interface displays the Hub Configuration Menu.
2. Type 5 and press Enter. The Hub Console Interface displays the following prompt:

   ```
   CAUTION: about to apply factory default to the hub.

   Console session will be lost if hub is factory
   defaulted.

   This will result in all information being cleared.

   This includes the IP configuration. Continue(Y/[N]):
   ```

3. Please consider whether you really want to reset the hub. If you do, you will lose all your information that you have built up during multiple configurations (for example, Port Security, Backup Links, Community Names).

4. If you are sure you want to clear all values and reset the hub, type Y and press Enter.

   Note that if backup links were configured, possible network loops will occur on a factory default.

Diagnostics Menu

Attribute	Description
Screen Name	Diagnostics Menu
Menu	--
Function	Displays a list of options available pertaining to network device troubleshooting.
Common Use	Launching any option pertaining to troubleshooting.
Browser Interface Window	--
Browser Interface Tab Bar	Diagnostics

The Diagnostics Menu contains several options pertaining to network device troubleshooting. You can isolate faults by running Link Test (MAC Addresses) or Ping Tests (IP Addresses). Options in the Diagnostics Menu are:

Link Test. Runs a test of the connection between the device (the "local" device) and a designated remote device. During the link test, IEEE 802.3 test packets are sent the number of times chosen from the local device to the designated remote device. The remote device returns the data to the local device, where it is compared to the data transmitted. If the received data matches the transmitted data, the test passes.

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.

Ping Test. Runs a test of the path between the managed device and another device on an IP network that responds to IP (Internet Protocol) 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 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.

Browse Hub Configuration. Provides a master dump of many status screens available from the Hub Console Interface. The screens all show their current values.

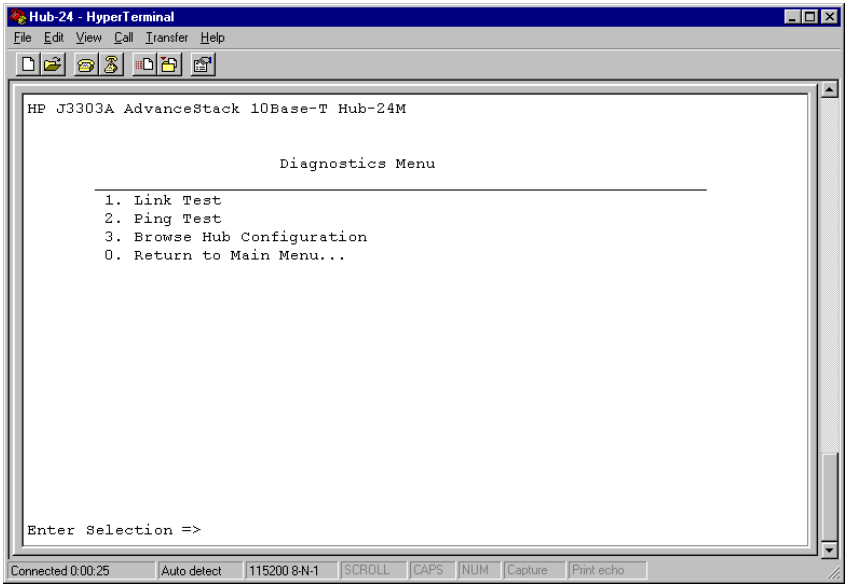


Figure 6-41. The Diagnostics Menu

Ping Test

Attribute	Description
Screen Name	Ping Test
Menu	Diagnostics
Function	Tests the path between the managed device and another device on an IP network that responds to packets.
Common Use	Indicates whether the hub is communicating properly with devices on the network or other networks.
Browser Interface Window	Ping/Link Test
Browser Interface Tab Bar	Diagnostics
Default Setting	• Number of Repetitions: 10 • Timeout in Seconds: 2

The Ping Test tests the network layer (IP Address) path between the managed device 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. The Ping Test is useful because they can tell you whether the HP ProCurve 10Base-T Hub you are managing is communicating properly with another device on the network.

The Ping Test Window in the Browser Interface displays the following graphical objects:

Status Bar. Displays varying portions of the bar in green and red. The amount of both green and red area is a proportional representation of how many successful and failed tests have been reported in the current session. If the bar is mostly red, you may want to check for connection problems.

Destination IP/MAC Address. Indicates the network address (for the Ping Test) or the MAC address (for the Link Test) of the device to which you want to test a connection with the current device.

Number of Packets to Send. Indicates the number of times you want the current device to attempt to test a connection with another device before terminating further connection tests. Can be 1, 5, 10, or 20 on the Browser Interface and 1 through 10,000 in the Hub Console Interface.

Timeout in Seconds. Indicates the number of seconds you want the current device to attempt to test a connection with another device before determining the current test shows a failed connection and reinitiating a test. Can be between 1 through 30.

Start. Initiates the connectivity test.

Stop. Halts the Ping Test.

Defaults. Places default values for the connectivity test parameters. The default values are:

The Ping Test fields in the Hub Console are as follows:

Test Attempts. Indicates the number of times the hub tried to successfully send a packet to the test device.

Test Successes. Indicates he number of times the hub successfully sent a packet to the test device.

Min Response Time (ms). Indicates the number of milliseconds of the least time consuming packet sending test attempt.

Max Response Time (ms). Indicates the number of milliseconds of the most time consuming packet sending test attempt.

Total Response Time (ms). Indicates the total number of milliseconds for all packets sending test attempts.

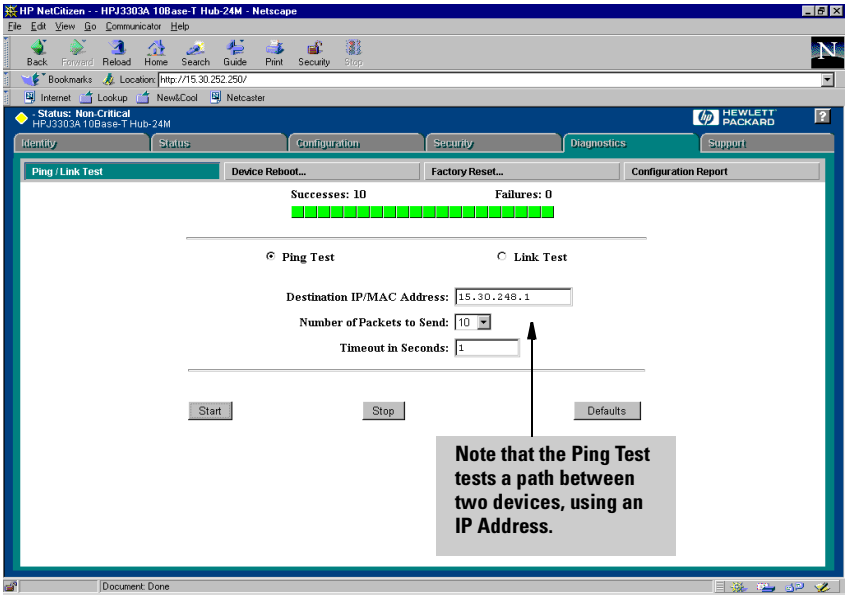


Figure 6-42. The Ping/Link Test Window Running a Ping Test

Running a Ping Test in the Browser Interface

To run a Ping Test from the Browser Interface, perform the following steps:

1. From the Tab Bar, click on the Diagnostics Tab. The Browser Interface displays the Diagnostics Button Bar.
2. From the Diagnostics Button Bar, click the left mouse button the Ping/Link Test button. The Browser Interface displays the Ping/Link Test Window. Note that one of the top two radio buttons can be selected. If this session is your first time in the Ping/Link Test Window for your HP ProCurve 10Base-T Hub, the Ping Test radio button will be selected.
3. Decide whether you want to use the default values set up for either a Ping or Link Test. If you do, click the left mouse button the Defaults Button and go to Step 7. If not, go to the next step.
4. Click the left mouse button on the Ping Test radio button.
5. In the Destination IP/MAC Address box, type an IP Address. for example, 25.100.16.4
6. In the Number of Packets to Send box, use the list box to select a number, either 1, 5, 10, or 20, to indicate the number packets the HP ProCurve 10Base-T Hub should send to the test device to determine whether a valid connection exists between the two devices.

7. In the Timeout in Seconds box, type a number between 1 and 30 that indicates the number of seconds the hub should wait for a response to a test packet request from the target device.
8. Click the left mouse button on the Start button.

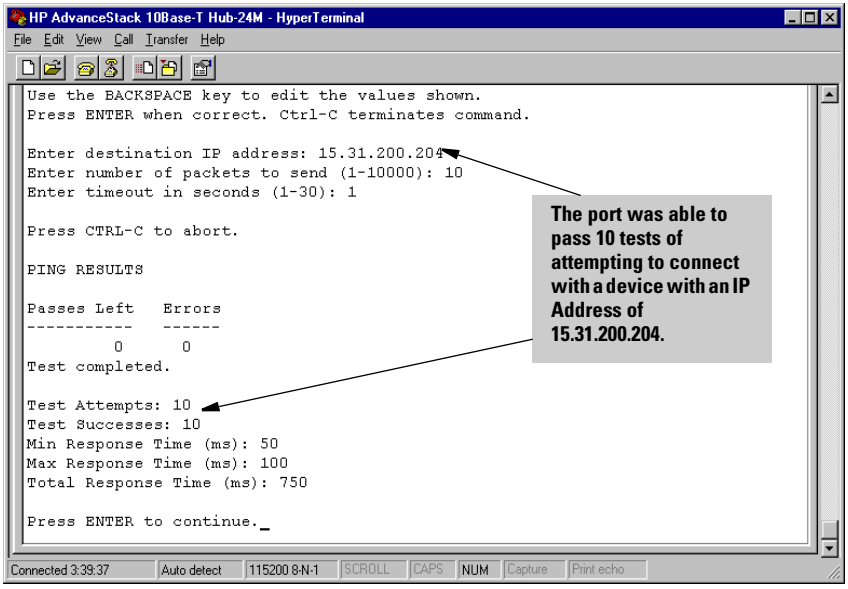


Figure 6-43. The Ping/Link Test Screen Running a Ping Test

Running a Ping Test in the Console

To run a Ping Test in the Hub Console Interface, perform the following steps:

1. From the Main Menu, type 4 and press Enter. The Hub Console Interface displays the Diagnostics Menu.
2. From the Diagnostics Menu, type 2 and press Enter. The Hub Console Interface displays the Ping Test Screen.
3. Type the IP Address of the hub at the Enter Destination IP Address prompt and press Enter. The Hub Console Interface displays the following prompt:

   ```
   Enter number of packets to send.
   ```

4. Type a number at that indicates the number of packets the hub should send to the test device to determine whether a valid connection exists between the two devices. Press Enter. The Hub Console Interface displays the following prompt:

   ```
   Enter timeout in seconds (1-30)
   ```

5. Type a number between 1 and 30 that indicates the number of seconds the hub should wait for a response from the target device. Press Enter.

   The Hub Console Interface indicates the following information:

   - **Test Attempts.** The number of times the hub tried to successfully send a packet to the test device.
   - **Test Successes.** The number of times the hub successfully sent a packet to the test device.
   - **Min Response Time (ms).** The number of milliseconds of the least time consuming packet sending test attempt.
   - **Max Response Time (ms).** The number of milliseconds of the most time consuming packet sending test attempt.
   - **Total Response Time (ms).** The total number of milliseconds for all packets sending test attempts.

Link Test

Attribute	Description
Screen Name	Link Test
Menu	Diagnostics
Function	Tests the connection between a local device and a designated remote device.
Common Use	Indicates whether the hub is communicating properly with another device.
Browser Interface Window	Ping/Link Test
Browser Interface Tab	Diagnostics
Default Settings	• Number of Packets to Send: 10 • Per-Packet Timeout in Seconds: 1

The Link Test is a test of the link layer (MAC Address) connection between a local device and a designated remote device. During the Link Test, an IEEE 802.3 test packets are sent from the local device to the remote device. The remote device returns the data to the local device, where it is compared to the data transmitted. If the received data matches the transmitted data, the test passes. The remote device must be able to recognize an IEEE 802.2 test packet to be able to respond.

The Link Test is useful because it can tell you whether the hub you are managing is communicating properly with another device.

The Link Test Window in the Browser Interface displays the following graphical objects:

Status Bar. Displays varying portions of the bar in green (at the left section of the bar) and red (at the right section of the bar). The amount of both green and red area is a proportional representation of how many successful and failed tests have been reported in the current session. If the bar is mostly red, you may want to check for connection problems.

Destination IP/MAC Address. Indicates the network address (for the Ping Test) or the MAC address (for the Link Test) of the device to which you want to test a connection with the current device.

Number of Packets to Send. Indicates the number of times you want the current device to attempt to test a connection with another device before terminating further connection tests. Can be 1, 5, 10, or 20 on the Browser Interface and 1 through 10,000 in the Hub Console Interface.

Timeout in Seconds. Indicates the number of seconds you want the current device to attempt to test a connection with another device before determining the current test shows a failed connection and reinitiating a test. Can be 1 through 30.

Start. Initiates the connectivity test.

Stop. Halts the Ping Test.

Defaults. Places default values for the connectivity test parameters. The default values are:

The fields in the Hub Console are as follows:

Test Attempts. Indicates the number of times the hub tried to successfully send a packet to the test device.

Test Successes. Indicates the number of times the hub successfully sent a packet to the test device.

Min Response Time (ms). Indicates the number of milliseconds of the least time consuming packet sending test attempt.

Max Response Time (ms). Indicates the number of milliseconds of the most time consuming packet sending test attempt.

Total Response Time (ms). Indicates the total number of milliseconds for all packets sending test attempts.

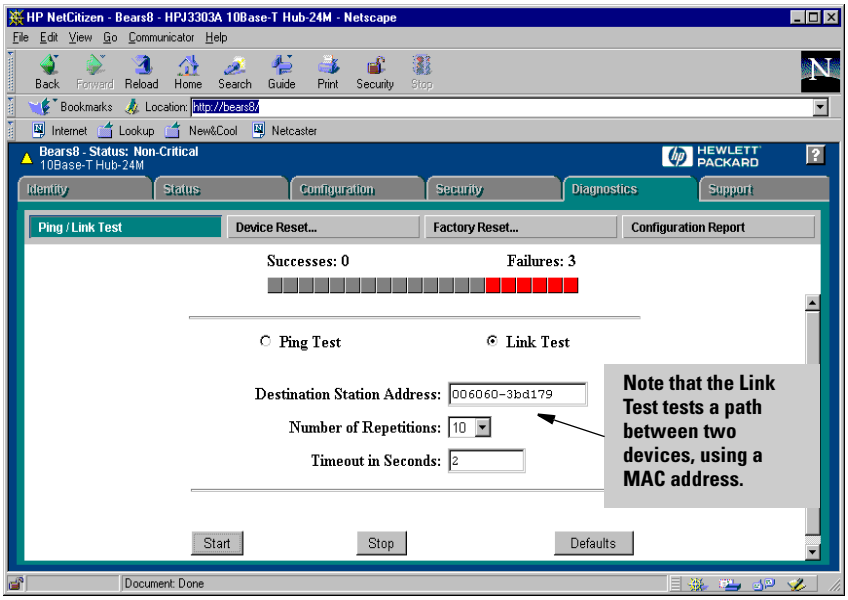


Figure 6-44. The Ping/Link Test Window Running a Link Test.

Running a Link Test in the Browser Interface

To run a Link Test from the Browser Interface, perform the following steps:

1. From the Tab Bar, click on the Diagnostics Tab. The Browser Interface displays the Diagnostics Button Bar.
2. From the Diagnostics Button Bar, click the left mouse button on the Ping/Link Test Button. The Browser Interface displays the Ping/Link Test Window. Note that one of the top two radio buttons can be selected. If this session is your first time in the Ping/Link Test Window for your hub, the Ping Test radio button will be selected.
3. Click the left mouse button on the Link Test radio button.
4. Decide whether you want to use the default values set up for a Link Test. If you do, click the left mouse button the Defaults Button and go to Step 7. If not, go to the next step.
5. In the Destination IP/MAC Address box, type the MAC address, for example, 006060-3bd179.

6. In the Number of Packets to Send box, use the list box to select a number, either 1, 5, 10, or 20, to indicate the number packets the hub should send to the test device to determine whether a valid connection exists between the two devices.
7. In the Timeout in Seconds field, type a number between 1 and 30 that indicates the number of seconds you want the hub should wait for a response to a test packet request from the target device.
8. Click the left mouse button on the Start button.

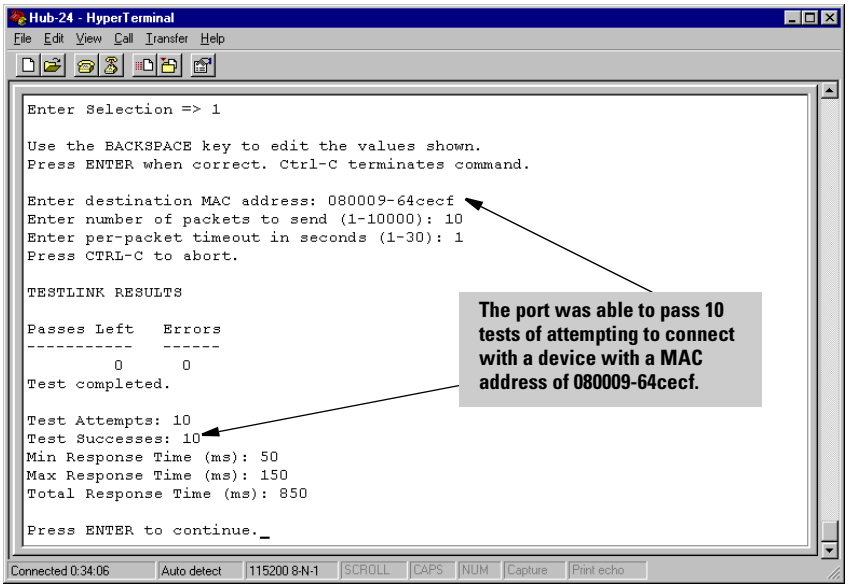


Figure 6-45. The Ping/Link Test Screen Running a Link Test

Running a Link Test in the Console

To run a Link Test from the Hub Console Interface, perform the following tasks:

1. From the Main Menu, type 4 and press Enter. The Hub Console Interface displays the Diagnostics Menu.
2. From the Diagnostics Menu, type 1 and press Enter. The Hub Console Interface displays the Link Test Screen.
3. Type the MAC address of the hub at the `Enter Destination MAC Address` prompt and press Enter. The Hub Console Interface displays the following prompt:

   `Enter number of packets to send.`
4. Type a number at that indicates the number of packets the hub should send to the test device to determine whether a valid connection exists between the two devices. Press Enter. The Hub Console Interface displays the following prompt:

   `Enter timeout in seconds (1-30)`

5. Type a number between 1 and 30 that indicates the number of seconds the hub should wait for a response to a test packet request from the target device.Press Enter

   The Hub Console Interface indicates the following information:

   Test Attempts. The number of times the hub tried to successfully send a packet to the test device.

   Test Successes. The number of times the hub successfully sent a packet to the test device.

   Min Response Time (ms). The number of milliseconds of the least time consuming packet sending test attempt.

   Max Response Time (ms). The number of milliseconds of the most time consuming packet sending test attempt.

   Total Response Time (ms). The total number of milliseconds for all packets sending test attempts.

Browse Hub Configuration

Attribute	Description
Screen Name	Browse Hub Configuration
Menu	Diagnostics
Function	Displays a master dump of many status screens available, showing current values.
Common Use	To obtain a quick glance at all settings and status information without having to search for specific screens.
Browser Interface Window	Configuration Report
Browser Interface Tab	Diagnostics
Default Settings	See Appropriate Screens

The Browse Hub Configuration Screen provides a master dump of many status screens available from the Hub Console Interface. Each screen shows its current values. The screens included in the dump are:

- General Status
- IP Configuration
- Web Accesses Status
- Current Timeout Value
- Backup Links Configuration
- Community List
- Authorized Manager List
- Port Status Information
- Security Configuration

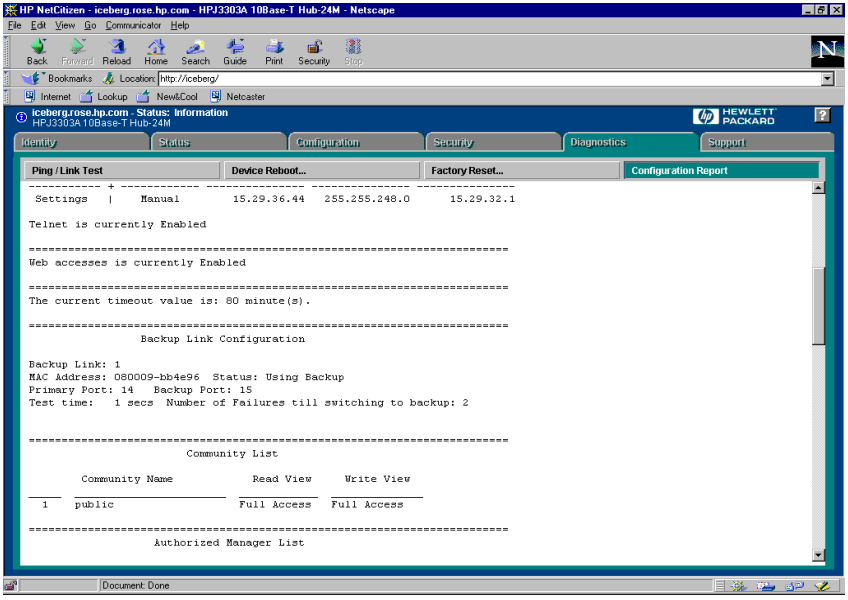


Figure 6-46. The Configuration Report Window

Viewing the Hub Configuration in the Browser Interface

To view the whole hub configuration from the Browser Interface, perform the following steps:

1. From the Tab Bar, click on the Diagnostics Tab. The Browser Interface displays the Diagnostics Button Bar.
2. From the Diagnostics Button Bar, click on the Configuration Report.
3. The Browser Interface displays information from multiple Browser Interface Windows.
4. Scroll through the various regions of the window to learn what values have been set for various parameters. You may want to print the window for convenient reading.

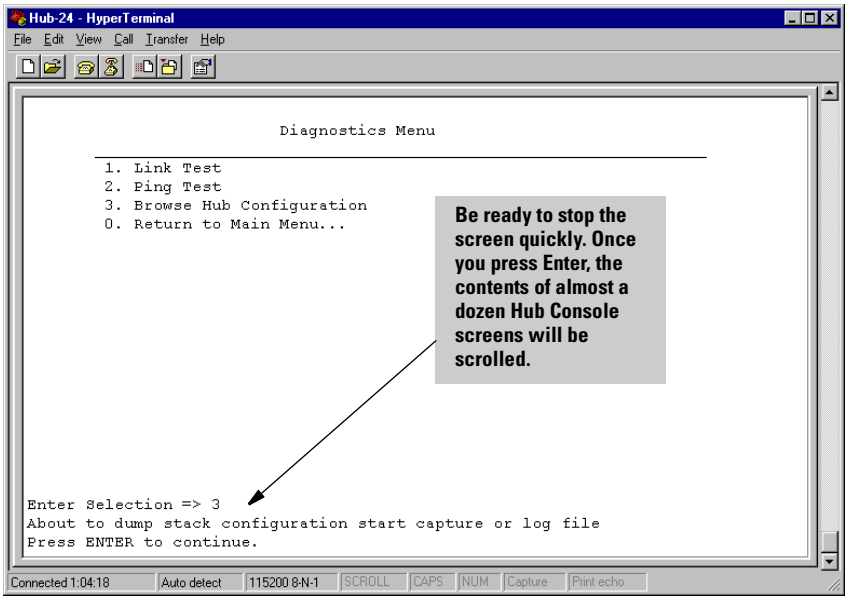


Figure 6-47. The Browse Hub Configuration Option

Viewing the Hub Configuration Screens in the Console

To browse the whole hub configuration in the console, perform the following steps:

1. Type 4 and press Enter from the Main Menu. The Hub Console Interface displays the Diagnostics Menu.
2. Type 3 and press Enter. The Hub Console Interface displays the following prompt:

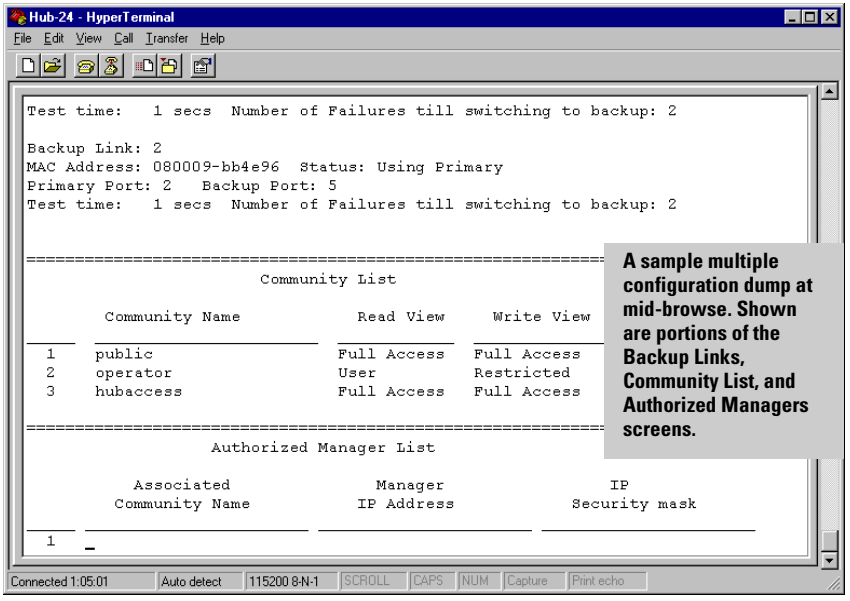
   ```
   About to dump stack configuration start capture or log file.

   Press ENTER to continue
   ```

3. Press Enter.

   The Hub Console Interface displays a continuous dump of screens from the environments listed above.

4. Press Ctl-S to stop the screen from scrolling. See the screen on the following page for a stopped dump midway between two screens.
5. Press Ctrl-Q to direct the Hub Console Interface to continue scrolling.

6. Review values from the screen in which you are interested. To capture the values in a log file, go to the next section.



A sample multiple configuration dump at mid-browse. Shown are portions of the Backup Links, Community List, and Authorized Managers screens.

Figure 6-48. The Browse Configuration Screen Displaying Multiple Screens

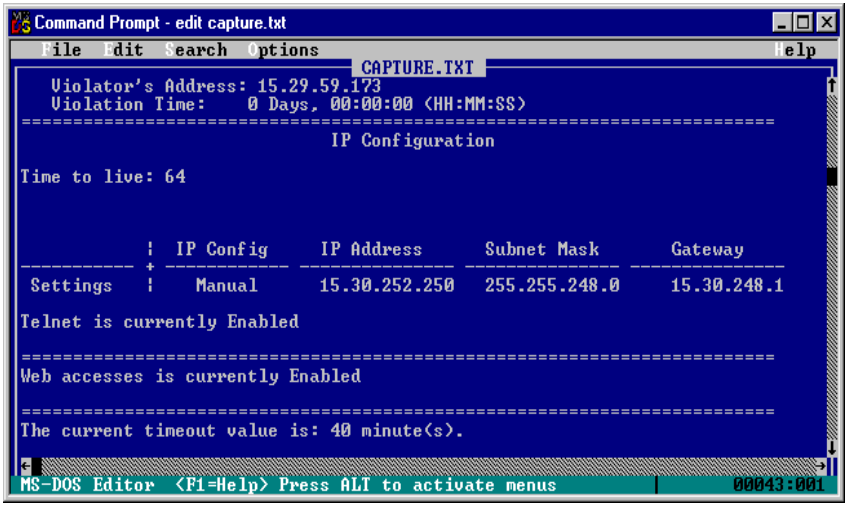


Figure 6-49. A Browse Hub Configuration Log File Viewed in the DOS Editor

Exporting the Hub Configuration Screens to a Log File

The following procedure assumes you are working in HyperTerminal in a Windows environment. To send the configuration data to a log file, perform the following tasks:

1. From the HyperTerminal menu bar, click on the Transfer Menu. HyperTerminal displays a series of menu options.
2. Click on the Capture Text option. HyperTerminal displays the Capture Text dialog box. The dialog 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.
3. If you want to use this filename, go to the next step. If you want to change the filename, the path, or the drive that it is on, use the Browse Button to locate the directory and drive you want and type in the desired filename.
4. When you are satisfied with your target filename, click on the Start Button. 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.
5. Run the Browse Hub Configuration option.
6. Using a standard DOS or Windows text editor, open the file. Review the settings.

Reboot Hub

Attribute	Description
Screen Name	Reboot Hub
Menu	Main Menu
Function	Clears counters on hub as though the hub has been powered on and off.
Common Use	To remove settings from your hub to begin a fresh new session.
Browser Interface Window	Reboot
Browser Interface Tab	Diagnostics
Default Settings	None

The Reboot Hub option enables you to reset factory settings on the hub.

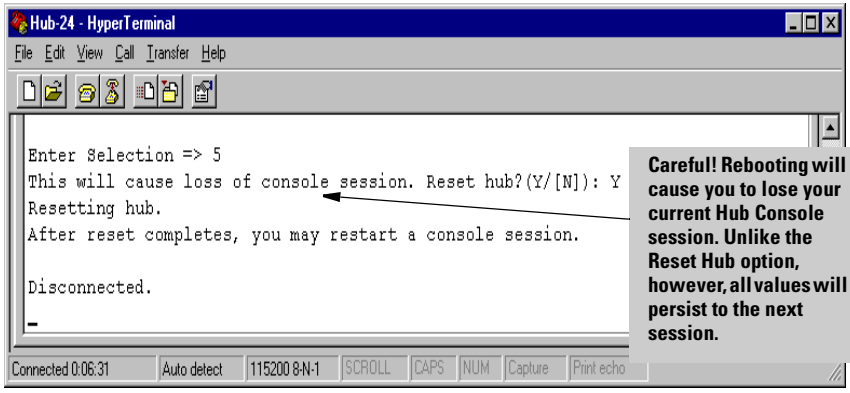


Figure 6-50. The Reboot Hub Option

Rebooting the Hub in the Console

To reboot the hub, perform the following steps:

1. From the Main Menu, type 5 and press Enter. The Hub Console Interface displays the following prompt:

   ```
   This will cause loss of console session. Reset Hub
   [Y]/[N]):
   ```

2. If you are sure you want to reboot the hub, type `Y` and press Enter. The hub will reboot and the Hub Console Interface displays the following prompt:

   ```
   Disconnected.
   ```

Download OS

Attribute	Description
Screen Name	Download OS
Menu	Main Menu
Function	Installs new agent firmware.
Common Use	Upgrades to a better version of firmware.
Web Counterpart	None
Web Tab Bar	None
Default Settings	--

The Download OS Screen displays a port list that provides several columns of information about the state of all ports on the hub.

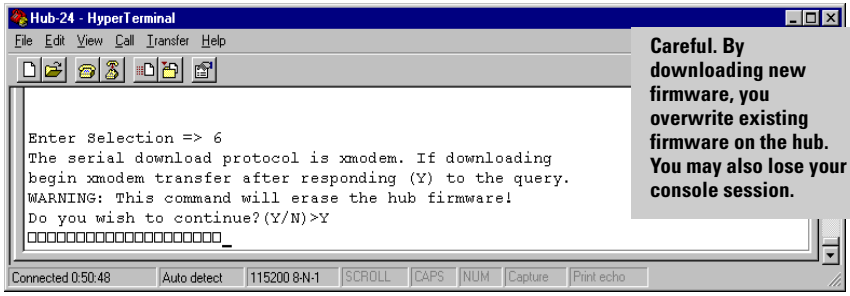


Figure 6-51. The Download OS Option

Downloading Firmware to the Hub in the Console

To download new firmware to the hub, perform the following steps:

1. Make sure you are connected to a firmware server with an Xmodem connection on your console.
2. See the support card at the beginning of this manual for information on downloading firmware.
3. From the Main Menu, type 6 and press Enter. The Hub Console Interface displays the following prompt:

   ```
   The serial download protocol is xmodem. If downloading

   begin xmodem transfer after responding (Y) to the
   query.

   WARNING: This command will erase the hub firmware!

   Do you wish to continue?(Y/N)>
   ```

4. If you are sure you are ready to proceed, type Y and press Enter. New firmware is downloaded to the hub. The Hub Console Interface may display a new menu that reflects the new firmware revision.

Return to the Command Prompt

Attribute	Description
Screen Name	Return to the Command Prompt
Menu	--
Function	Returns you to the Command Prompt region of the Hub Console Interface
Common Use	Enabling you to use command prompts to perform tasks.
Browser Interface Window	None
Browser Interface Tab	None
Default Settings	None

The Return to the Command Prompt enables you to escape the Hub Console Interface menu system.

To escape the menu system, simply type 7 at the Main Menu prompt and press Enter

Support URL

Attribute	Description
Screen Name	None
Menu	None
Function	Enables you to change the default World Wide Web URL for your Browser Interface support site.
Common Use	Changing your World Wide Web URL for your Browser Interface support site.
Browser Interface Window	Support URL
Browser Interface Tab	Configuration
Default Setting	http://www.hp.com/go/procurve

The Support URL Window enables you to change the World Wide Web Universal Resource Locator (URL) for your Browser Interface support site. The default URL is:

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

The Support URL Window contains the following objects:

Support URL box. Displays the current URL for your Browser Interface support site.

Apply Changes Button. Stores the new URL string specified in the Support URL box so that the address will now be the current string that launches the Browser Interface support site.

Clear Changes Button. Removes any changes you made to the URL string in the event you made a mistake typing them and restores the current URL in the Support URL box.

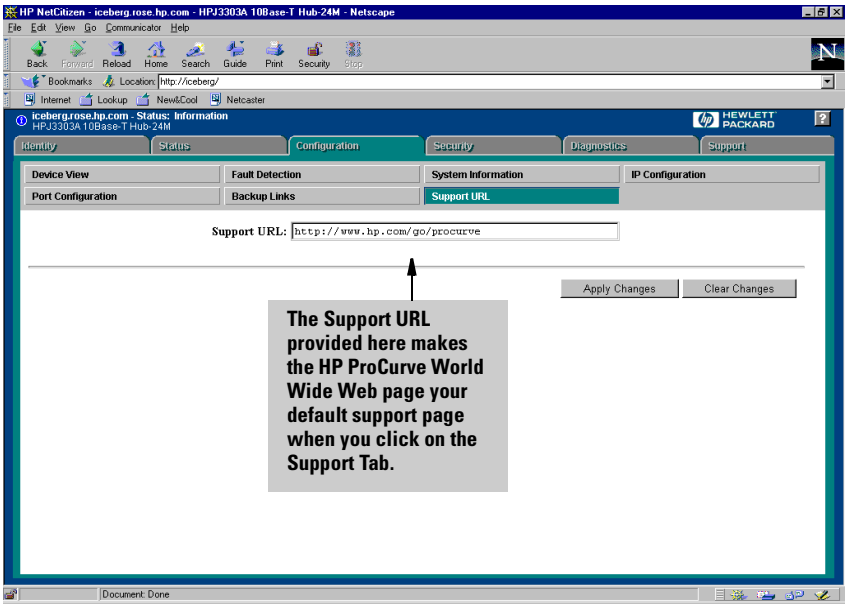


Figure 6-52. The Support URL Window

Changing Your Support URL in the Browser Interface

To change your Support URL, perform the following steps:

1. From the Tab Bar, click on the Configuration Tab. The Browser Interface displays the Configuration Button Bar.
2. From the Configuration Button Bar, click on the Support URL tab. The Browser Interface displays the Support URL Window.
3. Click the left mouse button anywhere in the Support URL box. The current support URL string is highlighted or darkened, indicating you have selected the string.
4. Press the Delete key on your keyboard.
5. Type the URL string that will launch the support site you want.
6. Click on the Apply Changes button. If you decide you want to return to the current URL before clicking on the Apply Changes button, click on the Clear Changes button to remove whatever new text you have typed in the Support URL box. The Browser Interface reinserts the current URL string.

Support

Attribute	Description
Screen Name	None
Menu	None
Function	Displays the support site specified in the Support URL.
Common Use	To learn more about the nature of the Browser Interface.
Browser Interface Window	Support
Browser Interface Tab	Support
Default Settings	None

The Support Tab in the Browser Interface displays the support site specified in the Support URL.

How to Find Support Material in the Browser Interface

To find support material for use of HP ProCurve 10Base-T Hubs, using the Browser Interface, perform the following steps:

1. From the Tab Bar, click on the Support Tab. The Browser Interface displays the Home Page of the Hewlett-Packard ProCurve Networking Web Site.
2. From the ProCurve sidebar to the left, click on the Support Button.
3. Click on all support-related strings.

Troubleshooting

This chapter describes ways to troubleshoot the hub. Topics covered are:

- troubleshooting approaches
- troubleshooting some common problems
- diagnosing with the LEDs

Troubleshooting Approaches

You can diagnose problems on all HP ProCurve 10Base-T Hubs by checking the LEDs on the front of the hub as described in the section, “Diagnosing With the LEDs” in this chapter.

You can also diagnose the managed hubs, HP J3301A and HP J3303A, with these tools:

- By using the Browser Interface, a Web-based interface that provides a full management environment, as described in chapter 4, “Running the Browser Interface”.
- By using the Hub Console’s diagnostic functions as described in chapter 2, “Running the Hub Console”.
- By using the HP Top Tools for Hubs and Switches or other SNMP management tool as described in the online help in the management application.

Troubleshooting Some Common Problems

Use the following table to diagnose the problem with your HP ProCurve 10Base-T Hub.

Problem	Solution
How do I reset the hub?	You can reset the hub three five different ways: • From the device, remove the plug on the power cord from the power source or the hub and reconnect it. • From the device, press the Reset Button. • From the Hub Console Interface, select either the Reboot Hub option to preserve your settings or select the Reset Hub to Factory Default option to completely reset the hub's factory defaults. • From the Browser Interface, select the Factory Reset Button. • From HP Top Tools for Hubs and Switches, perform a reset from the Reset Parameters dialog box. If this condition persists, see your LAN dealer.
None of the LEDs are on.	Verify that the power cord is plugged into an active power source and to the hub. Make sure these connections are snug. Try power cycling the hub by unplugging and plugging the hub back in. If the Power LED is still not on, verify that the AC source works by plugging another device into the outlet. Or try plugging the hub into a different outlet or try a different power cord. If this condition persists, call your HP-authorized LAN dealer or HP representative for assistance.
I lost the password.	Press the Clear button for 10 seconds. See page 2-4 for more details.
IP configuration errors have been reported.	Use the Hub Console's IP Configuration function as described in the *HP ProCurve 10Base-T Hubs Management and Configuration* guide.
I want to see if each cable is connected correctly.	Run Link Test in the Hub Console Interface. See the *HP ProCurve 10Base-T Hubs Management and Configuration* guide.
A user can't send data to another user.	Use the Ping or Link Test in the Hub Console Interface. See the *HP ProCurve 10Base-T Hubs Management and Configuration* guide.
The Fault LED is on.	Remove the plug on the power cord from the power source and reconnect it. If problem persists, the device has an internal failure. Contact your HP authorized dealer or reseller.

Diagnosing With the LEDs

Most problems with the hub can be diagnosed using the LEDs on its front panel. Use the following table to interpret LED patterns that indicate error conditions on the hub.

LED patterns indicating problems				Diagnostic Tips
Power	**Coll**	**Port LED**	**Fault**	
ON	*	**OFF**	*	Check cabling on the indicated port all the way out to the device attached to that port. Faulty wiring or a bad connection could exist somewhere in that connection. The end node or hub attached to the port is off. The port may be disabled. Use the Hub Console or management application to enable the port. If Port 1, check the position of the MDI/MDI-X switch. See the figure in chapter 1 that details the MDI/MDI-X switch.
ON	**ON**	*	*	Very frequent collisions are occurring, which could indicate a network fault or improperly terminated cable.
ON	*	**Slow Flash**	**Slow Flash**	The port has been auto-partitioned because of an excessive collision condition. Check cable connections and status of attached network devices for causes of the excess collisions. The hub will automatically recover after certain IEEE 802.3 criteria are successfully met.
ON	*	**Fast Flash**	*	Network management security violation occurred. See Port Security in Browser Interface or Hub Console Interface.
ON	*	*	**ON**	The hub has failed its self-test. Power-cycle the hub. If this condition persists, call your HP-authorized LAN dealer or HP representative for assistance.
***This LED is not important for the diagnosis.**				

Hub LED Operation

Two types of LEDs exist on the hub. They are:

- Hub Status LEDs. These LEDs reflect certain conditions that exist on the hub at large and are not explicitly referring to a given port.
- Port Status LEDs. These LEDs reflect basic conditions (for example, Link Beat being enabled) that exist on a specific port.

Status information for both are described in the following tables.

Interpreting the Hub Status LEDs

The hub status LEDs indicate whether the hub is functioning properly. The following table provides LED port information for the HP J3301A and HP J3303A.

LED	LED Color	Meaning of LED
Power	Green	**On** indicates the hub is receiving power.
		Off indicates the hub is not receiving power.
Activity	Green	**Flickering** (rapid flashing) indicates a packet is being transmitted to or from a port. Normally, the LED appears to flicker. In heavy traffic, it may appear on all the time. **Off** indicates no packet is being transmitted to or from a port.
Fault	Orange	**On** indicates an error has been detected on the hub. **Off** indicates no error has been detected on the hub. **Port LED Flash** on for.75 seconds and turn off for.75 seconds, indicating the port is partitioned. The Fault LED does NOT illuminate when ports are partitioned.
Collision	Orange	**On** indicates a collision is detected. If it appears on continuously (with no flicker), it is a possible indicator of a network fault or an improperly terminated cable. **Off** indicates no collision has been detected.

Interpreting the Port Status LEDs

The following table provides information on the hub port LEDs.

LED	Color	Meaning of LED
Twisted-pair Ports	Green	**On** indicates Link Beat is detected from the attached node and the port is enabled.
		Off indicates the port is not receiving the link beat signal from the attached node.
		Slow Flash* indicates the port has been partitioned due to excessive collisions. This port will reenable when the connected device or cable is repaired.
XCVR Port	Green	**On** indicates is enabled a transceiver module is installed. **Off** indicates the Xcvr port is disabled. Slow Flash indicates the port has been auto-partitioned.
* The slow flash is approximately once every 1.5 seconds (.75 seconds on and .75 seconds off).		

Index

Symbols

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

Printed in Singapore 6/98

Manual Part Number
5967-6862