HP J2603B Ethernet SNMP Module

For the HP AdvanceStack 10Base-T Hubs

At A Glance

The HP Ethernet SNMP Module (HP J2603B) is an optional component that can be added to an HP AdvanceStack 10Base-T Hub to provide extended hub management capabilities. The HP AdvanceStack 10Base-T hubs into which an SNMP Module can be installed include:

- HP AdvanceStack 10Base-T Hub-12 (HP J2600A)
- HP AdvanceStack 10Base-T Hub-24 (HP J2601A)
- HP AdvanceStack 10Base-T Hub-48 (HP J2602A)
Features

If the optional HP Ethernet SNMP Module is installed in your hub, the hub functionality is enhanced with these additional features:

- **Advanced embedded SNMP agent code** enabling the hub to be managed remotely from a network management station that supports Simple Network Management Protocol (SNMP) over IP (using the configured IP address) or Novell NetWare (IPX). The agent code also provides HP EASE (Embedded Advanced Sampling Environment), which samples network data for enhanced diagnostics from a network management station.

- **Extended hub management capabilities**, described later in this document in chapter 2, “Extended Hub Capabilities”.

- **Enhanced out-of-band management access including:**
  - support for higher baud rates beyond the default 9600 baud on the hub’s out-of-band management RS-232 port, and automatic sensing of the selected baud rate when connecting with the hub,
  - full V.22bis modem line control for remote out-of-band management access to the hub or stack of hubs.

- **Updatable firmware** that enables enhancements to be downloaded either from a computer attached to the out-of-band management port or over the network.

- **Advanced integrated design** including an Intel i960 RISC processor, 1 megabyte RAM, 8 kilobytes EEPROM for configuration data, and 256 kilobytes flash EEPROM for additional processing power and future upgrade capabilities.

- **Support for extended network functionality** through add-on auxiliary modules. The SNMP Module has a connector onto which you can attach an auxiliary module, for example the HP J2623A and HP J2624A Dial-A-LAN or HP J2628A Router 210 modules. You then install the combined module assembly in the HP AdvanceStack 10Base-T hub.

Contact your HP-authorized LAN dealer or HP sales representative for information on available auxiliary modules.
## Contents

### 1 Installation
- Installing the Module ........................................ 1-2
- Firmware Enhancements ....................................... 1-5
- Removing the Module .......................................... 1-6
- Clearing a Password ........................................... 1-7

### 2 Extended Hub Capabilities
- From HP Stack Manager ........................................ 2-2
  - IP Configuration ............................................. 2-3
  - Basic Security Features .................................... 2-3
  - Backup Link Configuration .................................. 2-3
  - Robust Port Control ......................................... 2-3
  - Network Test .................................................. 2-4
  - Modem Configuration ....................................... 2-4
  - Factory Default Reset ....................................... 2-4
- From HP Interconnect Manager ................................. 2-5
  - Features Provided .......................................... 2-5
  - Network Addressing Notes .................................. 2-6
- From the Console ............................................... 2-7
  - Directly, Using A Serial Cable and a Terminal .......... 2-7
  - Remotely, Using Telnet ...................................... 2-8
  - Remotely, Using a Modem and a Terminal .................. 2-8
- Using the Console ............................................. 2-9
3 Troubleshooting

- Diagnosing With the LEDs ........................................... 3-2
- LED Location .............................................................. 3-3
- Customer Support Services ............................................. 3-4
  - Hewlett-Packard FTP Library Service ......................... 3-5
  - HP Network Phone-In Support (NPS) ......................... 3-6
  - HP FIRST Fax Retrieval Service ................................. 3-6
  - CompuServe ......................................................... 3-7

A Specifications

B Modem Configuration

C Security Information

- Intruder Prevention ..................................................... C-2
- Eavesdrop Prevention .................................................. C-2
- Authorized Station Address .......................................... C-3
- Setting Inbound Security with Intruder Prevention .......... C-4
- Auto Port Disable ....................................................... C-5
- Send Alarm ............................................................... C-5
- Setting Outbound Security with Eavesdrop Prevention .... C-6

Index
Installation

- Installing the Module
- Firmware Enhancements
- Removing the Module
- Clearing a Password
Installing the Module

The HP Ethernet SNMP Module is installed in the Expansion Slot on the back of the HP AdvanceStack 10Base-T Hub.

**Warning**

Before installing the HP Ethernet SNMP Module, unplug the HP AdvanceStack Hub from the power source. Electrical shock could result if you attempt to install the module without unplugging the hub.

**Caution**

Static electricity can severely damage the sensitive electronic components on the HP Ethernet SNMP Module. When installing the module in your hub, follow these procedures to avoid damage from static electricity:

- Handle the module by its edges and avoid touching the components and the circuitry on the board.

- Equalize any static charge difference between your body and the hub by wearing a wrist strap and attaching it to the hub's metal body, or by frequently touching the hub's metal body while you are installing the module.
1. Unscrew the two captured screws holding the cover plate to the hub's Expansion Slot and remove the cover. Note that the screws are spring loaded and will release outward when unscrewed far enough. Do not unscrew them completely from the cover plate.

2. (Optional step). Install an auxiliary module on the HP Ethernet SNMP Module. See the instructions in the installation guide that came with the auxiliary module.

3. Insert the HP Ethernet SNMP Module (with the auxiliary module, if one has been installed) into the hub's expansion slot. Leading with the hub connector edge, line up the sides of the module with the rails on the sides of the hub's Expansion Slot. Then push the module into the slot until it is firmly seated in the connector in the back of the slot.

 Procedures continued on the next page.
Installation

4. Replace the cover plate over the Expansion Slot, tightening the two screws that hold it in place. Be careful not to overtighten the screws.

    If you have installed an auxiliary module and a cover plate is supplied with the module, install that cover plate in place of the plate that was originally on the hub.

    **For proper hub cooling, make sure you install the cover after the module or module assembly is installed!**

5. Connect the HP AdvanceStack hub to a power source and it will begin its power-on self-test. See the table below for the LED pattern that occurs during self test.

    If only the HP Ethernet SNMP Module is installed, the self test should take up to 40 seconds. If an auxiliary module is also installed, the self test may take up to 60 seconds.

### LED Pattern During Self Test

<table>
<thead>
<tr>
<th>LED</th>
<th>Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exp Slot (on the hub)</td>
<td>1 ON for approximately 3 to 5 seconds during hub hardware self test, then</td>
</tr>
<tr>
<td></td>
<td>2 FLASHING during self test of the module(s):</td>
</tr>
<tr>
<td></td>
<td>• up to 40 seconds if only an HP Ethernet SNMP Module is installed</td>
</tr>
<tr>
<td></td>
<td>• up to 60 seconds if an auxiliary module is also installed</td>
</tr>
<tr>
<td></td>
<td>When the hub, the HP Ethernet SNMP Module, and any auxiliary module successfully complete self-test, the Exp Slot LED changes to being continuously ON.</td>
</tr>
<tr>
<td>Fault (on the HP Ethernet SNMP Module)</td>
<td>• Not visible if only an HP Ethernet SNMP Module is installed—see the Exp Slot LED on the hub</td>
</tr>
<tr>
<td></td>
<td>• Visible and ON if an auxiliary module is also installed—the Fault LED on the HP Ethernet SNMP Module should be visible through the auxiliary modules cover plate</td>
</tr>
<tr>
<td></td>
<td>When the HP Ethernet SNMP Module successfully completes self test, this LED is OFF.</td>
</tr>
<tr>
<td>Auxiliary Module LEDs</td>
<td>See the documentation that came with the auxiliary module for information on the operation of the LEDs on that module.</td>
</tr>
</tbody>
</table>

If the Exp Slot (or AdvSlot) LED on the hub continues to flash after the normal self test completion times, see chapter 3, “Troubleshooting” later in this guide.
6. When the self-tests of the hub, the HP Ethernet SNMP Module, and any auxiliary module complete successfully, the Exp Slot LED on the front of the hub will be ON continuously. The hub and accessories are now operational. (Note that on some HP AdvanceStack 10Base-T hubs, this LED is labeled AdvSlot.)

See your hub manual for other procedures to complete the hub installation.

Firmware Enhancements

In the future, Hewlett-Packard may provide improvements to this product through firmware upgrades. The upgrade code can be downloaded from a PC attached to the hub’s RS-232 port or over the network. The update procedures are described in documents that come with the firmware enhancements.

You can determine the current firmware version on the SNMP Module from either HP Stack Manager, HP Interconnect Manager/Windows, or the console. In HP Stack Manager and HP Interconnect Manager, use the Identify function to obtain that information. Look for the SNMP Agent EEPROM version number in the Identify window. When you access the console, the version number appears.

You can get the latest agent firmware by using any of the following ways:

- Use the download instructions provided in chapter 3, “Troubleshooting”.
- Use the download instructions on the perforated quick reference card in this manual.
- Contact your HP-authorized LAN dealer or local HP sales office for the latest on firmware enhancements for your HP Ethernet SNMP Module.
Removing the Module

The HP Ethernet SNMP Module is removed from the hub by reversing the installation procedure described earlier in this document. Extractor handles are provided on the module to help you remove it from the hub's slot.

If an auxiliary module is attached to the HP Ethernet SNMP Module, the extractor handles may not be accessible. See the auxiliary module documentation for removal procedures.

**Caution**

If the HP Ethernet SNMP Module is removed from the hub and inserted into another hub, the IP address and any other configuration information in the module's firmware are lost. The HP Ethernet SNMP Module will reset itself to the factory defaults when the new hub is powered on.

If you remove the HP Ethernet SNMP Module from a hub and then re-insert it into the same hub, however, no firmware configuration information is lost.
Clearing a Password

There is a Password Clear button on the HP Ethernet SNMP Module that is accessed through a hole in the hub's Expansion Slot cover plate. If an auxiliary module has been installed and that module was supplied with a cover plate, additional holes may exist in that cover plate. The HP Ethernet SNMP Module's Password Clear button is behind the unlabeled hole toward the bottom of the plate.

You can use this button to clear a forgotten password that was previously configured on the hub. The password is configured from either HP Stack Manager or HP Interconnect Manager.

To clear the password, press and hold the button for approximately five seconds.

As an indication that the password has been cleared, the Security LED on the front of the hub will come on and stay on until the button is released.

Note

After the password has been cleared, access to the hub from the HP Stack Manager and from SNMP management stations will no longer be password protected. A new password can be assigned from either HP Stack Manager or HP Interconnect Manager.
Extended Hub Capabilities

SNMP Features:
- From HP Stack Manager
- From HP Interconnect Manager
- From the Console

Using the Console
When you install an HP Ethernet SNMP Module in your AdvanceStack 10Base-T Hub, the functionality from both out-of-band management (HP Stack Manager) and in-band management (from an SNMP network management station) is extended. Without the HP Ethernet SNMP Module installed, the hub cannot be directly managed in band. See your hub manual if you want a description of the basic functionality that is possible without the HP Ethernet SNMP module installed.

The HP AdvanceStack hubs are designed to operate unattended. With the HP Ethernet SNMP Module, several interfaces are provided with the hub for customizing its configuration, monitoring its activity, or running diagnostics.

This chapter describes the features available from:

- HP Stack Manager
- HP Interconnect/Manager
- the console

---

**From HP Stack Manager**

HP Stack Manager is the Windows-based software that is supplied with the HP AdvanceStack hubs. It is used to configure, monitor, and troubleshoot the hubs. With the HP Ethernet SNMP Module installed in an HP AdvanceStack 10Base-T Hub, the basic capabilities of the HP Stack Manager software (supplied with the hub) are extended to include:

- IP configuration
- basic security features
- backup link configuration
- robust port control
- network tests
- modem configuration
- factory default reset

A description of each extended feature follows on the next page. For specific information about how to use a feature, consult the online help system in HP Stack Manager.
IP Configuration

The IP Configuration window is used to define the parameters necessary for the hub to communicate with a network management station using SNMP in a TCP/IP network.

Basic Security Features

The following security features are configurable from HP Stack Manager. See the *HP AdvanceStack 10Base-T Hubs Installation and Reference Guide* for more information.

- Password protection that limits access to the hub configuration from both HP Stack Manager and HP Interconnect Manager.
- An authorized managers list that specifies the network addresses of the SNMP management stations authorized to manage the hub and whether they should receive SNMP event alarms.

The HP Ethernet SNMP Module also has an external switch that can be used to clear a configured password if you forget it. See “Clearing the Password” on page 1-7.

Backup Link Configuration

The Backup Link option is used to specify two of the hub’s network ports (AUI/Xcvr, ThinLAN, or twisted-pair) to be used in a backup (redundant) connection to another hub thus enhancing network fault tolerance. It enables you to automatically activate a second physical link between hubs if the primary link fails. The backup link is used only in the event of primary link failure, thus eliminating the possibility of loops in the network.

Robust Port Control

The Robust Port Control feature allows you to invoke options to improve the hub’s ability to tolerate network problems resulting from excessive collisions. The configurable options are:

- Intelligent Segmentation Recovery
- Late Collision Monitoring
Extended Hub Capabilities

See the HP Stack Manager online help and *HP AdvanceStack 10Base-T Hubs Installation and Reference Guide* for more information.

Network Test

The Network Test window enables you to perform Ping, IPX, and Link network tests. These tests are used to verify the connection between the hub and a specified network device. The devices tested must support the test(s) by being able to send appropriate response packets.

The Ping test sends Internet Control Message Protocol (ICMP) Echo Request ("ping") packets to another node with the specified IP address and waits for Echo Response packets in return.

The IPX test sends IPX test packets to the specified IPX device and waits for an IPX test packet in return.

The Link test sends IEEE 802.2 Test command packets and waits for an IEEE 802.2 Test response packet in return.

Modem Configuration

Use the Modem Configuration window if you are running HP Stack Manager from a PC that is connected to the hub's RS-232 port via a modem link. This window lets you define modem communications settings for both the remote modem that you attach to the hub and the local modem that you keep connected to your PC.

Factory Default Reset

When you install an HP Ethernet SNMP Module in your hub, the Reset function in HP Stack Manager offers an additional reset option, Factory Reset. Use this reset option to return the hub and the HP Ethernet SNMP Module to the original factory configuration. All configuration except the IP configuration is returned to the factory values.
From HP Interconnect Manager

The HP Ethernet SNMP Module has embedded SNMP agent code allowing an HP AdvanceStack 10Base-T Hub, with the module installed, to be managed by HP Interconnect Manager and any other SNMP-compliant network management product.

Features Provided

Most of the management features that are available through the out-of-band management tool, HP Stack Manager, are also available from a network management station running HP Interconnect Manager. This network management tool also provides the additional management features listed below. See the documentation accompanying HP Interconnect Manager for more information.

- **Port Security.** HP Interconnect Manager provides network management authorization, and hub access password protection features similar to those provided by HP Stack Manager.
  
  In addition, HP Interconnect Manager provides two types of port security:
  
  - *Intruder Prevention* for inbound data (from the end user to the hub)
  - *Eavesdrop Prevention* for outbound data (from the hub to the end user)

  Both of these types of security can be configured on each of the hub's network ports individually.

- **Capability to manage up to 16 hubs in a chain through a single HP Ethernet SNMP Module.** With only one of the hubs in the stack having an HP Ethernet SNMP Module, all the 10Base-T hubs in the entire stack can be managed over the network from a network management station.

- **Redundant SNMP management capability** if there is more than one HP Ethernet SNMP Module in the chain. If communication between the network management station and the hub with the HP Ethernet SNMP Module is interrupted, any other hub that has an HP Ethernet SNMP Module in the chain can take over the management communication. See the HP Interconnect Manager product documentation for more information.
Network Addressing Notes

The communication between an SNMP network management station and the agent code on the HP Ethernet SNMP Module takes place at the network layer. To communicate with an SNMP network management station, the hub with the HP Ethernet SNMP Module installed therefore needs a network address. If the communication is over a TCP/IP network, an IP address must be assigned. If the communication is over a Novell NetWare network, the agent code intentionally gets an IPX address from an IPX router or server on the network.

**IP Addressing:** By default, the hub with an HP Ethernet SNMP Module installed is configured to automatically seek an IP address from a BOOTP server on the network. This is done when the hub is powered on. If an IP address is not found, the HP Ethernet SNMP Module will seek an IP address every ten minutes until it finds an IP address. You can disable an HP Ethernet SNMP Module from polling by using the IPconfig command described later in this chapter.

To take advantage of this feature, you must set up your BOOTP (Internet Boot Protocol) server with the IP configuration for your hub before you connect the hub to the network and power it on. To set up your BOOTP server, see an example of a BOOTP table in appendix C in *HP AdvanceStack 10Base-T Hubs Installation and Reference Guide*.

Alternatively, you can manually configure an IP address on the hub by using the IP configuration function in HP Stack Manager or the IPconfig console command.

**IPX Addressing:** By default, the hub with an HP Ethernet SNMP Module installed will automatically acquire an address from an IPX router on the network.
From the Console

You can connect a terminal to the hub's console port in the following ways:

- directly, using a serial cable and a terminal (or a PC using a terminal emulator)
- remotely, using Telnet
- remotely, using a modem and a terminal

The HP AdvanceStack hubs support a single console session only. If a console session is already running, a second console session can override the console session.

Directly, Using A Serial Cable and a Terminal

To directly connect a terminal to a hub, follow these steps:

1. Connect an ASCII terminal, or a PC emulating an ASCII terminal, to the console port using an RS-232-C “null modem” cable. (For pin-outs and recommended cables see appendix A, “Cables and Connectors” in the HP AdvanceStack 10Base-T Hubs Installation and Reference Guide.)

2. Switch on the terminal's power (or switch on the PC's power and start the terminal emulation program). Configure the terminal for 8 bits per character, 1 stop bit, no parity, Xon/Xoff handshaking, and a baud rate of 38400, 19200, 9600, 4800, 2400, or 1200. If you are using a PC running Windows, you can connect up to 19200 baud.

3. Press [Return] several times for the => or Password prompt. The baud rate for communication between the hub and the terminal is set automatically when you press [Return].
Remotely, Using Telnet

The HP AdvanceStack hubs support a Telnet console session. Your Telnet syntax depends on your TCP/IP software or your terminal server. By default, Telnet is enabled. You can disable Telnet by using the IPconfig console command described on page 2-11.

To establish a Telnet session, follow these steps:

1. Verify the hub you are accessing has an HP Ethernet SNMP Module installed, that it has been configured with an IP address, and that it is accessible from your PC or workstation.

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

To end the Telnet session, type `DI` (the Disconnect command) to terminate the console session. Or use your Telnet application's command to close or quit the Telnet session.

Remotely, Using a Modem and a Terminal

1. Use a full-duplex, asynchronous (character-mode) modem only. The following modems have been tested at their rated speeds:
   - Hayes V-series ULTRA Smartmodem 14400
   - Hayes Smartmodem 2400
   - Multi Tech 14.4 (MT1432BA)
   - US Robotics Courier HST Dual Standard with ASL
   - Intel 14.4EX
   - Telebit WorldBlazer

2. Connect the modem to the hub's console port using an RS-232-C modem cable. (For pin-outs and recommended cables see appendix A, “Cables and Connectors” in the HP AdvanceStack 10Base-T Hubs Installation and Reference Guide.)
3. Configure the modem as described in appendix B, “Modem Configuration”.

4. At the remote site, connect the terminal (or PC emulating a terminal) to the remote modem. Make sure the terminal and modems are functioning properly, then establish the link between the terminal’s modem and the hub’s modem according to the modem instructions.

5. Press `[Return]` several times for the `=>` or Password prompt. The baud rate for communication between the hub and the modem is set automatically when you press `[Return]`.

Using the Console

The console session starts with a display similar to the following (the actual version numbers may be different):

If a password has not been assigned with the `Password` command, then you are not prompted for your password here.

If a console session is currently active, then you are prompted to break the current active console session.

HP J2603A Ethernet SNMP module
ROM A.01.00
EEPROM V.03.03
HW X.P3.11

Use HP Stack Manager or console commands for hub configuration.

Enter password:

A console session is currently active.

Do you want to break in? (Y/N) Y

Connecting...

Enter a console command, or HE or ? for help.

=>

If you are using Telnet, the message “Use HP Stack Manager...” is not relevant and is not displayed.
Extended Hub Capabilities

Console Commands

Enter at least the first two letters of a command to execute it, such as HE for the Help command. The Help command displays the following screen like, listing all commands.

Syntax Conventions on Help Screen:

< > – Indicates a required parameter.

[ ] – Indicates an optional parameter.

| – Used as a separator between acceptable variable values.

For example, SE <port|SHow|CLear> indicates that either a port ID, or the characters SH, or CL must be entered after the SE command.

The commands are described in the rest of the chapter.

HELP [cmd] or ? [cmd]

To see the help screen shown above or, if you include a specific command, the syntax and description of that specific console command. For the [cmd] parameter, use the first two letters of the command you wish to see.

Example: HE ST (This displays help for the Status command.)
AUxiliary

If an auxiliary module is attached to the HP Ethernet SNMP Module in the hub you have accessed, this command starts a console session for the auxiliary module. For example, you can communicate with an HP Dial-A-LAN Module or an HP Router 210 Module.

BAckup

To configure one of the hub’s ports for dedicated use in a backup (redundant) link to another hub.

The HP AdvanceStack hubs allows you to use any two of its network ports for a redundant link to another hub in your network. The backup link normally carries no traffic, but it is automatically activated if the primary link fails. Note that any of the ports can be the backup port to any other port.

When you enter the Backup command, you are prompted for these values:

<table>
<thead>
<tr>
<th></th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Port</td>
<td>Disabled</td>
<td>The port used for the backup link. Enter the port ID (see the Port command description for the port IDs). Or, enter DI (for disable) if you wish to remove an existing backup link configuration.</td>
</tr>
<tr>
<td>Primary Port</td>
<td>A1</td>
<td>The port used for the primary link. Enter the port ID.</td>
</tr>
<tr>
<td>Remote Station Address</td>
<td>000000-000000</td>
<td>The 12-digit hexadecimal station address of the hub at the remote end of the critical link.</td>
</tr>
<tr>
<td>Seconds Between Test Packets</td>
<td>1 second</td>
<td>How often you want the hub to send an IEEE 802.2 Test packet to the remote hub over the primary link.</td>
</tr>
<tr>
<td>Consecutive Failures</td>
<td>2 seconds</td>
<td>The number of consecutive Test packet response failures that will trigger activation of the backup link. For example, enter 5 to activate the backup link on the fifth failure.</td>
</tr>
</tbody>
</table>

The hub monitors the primary link by sending IEEE 802.2 Test packets at the specified frequency to the specified remote hub. If “n” consecutive Response packets are not returned from the remote hub, the primary port is disabled and the backup port is enabled.

When the primary link is repaired, you must re-enable the primary port by using the Port command. It is not automatically re-enabled. When the primary port is re-enabled, the backup port is disabled automatically and returned to backup mode. See “Reactiving the Primary Link” in appendix D, “Backup Links” in the HP AdvanceStack 10Base-T Hubs Installation and Reference Guide. This appendix also covers more information on backup links, including requirements, limitations, and sample topologies.
Chainlist

To display a list of all HP AdvanceStack hubs that are connected in the same distributed management chain as the hub you are accessing. The display includes the following fields:

- **Entry** – an index number for the other HP AdvanceStack 10Base-T hubs in the chain that do not have an HP Ethernet SNMP Module installed. These hubs can be accessed and controlled from your current console session by using the HUbselect command.

To access the other 10Base-T hubs in the chain in which SNMP modules are installed, you must either move the console serial connection to each of these hubs, or simply run HP Stack Manager, the free Windows-based console application that was supplied with your hub. Using HP Stack Manager, you can access any hub in the chain (with or without an SNMP Module) through a single out-of-band serial connection to any of the hubs in the chain, or by using Telnet.

- **Model** – the product number and name of the hub.

- **Station Address** – the unique 12-digit link-layer address for the hub. (Also called MAC address, Ethernet address, or physical address.)

- **Description** – a user-defined description of the hub. This field is entered from HP Stack Manager.

- **IP Address** – the IP address of the SNMP agent on the HP Ethernet SNMP Module. For convenience and clarity, we refer to this as the hub's IP address. If no IP address has been assigned, the entry is No IP address; if an HP Ethernet SNMP Module is not installed in the hub, the entry is No SNMP module.

Example: CH (This displays the following example table.)

<table>
<thead>
<tr>
<th>Entry</th>
<th>Model</th>
<th>Station Address</th>
<th>Description</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1*</td>
<td>HPJ2601A AdvanceStack Et</td>
<td>080009-64cecf</td>
<td>chain access pt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HPJ2410A 100VG Hub-15</td>
<td>080009-5d8c04</td>
<td>none</td>
<td>No SNMP module</td>
</tr>
<tr>
<td></td>
<td>HPJ2410A 100VG Hub-15</td>
<td>080009-2b0682</td>
<td>none</td>
<td>No IP address</td>
</tr>
<tr>
<td>4</td>
<td>HPJ2600A 10Base-T Hub-12</td>
<td>080009-6756d4</td>
<td>Tech Mkt. Hub-12, No SNMP module</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>HPJ2610A 10Base-T Hub-8</td>
<td>080009-1e61c4</td>
<td>Tech Mktg hub, No SNMP module</td>
<td></td>
</tr>
</tbody>
</table>

* Indicates hub that is currently selected
To display network activity counters for each network port, the hub’s SNMP agent, and the global count for all ports.

<table>
<thead>
<tr>
<th>Counters [A/B/C/D]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Packets</td>
</tr>
<tr>
<td>Collisions</td>
</tr>
<tr>
<td>CRC Errors</td>
</tr>
<tr>
<td>Alignment Errors</td>
</tr>
<tr>
<td>Giant Packets</td>
</tr>
<tr>
<td>Broadcast Packets</td>
</tr>
</tbody>
</table>

To terminate the console session and reset the console port baud rate to be automatically sensed. The command also disconnects the phone link if you accessed the console using modems.
Hubselect <hub_number>

To access an attached chained hub. If no hub number is specified, the hub directly connected to the console is selected.

The number is from the Entry column displayed when you use the CHainlist command. First enter the command CH to list the chain.

Example: CH (This displays the following example table.)

<table>
<thead>
<tr>
<th>Entry</th>
<th>Model</th>
<th>Station Address</th>
<th>Description</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1*</td>
<td>HPJ2601A AdvanceStack Et</td>
<td>080009-64cecf</td>
<td>chain access pt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HPJ2410A 100VG Hub-15</td>
<td>080009-5d8c04</td>
<td>none</td>
<td>No SNMP module</td>
</tr>
<tr>
<td></td>
<td>HPJ2410A 100VG Hub-15</td>
<td>80009-2b0682</td>
<td>none</td>
<td>No IP address</td>
</tr>
<tr>
<td>4</td>
<td>HPJ2600A 10Base-T Hub-12</td>
<td>080009-6756d4</td>
<td>Tech Mkt. Hub-12,No SNMP module</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HPJ2601A 10Base-T Hub-24</td>
<td>080009-973eef</td>
<td>Tech Mkt. Hub-24,192.1.1.1.10</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>HPJ2610A 10Base-T Hub-8</td>
<td>080009-1e61c4</td>
<td>Tech Mktg hubNo SNMP module</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HPJ2602A 10Base-T Hub-48</td>
<td>080009-975e35</td>
<td>Tech Mkt. Hub-48,No IP address</td>
<td></td>
</tr>
</tbody>
</table>

* Indicates hub that is currently selected

HUB 3 (This accesses the hub with Entry number 3.)

Now accessing hub with station address: 080009-6756d4

An Entry number is displayed only for other HP AdvanceStack 10Base-T hubs that do not have an HP Ethernet SNMP Module installed. Only hubs with Entry numbers can be accessed from the current console session. For more information about accessing hubs, see the CHainlist command.

Once you have connected to another hub, you can use the following commands on that hub only:

- CHainlist
- POrt
- COunters [A/B..]
- REset
- DIsconnect
- STatus
- HUbselect
- THinwatch

Note that the DIsconnect command is not hub specific and will end your console session.
**IPconfig**

To set IP (Internet Protocol) configuration parameters on the hub.

By default, the hub is configured to use BOOTP (Internet Boot Protocol) to automatically retrieve the IP parameters from a BOOTP server, or to use the Novell NetWare IPX protocol, and to enable Telnet access to the hub’s console interface. Use this command if you want to manually configure the IP address or disable Telnet.

*The IP configuration must be carefully controlled. If each device’s IP address is not unique on the network, severe network performance problems will occur.* A network administrator should maintain responsibility for the IP settings. See appendix C, “Network Addressing” in *HP AdvanceStack 10Base-T Installation and Reference Guide* for information on setting the IP configuration.

---

**Note**

At the end of the process of changing the IP configuration, the hub will be reset. This terminates the console session (and disconnects the phone line if using a modem) and resets the console port baud rate to be automatically sensed. To restart a console session, when the reset process completes, press [Return] several times for the prompt.

---

**When to Use IPconfig**

If any of the following is true, the hub’s IP parameters must be configured, either on a BOOTP server or on the hub through the console interface:

- The hub will be managed remotely with a network management product, such as HP OpenView Workgroup Node Manager or HP Interconnect Manager For OpenView Windows, over an IP network (a network that uses IP communications, for example TCP/IP).
- The network cable segments attached to the hub will be tested using the IP “Ping” test.
- Telnet access to the hub is desired.
Configuring for Network Management

If the hub is to be managed from a network management station, it must use the same networking protocol as the network management station. You have these choices:

- Novell NetWare IPX
- IP

Using Novell NetWare IPX  The HP AdvanceStack hubs are designed to automatically use Novell NetWare's IPX protocol. If you are using the hub on a Novell NetWare network, no configuration of the hub is required for it to communicate with a network management station that is also using the IPX protocol.

The hub determines its IPX address automatically from information received from a router or file server that is running IPX on the network, and from its own station address (also sometimes called the MAC address, physical address, or Ethernet address). See your Novell documentation for more information on IPX communications and addressing.

Using IP  You can use IP by using one of the following methods:

- using BOOTP by adding an entry for the hub in the BOOTP table on your BOOTP server, and enabling BOOTP through the hub's console interface (this is the default setting)
- using the console interface to configure the IP parameters

To use the console interface to configure the IP parameters, enter IP and the following text appears:

```plaintext
=>IP
Active IP parameters:
  BOOTP protocol enabled: YES
  Telnet access enabled: YES
  IP address: 0.0.0.0
  Subnet mask: 0.0.0.0
  Default router: 0.0.0.0
  Time to live: 64
Change IP configuration? [Y/N]:
```

The following table explains the IP parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOOTP protocol enabled</td>
<td>YES</td>
<td>Keep or set this value to YES if you are using a BOOTP server to provide the IP configuration to the hub. By default, the hub with an HP Ethernet SNMP Module installed is configured to automatically seek an IP address from a BOOTP server on the network. This is done when the hub is powered on. If an IP address is not found, the HP Ethernet SNMP Module will seek an IP address every ten minutes until it finds an IP address. Set this value to NO to disable an HP Ethernet SNMP Module from polling. If you are not using BOOTP to provide the hub’s IP configuration, you should set this parameter to NO.</td>
</tr>
<tr>
<td>Telnet access enabled</td>
<td>YES</td>
<td>Determine whether users are allowed to use Telnet to access the hub’s console interface.</td>
</tr>
<tr>
<td>IP address</td>
<td>0.0.0.0</td>
<td>The IP address of the hub (written in the format X.X.X.X). Each X is a decimal number between 0 and 255 separated by a decimal point. This address will be used unless the BOOTP protocol is enabled. The default value disables IP communications on the hub when BOOTP is also disabled.</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Automatically generated and depends on the class of IP address that has been entered.</td>
<td>The bit mask defining which portion of the IP address is the subnet address, written in the format X.X.X.X. All the devices on your network should use the same subnet mask. See your network administrator for the correct value.</td>
</tr>
<tr>
<td>Default router</td>
<td>0.0.0.0</td>
<td>The IP address of the nearest IP router in your network. If no IP routers are in your network, enter the address of a network management station, if any.</td>
</tr>
<tr>
<td>Time to live</td>
<td>64</td>
<td>The number of IP routers a packet is allowed to cross before the packet is discarded. Increase this value if the hub will be sending IP packets to a destination that is more than 64 routers away. The maximum is 255.</td>
</tr>
</tbody>
</table>
To configure the list of network management stations that are authorized to access and manage this hub, and to specify which of those stations should receive alarms. Use the SHow option to display the current list of authorized management stations without being prompted to edit the list.

The list consists of the IP or IPX address of the network management station and an indication of whether each management station should receive alarms (indications of specific network events that are configured for the hub from network management—also called SNMP event alarms). The start of the table is shown below. Up to ten network management stations can be entered into the table. Entry 0 (zero) is used for the “all managers allowed” entry.

<table>
<thead>
<tr>
<th>ID</th>
<th>Manager Address (IP or IPX)</th>
<th>Receive Alarms?</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>All managers allowed</td>
<td>NA</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The hub is initially shipped with all network management stations allowed to manage the hub, but the “all managers” entry does not identify where alarms are to be sent. Specific addresses must be entered into the table to identify where the alarms should be sent.

**Note**

If you want to restrict which management stations are allowed to manage the hub, delete entry 0. Then add the allowed management stations with the A command.

At the interface prompt, enter MA; the current authorized managers list is displayed and you are prompted to add or delete an entry in the list, or to enter E to end your editing.

**To add an entry**, enter A at the prompt. Enter the IP or IPX address of the network management station, or enter A to allow all managers to manage the hub, then indicate at the next prompt whether this management station should receive alarms generated by the hub. A new entry is added to the list.
Example: To add the network management station with IP address 190.40.101.10 to the list and to send alarms to that station, the process would appear as follows:

Add entry (A), Delete entry (D), or End changes (E): A
Enter Manager Address, or (A) to allow all managers access: 192.1.1.1
Should this manager receive alarms: (Y/N): Y

Add entry (A), Delete entry (D), or End changes (E): E
Current authorized manager list:

<table>
<thead>
<tr>
<th>ID</th>
<th>Manager Address (IP or IPX)</th>
<th>Receive Alarms?</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>All managers allowed</td>
<td>NA</td>
</tr>
<tr>
<td>1</td>
<td>190.040.101.010</td>
<td>YES</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To delete an entry, specify the ID number in the list corresponding to the network management station to be deleted.

Example: To delete the entry made in the example above, the steps would be:

Add entry (A), Delete entry (D), or End changes (E): D
Enter ID of entry to delete: 1

Add entry (A), Delete entry (D), or End changes (E): E
The table entry with ID 1 would now be a blank line.

**Password**

To set or change the password on the hub. The password is used to prevent unauthorized access to the hub from network management stations, and through the console interface. The hub is initially shipped without a password. Follow the prompts to enter a new password or to change the existing password. If you assign a password, it is also used as the SNMP community name.

If you decide to delete the password, enter the Password command, then press [Return] without entering any characters at the password prompt.

**Clearing a Forgotten Hub Password:** If you have forgotten or misplaced the password, see page 1-7.
**Plng**

To test the path between the hub and another device that responds to IP packets. The hub sends Internet Control Message Protocol (ICMP) Echo Request (Ping) packets to another node with the specified IP address and waits for Echo Response packets in return.

When you run the Ping command, you will be prompted for:
- the IP address of the destination device (in the format X.X.X.X)
- the number of packets to send
- the timeout value (the number of seconds to wait for a response)

If any errors are reported during this test, there may be a fault in the path used during the test or in the destination device. For more information about testing network links, see chapter 3, “Troubleshooting”.

**P0rt <port> <ON|OFF>**

To enable (set to ON) or disable (set to OFF) a hub port. The initial setting for all ports is enabled (ON). You can use the Status command to check the current status of all the ports. The `<port>` parameter can be:
- for hubs with 24 ports or more, a twisted-pair port group letter (A, B, C, or D) followed by a number.
- for hubs with less than 24 ports, a twisted-pair port number only.
- XCVR or XC for the Xcvr port
- THINLAN or TH for the ThinLAN port
- ALL or AL for all ports

Example 1:  P0 A1 OFF  (This disables port A1.)
Example 2:  P0 A OFF  (This disables all the twisted-pair ports in group A.)
Example 3:  P0 7 OFF  (This disables port 7 on an eight port hub.)
Example 4:  P0 XC OFF  (This disables the AUI/Xcvr port.)
Example 5:  P0 THINLAN OFF  (This disables the ThinLAN port.)
Example 6:  P0 AL ON  (This enables all of the ports.)
**REset**

To run a hub self-test and reset the hub. This command also resets all the network statistic counters, and the time since the last reset to 0. The current configuration is unchanged. The hub is not accessible from network management software while it is being tested, but it continues to repeat data. For hubs in the distributed management chain, LEDs will not flash during a reset, and counters and time will not be reset. If the hub is faulty, at the end of the reset process the Fault LED on the front of the hub will stay on.

This command also terminates the console session (and disconnects the phone line if you are using a modem to access the console) and resets the console port baud rate to be automatically sensed. To restart the console session, first re-establish the phone link (if used), then press [Return] several times for the prompt.

**RObustness**

Allows you to invoke options to improve the hub’s ability to tolerate network problems resulting from excessive collisions. The configurable options are:

- Intelligent Segmentation Recovery
- Late Collision Monitoring

By default, the robustness features are off. The Intelligent Segmentation Recovery option makes it difficult for a problem port to automatically re-enable itself to send traffic on the network.

The Late Collision Monitoring option monitors non-cascaded ports or all ports for excessive late collisions. If monitored ports experience excessive late collisions, these ports are disabled. For more information about robustness, see auto-segmentation in chapter 1 of the *HP AdvanceStack 10Base-T Hubs Installation and Reference Guide.*

**SEcure <port|SHow|CLear>**

To control or display the hub’s security configuration, and to clear security violation indicators. The <port> parameter can be:

- for hubs with 24 ports or more, a twisted-pair port group letter (A, B, C, or D) followed by a number.
- for hubs with less than 24 ports, a twisted-pair port number only.
- XCVR or XC for the Xcvr port
- THINLAN or TH for the ThinLAN port
- ALL or AL for all ports
Security Configuration Parameter Definitions

The following security parameters are configurable on each of the hub’s network ports. These parameters are defined on the next two pages:

- Address selection method, or authorized station address
- Send alarm when intruder detected
- Eavesdrop prevention

An additional parameter, “Disable port when intruder detected”, is set automatically by your selection of the address selection method. See “Auto Port Disable” in appendix C for information on this parameter.

Address selection method, or authorized station address: This is the method by which the hub automatically learns the address of the device that is authorized to use the port, or you can enter a specific address. The following methods are configurable:

- Learn Continuously—provides minimum port security. The hub learns the address of the first device attached to the port and makes it the authorized station address. If a different device is later attached to the port, the new address is learned and becomes the authorized address. Each new device attached becomes the authorized device. You can be informed of any such changes by setting the Send Alarm parameter to YES. In that case, when a new address is detected, the Security and port LEDs flash, the intruder's station address is displayed on the console Status command screen, and an alarm is sent to the authorized network management station(s).

- Use the First Address Heard—provides medium port security. The hub learns the address of the first device attached to the port and makes it the authorized station address. If you have any security configured for the port (Send Alarm and/or Eavesdrop Prevention parameters are set to YES), when a different device is later attached to the port, the new address is registered as an “intruder address”; a security violation has occurred. In that case, the port is automatically disabled, and the Security and affected port LEDs flash. An alarm is also sent to the authorized network management station(s) if the Send Alarm parameter is set to YES.

- Assign an Address—provides the highest security. You enter the address of the device that is authorized to be attached to the port. If you have any security configured for the port (Send Alarm and/or Eavesdrop Prevention parameters are set to YES), when a different device is later attached to the port, the new address is registered as an “intruder address”; a security violation has occurred. In that case, the port is automatically disabled, and the Security and port LEDs...
flash. An alarm is also sent to the authorized network management station(s) if the Send Alarm parameter is set to YES.

- **Port Security Off**—*disables port security.* This is a convenient way to remove the port security. It automatically sets the Send Alarm and Eavesdrop Prevention parameters to OFF (and therefore, the Disable Port parameter will also be OFF).

**Send Alarm when intruder detected:** Configures the hub to send an alarm (SNMP trap) to a network management station whenever an unauthorized address (an intruder) is detected on the port. *Note that for the alarm to actually be sent, you must have first used the Managers command to configure one or more network managers to receive alarms.* See the Managers command description earlier in this chapter.

**Eavesdrop prevention:** Configures the hub to prevent the port from hearing data that is intended for another port. Only the data packets that have a destination address that matches the port's authorized address are sent to the port. If Eavesdrop Prevention is not enabled on all ports, the hub functions like a repeater and every packet seen by the hub is forwarded to the non-Eavesdrop Prevention ports. See appendix C, “Security Information”, for a detailed description of this feature.

### Configuring Security on a Single Port

To set or change the security configuration for a single port on the hub (twisted-pair, ThinLAN, or Xcvr), enter SE and the port’s ID; for example, SE A4. The port’s current security configuration is displayed, followed by a prompt to change the configuration or not.

If you choose to change the configuration, you are then prompted for the following parameters (defined on the previous page):

- Address selection method, or authorized station address

You are first prompted if you want to change the address selection method or the authorized address. Press [Return] or enter N to retain the current value. Enter Y to change the value and you are prompted to select one of the following methods:
  - use First address heard (enter F)
  - learn address Continuously (enter C)
  - Assign an address (enter A)
  - port security Off (enter O)

- Send alarm when intruder detected
- Eavesdrop prevention
Configuring Security on All Twisted-Pair Ports

To set or change the security configuration for all the twisted-pair ports together, enter `SE ALL`. This method is most useful when you are using the same security configuration for all the twisted-pair ports, either at initial setup or when you want to change the configuration for all the ports. You are prompted whether to continue this process or not. If you choose to continue, you are then prompted for:

- Address selection method:
  - If you select `First heard for all ports (F)`, `learn continuously for all ports (C)`, or `security Off for all ports (O)`, the setting you select will be applied to all the twisted-pair ports. If you enter F, the authorized address for each of the twisted-pair ports will be the source address in the first packet received from the attached device. If you enter C, each of the twisted-pair ports will continuously update the authorized address when the attached devices change. If you enter O, the security will be turned off for all the twisted-pair ports; that is, the security parameters will all be set to NO (configured address selection methods, and learned or assigned addresses are not changed).

- If you select `assign Each port (E)`, a table like the following is displayed:

<table>
<thead>
<tr>
<th>PORT</th>
<th>ADDRESS SELECTION METHOD</th>
<th>AUTHORIZED ADDRESS</th>
<th>F, C, or a station address</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>CONTINUOUS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>A2</td>
<td>CONTINUOUS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>A3</td>
<td>CONTINUOUS</td>
<td>NONE</td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

  For each port, enter an address selection method (F or C), or a specific station address, or press [Return] to retain the current value. Continue this process until all of the ports are displayed. If you do not want to configure all twisted-pair ports, note that you can terminate the address selection method by pressing [Esc] once. In either case, you are then prompted for the settings for the Send Alarm and Eavesdrop Prevention parameters, as described on the next page.
Send Alarm when intruder detected? and Eavesdrop prevention?:

These parameters are defined earlier in the chapter under “Security Configuration Parameter Definitions”.

*The values you select for these parameters will be applied to all the twisted-pair ports for which you have selected (or retained) the address selection method.*

If, for example, you pressed the Esc key after selecting an address selection method for port A10, the Send Alarm and Eavesdrop prevention values you select would be applied to ports A1 through A10 only. For all remaining ports, the previous value for these parameters would be retained.

**Showing the Security Configuration**

Enter the command `SE SH` to display the security configuration for all of the hubs ports. A table like the following is presented:

<table>
<thead>
<tr>
<th>PORT</th>
<th>ADDRESS SELECTION METHOD</th>
<th>AUTHORIZED ADDRESS</th>
<th>EAVESDROP PREVENTION</th>
<th>SEND ALARM</th>
<th>DISABLE PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>CONTINUOUS</td>
<td>123456-890123</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>A2</td>
<td>CONTINUOUS</td>
<td>NONE</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>A3</td>
<td>FIRST HEARD</td>
<td>123456-789012</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
</tbody>
</table>

The vertical bar between Send Alarm and Disable Port indicates that the value for the Disable Port parameter is not directly configurable. This parameter is automatically set by the Address Selection Method. If the method is either First Heard or Assigned, and if at least one of the other security parameters is set to YES, the Disable Port parameter will be YES. If the method is Continuous, the Disable Port parameter is always automatically set to NO.

**Clearing Security Violation Indicators**

Enter the command `SE CL` to clear any security violation indicators and to “rearm” the indicators to be ready for the next intrusion. The indications are slightly different between port security violations and network management security violations, as described next.
For Port Security: The security violations are indicated by the Security LED and the LED for the affected port blinking simultaneously, and the intruder’s station address being added to the Status command screen for the affected port. Security violations occur when a non-authorized address is detected on a port and at least one of the intruder prevention parameters (Send Alarm or Disable Port) is set to YES.

For Network Management Security: The security violations are indicated by the Security LED flashing and the violating network management station’s address being displayed on the Status command screen.

A network management security violation occurs when a network management station that is not on the authorized management station list attempts to issue SNMP “set” commands to the hub, or when a network management station uses an invalid password (SNMP community name) to access the hub.

See the Managers command description, earlier in this chapter, for information on the authorized management station list. By default, all network management stations are allowed to manage the hub. Under this configuration, network management security violations will not occur.

Notes
If the port was disabled because of a security violation (Disable Port = YES), to re-enable the port you must enter the port ON command for that port.

The Security Clear command does not remove the cause of the security violation, for example the wrong device being attached to a port. Until the cause is removed, the violation can reoccur immediately after issuing the SE CL command. It may appear as if the violation indication was never cleared.
**SPeed <new speed>**

To change the console port baud rate. Normally, the baud rate is automatically sensed. Use this command if you want to set the baud rate explicitly to 1200, 2400, 4800, 9600, 19200, or 38400. You will be prompted to set the terminal’s baud rate to the same speed and to press [Return] for the prompt. Example SP 9600. (Sets the baud rate to 9600.) Note that Windows supports up to 19200 baud only.

**STatus [A|B|C|D]**

To display status information for the hub (or optionally for a specified port group (A, B, C or D). You do not need to specify a letter for hubs with less than 24 ports. The status information includes:
- the time elapsed since the last reset (see the Reset command),
- the hub’s station address,
- the Thinwatch setting (see the Thinwatch command),
- if a network management security violation has occurred, the station address of the violating network management station,
- and a table with the port information described on the next two pages:

<table>
<thead>
<tr>
<th>Port ID</th>
<th>The port ID. (Additionally, bkg indicates that the port is configured as the backup link, pri indicates that the port is the primary link – see the Backup command).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Status</td>
<td>The status of each port:</td>
</tr>
<tr>
<td></td>
<td>ON means the port is enabled and is not auto-segmented.</td>
</tr>
<tr>
<td></td>
<td>OFF means the port has been disabled by the Port command or because of a security violation.</td>
</tr>
<tr>
<td></td>
<td>SEGMENTED means the port has been auto-segmented. (See “Auto-Segmentation” in the HP AdvanceStack 10Base-T Hubs Installation and Reference Guide.)</td>
</tr>
<tr>
<td></td>
<td>ON/REVERSED means that reversed wiring polarity on the receive pair has been detected on a twisted-pair cable and the hub has compensated.</td>
</tr>
<tr>
<td>Link Beat</td>
<td>Informs the hub of the presence of a device connected to it over twisted-pair cable.</td>
</tr>
<tr>
<td>Station Address</td>
<td>The unique 12-digit link-layer address for the hub. (Also called MAC address, Ethernet address, or physical address.)</td>
</tr>
<tr>
<td>INTRUDER ADDRESS</td>
<td>The address of a device not authorized to access the hub.</td>
</tr>
</tbody>
</table>
Extended Hub Capabilities

**TEstlink**

To run a test of the link between the hub and another IEEE 802.3 device.

---

**Note**

The destination device must be able to send an IEEE 802.2 Test Response packet upon receipt of an IEEE 802.2 Test command packet. Any HP AdvanceStack Hub, HP SNMP-managed bridge, or HP router will respond with the correct packet. HP LAN adapters can be setup up easily to respond to these standard Test command packets.

You will be prompted for the 12-digit hexadecimal station address (also called MAC address, Ethernet address, or physical address) of the destination device. You will then be prompted for the number of test packets to send.

If any errors are reported during this test, there may be a fault on the link being tested or on the destination device. For more information about testing network links, see chapter 3, “Troubleshooting”.

---

**TThinwatch <ON|OFF>**

To enable (set to ON) or disable (set to OFF) Thinwatch on the ThinLAN port. With Thinwatch enabled, the Fault and ThinLAN port LEDs will flash whenever the ThinLAN port is auto-segmented. (If you don’t enable Thinwatch, the LEDs won’t flash.)

Auto-segmentation occurs on the ThinLAN port when it is enabled but has no connector on it, the connected segment is not properly terminated, or it experiences excessive collisions.

The default setting is disabled. Enable Thinwatch if the ThinLAN port is being used; disable Thinwatch if the ThinLAN port is not being used.

Example: TH ON  (This enables Thinwatch.)
Troubleshooting

- Diagnosing with the LEDs
- LED Location
- Customer Support Services
Troubleshooting

The primary tools for troubleshooting the SNMP Module are the LEDs on the front of the hub and, in some cases, the single LED on the SNMP Module in combination with the LEDs on an auxiliary module. The location of these LEDs are described on the next page.

Diagnosing With the LEDs

1. When the hub is first powered on or when it is reset, it executes its self test and also causes the SNMP Module and any auxiliary module to execute their self tests. If only the SNMP Module is installed, the self test should take up to 40 seconds. If an auxiliary module is also installed, the self test may take up to 60 seconds. During the self test of the modules, the Exp Slot LED on the front of the hub flashes.

   If you suspect improper operation of the SNMP or auxiliary module, you can reset the hub and use the self test results to verify the module status.

2. If beyond the self test time the Exp Slot LED continues to flash instead of turning continuously ON, there may be an error condition on the HP Ethernet SNMP Module and/or the auxiliary module.

   - If only the SNMP Module is installed, proceed to step 3.
   - If an auxiliary module is also installed, more information on the cause of the self test failure may be available by viewing the hub’s Expansion Slot cover plate. If the Fault LED on the SNMP Module is visible and is ON, the SNMP Module has failed its self test. In this case, ignore any LEDs on the auxiliary module. If the Fault LED on the SNMP Module is OFF, the SNMP Module has passed its self test; the problem may be with the auxiliary module. If there are LEDs on the auxiliary module, check them for indications of failure. See your auxiliary module documentation for more information.

3. Verify that the modules are installed correctly. If they are installed incorrectly, repeat the installation procedure, taking special care to ensure that any auxiliary module is properly connected to the SNMP Module, and that the SNMP Module's hub connector is firmly seated in the connector at the back of the hub’s Expansion Slot.

4. If repeating the installation procedure does not rectify the problem and the Exp Slot LED on the hub still fails to stay continuously ON, contact your HP-authorized LAN dealer or HP representative for replacement information.
LED Location

The Hub LEDs

The LEDs on the front of the HP AdvanceStack 10Base-T Hub are shown in the illustration above. Pay particular attention to the LED labeled Exp Slot (AdvSlot on some HP AdvanceStack hubs). It describes the self test status of all the modules installed in the Expansion Slot. The module LEDs define the status of each individual module.

The Module LED(s)

On the back of the hub, a single LED is installed on the HP Ethernet SNMP Module as shown in the illustration in the “At a Glance” section at the beginning of this guide. If the module is installed into the hub in combination with an auxiliary module, this LED may be used to indicate if a self test failure has occurred on the SNMP Module and to distinguish that from a self test failure on an auxiliary module.

The SNMP Module LED  If the HP Ethernet SNMP Module alone is installed, the hub’s LEDs provide all the diagnostic information needed; the SNMP Module’s LED is not used and is covered by the cover plate.

The Auxiliary Module LEDs  If an auxiliary module is attached to the SNMP Module, it may have additional LEDs that can be used for troubleshooting. In addition, the auxiliary module’s cover plate may reveal the LED on the HP Ethernet SNMP Module so that you may distinguish between a failure on the SNMP Module and on the attached auxiliary module.
Customer Support Services

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

- Hewlett-Packard BBS and World Wide Web
- Hewlett-Packard FTP Library Service on the Internet
- HP FIRST FAX Retrieval Service
- CompuServe

HP Interconnect Manager (icmupdt.exe), HP Stack Manager (stkmgr.exe) and SNMP firmware for your AdvanceStack hubs (asfw.exe) are available through the HP BBS, World Wide Web, CompuServe, and the HP FTP Library Service. After you download the file(s) from one of these sources, you type *filename/x*. For example, *icmupdt/x*

**HP BBS and World Wide Web**

The HP BBS phone number is (208) 344-1691. Set your modem communication settings to:

- parity = N
- data bits = 8
- stop bits = 1
- baud rates = 300, 1200, 2400, 4800, 9600, or 14400

The URL address for the World Wide Web is:

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

From this web site, you can download files and learn about HP networking products. After you download the file, extract the file (e.g., *icmupdt/x*)
Hewlett-Packard FTP Library Service

To access the HP FTP Library, follow these steps:

1. Enter the command:
   
   ftp ftp-boi.external.hp.com

   The ftp> prompt appears.

2. At the ftp > prompt, enter:

   anonymous

3. At the password prompt, enter your internet e-mail address.

4. At the ftp > prompt, set the transfer type to binary:

   bin

5. Change directories:

   cd pub/networking/software

6. Retrieve the file by entering:

   get filename (e.g., get asfw.exe)

7. Quit the FTP session by entering:

   quit

8. Extract the file (e.g., asfw /x)
Troubleshooting

HP Network Phone-In Support (NPS)

You can usually receive the support assistant you need by calling your HP Authorized Dealer or the nearest HP Sales and Support Office. In addition, the HP Network Phone-In Support (NPS) service provides expert technical assistance for U.S.A. customers through an NPS contract or at an hourly rate (1-800-790-5544) Monday through Friday, 5 am to 6 pm.

HP FIRST Fax Retrieval Service

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

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

To access HP FIRST, dial one of the following phone numbers from your touch-tone telephone:

<table>
<thead>
<tr>
<th>Location</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. and Canada Only</td>
<td>(800) 333-1917 and press 1 for HP FIRST</td>
</tr>
<tr>
<td>Outside the U.S. and Canada</td>
<td>(208) 344-4809 and press 9 for HP FIRST</td>
</tr>
</tbody>
</table>

To receive a list of currently available documents, enter document number 19941. The information you requested will be sent to you by return fax.
CompuServe

CompuServe is an electronic information and communication service run by an independent company. The service is typically accessed with a computer and modem and uses standard voice telephone lines for transmitting and receiving data. CompuServe is available 24 hours-a-day, seven days per week. The participants pay a monthly fee as well as an hourly connect charge for this service. To get the latest agent firmware from CompuServe, follow these steps:

1. Login to CompuServe.
2. Type: go hpsys
3. Type: lib 7
4. Type: download asfw.exe
5. The asfw.exe file is a self-extracting file. On your PC, extract the files by entering:
   asfw /x
   A readme file is extracted and includes instructions to download the agent firmware to your HP Ethernet SNMP Module.
Specifications
Specifications

Physical
Dimensions 17.8 cm by 13.5 cm (7 in by 5.25 in)
Weight 170 g (6.0 oz)

Environmental
Operating temperature: 0°C to 55°C (32°F to 131°F)
Nonoperating temperature: -40°C to 70°C (-40°F to 158°F)
Relative humidity: 15% to 95% at 40°C (104°F) non-condensing
Maximum altitude: 4.6 km (15,000 feet)

Electromagnetic
Emissions
FCC part 15 Class A
EN55022 / CISPR-22 Class A
VCCI Level 1
Complies with Canadian EMC Class A requirements.

Immunity
See the Declaration of Conformity in the HP AdvanceStack 10Base-T Hubs Installation and Reference Guide.

Acoustic Noise
Not applicable
Modem Configuration
Modem Configuration

Before installing the modems (one attached to the hub and one attached to the terminal/PC), configure them by either issuing the appropriate AT command or by setting the modem’s switches, as described in the tables in the rest of this appendix.

**Hayes V-Series ULTRA Smartmodem 14400**

<table>
<thead>
<tr>
<th>At the hub end:</th>
<th>Issue the following AT command: AT&amp;FS0=1&amp;D2&amp;S2&amp;Y0&amp;W0</th>
</tr>
</thead>
<tbody>
<tr>
<td>At the user end:</td>
<td>Issue the following AT command: AT&amp;FY0&amp;W0 (returns modem to factory default)</td>
</tr>
</tbody>
</table>

**Hayes Smartmodem 2400**

| At the hub end: | Issue the following AT command: AT&FE0S0=1&S1&C1&D2&Y0&W0  
| Then, connect the modem to the hub and power cycle the modem while the hub is powered on. |
| At the user end: | Issue the following AT command: AT&FY0&W0 (returns modem to factory default) |

**Multi Tech 14.4 (MT1432BA)**

| At the hub end: | Issue the following AT command: AT&FS0=1&W0 |
| At the user end: | Issue the following AT command: AT&FW0 (returns modem to factory default) |
## US Robotics Courier HST Dual Standard with ASL

| At the hub end: | Switch 1 UP—DTR normal  
| Switch 5 UP—Auto Answer on ring  
| Switch 6 UP—carrier detect when modem is online  
| Switch 8 DOWN—AT command set recognized  
| Switch 9 UP—modem disconnects when session ended  
| Switch 10 UP—load software from NVRAM at power on |

| At the user end: | Switch 1 UP—DTR normal  
| Switch 4 UP—modem echoes (displays) commands  
| Switch 5 DOWN—Auto Answer suppressed  
| Switch 6 UP—carrier detect when modem is online  
| Switch 8 DOWN—AT command set recognized  
| Switch 9 UP—modem disconnects when session ended  
| Switch 10 UP—load software from NVRAM at power on |

## Intel 14.4EX

| At the hub end: | Issue the following AT command:  
| AT&FS0=1&S1&Y0&W0 |

| At the user end: | Issue the following AT command:  
| AT,F0&Y0&W0 (returns modem to factory default) |

## Telebit WorldBlazer

| At the hub end: | Set the A/B switch to A  
| Issue the following AT command:  
| AT&F0&R1&W0 |

| At the user end: | Set the A/B switch to A  
| Issue the following AT command:  
| AT&F0&W0 |
Security Information
In addition to password protection and network management access protection described in chapter 2, the HP AdvanceStack hub with an HP Ethernet SNMP Module installed provides two major types of per-port security:

- **Intruder Prevention** for inbound data (from the end user to the hub).
- **Eavesdrop Prevention** for outbound data (from the hub to the end user).

Both of these types of security can be configured on each port individually (all twisted-pair ports, plus the Xcvr port, and the BNC port) through the SEcure command on the ASCII console interface. These per-port security features are enabled by comparing the source and destination address of each packet received or transmitted by the hub to each port’s Authorized Station Address—the station address of the device that is authorized to communicate through that hub port.

These features are not yet available through HP Stack Manager but they can be set through the network management program HP Interconnect/Manager.

### Intruder Prevention

Intruder Prevention stops an unauthorized computer (or other device) from actively gaining access to the network. When a port is configured for Intruder Prevention, the hub examines the source address of each packet coming in through that port and compares it with the authorized station address. If the addresses are not the same, the hub concludes that an intruder is attempting to gain access to the network and takes the appropriate action (as configured): either disabling the port, sending an alarm to the network management station, or both. See “Setting Inbound Security with Intruder Prevention” later in this appendix.

### Eavesdrop Prevention

Eavesdrop Prevention stops a computer (or other device) from seeing network traffic that is not intended for that port. When Eavesdrop Prevention is configured on a port, the hub compares the port’s authorized station address with the destination address of any outbound packet. If the addresses match, the hub concludes that the packet is destined for the computer attached to the port, and it sends the packet out through the port unaltered. However, if the addresses do not match, the hub prevents the computer from seeing the packet’s contents by substituting a meaningless string of 1’s and 0’s. *Note that broadcast and multicast packets are repeated to all the ports, even when Eavesdrop Prevention is activated.* See “Setting Outbound Security with Eavesdrop Prevention” later in this appendix.
Authorized Station Address

To provide data security on a hub port, a single, unique station address must be configured as the authorized station address for each port. You can configure the authorized station address either by assigning it or by designating the port to learn it automatically. This configuration is performed with the Secure command from the hub's console. See the Secure command description in chapter 2.

Assigning the Authorized Station Address

You can assign an authorized station address by entering it manually at the hub console interface or at the network management station. Assigning a specific address provides the maximum control of the port's authorized station address. The Intruder Prevention and Eavesdrop Prevention security that you have configured for that port is implemented as soon as the address is assigned.

Learning the Authorized Station Address

You can set the hub to learn a port's authorized station address automatically by using either a “first heard” or a “learn continuous” method. The method used to learn the authorized station address should be chosen based on the level of data security required on a port. In each case, the security configuration for that port is implemented when the port receives a packet from the attached device. It learns the device's address from the source address field in the packet.

First-Heard Method  The “first heard” method automatically assigns the first address detected on the port as the authorized station address. This method is useful to quickly identify and authorize end users whose ports may require both Eavesdrop Prevention and Intruder Prevention. Under this method, the port will be disabled automatically if an intruder is detected.

Learn-Continuous Method  The “learn continuous” method allows the hub to continuously update the authorized station address configured for a port. Each new device connected to the port becomes the new authorized device. This security method is useful for dynamic workgroups that experience frequent changes to end-user configuration and require minimal data security protection. In the “learn continuous” mode, the port may be configured to provide the Eavesdrop Prevention data security and the send-alarm security violation notification. Under this method, the port will not be disabled if an intruder is detected.
Setting Inbound Security with Intruder Prevention

The picture below illustrates the use of inbound security using Intruder Prevention. This type of data security allows only one authorized user per port to access the network. The authorized user is identified by the authorized station address of the end node attached to the port.

Intruder prevention includes an “auto port disable” data security feature and a “send alarm” security violation notification feature. These features are described on the next page.

In the above illustration, the authorized end user is represented by PC 101, and the intruder is represented by PC 202. (For illustration purposes, the numbers 101, and 202 are used to represent 12-digit hexadecimal station addresses.) The HP AdvanceStack hub compares the authorized station address, 101, to the source address of the packet received by the Intruder, 202. The hub detects the unauthorized station address and automatically disables the port, and sends an alarm (a security violation trap notification) to the authorized network management station.
Auto Port Disable

Any port may be configured to be disabled automatically when an intruder’s station address is detected. *This feature is automatically controlled by your selection of the Authorized Address Selection Method for the port: If the address used is the “first heard” or an “assigned” address, the port will be disabled automatically when an intruder is detected. If the address is “learned continuously”, the port will not be automatically disabled.*

**Note**

Auto port disable may not be used on cascaded ports, ports connected to a network with multiple end users, or ports configured to learn the authorized station address continuously.

The auto port disable feature compares the authorized station address of the port to the source address of the packet inbound to the hub at that port. If the authorized address and the source address do not match, the HP AdvanceStack hub will automatically disable the port.

Once a port is disabled because of a security violation, to resume operation, the port must be re-enabled either by using the hub console interface’s Port command, or from the network management station.

*A bit error in the source address field of the packet will not cause the port to be disabled. In this case, the hub detects a CRC error for the packet and does not consider it as a security violation.*

Send Alarm

Any port may be configured to send an alarm (trap notification) to the network management station when an unauthorized station address or a new station address is detected on a secure port.

To use the “send alarm” feature, you must authorize at least one network management station to receive the trap notifications by entering the IP or IPX address of the network management station in the authorized managers list. Use the Managers command from the hub’s console to configure these addresses. See chapter 2 for more information on this command.
Setting Outbound Security with Eavesdrop Prevention

Eavesdrop Prevention allows a port to receive a packet transmitted on the network as valid data only if the port's station address matches the packet's destination address. If the port's station address does not match the packet destination address, the port will receive a packet containing a meaningless data field of alternating 1's and 0's. Multicast and broadcast packets are transmitted to all ports unmodified.

Note that sending a packet containing alternating 1's and 0's will continue to allow the port to detect the traffic on the network, so that the CSMA/CD network requirements are met. However, the port will correctly record the invalid data packet received as a CRC error. An end-user attached to an HP AdvanceStack hub implementing Eavesdrop Prevention data security will normally record a high number of CRC errors on the computer card statistics.

The illustration on the next page shows the use of outbound data security using Eavesdrop Prevention. This type of data security should be enabled on any port that is to receive data on a "need to know" basis. The port must have an authorized station address configured and must be connected to only one end-user.

*Eavesdrop Prevention may not be used on cascaded ports, or ports connected to a network with multiple end users.*
In the illustration below, Server 104 is transmitting a packet destined for PC 101. (For illustration purposes, the numbers 101, 102, 103, and 104 are used to represent 12-digit hexadecimal station addresses.) The ports for PC 101 and PC 102 have Eavesdrop Prevention enabled or configured ON. Because PC 101's station address matches the packet destination address, it receives the packet unaltered. However, PC 102's station address does not match the packet destination address and therefore it receives a useless packet (the packet data field contains a meaningless pattern of alternating 1's and 0's.) The port for PC 103 does not have Eavesdrop Prevention enabled and therefore PC 103 receives the packet unaltered from Server 104.
A
AdvanceStack hub
    installing an SNMP Module into ... 1-2
Alignment errors, counter ... 2-13
Assigning an address for port security ... C-3
Authorized station address ... C-3
    assigning an address ... 2-22, C-3
methods for selecting ... 2-22
Auto port disable, security feature ... 2-22, 2-25, C-5
Auxiliary command ... 2-11
auxiliary module
    connecting to using the AUsiliary command ... 2-11
B
Backup command ... 2-11 – 2-12
Backup Link Configuration
    from HP Stack Manager ... 2-3
Backup port ... 2-11
Baud rate ... 2-7
BBS
    obtaining software from ... 3-4
BOOTP ... 2-16
    polling intervals ... 2-6
Broadcast packets, counter ... 2-13
bulletin board
    obtaining software from ... 3-4
C
Chainlist command ... 2-12
Collisions, counter ... 2-13
Commands
    backup link ... 2-11 – 2-12
    chainlist ... 2-12
    counters ... 2-13
    disconnect ... 2-13 – 2-14
    help ... 2-10
    hubselect ... 2-14
    IPconfig ... 2-15
    managers ... 2-18
    password ... 2-19
    ping ... 2-20
    port ... 2-20
    reset ... 2-21
    robustness ... 2-21
    security ... 2-21
    speed ... 2-27
    status ... 2-27
    testlink ... 2-28
    thinwatch ... 2-28

CompuServe
    obtaining files from ... 3-7
Connecting a console
    using a terminal connected directly ... 2-7
Consecutive failures ... 2-11
Console
    commands ... 2-10
    connecting a terminal directly ... 2-7
    starting a session ... 2-7
    syntax conventions for commands ... 2-10
    terminating a session ... 2-13 – 2-14
Counters command ... 2-13
CRC errors, counter ... 2-13
customer service
types of ... 3-4

D
daughter cards
    See also see AUsiliary command

D
disconnect command ... 2-13 – 2-14

E
Eavesdrop prevention ... C-2
    configuration ... 2-23
    setting outbound security ... C-6
Error counters ... 2-13
Ethernet address
    See station address
Ethernet SNMP Module
    installing ... 1-2
    removing from a hub ... 1-6
Expansion Slot
    installing an SNMP Module into ... 1-2

F
Factory Default Reset
    from HP Stack Manager ... 2-4
Fault LED
    on the SNMP Module ... 1-4
fax
    using to get HP product information ... 3-6
firmware configuration
    during transfer to another hub ... 1-6
Firmware enhancements ... 1-5
ftp
    obtaining files from HP ... 3-5
Giant packets, counter ... 2-13

H
Help command ... 2-10
Hourly support
calling for ... 3-6
HP Dial-A-LAN module
connecting with the AUxiliary command ... 2-11
HP FIRST FAX Retrieval Service
using ... 3-6
HP FTP Library Service
using ... 3-5
HP Interconnect Manager
features with SNMP Module ... 2-5
HP Router 210 module
connecting with AUxiliary command ... 2-11
HP Stack Manager
features of ... 2-2
Hub
installing the SNMP Module into ... 1-2
Hubselect command ... 2-14

I
ICMP Echo Request packets (Ping test) ... 2-20
installing the SNMP Module ... 1-2
Internet
obtaining latest drivers from ... 3-5
obtaining software from ... 3-4
Intruder prevention ... C-2
auto port disable ... C-5
send alarm ... C-5
setting inbound security ... C-4
IP address ... 2-17
IP addressing ... 2-6
IP Configuration
from HP Stack Manager ... 2-3
IPconfig command ... 2-15
IPX addressing ... 2-6

L
LEDs
during self test ... 1-4

M
MAC address
See station address
Managers command ... 2-18
Modem Configuration
from HP Stack Manager ... 2-4
Modems
configuration ... B-2

N
Network Addressing
from HP Interconnect Manager ... 2-6
Network management
security violations ... 2-26
Network Test
from HP Stack Manager ... 2-4

O
Outbound security ... C-6

P
Password command ... 2-19
Physical address
See station address
Ping command ... 2-20
Port command ... 2-20
Port Security
from HP Interconnect Manager ... 2-5
Port status
display ... 2-27
Primary default router ... 2-17

R
Redundant SNMP management
from HP Interconnect Manager ... 2-5
Remote station address ... 2-11
Removing an SNMP Module ... 1-6
Reset command ... 2-21
Resetting the hub
reset command ... 2-21
Robust Port Control
from HP Stack Manager ... 2-3
Robustness command ... 2-21
S
Secure command ... 2-21
Security
authorized station address ... C-3
auto port disable ... 2-22, C-5
clearing the violation indicators ... 2-25
configuring a single port ... 2-23
configuring all twisted-pair ports ... 2-24
detailed description ... C-2
eavesdrop prevention ... 2-23, C-2, C-6
from HP Stack Manager ... 2-3
intruder prevention ... C-2
network management security violations ... 2-26
send alarm ... 2-23, C-5
showing the current configuration ... 2-25
Security command ... 2-21
Security violation indicators
clearing ... 2-25
network management security violations ... 2-26
port security violations ... 2-26
Self test
LED pattern during ... 1-4
Send alarm ... C-5
Send alarm, security parameter
configuration ... 2-23
SNMP Module
installing ... 1-2
removing from a hub ... 1-6
Speed command ... 2-27
Stack Manager
See HP Stack Manager
Starting a console session ... 2-7
static electricity
handling procedures ... 1-2
Station address
use in IPX address ... 2-16
Status command ... 2-27
Subnet mask ... 2-17
Syntax conventions for console commands ... 2-10

T
technical support
types of ... 3-4
Telnet session
establishing ... 2-8
Terminating a console session ... 2-13 – 2-14
Test packets ... 2-11
Testlink command ... 2-28
Thinwatch command ... 2-28
Time to live ... 2-17
Total packets ... 2-13

W
World Wide Web
obtaining software from ... 3-4
WWW
obtaining software from ... 3-4

Index

4-Index