HP | ProCurve | Hubs & Switches

HP ProCurve

HP TopTools for Hubs & Switches User Guide

Less Work, More Network

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

HP TopTools for Hubs & Switches

User Guide

Applicable Product

HP TopTools for Hubs & Switches J2569R

Trademark Credits

Microsoft Windows®, Windows 95®, Windows 98®, Windows 2000®, Microsoft Windows NT®, Microsoft Internet Explorer® and MSIE® are U.S. registered trademarks of Microsoft Corporation.

Ethernet is a registered trademark of Xerox Corporation.

Unicenter and TNG are registered trademarks of Computer Associates International, Inc.

IBM Tivoli and IBM NetView are registered trademarks of International Business Machines 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.

U.S. Government Restricted Rights

The software and any accompanying documentation have been developed entirely at private expense. They are delivered and licensed as "commercial computer software" as defined in DFARS 252.227-7013 (Oct 1988), DFARS 252.221-7015 (May 1991), or DFARS 252.227-7014 (Jun 1995), as a "commercial item" as defined in FAR 2.101(a), or as "Restricted computer software" as defined in FAR 52.227-19 (Jun 1987)(or any equivalent agency regulation or contract clause), whichever is applicable. You have only those rights provided for such Software and any accompanying documentation by the applicable FAR or DFARS clause or the HP standard software agreement for the product involved.

Warranty

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

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

Contents

3 System Requirements

4 Discovering Your Devices

5 Alerts

6 Networking Devices

7 Group Policies

8 Viewing Your Maps

9 Monitoring Network Traffic

10 Planning for Network Growth

1

Quick Start

This chapter provides a quick overview of important tasks that you can perform with HP TopTools for Hubs & Switches.

Starting HP TopTools for Hubs & Switches

To start HP TopTools for Hubs & Switches:

1. Click on the **HP TopTools** icon. Your browser will display the home page of the TopTools application.
2. In the TopTools home page, click on the **Home** button in the navigation frame, or click on the image of the switch.
3. Select **Hubs & Switches Home** from the Home button menu.

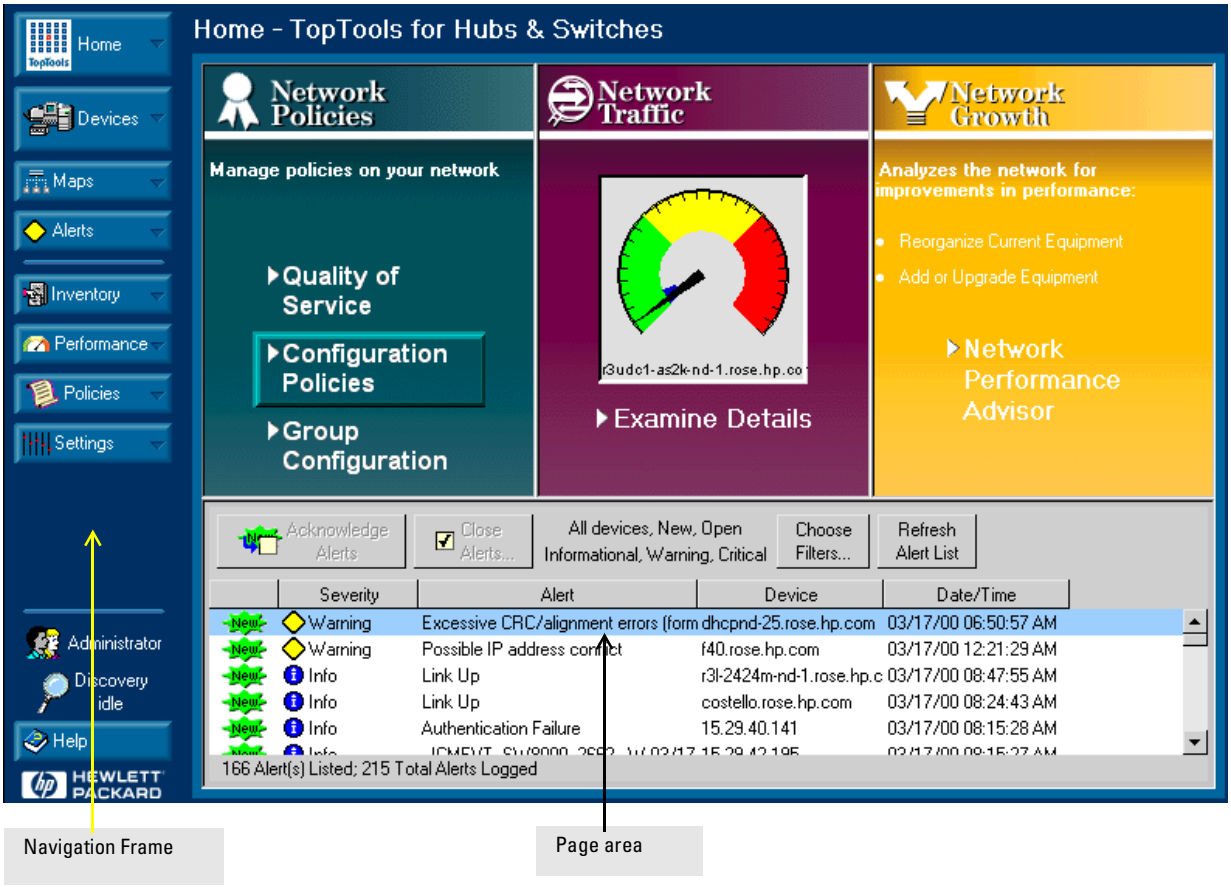


Figure 1-1. Home Page for HP TopTools for Hubs & Switches

Getting Around in HP TopTools

The browser-based tabbed presentation of HP TopTools makes it easy to access the page you need to perform management tasks. Click on a button in the navigation frame on the left side of the home page to see a list of tasks and features, then select a task from the list to open that page in the browser.

To go back to a previous page, click on the **back** arrow at the top of the browser window, or right-mouse-click in the page and select **back**.

Use the tabs or buttons at the top of a page to go quickly from task to task. Click on the **Home** button and select **Hubs & Switches Home** to return to the HP TopTools for Hubs & Switches home page.

The online help provides detailed information on how to perform HP TopTools tasks, as well as information about devices that are not manageable with the browser.

Viewing Your Network Devices

Devices

To view a list of your network devices, click on the **Devices** button in the navigation frame and select **Device Types** from the menu. Click on the **Networking Devices** folder to display each network device showing its type, connectivity status, the number of new and open alerts, and its management capability.

Right-mouse-click on a hub or switch and select **Properties (Device View)** from the menu to launch the Device View (formerly the Closeup View). You can perform many configuration tasks in the Device View.

See the chapter **Networking Devices** for more information about the Devices page.

Maps

To display a graphical representation of your physical network topology, click on the **Maps** button in the navigation frame, then double-click on a network in the Maps page. The default display is your local network. You can add more networks to be discovered in the **Settings - Discovery** page. Click on the **Settings** button in the navigation frame and select **Discovery**.

Double click on a hub or switch icon in the map to display the **Device View**, where you are able to perform configuration functions.

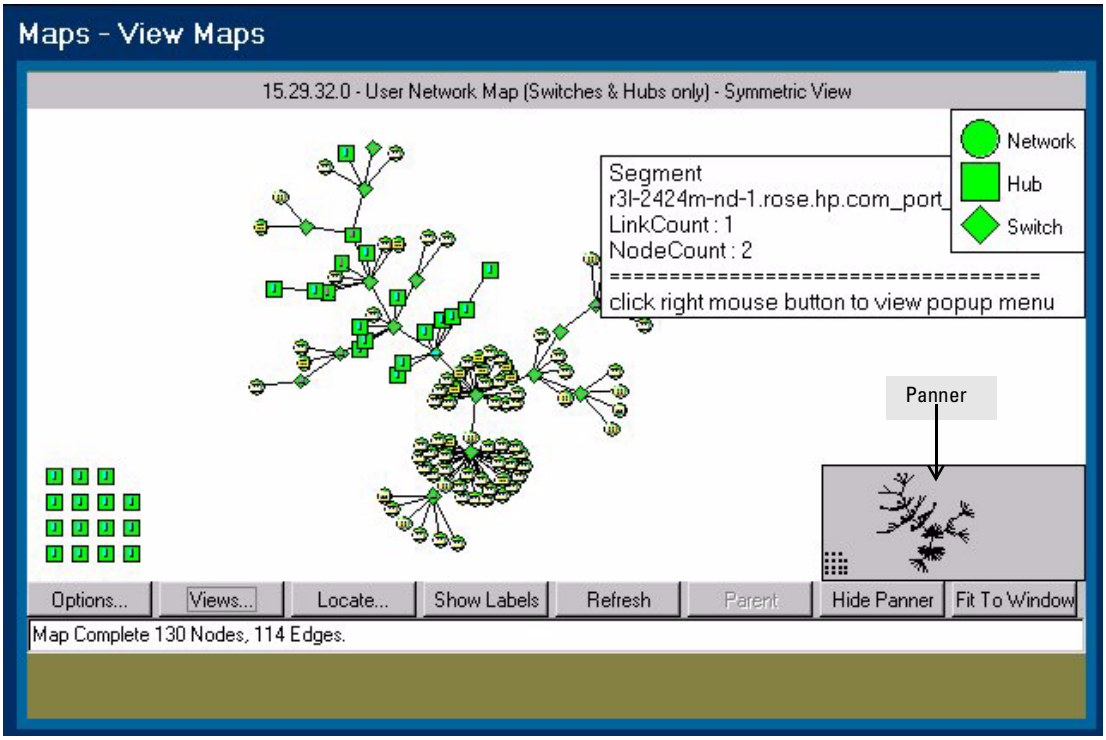


Figure 1-2. An Example of a Subnet Map

Using the Panner

The panner lets you easily focus in on a portion of your map. If it is not already displayed in the lower right corner of the map, select the **Show Panner** button to display the panner. In the Panner window, drag a rectangle around the portion of your network that you would like enlarged in the map view.

Click on the **Fit to Window** button to restore the map to its original size.

See the chapter **Managing Your Maps** for more detailed information on using maps.

Policies

Quality of Service

Quality of Service is a method for classifying and prioritizing traffic in a network. You can establish a traffic priority policy to control and improve the throughput of data. This allows the more important traffic to move through the network at acceptable speeds regardless of the bandwidth usage.

The **Quality of Service** feature available in HP TopTools for Hubs & Switches allows you to set up consistent traffic prioritization policies across the ProCurve switches in your network. The **Class of Service** features can be configured on an individual switch using the switch's console or web browser interface.

Click on the **Policies** button in the navigation frame and select **Quality of Service** from the menu.

See the chapter **Quality of Service** for more detailed information on these features.

Group Policies

Use Group Policies to automatically configure several features. To use Group Policies, the devices must be capable of management by a browser. The automatic management features include:

- Automatic checking of device firmware versions
- Sending all alerts to the HP TopTools management station (enabled by default)
- Switch Configuration
  - Automatic Broadcast Control
  - IP Multicasting
  - Spanning Tree Protocol
- Security Configuration by Group
- Alert Configuration by Group

See the chapter **Group Policies** for more information.

Examining Alerts

The bottom half of the HP TopTools for Hubs & Switches home page displays the Alert Log.

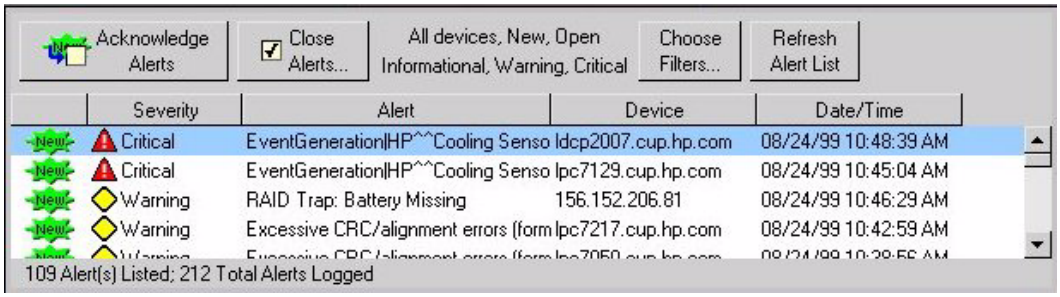


Figure 1-3. Alert Log

The Alert Log's "Find/ Fix/Inform" capability helps you proactively manage your network by displaying network traps and problem conditions in one easily accessible browser page. Click on the **Alerts** button in the navigation frame and select **View Alerts** to open the Alerts page. Click on an alert in the list at the top of the Alerts page to view more detailed information about that alert.

See the chapter **Alerts** for more detailed information about the Alert page.

See **Configure Action on Alerts** for information on configuring actions to take when certain types of events occur.

Configuring and Monitoring Devices

The Device View displays a graphical representation of a device. The Device View of an HP hub or switch can be accessed in the following ways:

- Click on the **Devices** button in the navigation frame and select **Device Types**. Select **Networking Devices**. Double-click on a device in the **Devices** page.
- Double-click on a device in the Topology list.
- Double click on a device in the topology map.
- Click on a device in the Device page, then select **Properties (Device View)** from the **Actions** menu at the top left of the Devices page.
- Right-mouse-click on a device in a map and select **Properties (Device View)** from the menu.

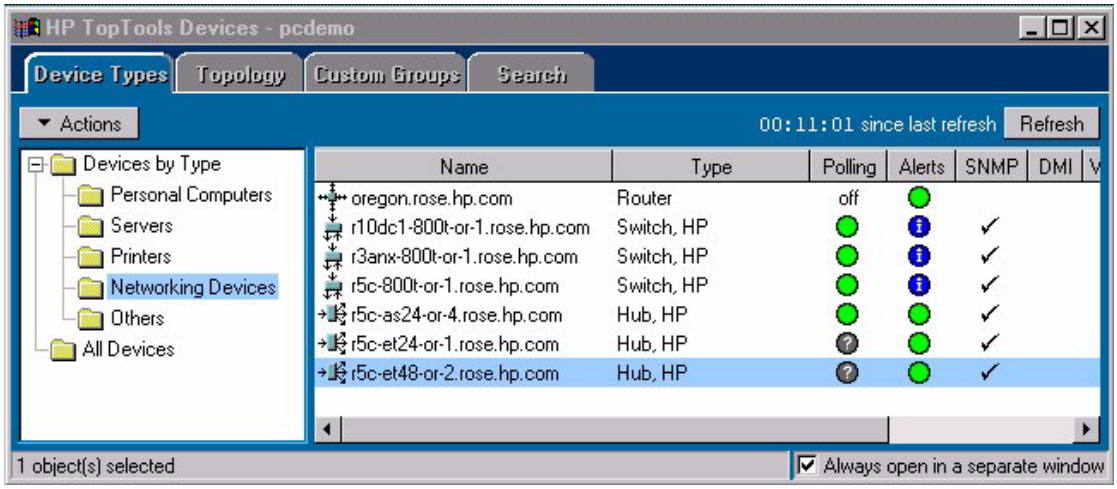


Figure 1-4. List of Networking Devices

Note

Double-clicking on a device in the Devices page that is not a hub or switch will display information about the device's identity and status.

Note

Double-clicking on an HP device that does not support a browser interface will launch the Closeup View of the device in a separate window if you are at the management station.

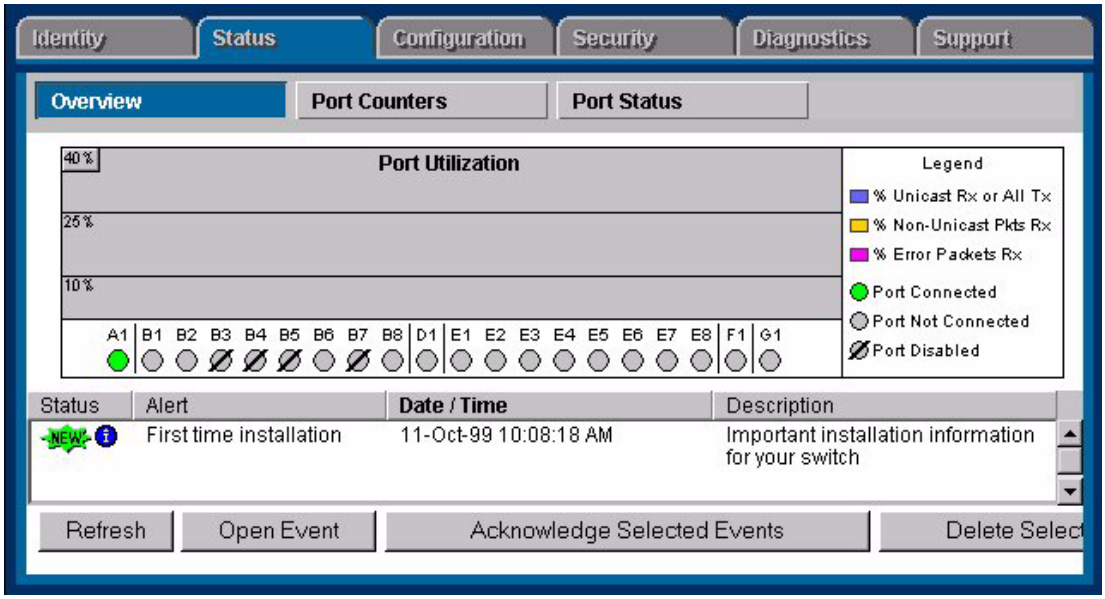


Figure 1-5. Device View - Status Page

The tabs in the Device View page provide access to various configuration features for the device. You can enable and disable individual ports (click on the port to select it), or click on the **Select All Ports** button to enable or disable all the ports of a device in one step.

See **Configuring Your Device** for more information about using the Device View. To obtain generic SNMP information about devices that cannot be managed with a browser, select **Properties** from the **Actions** menu at the top of the Devices page.

Use the online help to obtain more information about configuring devices that cannot be managed in a browser.

Viewing Network Traffic

To look at the traffic bottlenecks in your network in real time, click on the **Performance** button in the navigation frame and select **Traffic Monitor** from the menu.

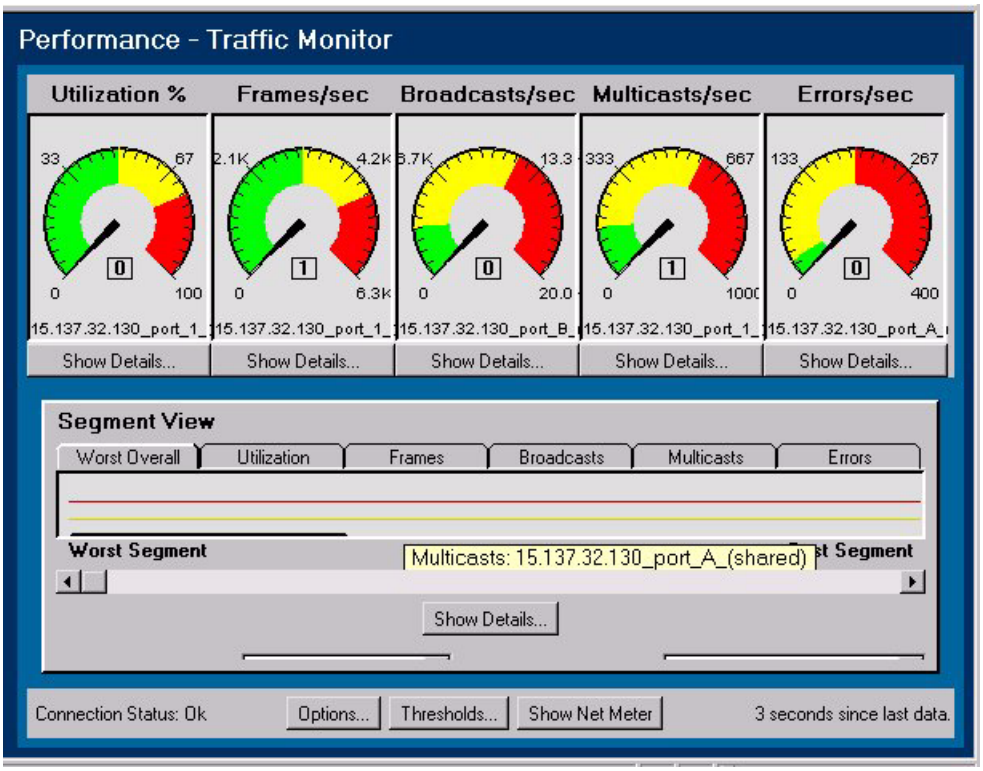
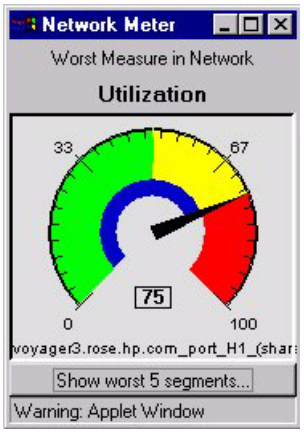


Figure 1-6. Traffic Monitor Page

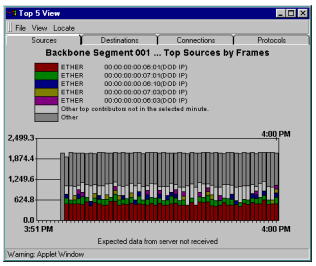
The performance gauges at the top of the page display measurements of five important attributes affecting the performance of your network for a selected segment. The histogram below the gauges displays the value of an attribute, such as broadcasts/sec, for the segments in a selected segment group.

Network Meter



Use the Network Meter to display an "at-a-glance" look at the most severe traffic problem on the network being monitored. Click on the **Show Net Meter** button at the bottom of the Traffic Monitor page to start the Network Meter. You can keep the Network Meter on your PC desktop to give you a continuous view of the status of your network traffic. Click on **Show Worst 5 Segments** at the bottom of the Network Meter to see the segments with the most traffic problems.

Top Talkers



You can quickly determine who the top talkers are in your network. Click on the **Show Details** button below the gauges on the Traffic Monitor page to display the Top5 browser window. The graph identifies the top five nodes causing the most network activity on the segments for the selected minute. The graph presents real-time information and is updated every minute.

See the chapter **Monitoring Network Traffic** for more information about the Traffic Monitor features.

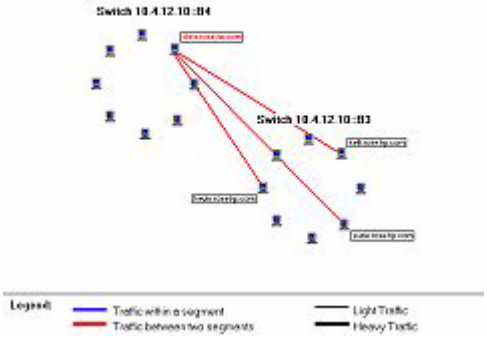
Optimizing Your Network

The HP Network Performance Advisor performs automatic traffic analysis and displays the results in easy-to-understand tables and charts. The reports make useful recommendations on how to improve network performance. The Advisor provides proactive analysis of a network, in contrast to the real-time, reactive analysis provided by Traffic Monitor.

To begin proactive analysis of your network, click on **Network Performance Advisor** in the HP TopTools for Hubs & Switches home page.

The Welcome page provides you with a brief description of the purpose of the two reports. Select the **How to Improve Performance** tab to begin creating a report.

To view a completed report, select the **Explore Report** tab. Select the report and click on the **View Report** button at the bottom of the page.



See the chapter **Planning for Network Growth** for more detailed information on planning reports.

How to Get Support

Product support is also available on the World Wide Web. The URL is:

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

Click on **Technical Support.** The information available at this site includes:

- HP network device MIBs
- HP network device firmware
- Software updates
- Frequently asked questions (FAQs)

In addition, you can call your HP Authorized Dealer or the nearest HP Sales and Support Office.

2

Introduction

Topics covered in this chapter include:

Introduction to HP TopTools

By using standards-based management with a browser interface, HP TopTools provides you with an easy way to manage all your network devices from one application. HP TopTools diagnoses problems quickly and automatically, then corrects the problem or gives clear directions on how to fix it.

HP TopTools runs alone or with popular management platforms such as HP NNM-NT (HP OpenView), CA Unicenter TNG, IBM Tivoli, and IBM NetView, providing an integrated solution that ranges from small workgroups through large enterprises.

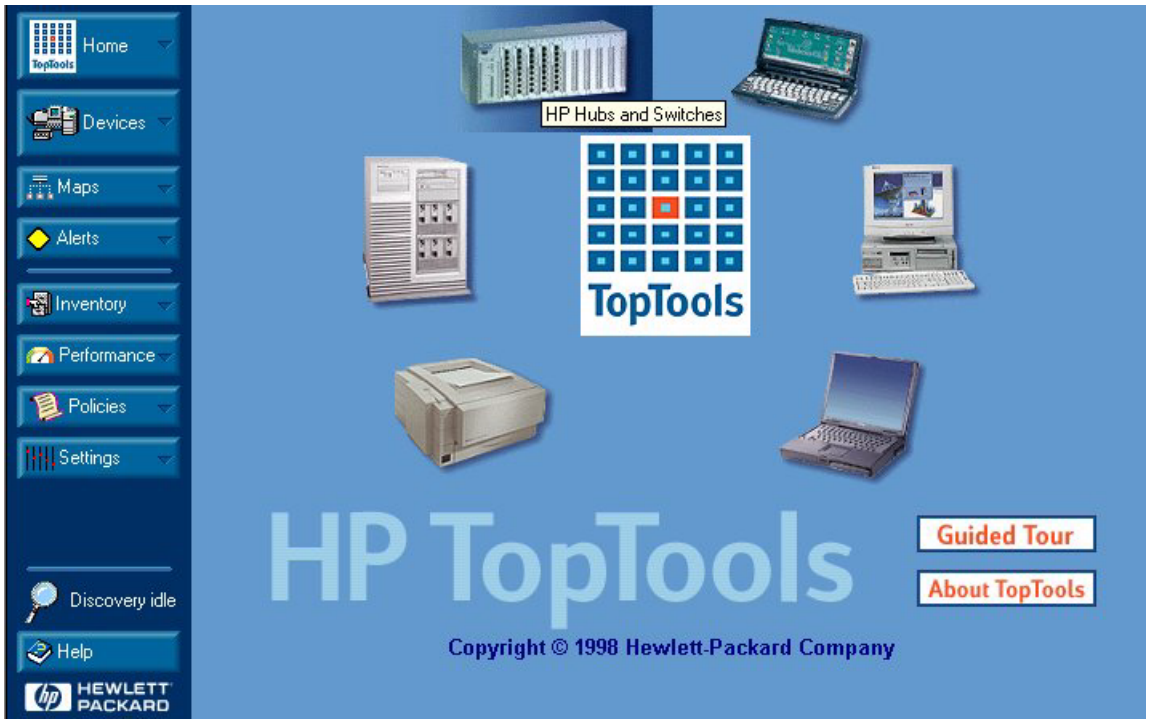


Figure 2-1. HP TopTools Home Page

HP TopTools for Hubs & Switches

HP TopTools for Hubs & Switches is a device management and network optimization application. You can access the HP TopTools features with a browser anywhere on the network. HP TopTools gives you the ability to monitor your network traffic on one workstation while using another workstation to configure devices, examine alert messages or run optimization reports.

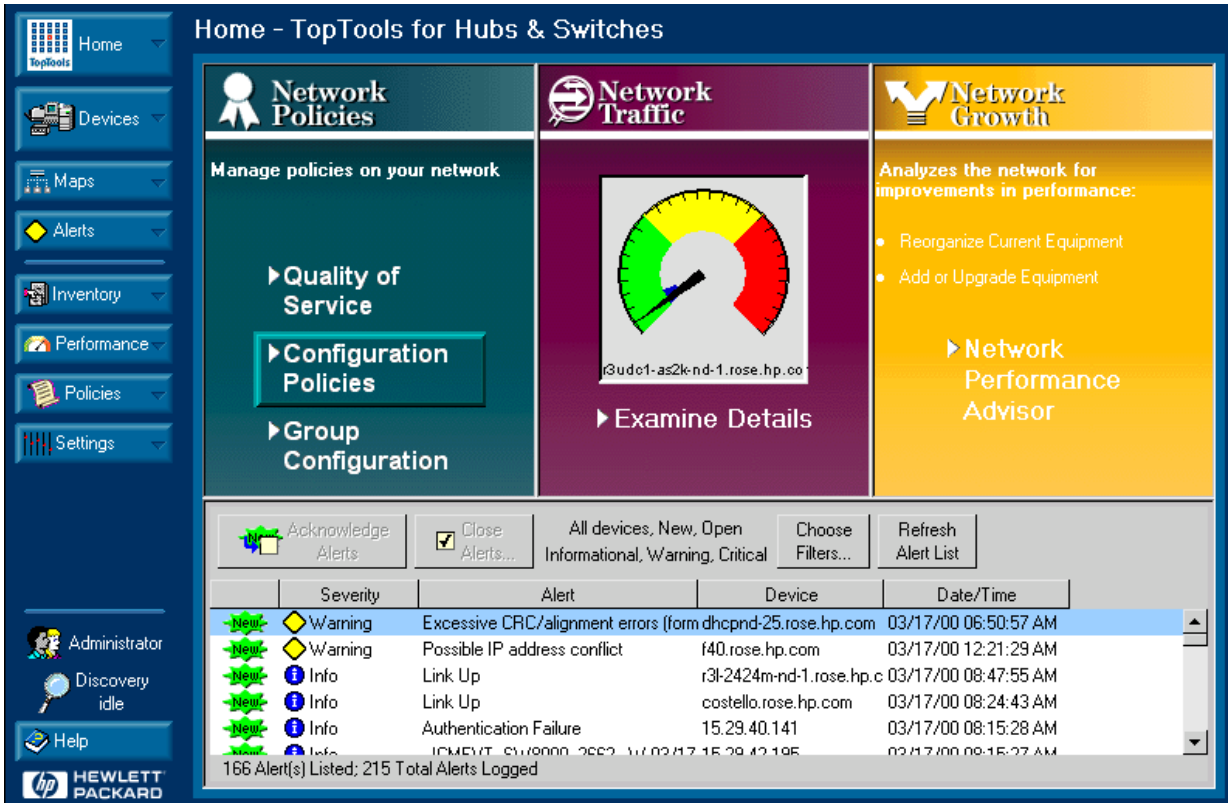


Figure 2-2. HP TopTools for Hubs & Switches Home Page

Browser-based management of devices combines network management with the simplicity of using a browser to view device performance and configuration information. You can easily access, configure and monitor your network with devices that support the browser interface. HP TopTools Group Configuration and diagnostic features provide quick solutions to network problems.

Note

Your devices must have an IP address in order to be managed by HP TopTools with a browser. The management station must have an assigned IP address.

This User Guide will help you get started with HP TopTools for Hubs & Switches. We assume that you have supervisory access to your network system and devices. Your system should be fully operational. You should know what an “IP” (Internet Protocol) or “IPX” (Internetwork Packet Exchange protocol) network is. You should already have the appropriate network software running and know how to use your network utilities.

For more information on other HP TopTools functions, see the online *HP TopTools Administrator’s Guide* or online help.

See **HP Devices Supported.**

Network Devices Features

Viewing a List of Devices

To view a list of your networking devices, click on **Devices, Device Types** and select **Networking Devices**. The Networking Devices folder contains the hubs, switches and routers discovered in your network. Double click on a device in the list to launch the Device View for configuring the device.

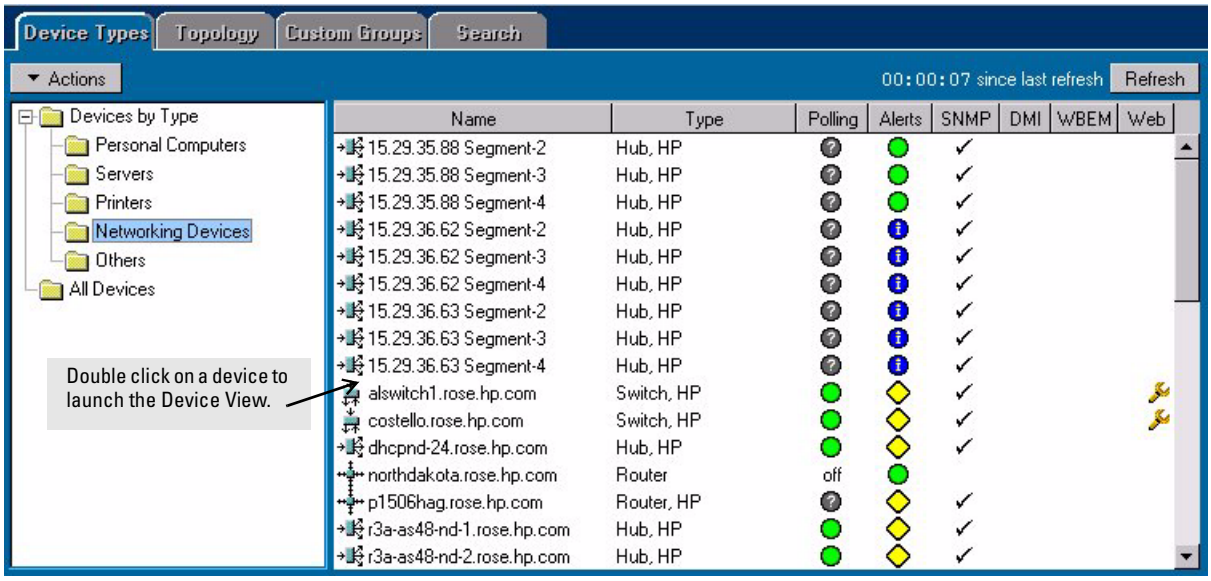


Figure 2-3. The Networking Devices List

See the chapter **Networking Devices** for more information on managing devices.

See the chapter **Accessing Hub Features** for information about configuring hubs.

See the chapter **Managing Switches** for information about configuring switches.

Maps

The Maps page displays a graphical representation of the devices in your network. You can launch the Device View for an HP device by double-clicking on a device in the map or right-mouse-clicking on a device and selecting **Properties (Device View)** from the popup menu.

See the chapter **Managing Your Maps** for more information on maps.

Group Policies

Use the Group Policies feature to establish settings for all of your devices at one time. For example, you can set up **Automatic Broadcast Control** for your switches.

See the chapter **Group Policies** for more information on these features.

Network Traffic

The **Traffic Monitor** presents real-time information about the status of your network. You can set thresholds for five important measures, which when exceeded trigger an event that appears in the Alert Log. Use the Top5 View to determine who the Top Talkers are in a segment.

Network Growth

The **HP Network Performance Advisor** is an intuitive, intelligent interpretation tool that provides you with information about the entire network. The Advisor performs automatic traffic analysis and displays the results in easy-to-understand tables and charts. The reports created by the Advisor make useful recommendations on how to improve network performance. The Advisor also provides inventory information for each segment in the network. The analysis and data provided by the Advisor assist the system administrator in making a sound business case for changes to the network.

The Network Performance Advisor creates reports that make recommendations about reducing utilization on the network segments to increase network performance. It provides proactive analysis of a network, in contrast to the real-time, reactive analysis provided by Traffic Monitor.

HP Devices Supported

HP TopTools for Hubs & Switches provides Device Views (manageable by browser) or Closeup Views to fully manage the following HP devices. The devices that can be managed with a browser are indicated.

Table 2-1. HP Hubs and Bridges Supported

Product Number	Description	Browser-manageable
28673A	HP 10:10 LAN Bridge	No
28674A	HP Remote Ethernet Bridge	No

Product Number	Description	Browser-manageable
28674B	HP Remote Bridge RB	No
28682A	HP Fiber-Optic Hub Plus	No
28688A/B	HP EtherTwist Hub Plus	No
28692A	HP ThinLAN Hub Plus	No
28699A	HP EtherTwist Hub Plus/48	No
J2355S	HP EtherTwist Hub Plus/24 S	No
J2410A Note 1	HP AdvanceStack 100VG Hub-15	No
J2413A Note 2	HP AdvanceStack 100VG Hub-7M	No
J2415A Note2	HP AdvanceStack 100VG Hub-14	No
J2600A Note 3	HP AdvanceStack 10Base-T Hub-12	No
J2601A/B Note 3	HP AdvanceStack 10Base-T Hub-24	No
J2602A/B Note 3	HP AdvanceStack 10Base-T Hub-48	No
J2610A/B Note 4	HP AdvanceStack 10Base-T Hub-8U	No
J2611A/B Note 4	HP AdvanceStack 10Base-T Hub-16U	No
J2630A Note 3	HP AdvanceStack 10Base-T Hub-12 w/ SNMP	No
J2631A/B Note 3	HP AdvanceStack 10Base-T Hub-24 w/ SNMP	No
J2632A/B Note 3	HP AdvanceStack 10Base-T Hub-48 w/ SNMP	No
J3200A Note 5	HP AdvanceStack 10BT S Hub-12R	Yes (firmware A.03.xx)
J3201A Note 5	HP AdvanceStack 10BT S Hub-12R w/ Mgmt	Yes (firmware A.03.xx)
J3202A Note 5	HP AdvanceStack 10Base-T S Hub-24R	Yes (firmware A.03.xx)
J3203A Note 5	HP AdvanceStack 10BT S Hub-24R w/ Mgmt	Yes (firmware A.03.xx)

Product Number	Description	Browser-manageable
J3204A Note 5	HP AdvanceStack 10Base-T S Hub-24T	Yes (firmware A.03.xx)
J3205A Note 5	HP AdvanceStack 10Base-T S Hub-24T w/Mgmt	Yes (firmware A.03.xx)
J3288A Note 6	HP ProCurve 10/100 Hub 12M	Yes
J3289A Note 6	HP ProCurve 10/100 Hub 24M	Yes
J3301A Note 6	HP ProCurve 10Base-T Hub 12M	Yes
J3303A Note6	HP ProCurve 10Base-T Hub 24M	Yes

Note 1 Requires J2414A or J2414B HP AdvanceStack 100VG SNMP/Bridge Module.

Note 2 Requires J2414B HP AdvanceStack 100VG SNMP/Bridge Module.

Note 3 Requires J2603A/B HP AdvanceStack 10Base-T SNMP Module. HP AdvanceStack 10Base-T hubs provided with SNMP module preinstalled include: HP J2630A (12-port), HP J2631A/B (24-port), HP J2632A/B (48-port).

Note 4 Requires J2612A/B HP AdvanceStack 10Base-T DMM Module for J2610A and J2611A.
Requires J3133A HP AdvanceStack 8U/16U SNMP Module for J2610B and J2611B.

Note 5 Requires J3210A HP AdvanceStack 10BT Management Pack. HP AdvanceStack 10Base-T Switching hubs provided with Management. Pack preinstalled include: HP J3201A (12R), HP J3203A (24R), HP J3204A (24T).

Note 6 No IPX Network Management Support.

Table 2-2. HP Switches Supported

Product Number	Description	Browser-manageable
J2980A Note 1	HP AdvanceStack 10/100 LAN Switch	No
J3100A/B	HP AdvanceStack Switch 2000	Yes (J3100B w/ firmware B.04.xx)
J3125A Note 2	HP AdvanceStack Switch 200	No
J3126A Note 2	HP AdvanceStack Switch 100	No
J3175A Note 3	HP AdvanceStack Switch 208T	No

Product Number	Description	Browser-manageable
J3177A Note 3	HP AdvanceStack Switch 224T	No
J3245A	HP AdvanceStack Switch 800T	Yes (Firmware B.04.xx)
J3298A Note 2	HP ProCurve Switch 212M	Yes
J3299A Note 2	HP ProCurve Switch 224M	Yes
J4093A Note 2	HP ProCurve Switch 2424M	Yes
J4120A	HP ProCurve Switch 1600M	Yes
J4110a Note 2	HP ProCurve Switch 8000M	Yes
J4121A Note 2	HP ProCurve Switch 4000M	Yes
J4122A Note 2	HP ProCurve Switch 2400M	Yes
J4138A Note 2	HP ProCurve Routing Switch 9308M	Yes
J4139A Note 2	HP ProCurve Routing Switch 9304M	Yes
J4840A	HP ProCurve Routing Switch 6308M-SX	Yes
J4841A	HP ProCurve Routing Switch 6208M-SX	Yes
J4812A	HP ProCurve Switch 2512M	Yes
J4813A	HP ProCurve Switch 2524M	Yes

Note 1 HP J2980A 10/100 LAN Switch is not supported on IPX networks. To discover this device on an IP network, the SNMP community name "public" must be configured on the device.
The J2981A HP 100VG Switch Module and J2984A HP 100TX Switch Module are available for the HP J2980A.

Note 2 No IPX Network Management Support.

Note 3 Requires J3178A HP AdvanceStack Switch 208/224 Management Module.

Learning to Use HP TopTools

The following information is available for learning HP TopTools for Hubs & Switches:

- This User Guide—helps you become familiar with the application.

- Online help information—provides information through Help buttons in dialog boxes, and through a table of contents with hypertext links to procedures and reference information.

HP TopTools Technical Product Support

Product support is also available on the World Wide Web. The URL is:

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

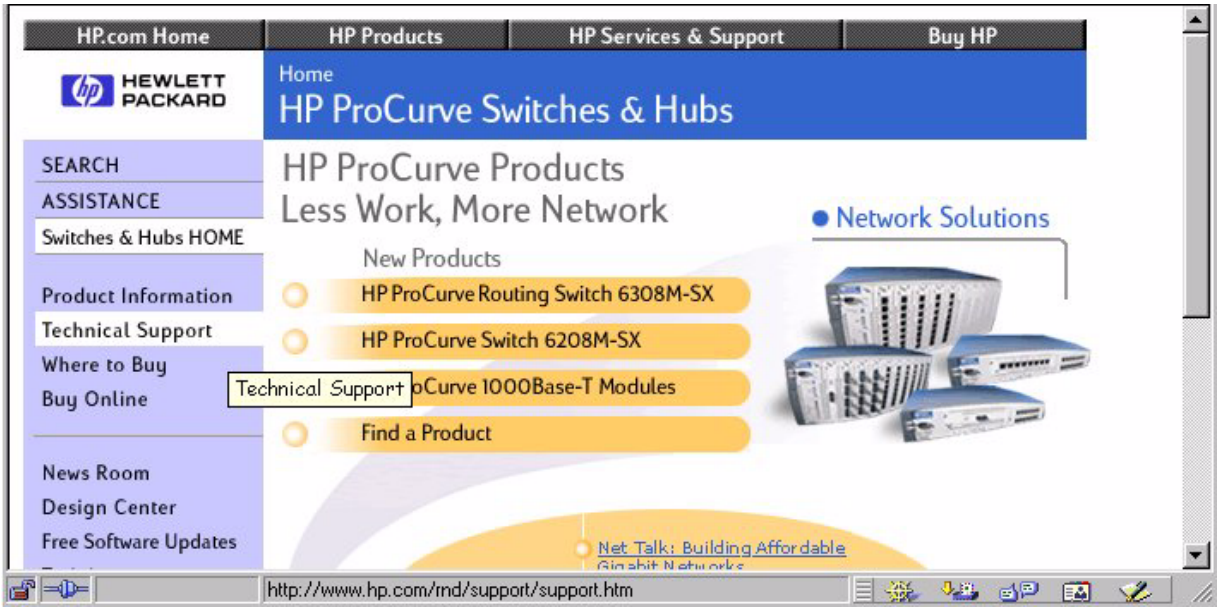


Figure 2-4. HP ProCurve Switches & Hubs Home Page

Click on **Technical Support**. The information available at this site includes:

- HP network device MIBs
- HP network device firmware
- Software updates
- Frequently asked questions (FAQs)

In addition, you can call your HP Authorized Dealer or the nearest HP Sales and Support Office.

3

System Requirements

Hardware and Software Requirements

HP TopTools for Hubs & Switches runs on Windows NT and Windows 2000. The system requirements are listed in the following table.

Table 3-1. System Requirements

	Item	Requirements
	Computer System	IBM PC-compatible computer, 266 MHz processor; 400 MHz recommended
	Minimum RAM	128 Mbytes; 192 Mbytes recommended
	Free Disk Space	175 Mbytes Note: At least 400 MB is needed to install all the required Microsoft components on a computer that has only the Windows NT operating system installed.
	Paging File Size	150 MB
	Disk Drive	CD-ROM drive
Hardware	Video Monitor and Interface Card	Super VGA (16-bit color display) video monitor and interface card
	LAN Adapter	Any LAN adapter card supported by the system
	Other	A mouse or other pointing device that is supported by the system
Note: Dual-homed or multi-homed PCs are not supported. DHCP clients are supported. **The IP address of the management station cannot be static or dynamic DHCP.**		
Software	Supported Management Platforms	TopTools HP OpenView Network Node Manager
	Browsers	Microsoft Internet Explorer (MSIE) 5.0 with Task Scheduler, supplied on the TopTools CD-ROM
	Operating System	Microsoft Windows NT version 4.0 with Service Pack 6a (workstation or server)
	Web Server	Windows NT 4.0 Options Pack from Microsoft

Note

Be sure to obtain an assigned IP address for the management station before installing TopTools. Do not use either a static or dynamic IP address.

4

Discovering Your Devices

This chapter contains information about:

Beginning Discovery

Discovery is the process of identifying the devices in your network and determining how these devices are connected. The discovered devices are displayed in the Devices page and added to a devices database maintained by HP TopTools to represent your network. HP TopTools for Hubs & Switches can discover network devices that have valid IP or IPX addresses. Such devices include:

- HP's manageable hubs, bridges and switches that have valid IP or IPX addresses.
- Third-party (“multivendor”) devices that have valid IP or IPX addresses and support SNMP (for example, hubs and bridges from other vendors). These nodes may not be mapped or managed with HP TopTools.
- Devices that have IP or IPX addresses, even if they do not support SNMP. (For example, IPX workstations and fileservers).
- Other devices, including HP JetDirect printers and plotters (IP or IPX).

Note

Discovery is a resource-intensive process and may take some time.

To begin discovering the devices in your network, click on the **Settings** button in the navigation frame and select **Discovery** from the menu. The Settings - Discovery page displays.

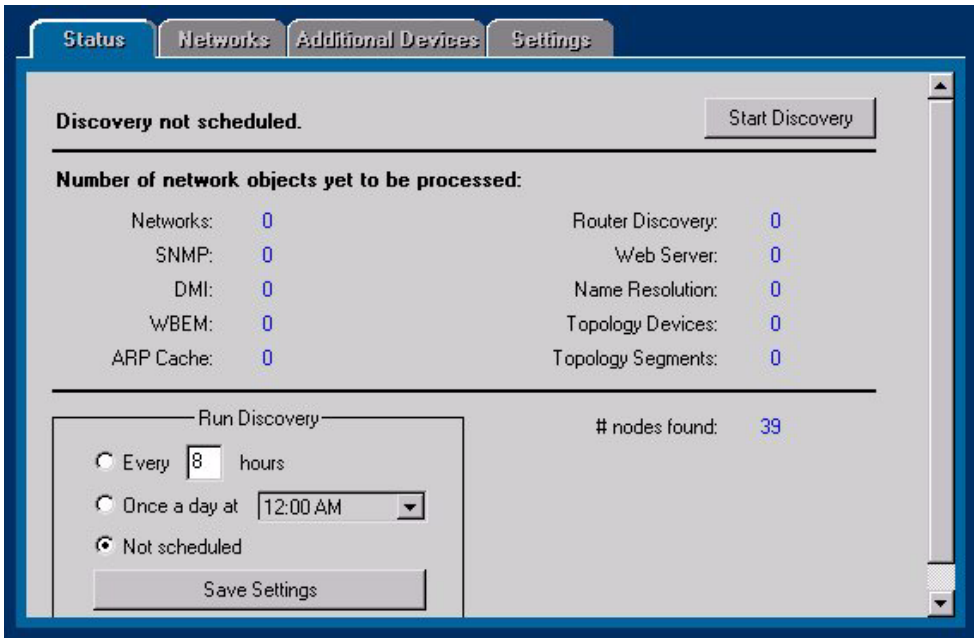


Figure 4-1. Status Page of Settings for Discovery

Discovery Status

The Status page shows the following information about network discovery:

- The date and time the last discovery finished
- The number of network objects that have not been processed yet
- If discovery is scheduled, how often it is set to run, and when

You can manually start discovery by clicking on the **Start Discovery** button at the top of the page.

Save your settings by clicking on the **Save Settings** button.

Selecting Networks

Click on the **Networks** tab to select the networks whose component devices you want to add to the device database. You can specify a range of subnets, for example, 10.4.8.0 - 10.4.15.0. You can also specify a particular network and subnet mask. The subnet mask is used to determine the range of addresses in your network.

To select a network, double click on it in the list of **Known Networks**. The box to the right will be checked and the network added to the list of networks to search.

To remove a network, double click on the network in the **Known Networks** list.

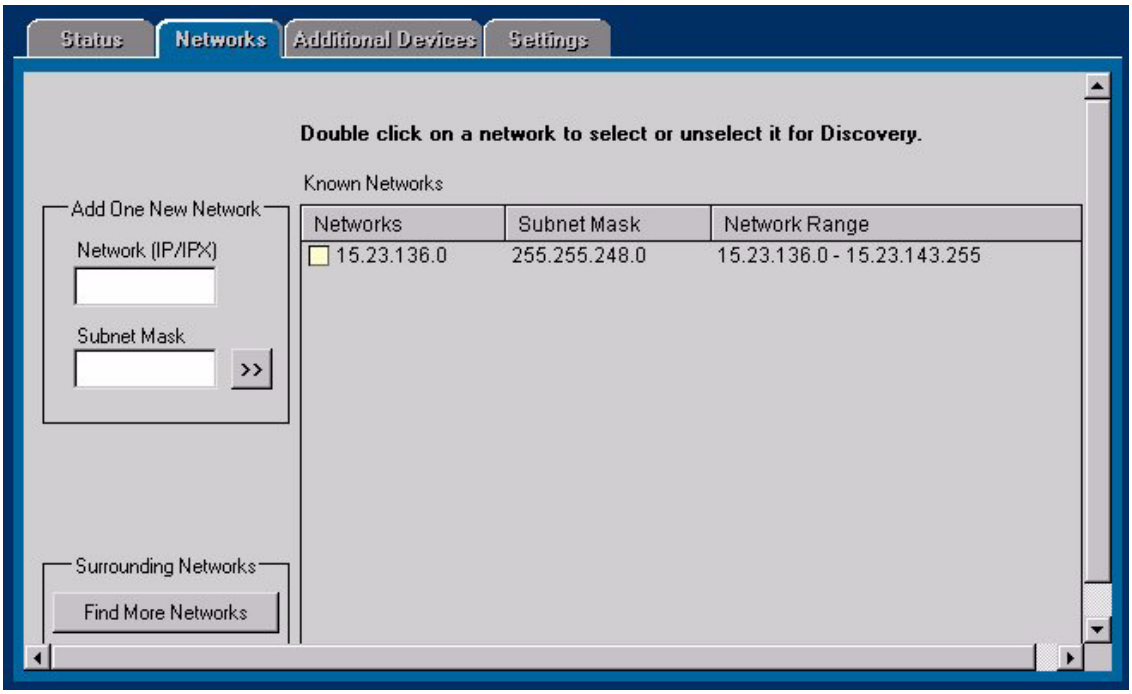


Figure 4-2. Networks Page of Settings for Discovery

To add a new network to be discovered that does not appear in the Known Networks list, enter the IP or IPX address of the network and its subnet mask in the **Add One New Network** area on the left side of the page. The IP subnet mask should be the same as the mask you specified when you configured your TCP/IP protocol stack. HP TopTools uses the subnet mask to calculate the address range for your network. Click on **>>** to include it in the Networks list.

Click on the **Find More Networks** button to discover other networks for which you do not have the address. The Discovery process needs to know the READ password for the routers connecting your network to other networks. If the router is not marked with an asterisk indicating that the password is known to HP TopTools, double-click on the network and enter its password.

When the list of networks is complete, select the Status tab and click on **Start Discovery**.

Adding Devices for Discovery

To add a specific device to a network for discovery, click on the **Additional Devices** tab in the Settings - Discovery page. Enter the IP or IPX address and the Community name of the device. The Community name will default to “public”. Click on **Add Device**.

Configuring Discovery Settings

You can configure the types of protocols and methods of discovery that you want to use. For example, you may want to discover only IP networks. The types are:

- IP—Discovers all IP devices in your network.
  - Ping Discovery—Ping packets are sent to discover every device on the subnet.
  - Web Server Discovery—All IP addresses are checked to discover if the device contains a Web Server. Management Stations are also discovered.
  - WMI (WBEM) Discovery—Checks for PCs that support WMI.
- IPX—Locates all IPX devices in your network.
- Segment and Hub Topology—Discovers how the segments are connected in the network.

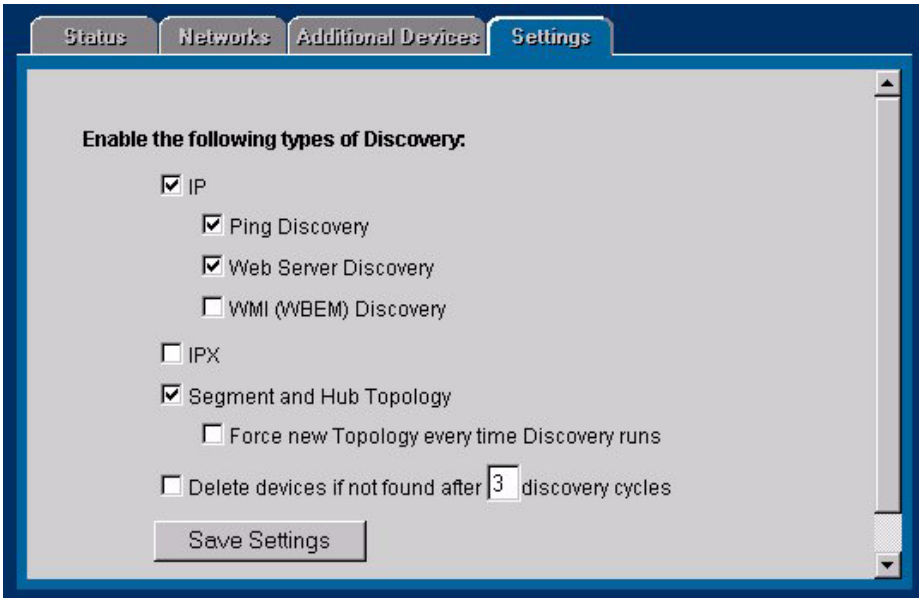


Figure 4-3. Settings Page of Settings - Discovery

Select the **Settings** tab in the Settings - Discovery page and check the appropriate boxes. Click on **Save Settings** to save your discovery settings.

Troubleshooting Discovery

If you do not see certain devices in the Networking Devices list after discovery, click on the **Others** folder (**Devices - Device Types**) to see if the devices are listed there. If so, perform these steps to have them discovered:

1. Right mouse click on the device or devices with type “unknown” in the list of devices contained in the Others folder.
2. Select **Security -> Set SNMP Passwords (Communities)** from the menu.
3. Enter a READ password (twice) for the device.
4. Enter a WRITE password (twice) for the device.
5. In the navigation frame, click on the **Actions** button and select **Update Discovery**.

You must do the Update Discovery so that HP TopTools for Hubs & Switches will re-read the configuration of the device for which you added the passwords. The device should now appear in the Networking Devices list and the topology map.

Inventory of Devices

HP TopTools creates several inventory reports listing basic information about your devices. Inventory listings for the devices on your local network are the default. To view the Inventory list, select the **Inventory** button in the navigation frame. To add more devices, select the **Additional Devices** tab in the Settings - Discovery page. You can print or email these reports.

See the HP TopTools online help for more detailed information.

5

Alerts

This chapter contains information on:

- **Interpreting the Alert Log**
- **Filtering Alerts**
- **Configuring Actions on Alerts**

Interpreting the Alert Log - Automatic Fault Finding

The Alert Log is displayed in the lower area of the HP TopTools for Hubs & Switches home page, the Alerts page, and the lower area of the device's Status - Overview page. Its "Find/Fix/ Inform" capability helps you proactively manage your network by displaying network traps and problem conditions in one easily accessible browser page. It displays messages about events that have occurred on the device, such as loss of link, a problem cable, or a broadcast storm. When a new alert occurs, an icon indicating its severity appears on the Alerts button. The alert is also added to the device description in the Devices page. You can access the Alert Log by selecting **View Alerts** from the **Alerts** button menu the navigation frame or by clicking on the alert.

To ensure that you are seeing the latest alerts, click on the **Refresh Alert List** button.

Closing an alert indicates that it is no longer a problem. Closed alerts are stored in the alerts database for a time period specified in the Configure Actions on Alerts page.

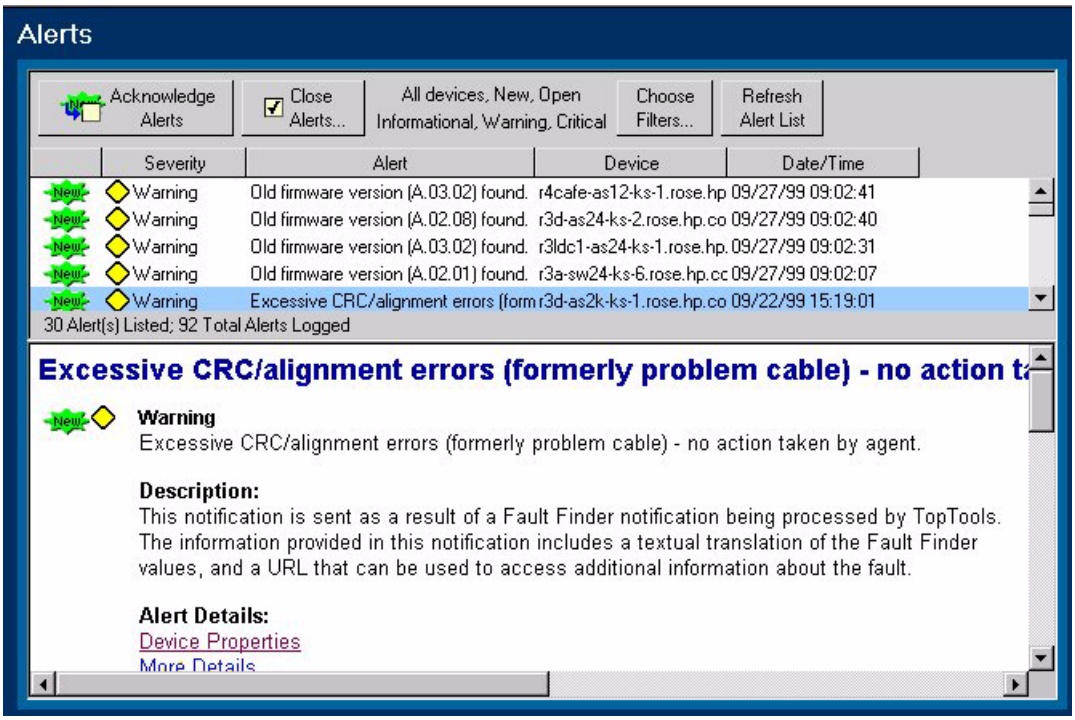


Figure 5-1. Alerts Page

The Alerts page displays more information about the alert as well as some suggestions for fixing the problem. When you have reviewed an alert, the "New" icon is no longer displayed.

The following table shows the common faults and how they are indicated.

Table 5-1. Common Faults

Fault	Description, Cause and Actions
Too many undersized/giant packets	Description: A device on this port is transmitting packets shorter than 64 bytes or longer than 1518 bytes (longer than 1522 bytes if tagged), with valid CRCs. Possible Causes: a misconfigured NIC or a malfunctioning NIC, NIC driver, or transceiver Actions: 1. Check the NIC for a misconfiguration. 2. Update the NIC driver software. 3. Replace the malfunctioning NIC or transceiver. 4. Check for a short-circuit in the cable patch connected to this port.
Excessive jabbering	Description: A device on this port is continually transmitting packets (jabbering). This is detected as oversize packets with CRC errors. Possible causes: A misconfigured NIC, or a malfunctioning NIC or transceiver. It could also be caused by a short-circuit in the network cable path. Actions: 1. Check NIC for a misconfiguration. 2. Update the NIC driver software. 3. Replace the NIC or transceiver. 4. Check for a short-circuit in the cable path connected to this port.
Excessive CRC/ alignment errors	Description: A high percentage of data errors was detected on this port. Possible Causes: • Faulty cabling or topology • Half/full duplex mismatch • Misconfigured NIC • Malfunctioning NIC, NIC driver or transceiver Actions: 1. If the port is 100Base-T, make sure the cable, connectors, punch-down blocks, and patch panels connecting to the port are Category 5 or better. Verify the installation with a Category 5 test device. 2. Check the directly-connected device for mismatches in half/full duplex operation (half duplex on the switch and full duplex on the connected device, or the reverse). 3. Update the NIC driver software. 4. Verify that the network topology conforms to IEEE 802.3 standards. 5. Replace or relocate the cable. 6. Check the wiring closet components, transceivers, and NICs for proper operation.

Table 5-1. Common Faults

Fault	Description, Cause and Actions
Excessive late collisions	Description: Late collisions (collisions detected after transmitting approximately 64 bytes) were detected on this port. Possible Causes: • An overextended LAN topology • Half/full duplex mismatch • Misconfigured or faulty device connected to the port Actions: 1. Verify that the network topology conforms to IEEE 802.3 standards. Insert bridges or switches, if needed, to extend the network topology. 2. Check the directly-connected device for mismatches if half/full duplex operation (half duplex on the switch and full duplex on the connected device). 3. If this port is 100Base-T, make sure the cable connecting to the port is Category 5 or better. 4. Check for faulty cabling, transceivers, and NICs.
High collision or drop rate	Description: A large number of collisions or packet drops have occurred on the port. Possible Causes: • an extremely high level of traffic on this port • Half/full duplex mismatch • A misconfigured or malfunctioning NIC or transceiver on a device connected to the port • A topology loop in the network Actions: 1. Use a network monitoring device or application to determine the traffic levels on the affected segment. If needed, consider subdividing that segment with switches or bridges, or moving high-traffic devices to their own switch ports. 2. Check the directly-connected device for mismatches in half/full duplex operation (half duplex on the switch and full duplex on the connected device). 3. Check for a misconfigured NIC or transceiver (for example, a transceiver configured for “loopback test” or “SQE test”). 4. Verify that there are no topology loops in your network. If not enabled, you may also enable spanning tree. See the Switch Configuration menu.
Excessive broadcasts	Description: An excessively high rate of broadcast packets were received on the port. This degrades the performance of all devices connected to this switch. Possible Causes: This is usually caused by a network topology loop, but can also be due to a malfunctioning device, NIC, NIC driver, or software application. Actions: 1. Verify that there are no topology loops in your network. 2. Find and correct any malfunctioning devices or NICs on the segment. 3. Find and correct any malfunctioning applications on devices on the segment.

The Find/Fix/Inform function runs continuously in the background at a sensitivity threshold level that you select. Sensitivity threshold settings control the severity of the alerts that are displayed. The settings internally adjust the counter thresholds automatically.

Sensitivity settings are selected in the Configuration page for the device. Select the **Fault Detection** button. For hubs, you can set the sensitivity for logging network problems and disabling ports. Switches only have a sensitivity setting for logging network problems. Switches are more capable than hubs of isolating problems occurring on a single port.

The sensitivity settings are:

- **High Sensitivity**: The device will act when a network problem of any severity occurs. Network problems are automatically detected and entered into the Alert Log (located under the Status Tab).
- **Medium Sensitivity**: The device will act when serious network problems occur.
- **Low Sensitivity**: the device will act only when severe network problems occur. These are problems that may bring the network down.
- **Never**: The device will never take any actions regardless of the severity of the problem.

Only serious and persistent problems that impact other users on the network will cause a hub to disable a port. These problems include:

- A problem XCVR or NIC
- A broadcast storm
- Excessive Auto Partitions
- A network loop

A warning is entered in the Alert Log shortly before the port is disabled. Another entry is made indicating that the port has been disabled.

Launching the Device View

Click on the hyperlink “Device Properties” to display a page with Identity and Status information about the device.

Acknowledging Alerts

Click on the **Acknowledge Alerts** button to indicate that you have seen the alert. Acknowledging an alert changes its state from *new* to *open*.

Closing Alerts

To close an alert and remove it from the Alert Log, select the alert and click on the **Close Alerts** button. You can set a filter to display closed alerts in the Alerts page.

Sorting Alerts

There are four column title buttons that can be used to sort the alerts:

- According to severity
- A description of the alert,
- The name of the device
- The date and time of the alert

First Time Installation Information

There will be an entry in the Alert Log for first time installation information for the device.

Filtering Alerts

Selecting Alert Log Filters

You can choose to display only certain types of alerts in the Alerts page by setting alert filters. Click on the **Choose Filters** button in the Alert Log area to display the **Select Alert Log Filters** page.

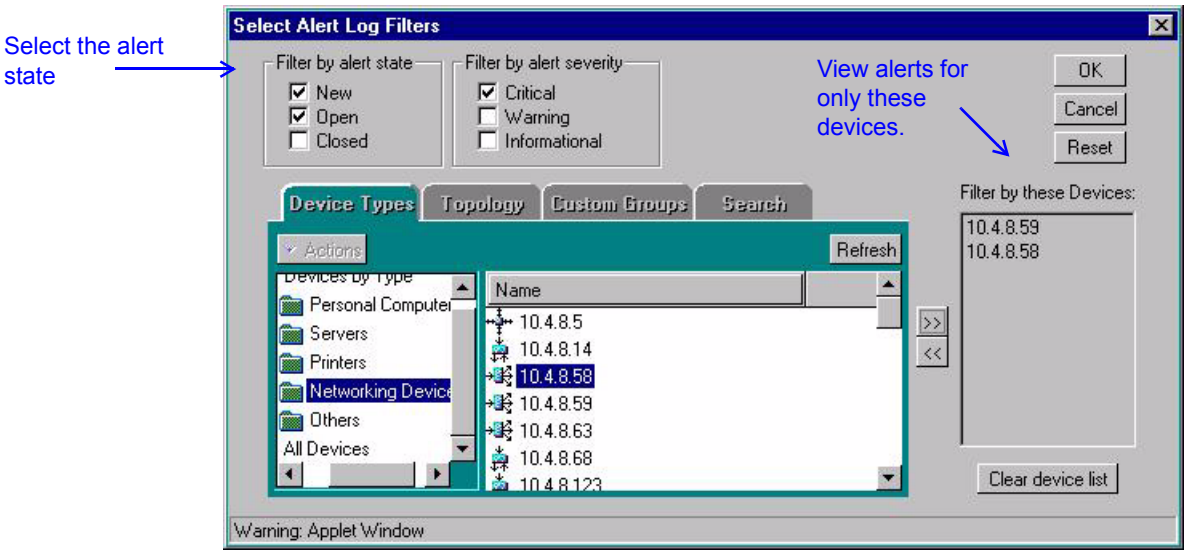


Figure 5-2. Select Alert Log Filters Page

Filtering by Alert State

To view only certain alert states in the Alerts page, for instance, only new and open alerts, check the appropriate boxes in the Filter by Alert State area of the browser window.

Filtering by Alert Severity

Select an alert severity, for instance, critical, to view only the critical alerts in the Alerts page.

Filtering by Device

Select one or more devices from the list and click on the **>>** button to add them to the **Filter by these Devices** box. Only the alerts for these devices are displayed in the Alerts page. If you have also selected an alert state and severity, for example, *New* alerts that are *Critical*, only those alerts are shown for the selected devices.

To remove a device, select the device in the list and click on the **<<** button. To clear all the devices from the box, click on the **Clear device list** button below the box.

Selecting Alert Log Filters - Topology

You can set filters for an entire segment or network. Select the **Topology** tab, then select the segment or network to filter. Click on the **>>** button to add the segment or network to the **Filter by these Devices** box.

Use the **Show** field at the top of the page to control the display of the folders. See **Device Topology** in the Networking Devices chapter for more information about the Show field.

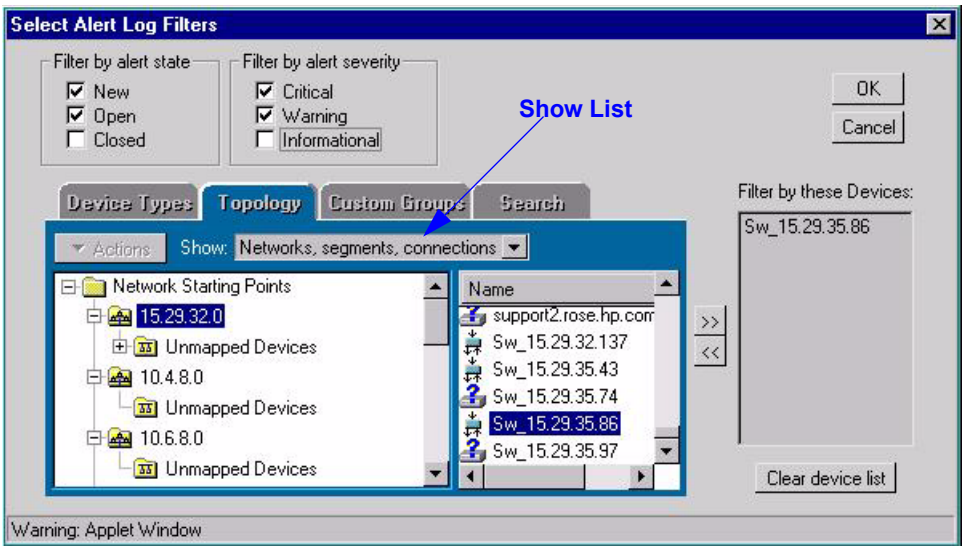


Figure 5-3. Select Alert Log Filters — Topology Page

Selecting Alert Log Filters - Custom Groups

If you have created any Custom Groups of devices, you can apply filter criteria to these groups.

Selecting Alert Log Filters - Search

You can obtain a list of all of your devices with certain characteristics by using the Search feature. To find one or more devices, select the parameters, such as “Ping Status is Critical” or “Device Type is PC”, or any other combination that is available in the drop down lists. Click on the **Start Search** button.

Click on the **+** or **-** boxes to add or remove search criteria.

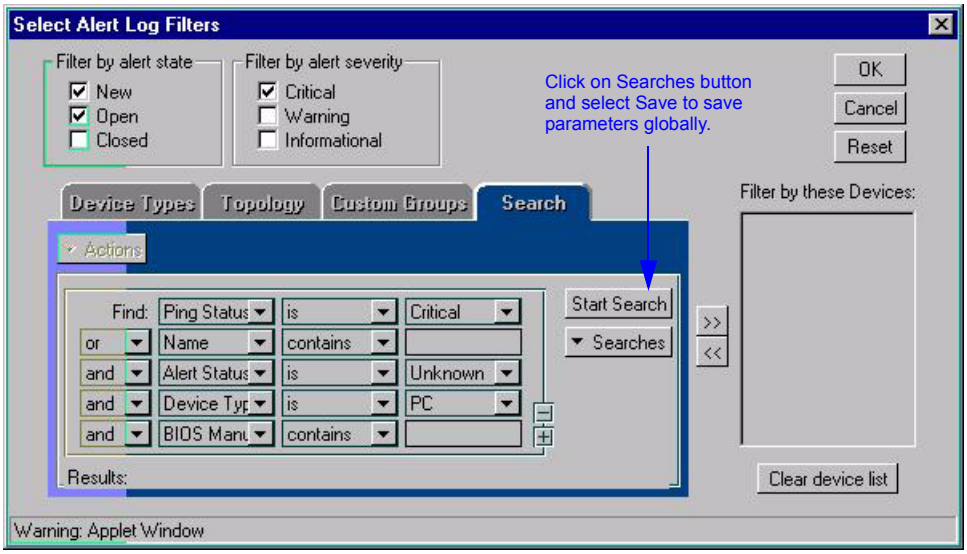


Figure 5-4. Search Page

To save your search parameters, select **Save** from the Searches drop down list and enter a name for the search. These parameters are saved globally so that you can use the same parameters again by clicking on the **Searches** button and selecting the name you saved.

If you want to rename or delete your saved search parameters, click on the **Searches** button and select **Manage**. Highlight the name that you want to rename or delete and click the appropriate button.

Configuring Action on Alerts

You may want to have certain actions executed when an event occurs, such as executing a program. Click on the **Alerts** button in the navigation frame and select **Configure Action on Alerts** from the menu.

Use the Alerts - Configure Actions on the Alerts page to enter the path of the desired program for each alert severity. You can launch several programs by using a batch file in this field.

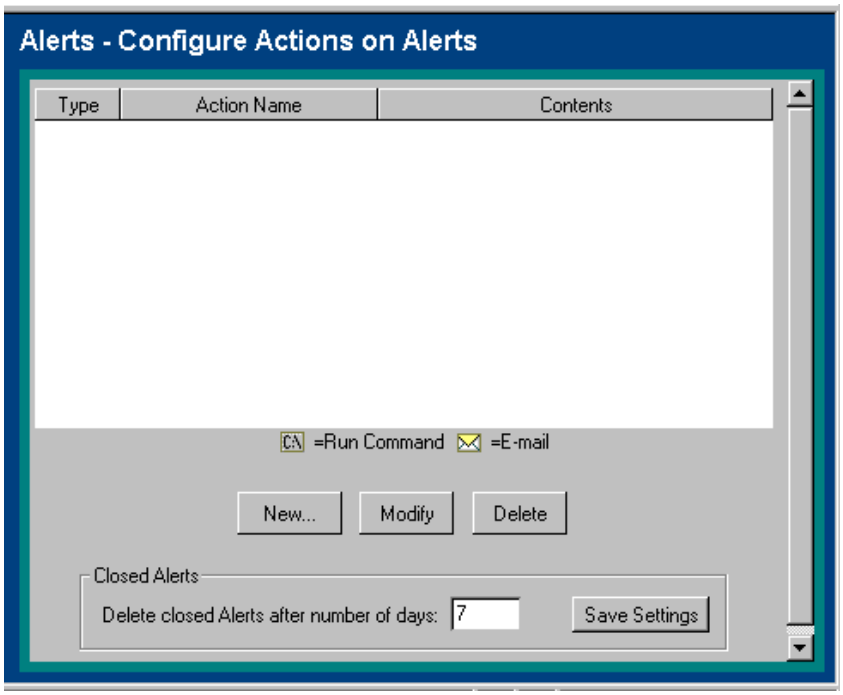


Figure 5-5. Configure Actions on Alerts Page

If your program requires information about the event (for example, device name and alert severity for inclusion in an e-mail message to you), use one of the following substitution parameters within the command line:

- $(dev) - Substitute the name or IP/IPX address of the device that generated the event. The name is usually the domain name.
- $(addr) - Address (IP or IPX) of the device that generated the event.
- $(desc) - Short description text generated for the event that describes the event.
- $(xdesc) - Long description text generated for the event that describes the event.
- $(stat) - Severity of the event as one of the following strings: “Informational”, “Warning”, or “Critical”.
- $(evtid) - Identifier string for the event, for example, the trap OID of an SNMP trap.
- $(name) - Name of the event. Event names are assigned to each type of event as a way to uniquely identify events instead of using event identifiers.
- $(url) - URL generate for the event.

Click on **Save Settings**. The program(s) run whenever an alert of the specified severity is logged to the Alerts page.

Deleting Closed Alerts

The field at the bottom of the Configure Actions on Alerts page allows you to enter the number of days after which you would like closed alerts deleted from the alerts database.

6

Networking Devices

This chapter contains information on:

- **Listing Devices**
- **Configuring Polling**
- **Selecting Actions for Devices**
- **Device Topology**
- **Node Port Table**
- **Custom Groups**
- **Searching for Devices**

See the chapter **Group Policies** for information on automatic configuration.

Listing Devices

The Devices page lists alphabetically all the devices that have been discovered in your network. The default display is your local network.

To view a list of your network devices, select **Devices, Device Types** in the navigation frame. Click on the Networking Devices folder to display each network device in the right frame showing its type, connectivity status, the number of new and open alerts, and its management capabilities (SNMP and/or Web browser).

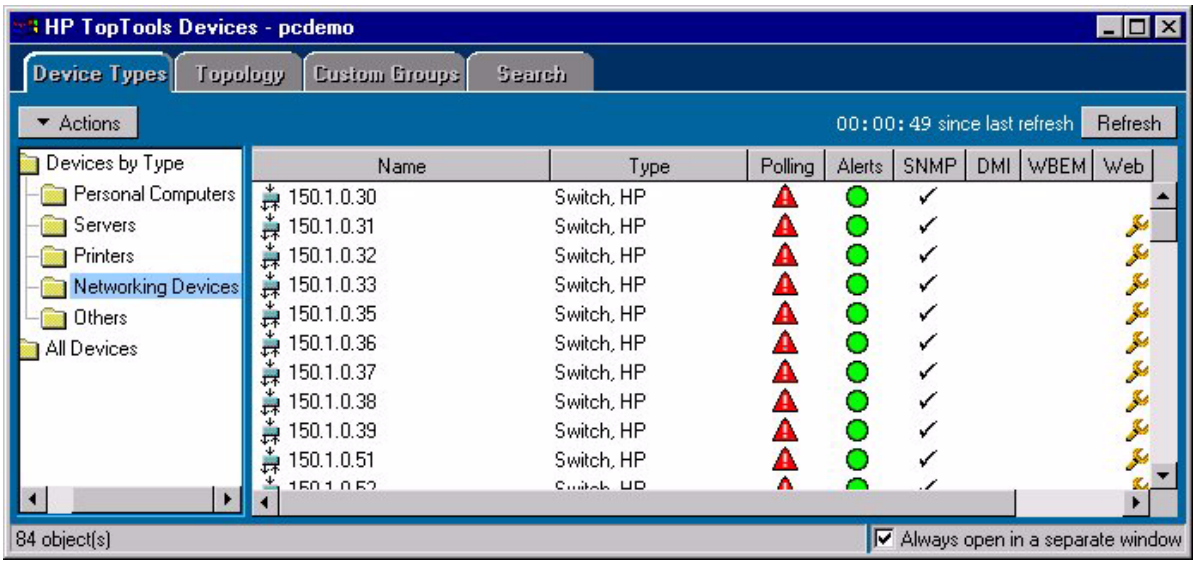


Figure 6-1. List of Networking Devices

Check the box at the bottom right to have the page always open in a separate window.

Note

If the device is not manageable by browser, you must launch the Device View from the Management Station where HP TopTools for Hubs & Switches is installed.

Configuring Polling

Polling a device involves sending a request to the device and waiting for a response. If the device does not respond to a request within a certain time interval, it is considered down and an alert is entered in the Alert page. You can set a number of polling parameters in the Settings - Device Communication page.

To start configuring polling for devices:

1. Click on the **Devices** button in the navigation frame.
2. Select **Device Types** from the menu.
3. Click on a device in the right frame.
4. Click on the **Settings** button in the navigation frame and select **Device Communication** from the list.

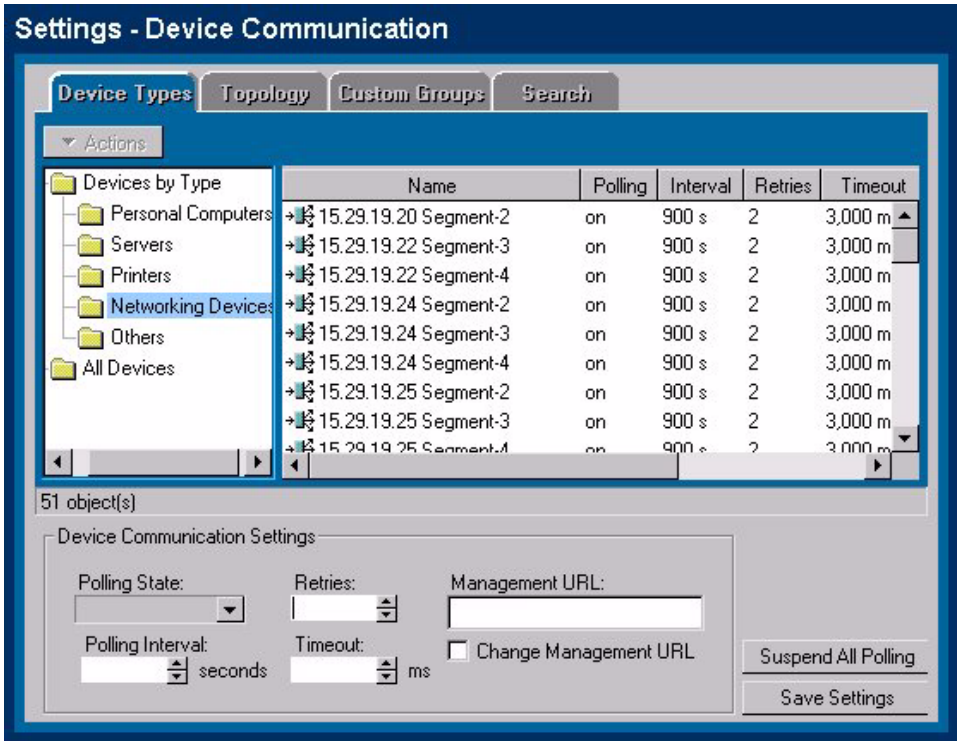


Figure 6-2. Device Communication Settings

The settings are:

- Polling State—On or Off for selected devices. Select **Do Not Change** to keep the previous settings.
- Retries—The number of times a device will be polled before entering an alert in the Alert page.
- Polling Interval —The amount of time in seconds between requests for a response.
- Timeout—The amount of time in seconds that HP TopTools will wait for a response from a device before sending another request.
- Management URL—If http discovery has found a management station, its address will appear in the Management URL field. You can override this URL if you want to change it.

Click on the **Suspend All Polling** button to stop polling. The button now reads **Resume Polling**. Click on it to start polling again.

Selecting Actions for Devices

Click on the **Actions** button at the top left of the page to select an action to perform. Alternatively, right-click on a device in the list and select an action from the menu. Depending on the device, the Actions include:

- View Alerts—Displays the Alerts page with any alerts that have occurred for the device.
- Check Connectivity (Ping)—Use ping to test the network connection to a device.
- Set Friendly Name—Create an easy-to-remember name for a device.
- Update Discovery—Re-reads the configuration of the selected network device or devices to see if changes have occurred.
- Add to Custom Group—Add a device to a custom group.
- Delete—Delete the selected device from the devices page.
- Find in Topology View—Locate a device in the Topology View.
- Security (Set SNMP Passwords - Communities)—Set up device security by entering passwords.
- **SNMP/Trap Configuration**—Set the thresholds for SNMP traps. Only appears for switches with browser interfaces.
- Update Firmware—Download the latest device firmware (see **Downloading Firmware** for instructions).
- Telnet—Start a telnet session with a device (available only for devices that support telnet).
- Node Port Table—View a table showing the devices attached to each port of the selected device.
- Management Home Page—Displays the Status page for the selected device.
- Properties—Display some generic SNMP information about the device including the system name, IP/IPX address, uptime, device description and status.

You can perform actions on up to 100 devices at a time. Use Ctrl-click to select more than one device from the list.

SNMP/Trap Configuration

In order for traps to function, you must set the trap in the Thresholds dialog box. You must be at the management station to set traps. This menu selection only appears for switches that are browser-manageable. Do the following:

1. Select **SNMP/Trap Configuration** from the Actions menu.
2. In the Device Configuration dialog box select the **Thresholds** tab and set the thresholds for the traps you are interested in receiving.
   - Threshold—the value of the event at which the trap or alarm is triggered
   - Tolerance—the device does not send another event to the manager until the value goes below the tolerance value and the threshold value is reached again. The default is 80% of the threshold value.
   - Time Interval—the time elapsed while HP TopTools examines specified traffic for threshold and tolerance violations. If the threshold is reached with the time interval specified, an event is triggered.

3. Select the **Trap Receivers** tab and set the management stations that should receive traps.
4. Select the **Authorized Managers** tab and set the management stations that can send and receive SNMP requests for the device.

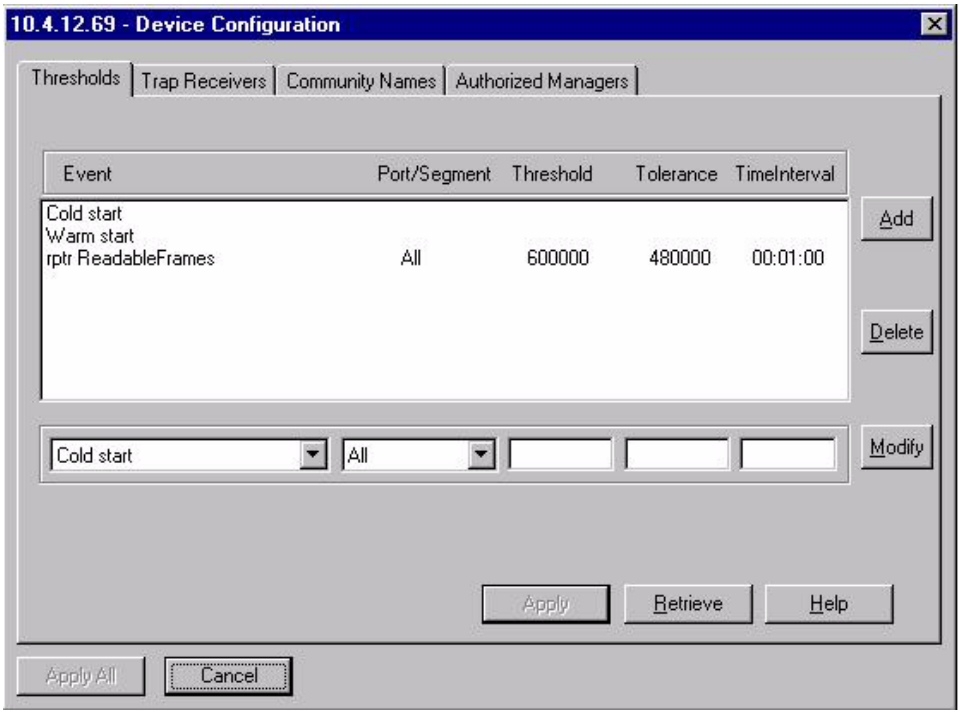


Figure 6-3. Thresholds Dialog Box

Device Topology

The Topology view displays a hierarchical representation of your network device connections. If HP TopTools is not able to associate a device with a segment, the device is listed as unmapped.

Note

Your hubs and switches must have the Community Name “public” set to READ and WRITE in order for your devices to be mapped.

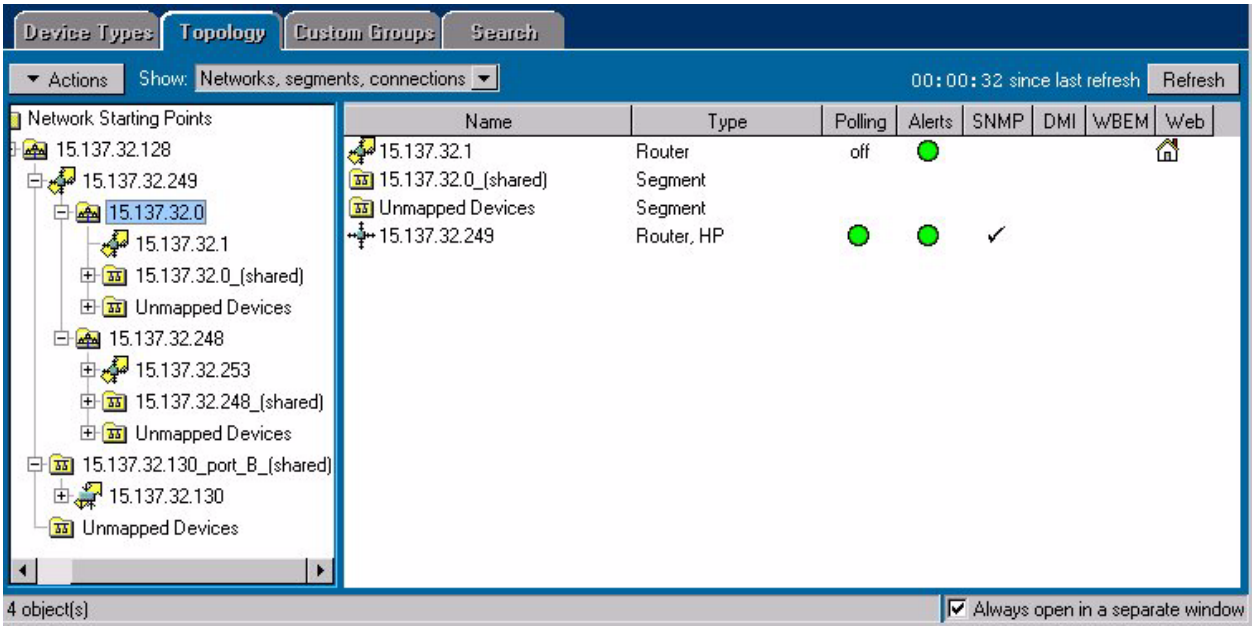


Figure 6-4. The Topology of Networking Devices

You can choose how to display the topology hierarchy by selecting from the **Show** drop down list at the top of the page:

- Network—Displays folders representing networks. All the devices in the network are displayed. Double-click on a router to view all the networks connected to that router.
- Networks, Segments—Displays folders representing networks. The network folders contain folders representing segments in the network. Click on a segment folder to see the devices in that segment.
- Networks, Segments, Connections—Displays network folders containing segment folders. Segment folders contain folders representing connections. Connection folders list the devices associated with that connection.

Double-click on a hub or switch in the list to launch the Device View for device configuration.

Node Port Table

To view the devices attached to the ports of a device, right-click on the device in the networking devices list (Devices, Device Types, Networking Devices). Select **Node Port Table**. The Node Port table for the selected device displays. The table shows the following:

- Node address
- Port number of the selected device

- Type of port, for example, 10Base-T
- The address of the device connected to the port
- The port number connected to on the device

Devices that are underlined (linked) have more devices connected to them. Click on the device address; a new table with that device's connections displays.

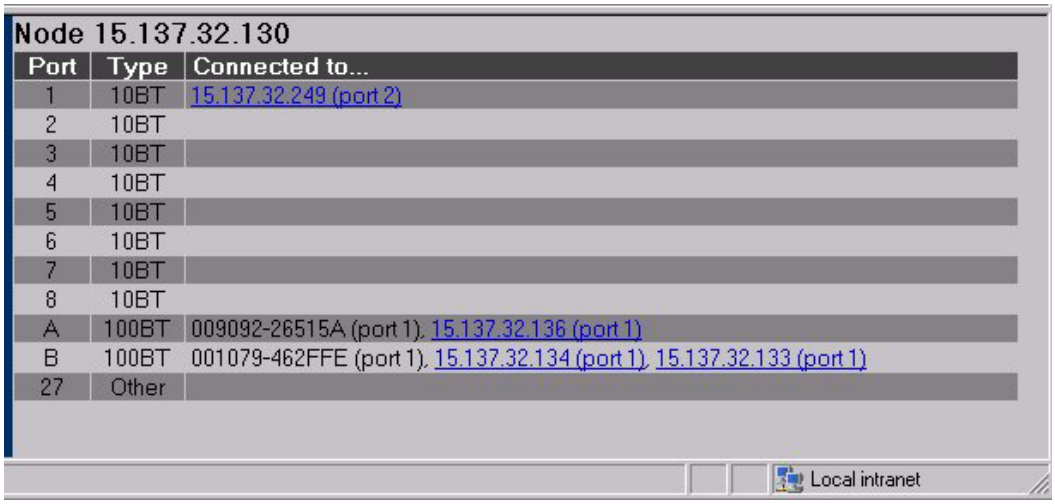


Figure 6-5. Node Port Table for device 15.37.32.130

When a link has been clicked on, it is no longer blue.

Custom Groups

You may want to perform certain maintenance tasks on a group of devices, for example, **downloading** the latest firmware for a type of hub. Select the devices that you want in the Custom group by clicking on the device in the list, then selecting **Add to Custom Group** from the **Actions** menu. You can select multiple devices at one time by using Ctrl-click on each device that you want to include. Enter the name of the **Custom Group** and click **OK**.

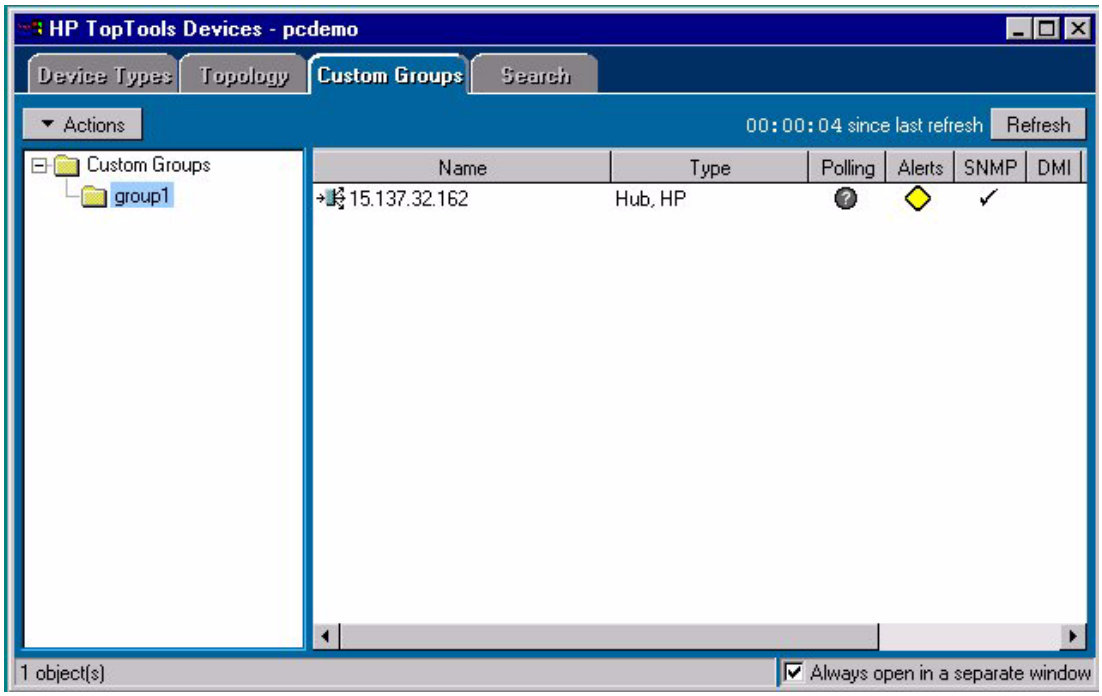


Figure 6-6. Custom Groups Page

A quick way to create a Custom Group uses the Search function. Select the **Search** tab in the Devices page. Enter the type of device that you want as members of your group. Save the results of the search, this becomes your Custom group. You can add and delete devices from the group.

Searching for Devices

You can obtain a list of all of your devices with certain characteristics by using the Search feature. To find one or more devices, select the parameters, such as “Ping Status is Critical” or “Device Type is PC”, or any other combination that is available in the drop down lists. Click on the **Start Search** button.

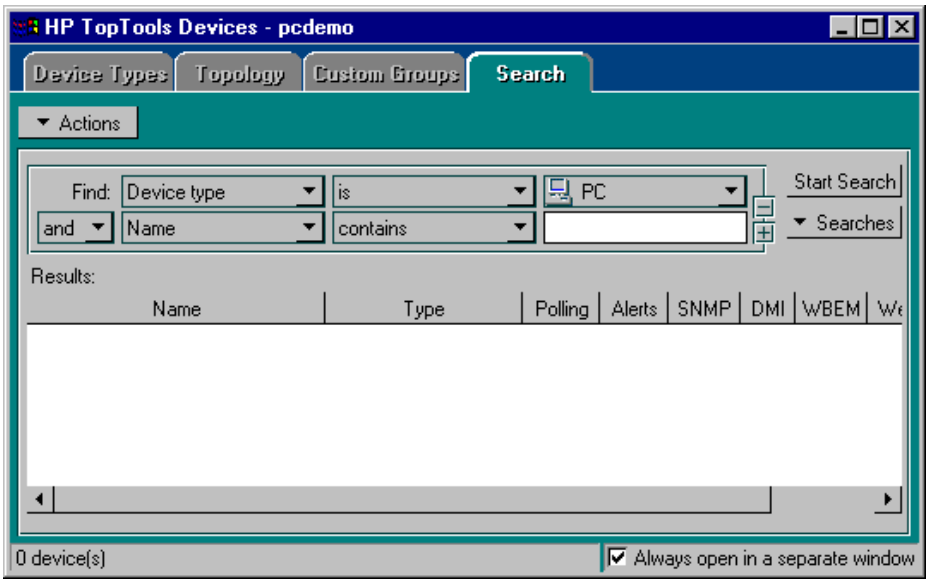


Figure 6-7. Search Page

Click on the **+** or **-** boxes to add or remove search criteria.

To save your search parameters, select **Save** from the Searches drop down list and enter a name for the search. These parameters are saved globally so that you can use the same parameters again by clicking on the **Searches** button and selecting the name you saved.

If you want to rename or delete your saved search parameters, click on the **Searches** button and select **Manage**. Highlight the name that you want to rename or delete and click the appropriate button.

7

Group Policies

With HP TopTools Group Policies feature, you can specify which devices are being configured for a particular policy.

This chapter includes information on:

Creating Groups

You can create up to 30 groups of devices for management by policy. There are two additional groups already created, “Unconfigured” and “Default”.

To begin creating groups for policy management, click on the **Policies** button in the HP TopTools navigation frame and select **Group Configuration**. The **Group Configuration** page displays the groups that have been configured. Initially only the Unconfigured group and the Default group will be listed.

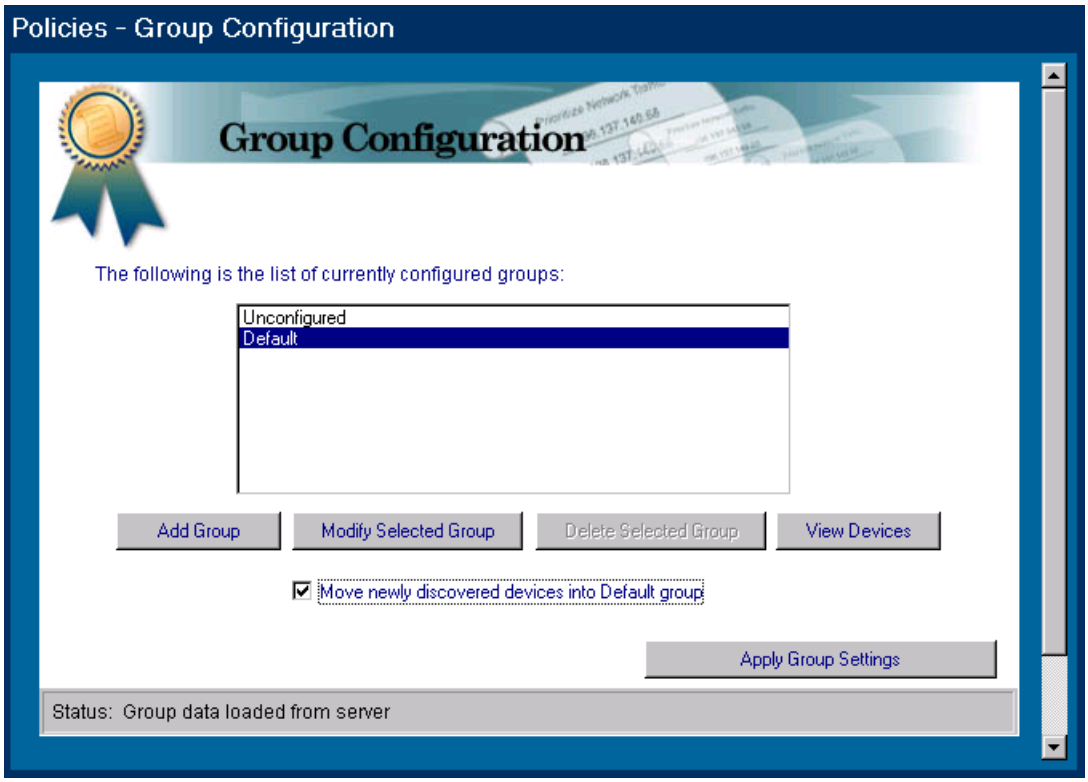


Figure 7-1. Main Page of Group Configuration

If you check the box labeled **Move newly discovered devices into Default group**, your new devices can have policies applied as soon as they are discovered. If you do not check this box, newly discovered devices are moved to the Unconfigured group, which does not have any policy settings. The default setting is to move newly discovered devices to the Default group.

Note

Only devices that support Policy Management will be listed for selection as members of a group.

Viewing the Devices in a Group

To view a list of the devices that are members of a group, select the group and click on the **View Devices** button. The **View Group Members** page lists the devices in that group. Click on **OK** to return to the main Group Configuration page.

Adding a Group

To create a new group and add it to the group list, click on the **Add Group** button. In the Group Configuration - Add Group page, enter a name for the group in the **New Group Name** field. Click on **OK** to add the group. Click on **Apply Group Settings** in the main Group Configuration page.

Note

You must click on **Apply Group Settings** for your changes to take effect.

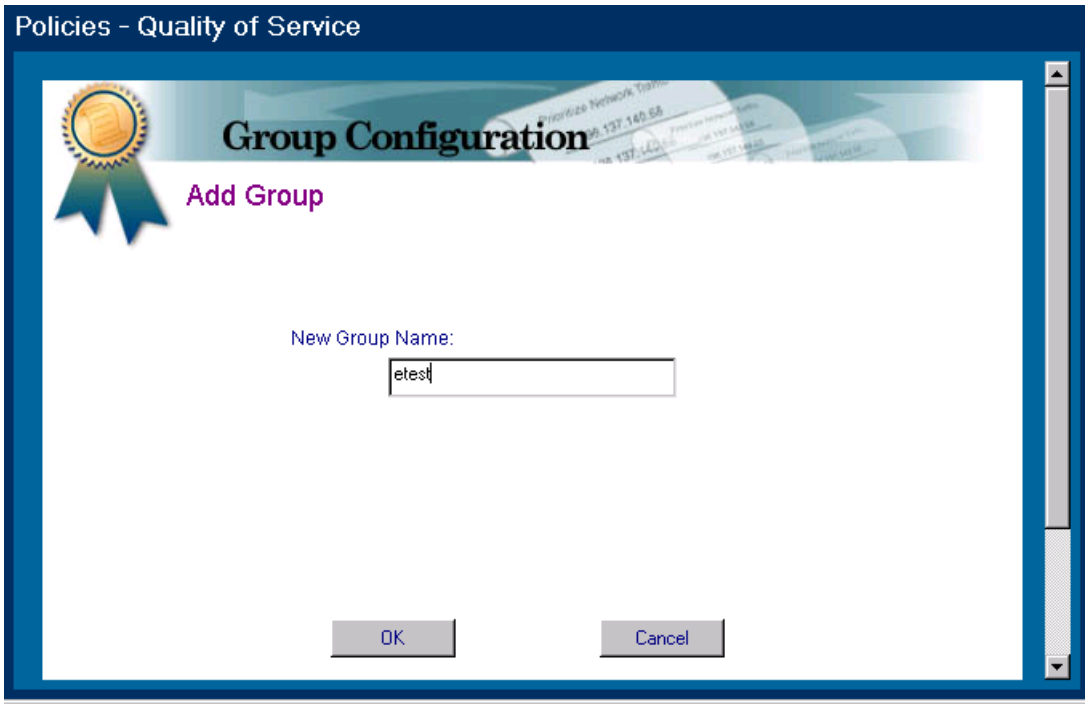


Figure 7-2. Add Group Page

If there are already 32 groups configured (including the Default and Unconfigured groups), a message will inform you that the maximum number of groups has been created.

Modifying a Group

To perform functions such as adding devices to a group, removing devices from a group, or renaming a group, select a group to be modified and click on the **Modify Selected Group** button in the main Group Configuration page. The Group Configuration - Modify Group page displays the current devices in that group.

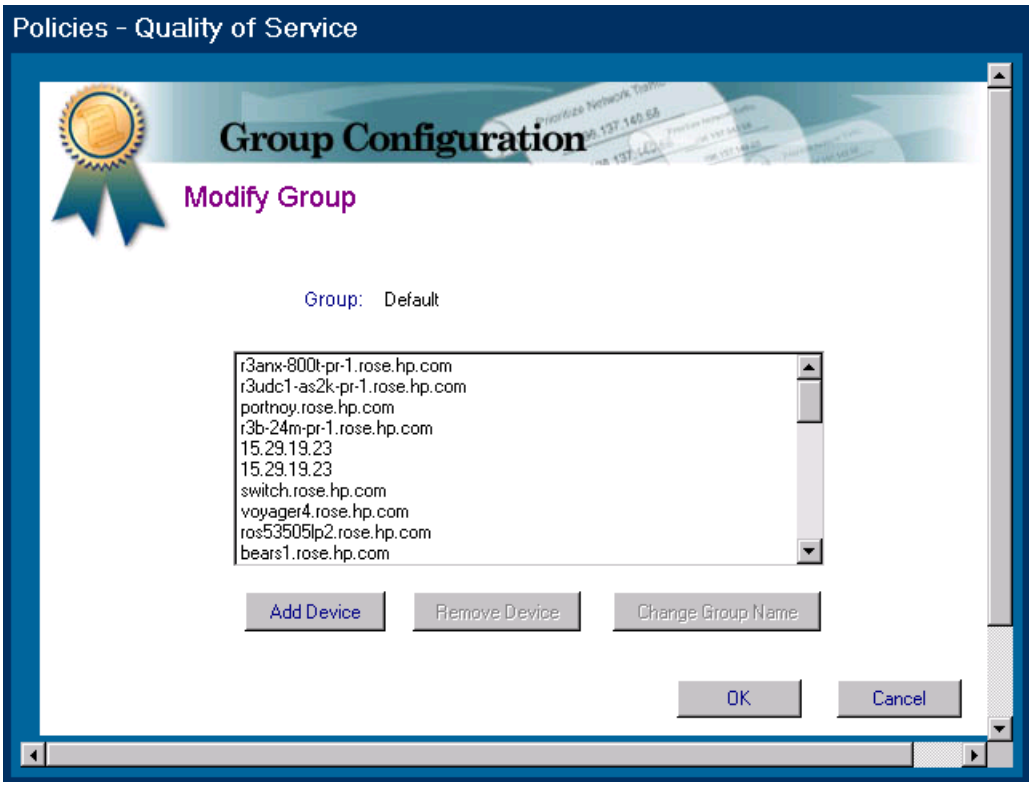


Figure 7-3. Group Configuration - Modify Group Page

Adding a Device to a Group

To add a device to a group, click on the **Add Device** button. Select a group from the **Source Group** list box. All the devices in that group will be displayed in the box below. Select a device in the **Source Group** list box, then click the **Add-->** button. The device appears in the **Target Group** list box. Repeat for as many devices as you want to move.

Note

All the devices displaying the same friendly name but a different IP address should be added to the same group. For example, if you see two devices with the friendly name of “Switch1” but one has an IP of 200.1.1.1 and one has an IP address of 200.1.1.2, they should both go in the same group.

When you are finished with your changes, click the **OK** button. Click on **Apply Group Settings** in the main Group Configuration page.

Clicking **Cancel** removes all your changes.

Note

A device can only be a member of one group.

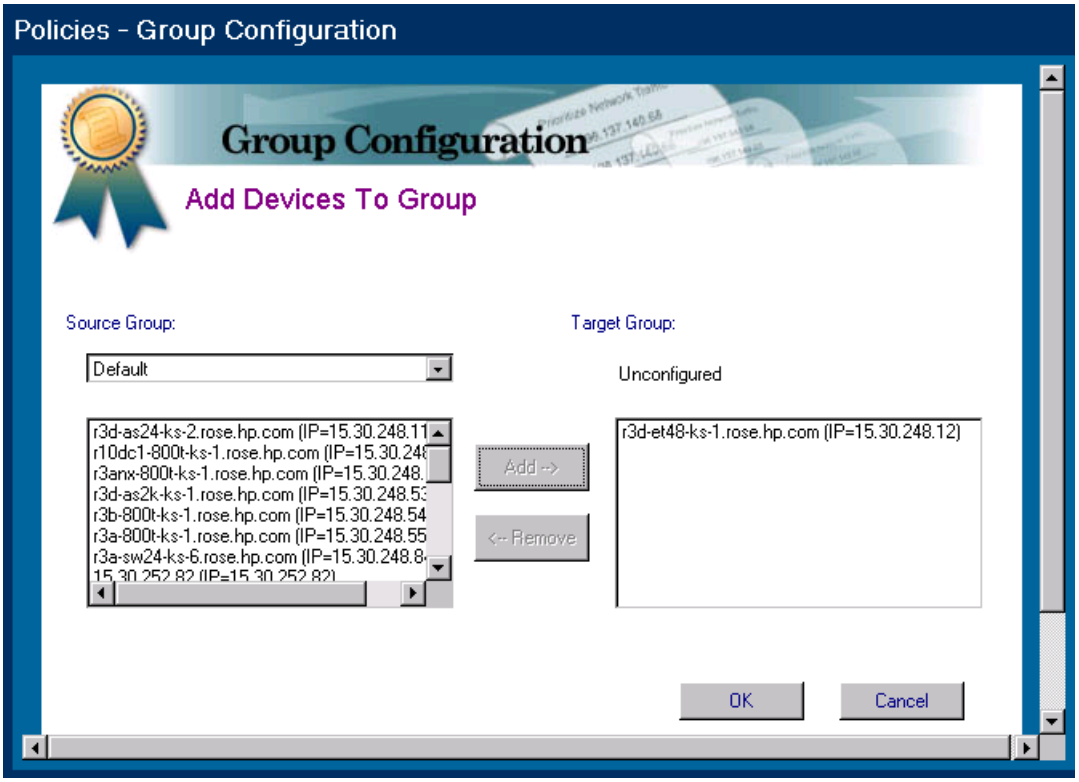


Figure 7-4. Adding a Device to a Group

Removing a Device from a Group

To remove a device from a group, select a device in the Group Configuration-Modify Group page and click on **Remove Device**. You will be asked to confirm the deletion. Select **Yes** to delete the device from the group. The device is moved to the Unconfigured group.

Click on **Apply Group Settings** in the main Group Configuration page.

Changing the Group Name

To change a group name, click on the **Change Group Name** button in the Modify Group page. Edit the existing group name in the **Group Name** field and click on **OK**. Click on **Apply Group Settings** in the main Group Configuration page.

Configuring Group Policies

Start configuring Group Policies by clicking on the **Policies** button in the HP TopTools navigation frame. Select **Configuration Policies** from the menu. The **Policies - Automatic Configuration Management of Hubs & Switches** page displays the following buttons:

- General—Displays SNMP system information and allows modification of that information
- Alerts—Allows selection for delivery of alerts to the TopTools server, removal of trap receivers from a displayed list, and setting fault sensitivity for alerts
- Advanced Switch Features—Turn on or off:
  - Automatic Broadcast Control (ABC) for a selected protocol
  - Multicasting (IGMP)
  - Spanning Tree Protocol (STP)
- Security—Displays and allows addition or modification of community names and authorized managers

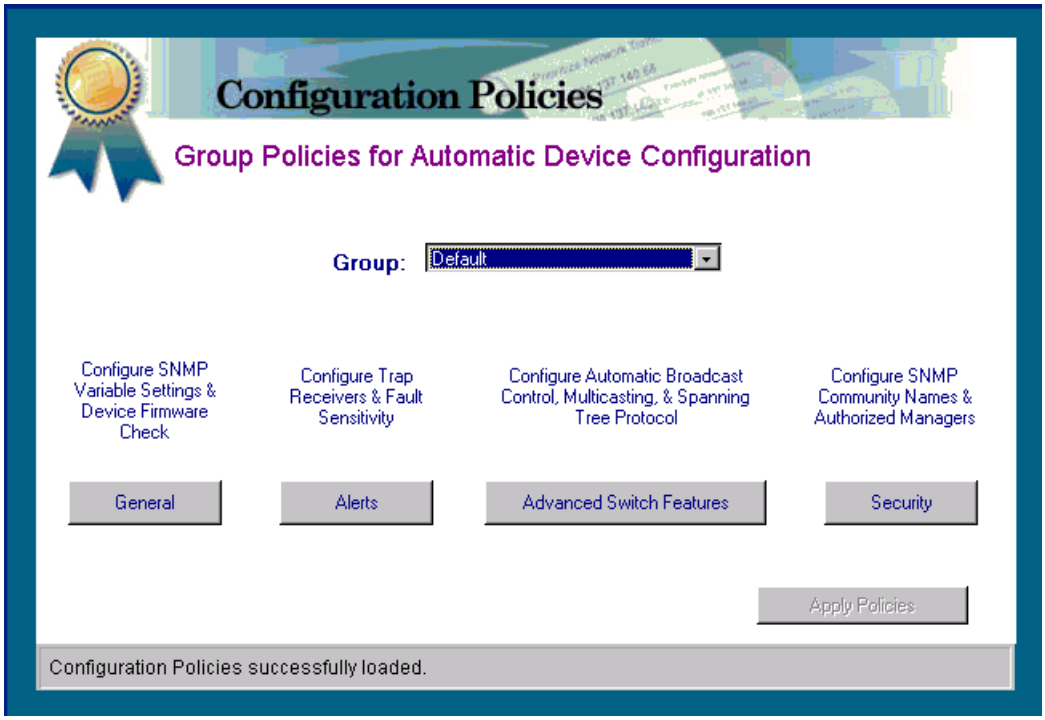


Figure 7-5. Main Configuration Policies Page

Note

The devices must have management by browser capability.

General Configuration Policies

SNMP System Information

To configure SNMP Information for a group, click on the **General** button in the **Configuration Policies** main page. The **General Polices** page for that group displays.

Three SNMP variables for the selected group are listed in the SNMP System Information box:

- sysContact—The person to contact about this group of devices
- sysLocation—The location of this group of devices.
- sysName—The name for the group of devices.

If <keep device setting> is selected, the current value stored in the switch is not modified.

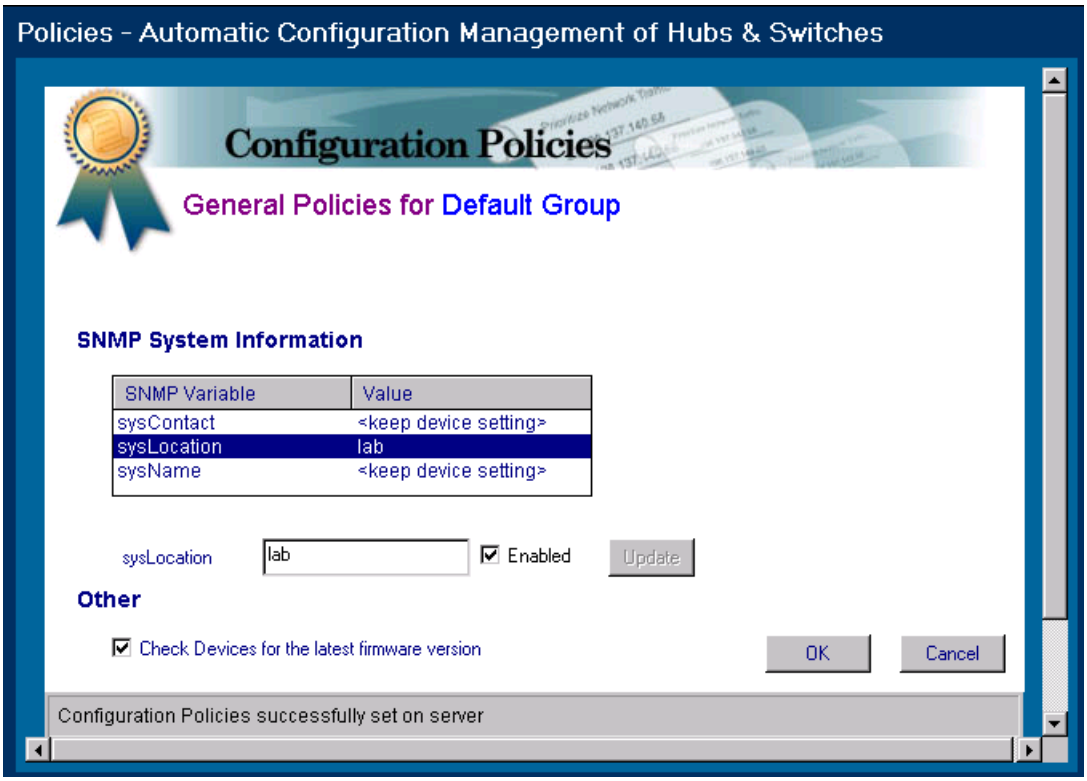


Figure 7-6. General Policies Page Showing SNMP System Information

To modify a field, select the field in the SNMP system Information box, then check the **Enabled** check box below if it is not currently checked. Enter the new information in the field to the right of the Enabled check box and click

Update. The new information appears in the box above. Click on **OK** to return to the main Configuration Policies page, then click on **Apply Policies** to save your changes.

Clicking on **Cancel** discards all your changes.

Checking Firmware Versions

When TopTools discovers a device in your network, the firmware version of the device is retrieved and compared against a list to determine if there is a newer firmware version available. If a newer firmware version is available, a message is entered in the Alerts page (click on the Alerts button in the navigation frame). See **Downloading Firmware** for instructions on downloading the newer firmware.

Alert Configuration Policies

To configure group policies for alert notification and fault sensitivity, click on the **Alerts** button in the **Configuration Policies** main page. The **Alert Policies** page for that group displays.

Use the **Trap Receivers** list box to specify the management stations that can capture traps for web-enabled HP hubs and switches in your network.

Enter the IP addresses of the hosts that should receive traps. The maximum number of additional trap receivers that you can add is nine. The HP TopTools management station is a trap receiver by default.

See **SNMP Configuration** for information about setting traps.

The device will automatically send traps to the trap receivers entered in the trap receivers list box. You can configure actions to take when traps occur, such as paging a network administrator, by using the **Configure Actions on Events** feature listed in the **Alerts** button in the HP TopTools home page.

Traps will be sent for all standard SNMP events, as well as some additional fixed events. The fixed events for hubs and switches include:

- coldStart: The device reinitialized itself and its configuration may have changed.
- warmStart: The device reinitialized itself but its configuration is not changed.
- linkDown: Communication was lost on a device interface.
- linkUp: Communication was regained on a device interface.
- authorizationFailure: The device received an SNMP packet that was not authenticated.
- entConfigChange: A change, such as the addition of a card, was made to the device.
- hpicFaultfinderTrap: A possible error condition was detected by the fault finder.

Sending Alerts to the HP TopTools Management Station

When you check this box, all alerts will be sent to the HP TopTools Server in addition to any other trap receivers that you have designated. This feature is enabled by default.

Removing Trap Receivers

If the **Remove trap receivers not listed below** check box is checked, any trap receivers configured that are not displayed in the trap receivers list box will be removed as trap receivers.

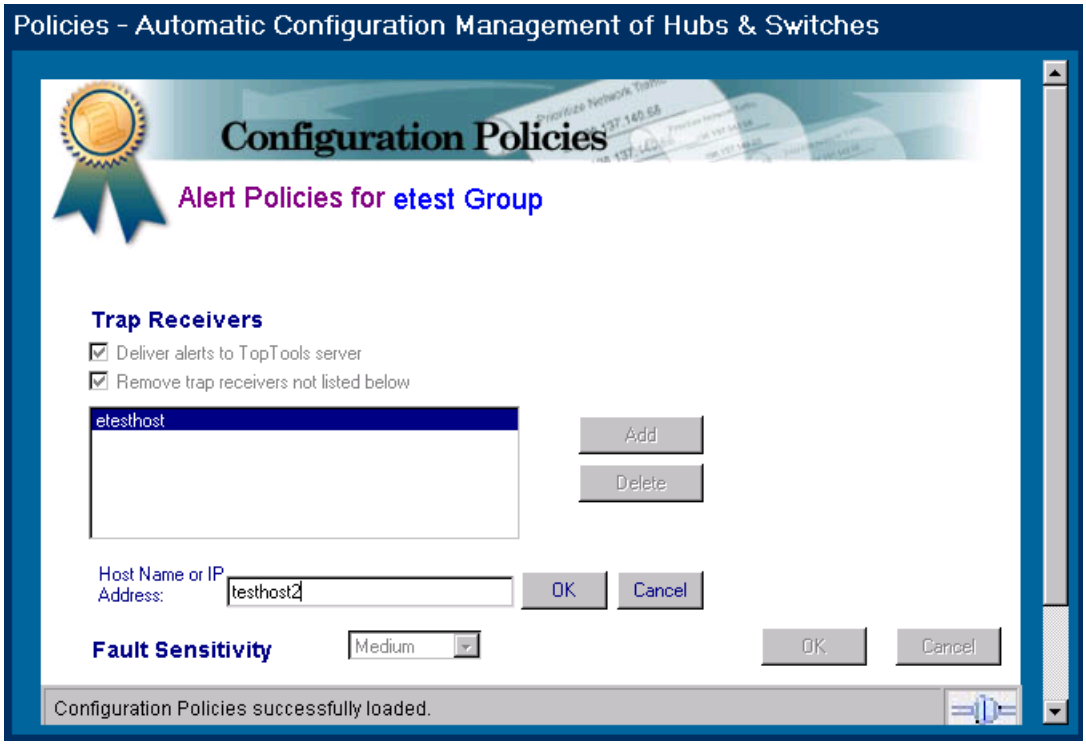


Figure 7-7. Alert Policies Page

Setting Fault Sensitivity

The Fault Sensitivity field allows you to set the sensitivity levels for the actions to be taken when a fault is detected on a port in your network. Switches only have a sensitivity setting for logging network problems. The sensitivity settings are:

High Sensitivity: The device will make an entry in the Alert Log (located in the Status tab of the Device page) when a network problem of any severity occurs.

Medium Sensitivity: The device will make an entry in the Alert Log when serious network problems occur.

Low Sensitivity: The device will make an entry in the Alert Log only when severe network problems occur. These are problems that may bring the network down.

Off: The device will never make any entries in the Alert Log regardless of the severity of the problem.

<keep device setting>: The current value stored in the switch is not modified

If you make any changes, you must click on **Apply Policies** in the main Configuration Policies page for your changes to take effect.

Advanced Switch Features

To configure Advanced Switch Features for a group, click on the **Advanced Switch Features** button in the **Configuration Policies** main page. The **Advanced Switch Features** page for that group displays.

The following features can be set for the selected group of switches:

- **Automatic Broadcast Control (ABC)**
- **IP Multicasting (IGMP)**
- **Spanning Tree Protocol (STP)**

The possible settings are:

- On - Turns the feature on for all switches in the selected group. On for ABC has more options:
  - On for IP only - Turns on ABC for IP devices only.
  - On for IPX only - Turns on ABC for IPX devices only.
  - On for IP/IPX - Turns on ABC for IP and IPX devices.
- Off - Turns the feature off for all switches
- <keep device setting> - The feature is not on or off. The device conforms to what has been set in the device console.

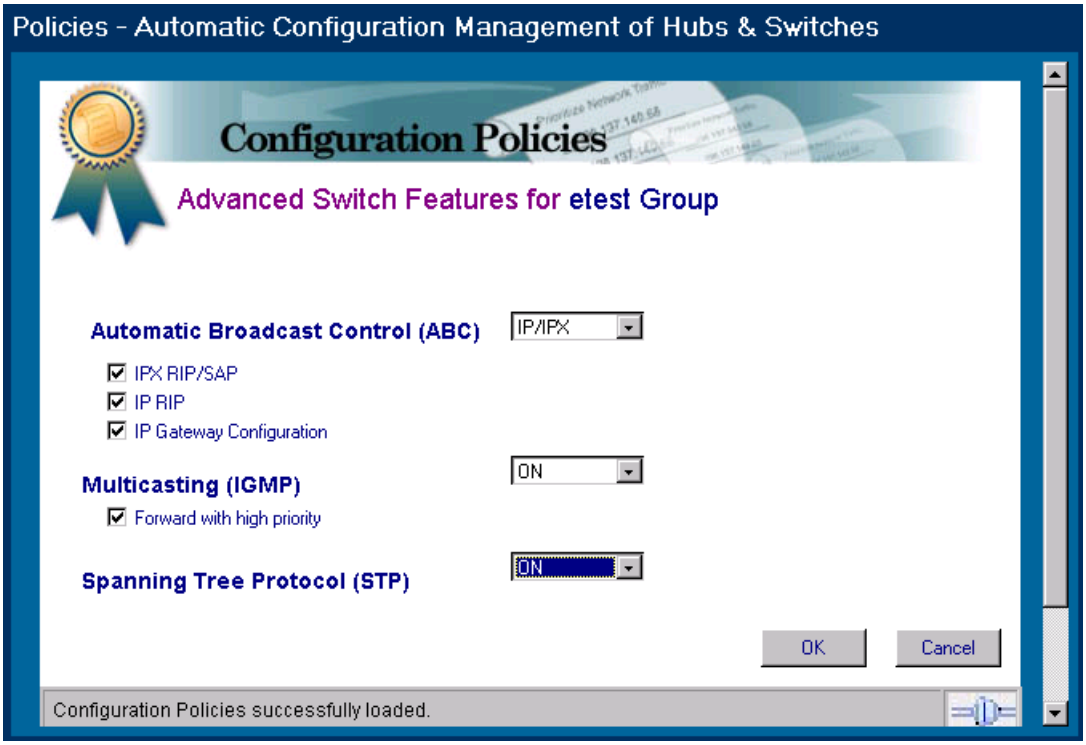


Figure 7-8. Advanced Switch Features Page

The problem of broadcast control is addressed in part by the use of two features, Automatic Broadcast Control (ABC) and Internet Group Management Protocol (IGMP).

Automatic Broadcast Control (ABC)

Automatic Broadcast Control (ABC) is a feature that controls broadcasts through IP/IPX Broadcast Reduction. IP/IPX Broadcast Reduction reduces the number of broadcasts propagated through the network.

Using ABC, the switch acts as a proxy server, replying to Address Resolution Protocol (ARP) requests, Nearest Server Query (NSQ) requests, and GetLocalTarget requests on behalf of the destination node. An ARP cache (learned address table) is created for each subnet allowing the switch to proxy reply with the resolved MAC address instead of forwarding the requests out all ports. This limits the broadcasts within the switching domain. The Service Advertising Protocol (SAP) table performs the same function in an IPX network. By using these tables, the switch can resolve addresses for any node in the network that it already knows about.

Routing Information Protocol

The switch also intercepts Routing Information Protocol (RIP) and SAP broadcasts and forwards these only to ports where routers and servers have been detected. This also reduces the number of broadcasts on the network.

For example, if User A sends out a broadcast message to connect to its server, the request is sent out of all ports on the switch. When the server responds to User A, the switch intercepts the response and learns that the server is on that port. When User B sends a request to the same server, the switch already knows which port that server is on and sends that information to User B, just as if the server had responded to the request. User B's request is not broadcast out any of the switch ports.

Enabling Broadcast Control for IP

The IP protocol uses Address Resolution Protocol (ARP) packets to find the MAC address of a node that corresponds to the network layer address. When Broadcast Control is enabled, the switch intercepts the ARP packet on its way to the destination node. If this destination is unknown to the switch, the switch floods the ARP request to all ports. When the destination port responds, the switch stores information about the source and destination MAC addresses and layer 3 addresses in its ARP cache. This information allows the switch to proxy a reply containing the MAC address of a destination to the source of an ARP request. The source can then send a unicast packet directly to the destination. The amount of broadcast traffic has been decreased.

Automatic IP RIP Control

To further reduce broadcast traffic, you can check Automatic IP RIP Control. IP RIP packets are sent out periodically (every 30 seconds) to distribute routing information. By enabling Automatic IP RIP Control, the switch will only forward RIP packets out the ports on which RIP packets have been received. Since routers are the only devices that generate RIP packets, this ensures that RIP packets are only sent out ports with routers attached to them. When this feature is not enabled, IP RIP packets are forwarded to all ports.

Enabling Broadcast Control for IPX

The IPX protocol broadcasts all of its known routes and services every minute by using IPX, RIP and Service Advertising Protocol (SAP) packets. When servers are booted up, they advertise their services using SAP. These frames must be forwarded by routers, which maintain a database of this information, allowing clients on the network to obtain the internetwork addresses of the servers where they can access services.

Automatic IPX RIP/SAP Control

To further reduce network traffic, you can check the Automatic IPX RIP/SAP Control check box. The switch will intercept RIPs and SAPs, broadcasting them only to ports where IPX routers or servers have been detected, or to ports that have been configured to transmit RIPs or SAPs. When this feature is not enabled, IPX RIP/SAP packets are forwarded to all ports.

Automatic IP Gateway Configuration

When Automatic IP Gateway Configuration is enabled, the switch will modify replies from the DHCP server so that the Default Gateway IP address of client becomes the client's own IP address. This is useful in a multinetted environment (where more than one IP network is configured in a single broadcast domain).

See **Routing Information Protocol.**

Internet Group Management Protocol (IGMP)

Multimedia and email applications need the ability to communicate to multiple destinations efficiently. IP multicasting allows hosts to dynamically register for sending or receiving multicast traffic.

The Internet Group Management Protocol is a method for automatically controlling multicast traffic through the network. Using multicasting, applications can send one copy of a packet addressed to a group of computers that wish to receive it. This method is more efficient than sending a separate copy to each node. Other advantages of multicasting include:

- information delivered in a timely, synchronized manner because all destination nodes receive the same packet
- information can be sent to destinations whose addresses are unknown
- reduces the number of packets on the network because only one multicast packet is sent.

IGMP uses multicast queriers and hosts that support IGMP to manage multicast traffic on the network. It specifies how the host informs the network that it is a member of a multicast group. A set of queriers and hosts that send and receive data from the same set of sources is a multicast group.

The HP switches have a standards-based IGMP implementation. The switches process IGMP packets by learning which of the switch's interfaces are linked to hosts that are members of multicast groups and multicast routers. It limits multicast traffic by monitoring the IGMP traffic to learn which hosts are in which multicast groups, then allowing IP multicast traffic to be sent only to ports with valid host group members.

When a switch receives an IGMP packet, it updates the internal IP multicast forwarding table with the IGMP membership read from that packet. The switch then sends the packet to the ports with members of the destination multicast group.

Special multicast routers/queriers communicate by using three message types - query, report, and leave group. The query message, sent by a querier, is used to discover which network interfaces belong to a multicast group. Each host responds to the query message with a report message that tells the querier the host is a member of the multicast group. The host also can send a report message to join a group or a leave message to leave a group.

Note

Using the console you can designate specific ports to always or never forward multicast packets.

Forward with High Priority

When **Forward with High Priority** is checked, any IGMP packets received by the switch will be forwarded in a prioritized manner, preceding packets with normal priority.

The Spanning Tree Protocol

The Spanning Tree Protocol (IEEE 802.1d) maintains a loop-free topology in networks with redundant bridges or switches. The spanning tree devices determine which devices will be active and which will be backups so that no two nodes in a network have more than one active path between them at any time. The Spanning Tree Protocol uses the most efficient path between segments. If a bridge or switch fails, the other bridges and switches reconfigure the network automatically. When the problem is repaired, the bridges and switches automatically return to the original network configuration.

Security Configuration Policies

To configure Security policies for a group, click on the **Security** button in the **Configuration Policies** main page. The **Security Policies** page for that group displays.

Communities

You can create up to five communities for each group. The default community is “public”.

Caution

Do not delete the “public” community.

The Read Access and Write Access choices are:

- None—Provides access to no tasks in HP TopTools

- Discovery—Enables a device to be discovered by HP Toptools for Hubs and Switches for mapping in a Topology view. The only tasks allowed are Link Test and Discovery.
- Restricted—Provides partial access to HP TopTools features (not Community Name settings or Authorized Managers)
- User—Provides almost complete access to HP TopTools features
- Full—Provides complete access to all HP TopTools features

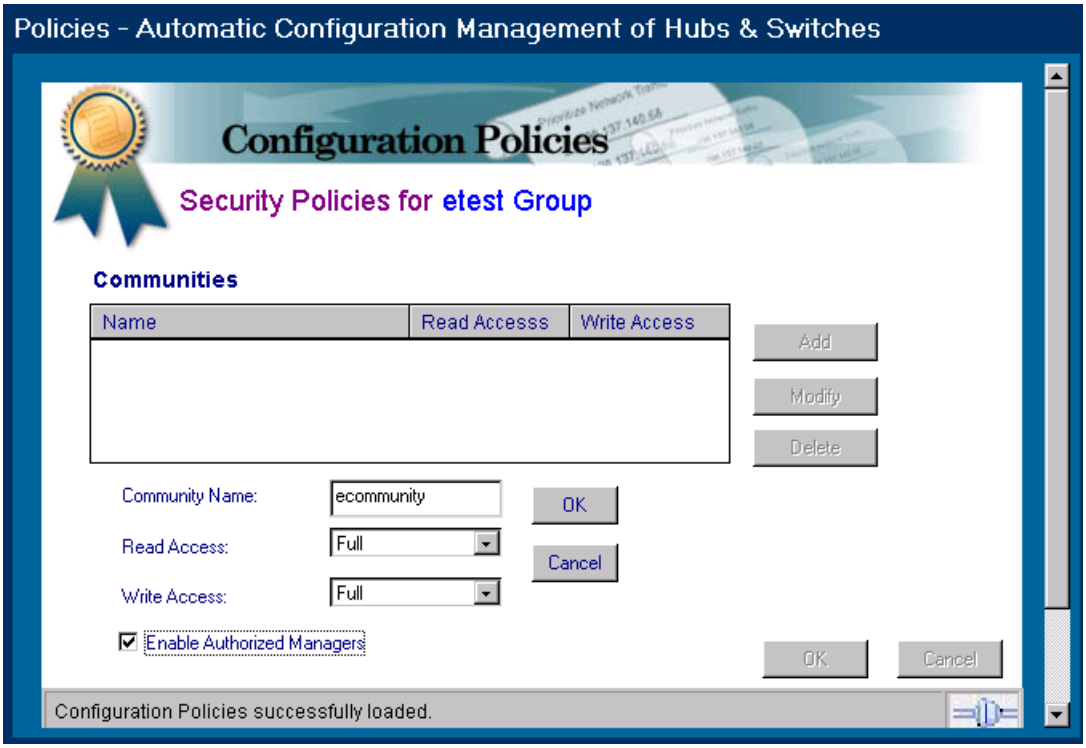


Figure 7-9. Security Policies Page

Adding a Community

To add a community for a group:

1. Click on the **Add** button. A blank field for the new community name appears below the Communities box.
2. Enter the name of the new community. Then select the **Read Access** and **Write Access** for that community.
3. Check the **Enable Authorized Managers** check box if you want to allow the addition of Authorized Managers to manage this community.
4. Click on **OK**.

Modifying a Community

To modify an existing community:

1. Select the community to be modified and click on the **Modify** button. The selected name appears in a field below the Communities box. You can change the name in this field.
2. If desired, change the **Read Access** and/or **Write Access**.
3. Check or uncheck the **Enable Authorized Managers** check box if you want to change the permission for an Authorized Manager to manage this community.
4. Click on **OK**.
5. Click on **Apply Policies** in the main Configuration Policies page.

If you enable Authorized Managers, this message appears below the check box: “The TopTools Server will automatically be added as an Authorized Manager”.

Deleting a Community

To delete a community for a group, select the community and click on the **Delete** button. Click on **Apply Policies** in the main Configuration Policies page.

Configuring Authorized Managers

The Authorized Managers box lists the managers that are authorized to manage the selected community in the Communities box. You can configure nine authorized managers; one additional manager is the HP TopTools server by default.

Adding or Deleting an Authorized Manager

To add an authorized manager for a community:

1. Select the community in the **Communities** box, then click on the **Add** button next to the Authorized Managers box. A blank field appears below the box.
2. Enter the **host name** or **IP address** of the new authorized manager in the field.
3. Click on the **OK** button.
4. Click on **Apply Policies** in the main Configuration Policies page.

To delete an authorized manager:

1. Select the community in the **Communities** box.
2. Select the authorized manager that you want to delete in the **Authorized Managers** box, then click on the **Delete** button.
3. Click on **Apply Policies** in the main Configuration Policies page.

8

Viewing Your Maps

This chapter contains information on:

- **Displaying Topology Maps**
- **Using the Panner**
- **Launching the Device View**
- **Options for Map Control**
- **Locating a Node**

Displaying Maps

When HP TopTools is started, the discovery process discovers the devices on your network. This information is used by the topology process to create a network topology and the physical maps. Two maps are created automatically:

- A map showing just the bridges, switches and segments
- A map showing the entire network.

Note

Your hubs and switches must have the Community Name "public" set to READ and WRITE in order for your devices to be mapped.

Click on the **Maps** button in the navigation frame to display the **Maps-View Maps** page. This page lists the IP subnets that have been discovered by HP TopTools. The following information is provided for each map:

- Name—The name of this map
- Type—Either a Network or Segment map
- Create Date—The date the map was created
- View—The style of the map, for example, hierarchical
- Owner—System (default maps created) or the User Id of the person who created the map

Maps appear in the list only after topology is complete. To display the map in a separate browser window, check the **Map in Separate Window** box at the bottom of the page, then double-click on a map in the list.

Click the **Full Network** button to generate a map of the entire network.

Select the **Delete** button to remove a map from the list and the map file on the server. It may take a minute for the map list to reflect the deletion.

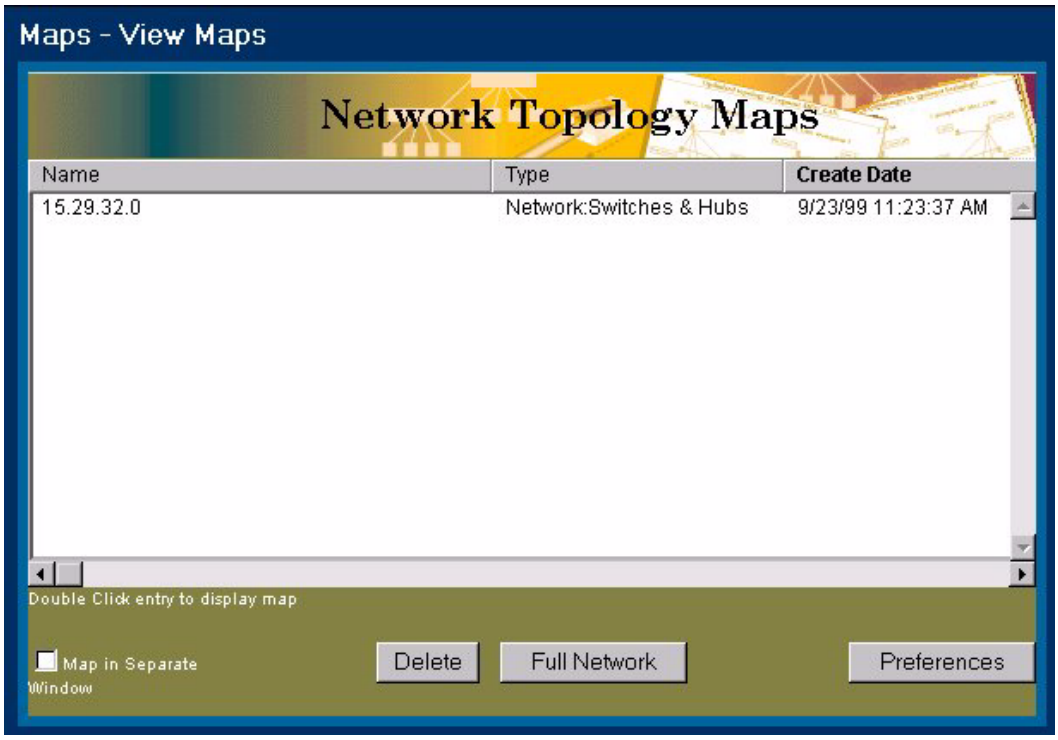


Figure 8-1. Network List for Displaying Map Views

Map Server Settings

Click on the **Preferences** button in the **Maps-View Maps** page to launch the Server Settings page. The Server Settings page lets you select the display characteristics for maps. These settings control how maps appear to all clients. An individual client can override some of the settings for the map being displayed by using the **View** button in the map window.

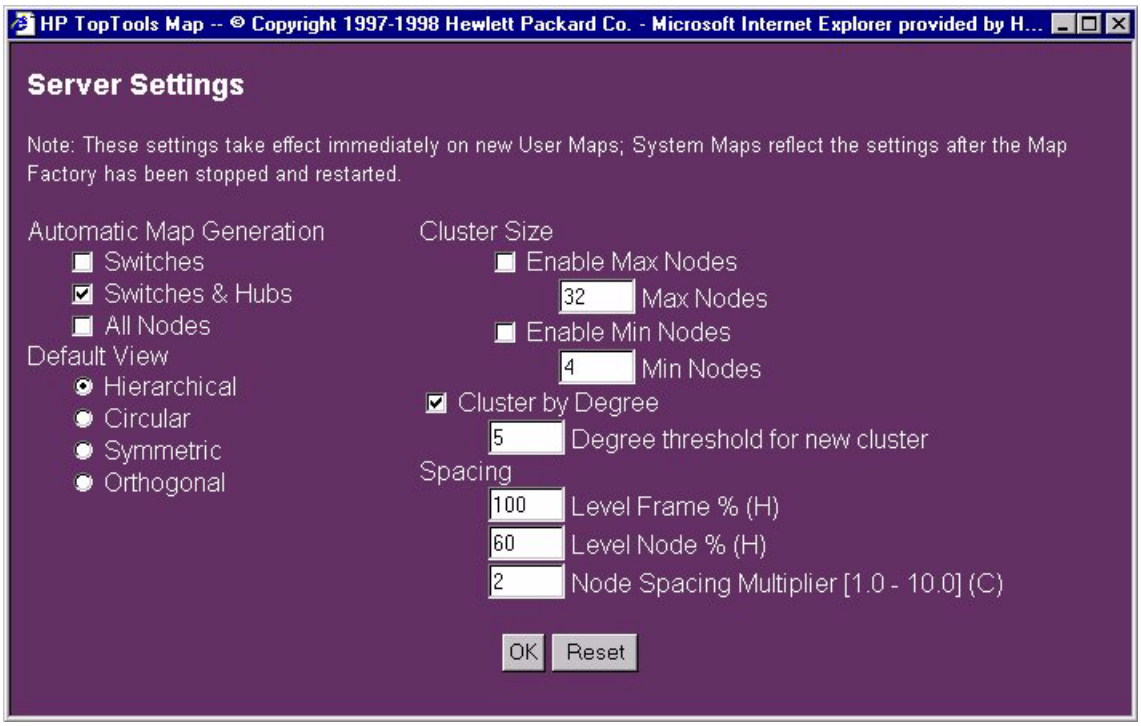


Figure 8-2. Map Settings

The Map Factory Service generates your topology maps after discovery is complete. You must stop and restart this service for your new map settings to take effect. Select the **Settings** button in the HP TopTools navigation frame and click on **Services**.

Automatic Map Generation

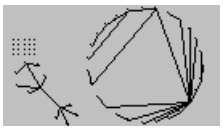
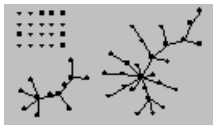
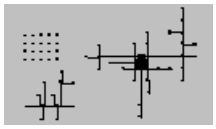
Select what devices you would like displayed in your map:

- Switches—Maps for switches and bridges are automatically created.
- Switches & Hubs—Maps for switches, bridges and hubs are automatically created. This is the default.
- All Nodes—Maps displaying all end nodes are automatically created.

Default View

You can choose the style of map layout that you prefer. The four styles are shown in the following table.

Table 8-1. Map Styles

	Hierarchical—The devices are presented in a tree-like structure, from a top-level device such as a switch, to its connecting hubs and end nodes.
	Circular—The network map is displayed with devices connected in a circular pattern. Segments connect the circles.
	Symmetric—The devices are spaced along an axis on the page, in a symmetrical fashion.
	Orthogonal—The devices are displayed along the x and y axis. This map resembles a circuit board layout.

Cluster Size

Use the Cluster Size option to adjust the size of the clusters in your map. The options are:

- Enable Max Nodes—Check this box to select a maximum number of nodes to be displayed in a cluster. Enter the number of nodes in the **Max Nodes** field. If a cluster has more nodes than the specified maximum, that cluster is divided into two clusters of approximately the same size, unless the resulting cluster has fewer nodes than the specified minimum. This process continues until all clusters have fewer nodes than the maximum value, and more nodes than the minimum value.
- Enable Min Nodes—Check this box to select a minimum number of nodes to be displayed in a cluster. Enter the number of nodes in the **Min Nodes** field. If a cluster has fewer nodes than the specified minimum, that cluster is merged with a neighboring cluster.
- Cluster By Degree—The Degree of a node is the number of ports on the device connected to the node. A node with a degree value greater than or equal to the value entered in **Cluster By Degree** will become the starting node of a new cluster.

Spacing

Spacing controls the amount of distance between nodes in the topology map so that they do not overlap each other. There are three spacing options:

Level Frame%—To increase the amount of space between node levels in a map, increase the percentage. Used in hierarchical map styles.

Level Node%—Sets the amount of space around each node. Increase this value to increase the amount of space around a node. Decrease this value to pull the nodes closer to each other. Used in hierarchical map styles.

Node Spacing Multiplier [1.0 - 10.0]—Used to calculate the node spacing between adjacent nodes in circular clusters. Increase this value to increase the spacing between adjacent nodes. Decrease this value to decrease the spacing between adjacent nodes. Used in circular map styles.

Launching a Map

Double-click on a subnet in the **Maps-View Maps** page to display a map of the subnet.

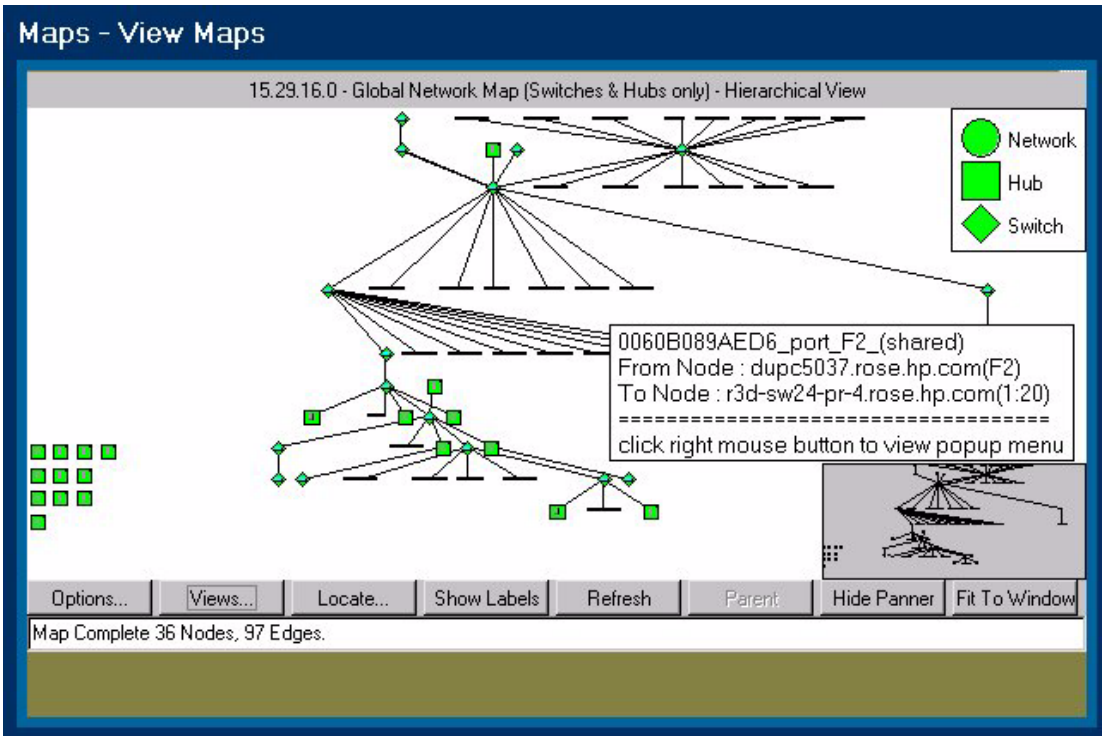


Figure 8-3. Subnet Map

The IP subnet map shows all the segments and managed routers, switches and bridges that form the subnet boundaries. IPX managed bridges that are located in the source IP network are also displayed. To drill down to the end node level, double-click on a segment.

Move your cursor over a device to display a tooltip with information about the name, IP address, and status of that device. Right-mouse click on the device to display the device popup menu. The **Properties (Device View)** selection launches the **Device View**. The **SNMP/Trap Configuration** menu item lets you configure traps and trap receivers for the device.

When you right-mouse-click on a segment you can select **Show Segment Map**.

The buttons at the bottom of the map are:

- **Options**—see below for a description of this feature.
- **Views**—see below for a description of this feature.
- **Locate**—see below for a description of this feature.
- Show/Hide labels—Displays or hides the address of the represented device.
- Refresh—Redraw the map. If new devices have been discovered, they will appear in the updated map.
- Parent—Show the map one level above the displayed map (unless you are already at the network level).
- Show/Hide Panner—Displays or removes the panner from the map window.
- Fit to Window—Displays the entire map view.

You can also access these parameters by right-mouse-clicking on the map background. The background popup menu also includes menu items for hiding the legend, disabling the map tool tips, and disabling the panner tool tips.

Using the Panner

The panner lets you easily focus in on a portion of your map. Click on **Show Panner** to display it in the lower right corner of your map. Using your mouse, drag a rectangle in the panner over the section of the network that you would like enlarged in your map. To restore the map to its original size, click on **Fit to Window**.

Launching the Device View

To configure a device, double-click on the device in the map or right-mouse-click on the device and select **Properties (Device View)** from the device popup menu. The **Status - Overview** page of the device is displayed in the browser. Use the tabs to view or change device settings, or to display device counters.

Note

You must display the Closeup View for older HP devices that do not support a browser interface from the management station where HP TopTools for Hubs & Switches is installed. See the online help for specific instructions about configuring older HP devices.

SNMP/Trap Configuration

See **SNMP/Trap Configuration** in the Networking Devices chapter for more information about configuring SNMP thresholds.

Options for Displaying Maps

There are several parameters you can set to control how your map looks and how often it is refreshed. Click on the **Options** button at the bottom of the page displaying a map and make your selections. Click on the **Apply** button to save them. To close the window without making any changes, click on **OK**. The **Cancel** button cancels any changes that you have not yet applied.

Options—Refresh Maps

If you select the **Automatic Map Refresh** option your map will refresh its display of devices automatically for a selected time period. If you want your map to refresh upon command only, select the **Manual Map Refresh** option.

Options—Labeling

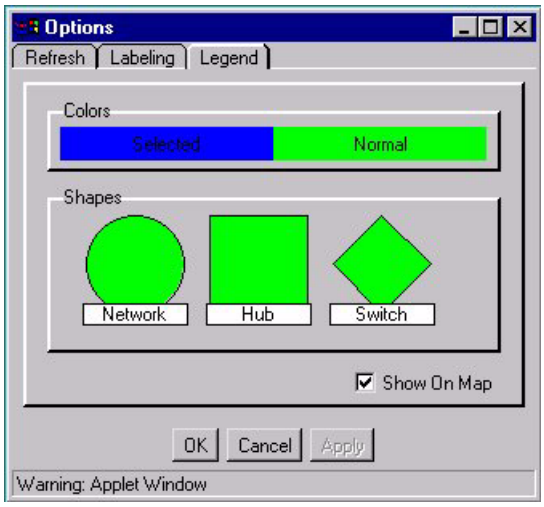
Choose how you would like your device labels to display in the map, by name or by device address. If you do not want to display labels, uncheck the **Show Label Names** box. Check the **Show Segment Names** box to display the names of segments in your map. Click on **Apply** to save your choices.

Note

Label options are only applicable when the **Show Labels** button on the Map is selected.

Options—Legend

Select this option to display the legend for the map. Check the box **Show on Map** to have the legend display on the map. Click on **Apply** to save your choices.



Changing Map Views

Click on the **Views** button to select the style of map layout that you prefer. See **Default View** for an explanation of the four styles.

Locating a Node

To locate a particular end node, click the **Locate** button at the bottom of the page displaying a map. In the Locate browser window, select the network that the node is in, then select the node. Click on the **Locate** button to locate the node. A dialog box displays stating that the node has been found and the appropriate map is opened (if it not open already).

Select **Pan** in the dialog box to set the panner window so that the located item is enlarged and centered in the map. If **Show labels** is turned on, the label under the located device is displayed in reverse video.

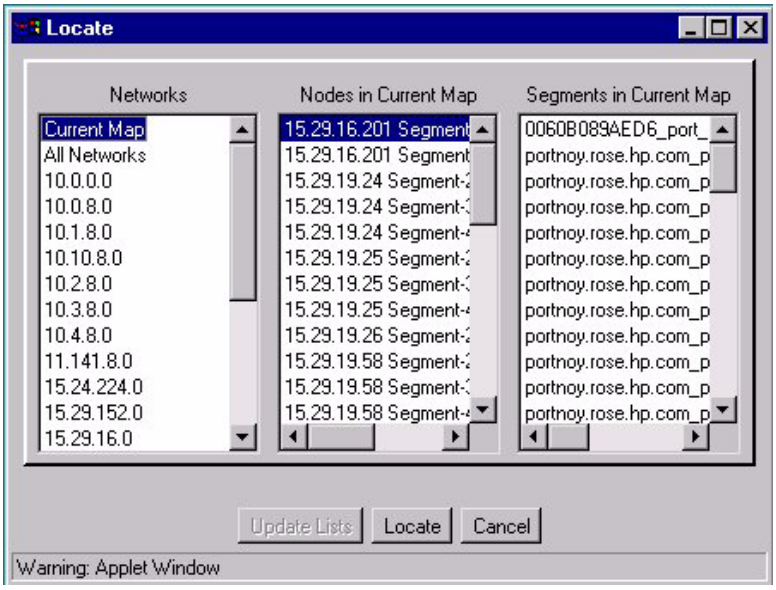


Figure 8-4. Locate a Specific Node in a Map

Note

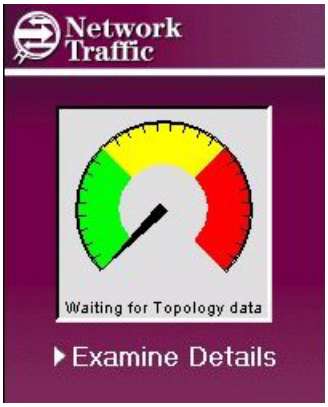
You also can locate a specific node from the Top5 browser window in Traffic Monitor.

9

Monitoring Network Traffic

This chapter describes the tools for monitoring your network using Traffic Monitor. It contains the following topics:

Using Traffic Monitor



The Traffic Monitor presents real-time information about the status of your network. When you select **Network Traffic, Examine Details** from the home page (or select **Traffic Monitor** from the **Performance** button menu), the page displays five gauges in the top half of the browser window and a histogram in the bottom half of the window. Each gauge displays the worst measurement in the entire network for that statistical attribute. The histogram below the gauges displays the value of an attribute, such as broadcasts/sec, for the segments in a selected segment group.

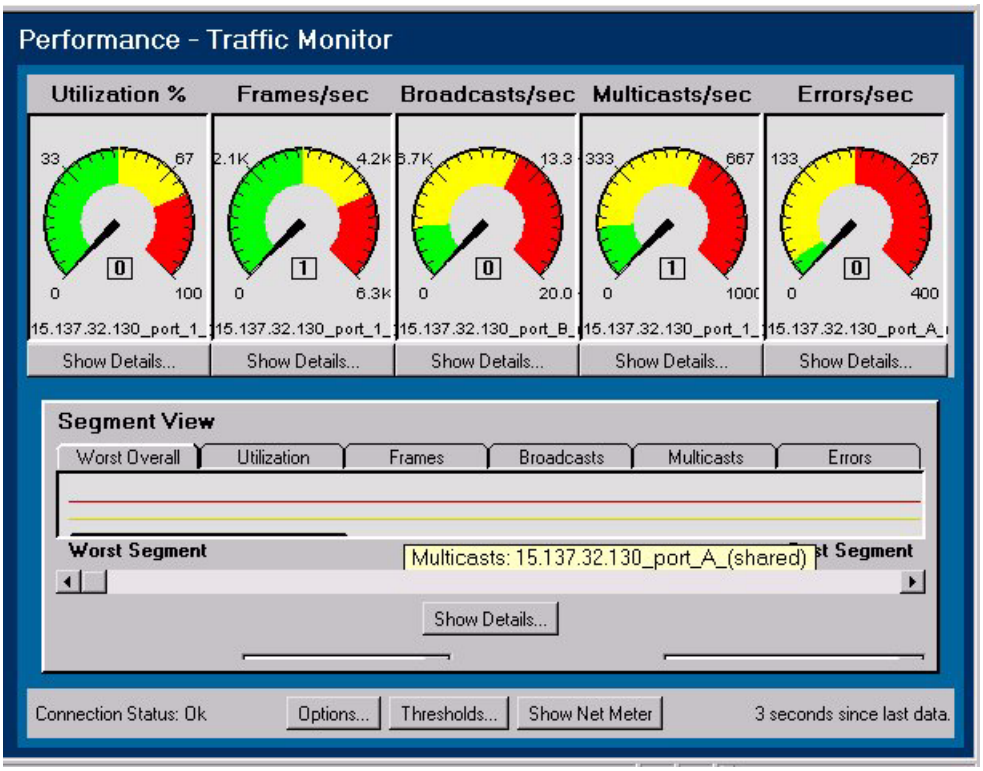


Figure 9-1. Traffic Monitor Main Page

The five statistical attributes sampled by Traffic Monitor are:

Utilization%: Represents the traffic on the selected network or segment as a percentage of a segment's bandwidth (based on the theoretical maximum for the type of connection) which is currently being utilized. Monitoring the utilization gives a measure of how much of the network capacity is being used on a particular segment. For example, if you are examining a 10 Mbps or a 100 Mbps segment, utilization can tell you how much of the 10 Mbps or 100 Mbps segment's bandwidth (in percentage such as 20%, 35%, 50%, etc.) is being used by the devices on the segment.

Frames/sec: Represents the number of frames per second being transmitted over the network or segment. Each protocol (such as Ethernet, IP, IPX, etc.) has a different frame or packet specification.

Broadcasts/sec: Represents the number of broadcast packets being transmitted over the network or segment per second. Broadcast packets are addressed to, and must be processed by, all nodes on the network. This indicator gives an estimation of the amount of bulk communications taking place over the network. In general, this type of activity should be kept to a minimum as point-to-point messages use bandwidth much more efficiently.

Multicasts/sec: Represents the number of multicast packets being transmitted per second over the network or segment. Multicast packets are special forms of broadcast packets where copies of the packets are delivered to a subset of all devices on the network. This indicator gives an estimation of the amount of bulk communications which are taking place over the network. As with broadcast packets, this type of activity should be kept to a minimum as unicast messages use bandwidth much more efficiently.

Errors/sec: Represents the number of errors that have occurred for the network or segment. The number of errors can help you determine whether the network is functioning properly.

Reading the Traffic Information Gauges

The gauges display the network traffic information for the current minute. The colors on the gauges are:

- green: value for the attribute is within the normal range
- yellow: value has exceeded the normal range, but is not critical
- red: value is in the critical range. Corrective action may be needed.
- blue inner band: The “high water mark”, which shows you the highest value for that segment in the last hour. This indicator can help you determine if there are any transient or intermittent problems for the segment, even though the current minute indicator shows normal activity.

The amount of green, yellow and red displayed in each gauge corresponds to the threshold settings for that segment. For example, if Segment A is a 10Base-T segment, and the current Threshold settings for Utilization% are as follows,

green: OK, 0-50% utilization

yellow: warning, 51-75% utilization

red: critical, 76-100% utilization

then the gauge for Utilization% for Segment A would display a green area up to 50%, a yellow area from 51% to 75%, and a red area from 76% to 100%. Click on the **Thresholds** button to set segment thresholds.

The number in the rectangular box below the gauge indicates the attribute value for the current minute.

Reading the Segment Histogram

Each bar in the histogram represents a segment. The segments are displayed left to right in worst to best order, the worst segment being the one with traffic that most exceeds any threshold value for that segment. If there are more than 30 segments to be displayed, a scroll bar will allow you to scroll horizontally in order to view all the segments.

The six tabs across the top of the histogram display the values for the segments for the selected segment group, or for the entire network if "All Segments" is selected in the Segment Groups list box. The Worst Overall tab displays in sorted order left to right the segments that have the most problems in the selected segment group. For example, if the histogram displays 10 segments in red, this indicates that these segments have exceeded at least one of the thresholds set for them. For one segment that might be the Errors threshold, for another it might be the Utilization% threshold. Holding the mouse over the segment bar will display a tool tip with the segment name and the measurement represented, for example, "Utilization: Shared Segment 001".

Clicking on the segment bar highlights that segment and displays it in the Selected Segment list box. If you have checked the "Link gauges to selected segment in histogram" check box (located in the Options button), the gauges change to reflect the attribute values for that segment.

Comparing Segments Across Different Medias

The yellow warning threshold line and the red critical threshold line are displayed across the histogram at the same level for all segments. Because the actual threshold values for various types of media are different, the segment bar heights are "normalized" to the threshold lines so that they can be compared visually. For example, if Segment A is a 10Base-T segment, its warning threshold for Frames/sec might be 3,000 frames/sec. For Segment B, a 100Base-T segment, the warning threshold for Frames/sec might be 30,000 frames/sec. In order to make a comparison, the height of the segment bar is a percentage above a threshold value, for example, 50% over the warning threshold. Both segments can have the same percentage above the warning threshold settings even though the actual value of Frames/sec is different for each segment.

Selecting Segment Groups and Segments

To display the segments for a specific segment group, select the segment group from the **Segment Groups** drop-down list at the bottom of the Traffic Monitor page. The segments for that subnet will be listed in the **Selected Segment** list box.

If you want to see the gauges reflect the values of attributes for a particular segment, click on **Options** and check **Link Gauges to selected segment in histogram**.

Setting Thresholds

When you click on **Thresholds** at the bottom of the Traffic Monitor page, a separate Thresholds browser window appears. A set of default thresholds is provided for each network attribute and is specific to a segment and its type. The values shown for the Ethernet tab are for a media speed of 10 Mbps. If your Ethernet is 100 Mbps or Gigabit, or if the segments are trunked, the threshold values are adjusted automatically. The thresholds for other types are also adjusted automatically when appropriate, for example, if the

segments are trunked. This will not be visible in the Thresholds window. For example, if four ports on a switch are trunked, a 10 Mbps Ethernet segment would now be four times as fast, or 40 Mbps. The threshold values are adjusted automatically to be appropriate for this speed. You can still set the threshold values for a specific segment by selecting that segment from the list in the Segments tab.

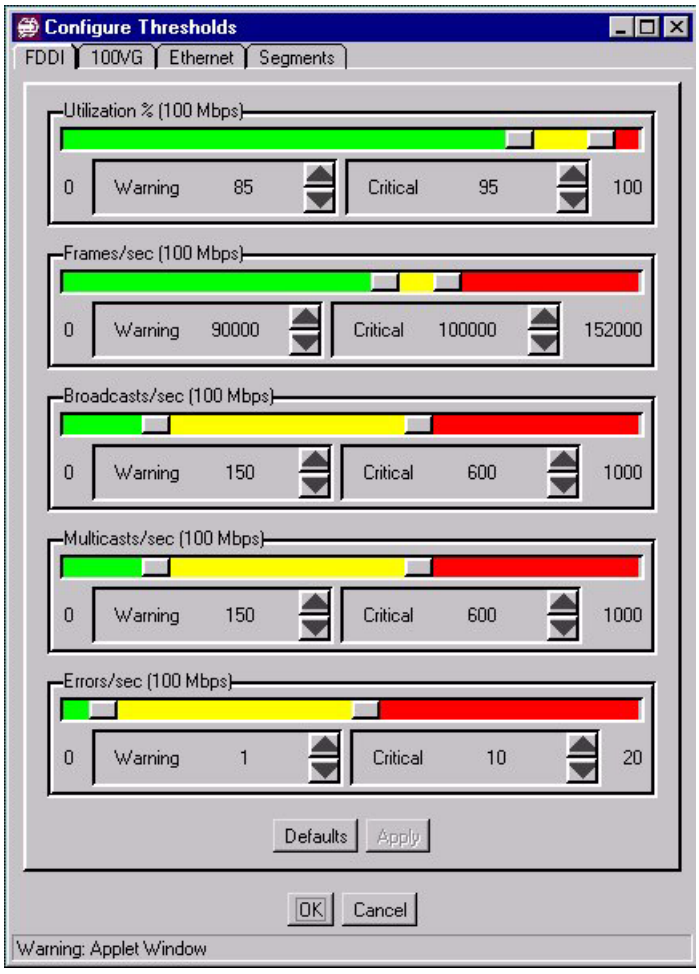


Figure 9-2. Thresholds Window

As a network attribute reaches a certain threshold, a corresponding color (either green, yellow, or red) is used to indicate the current state (normal, warning, or critical, respectively.) Changing the threshold ranges to better represent your network's normal activity will be a relative decision. For example, a normal threshold range for traffic utilization will vary from network to network, and segment to segment. It is recommended that you use the default threshold values first and adjust them to fit the traffic patterns on your network. By fine tuning the threshold levels, you can find the optimum operating conditions for each segment on your network, which makes it easier to see problems as they occur.

To change your threshold settings, select a network type such as Ethernet. The threshold values for the attributes for Ethernet segments are displayed. You can either move the sliders to the left or right to increase or decrease a threshold value, or click on the up/down controls underneath the sliders to fine tune the threshold values. As you move the sliders, these values will change accordingly. To save your changes, click on **Apply** at the bottom of the Threshold window. The changes are applied to all segments of that type, for example, all Ethernet segments. When you are finished making changes, click on **OK** to exit the window.

Note

If you click on **OK**, any changes that you have made and not yet applied will be applied. If you click on **Cancel**, any changes that haven't been applied are not applied. If you have applied changes before clicking on **Cancel**, those changes remain applied.

If you want to change the thresholds for a single segment, select the **Segments** tab at the top of the window. Select a segment from the list box. The Thresholds window now reflects the attribute threshold values for that segment. Click on **Apply** to save any changes.

Note

If you select a different segment from the list box before you have applied your changes, a message will appear asking you if you want to apply your changes.

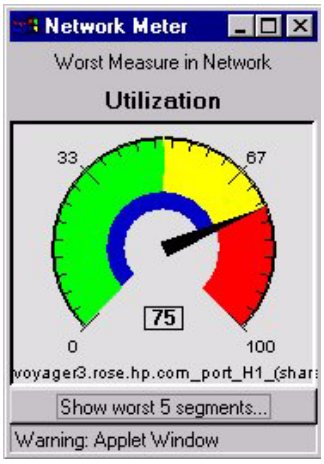
Initially, default values are in effect for all segment types. The **Defaults** button returns the threshold values for that segment or segment speed to the original default values.

Note

Traffic Monitor will send a trap to the configured trap receivers when a threshold has been exceeded. The Traffic Monitor page does not need to be open for Thresholds traps to be sent.

Displaying the Network Meter

The Network Meter provides an “at-a-glance” look at the most severe traffic problem on the network being monitored during the current minute. To launch the Network Meter, click on the **Net Meter** button below the histogram on the Traffic Monitor page. Clicking on the **Show Worst 5 Segments** button displays a window showing the top five thresholds that have been exceeded and the associated segments.



You can keep the Network Meter window anywhere on your PC desktop. It will continue to monitor the status of your network while you use your browser for other tasks. Click on **Hide Net Meter** to close the window. When you close your browser, the Network Meter will also close.

Options Button

Clicking on the **Options** button at the bottom of the Traffic Monitor page displays the **Link Gauges to selected segment in histogram** check box. Clicking on this check box causes the gauges in the Traffic Monitor page to display statistics for the segment that you have selected in the histogram.

Note

You may see the Network Meter needle indicating a warning or critical situation when the gauges in the Traffic Monitor page do not. The Network Meter displays the worst measurement for any segment in the network, but the gauges in the Traffic Monitor page display the traffic for the segment or groups of segments that you have selected. If you select **All Segments** and the segments are not linked to the gauges (Options), the Network Meter and the gauges will reflect the same conditions.

Who Are the Top 5 Talkers?

The Top5 View helps answer the question, “Who is causing the problem (who are the top talkers) on the segment?” by displaying a graph identifying the top five nodes causing the network activity on the segment for the selected minute. Click on the **Show Details** button below the gauges or at the bottom of the page to display the Top5 View window.

Note

If the segment has no devices that are sampling-capable, the Show Details button below the gauges is grayed out. You can select the segment in the histogram, then click the Show Details button at the bottom of the page to launch the Top5 view, but the only data displayed is “Other”.

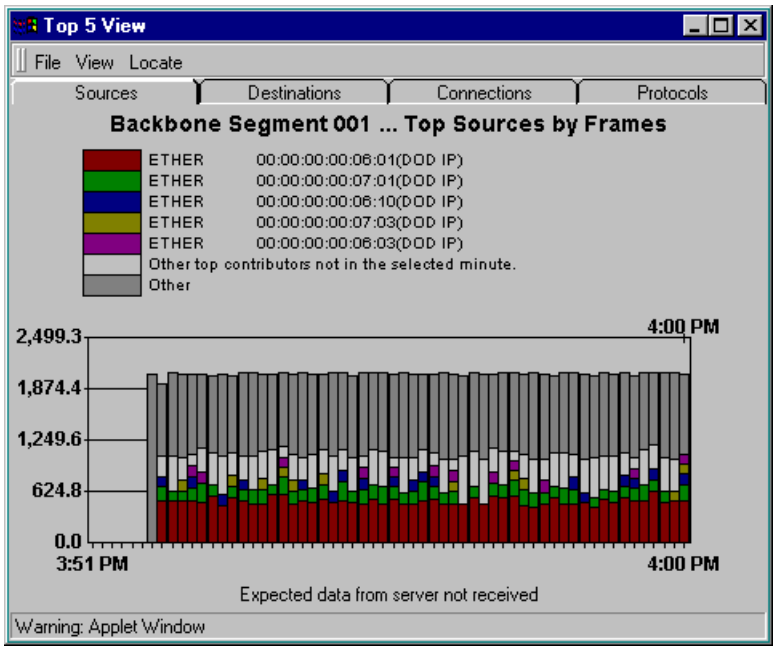


Figure 9-3. Top 5 Talkers

You can display graphs for each of the measured attributes showing:

- Top Sources (default)
- Top Destinations
- Top Connections
- Top Protocols

More than one graph can be displayed at a time, so you can look at the values for multiple attributes for each segment.

Since Traffic Monitor presents real-time information, the data will be "moving" on your graph. Data is graphed and updated every minute. The Top5 View displays up to 60 data points, that is, you can view the most recent hour of activity.

The right-most bar in the graph represents (up to) the top five nodes for the latest minute graphed. This bar is selected by default and is indicated with a black "tick" and the time sampled above it. The color-coded stacked bars represent the activity for up to the top five nodes and "other" nodes for the selected attribute and segment. The non-selected bars in the graph show how these top talkers have behaved over the past hour. This lets you view trends over the last hour for the five top talkers of the selected minute.

The yellow and the red horizontal lines on the background of the graph represent the warning and critical values, respectively, for the selected segment. These lines only appear when the graph scale is high enough.

The colors are in the same order as they appear in the legend, that is, the node with the greatest activity is represented by the color at the bottom of the stacked bar. The white portion of the stacked bar represents the top talkers in minutes who are not top talkers in the selected minute; the dark gray portion of the stacked bar represents all other activity. You can visually trace the same color across the graph to see trends of activity over the past hour.

Information for the top five colors in the legend identifies the source and destination nodes of the top five connections for every data point on the graph. The information in the color legend will change as the data points are graphed. Depending on the parameters you have selected, the information provided by the legend can include:

- The layer 3 or layer 2 (MAC) address
- The network protocol or service being used. The highest network protocol for the communication path is displayed.
- The direction of data flow (the source and destination nodes)

Here is an example of information that you might see in the legend:

ETHER 00:00:10:44:36:12 (DOD IP)

The first item displayed (ETHER) is the highest (in the network stack) decoded network protocol used for this destination. The number to the right (00:00:10:44:36:12) is the IP address of the destination. The last item displayed in parentheses (DOD IP) is the network service this source node is using to communicate in this network connection. If the network service is a well-known service such as telnet or ftp, then the service name appears inside the parentheses. If the network service is not well-known, then its socket number is displayed in the parentheses.

Other Top Talkers Not in Selected Minute

You may get more information from the Top5 View by clicking on a stacked bar that contains a white stack. The white stack represents the top talkers that occurred in a minute other than the selected minute. For example, if the selected minute is 2:01, but you notice that there is a tall bar with a large white portion that occurred at 1:30, you can click on the 1:30 bar to see who the top talkers were during that minute. The stacked bar and the legend change to represent the top talkers that occurred at 1:30.

Note

If your graph is displaying stacked bars with large portions of white, it is possible that the selected minute is not displaying the most active nodes.

Others

The dark gray portion of the stacked bar represents a summation of all of the other activity that occurred during that minute. There is no additional information contained in this portion of the bar. It can be a useful indicator of an overloaded network when what you see on the graph is large areas of dark gray with no particular user causing a problem.

If your graph displays large portions of gray, selecting another parameter, such as “Top Destinations”, may show different results. For example, if a large number of nodes begin backing up to a single server, displaying the Top Destinations graph would show the server as the “top talker”.

Note

If your graph is only displaying “Other” data, there may be a problem with the data sampler for this segment.

Top5 View Menu Items

The Top5 View has three menu selections. The functions of each are described in the following table.

Table 9-1. Functions of the Top5 Menu

Menu Item	Function
File	Close: Closes the Top5 View window
View	Displays a new graph for each attribute: • Utilization% • Frames/sec • Broadcasts/sec • Multicasts/sec
Locate	• Locate End Node: Opens the Locate End Node dialog box. • Locate Segment: Opens a topology map with the selected segment highlighted.

Locating A Segment or End Node

The Locate menu item lets you select a specific node or segment. Select an end node or segment from the list or enter the IP address of the node you want to locate.

The located end node or segment will be highlighted in royal blue in the topology map.

Traffic Data Collector Settings

Starting with HP TopTools for Hubs & Switches version 5, you can collect data from all segments in your network automatically, or collect data from selected ports of a device (manual mode). With manual selection, you can also choose the type of data to be collected, for example, Extended RMON (X-RMON) data or just traffic data.

Setting the Traffic Data Collector to manual mode is advantageous if you have a large network and don't want to monitor every segment. You don't have to wait for a lengthy Topology process to complete in manual mode; you can configure the specific segments you want to monitor, up to a total of 2000 segments.

To access the Traffic Data Collector Configuration, click on the **Performance** button in the navigation frame. Select **Traffic Data Collector Settings** from the menu. The Performance - Traffic Data Collector Settings page appears with the **Configuration** tab displayed.

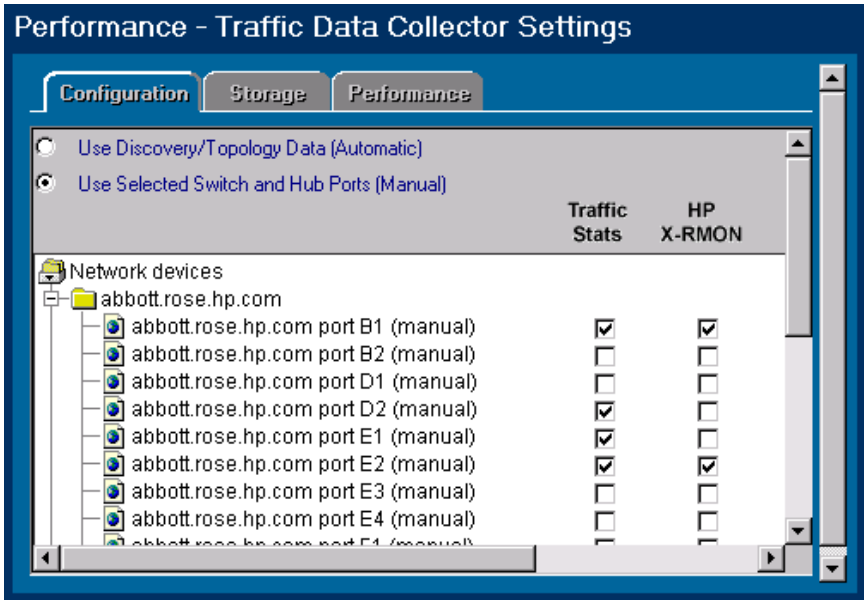


Figure 9-4. Traffic Data Collector Configuration Page

Nothing is displayed in the Traffic Data Manual Configuration table if **Use Discovery/Topology Data (Automatic)** is checked.

Automatic Monitoring

If you want to enable Automatic monitoring, check the radio button labeled **Use Discovery/Topology Data (Automatic)**. The Traffic Data Manual Configuration table will be removed and manual selection disabled. The Traffic Data Collector automatically restarts and retrieves the segments to be monitored from the information gathered during the Topology process.

Manual Monitoring

To use Traffic Data Collector in manual mode, check the radio button labeled **Use Selected Switch and Hub Ports (Manual)**. The Traffic Data Collector automatically restarts and retrieves the segments to monitor from a topology-independent database. The retrieved segments are displayed in the Traffic Data Manual Configuration table.

Begin adding devices to the table by clicking on the **Add Devices** button at the bottom of the page.

Adding Ports for Manual Monitoring

When you select the **Add Devices** button, the Add Devices dialog box displays a list of devices that are not being monitored. This list is comprised of devices discovered during the Discovery process and any devices added manually (Settings -> Discovery -> Additional Devices). Discovery (but not Topology) must have run before any devices can be added.

Click on the device(s) you want monitored, then click on the **Add** button. The device will be added to the Traffic Data Manual Configuration table in the Configuration page, represented by a folder. Double-clicking on the folder displays the ports for that device.

After selecting the devices to add, click on the **Restart Collector** button. The Traffic Data Collector restarts with these devices.

Configuring Ports for Manual Monitoring

There are two check boxes for each port of a manually monitored device. They are:

- Traffic Stats—The MIB-II SNMP counters (how much traffic is on the network), and any RMON counters supported by that device.
- HP X-RMON—The RMON data that allows you to see who is talking to whom on the network.

You can check the Traffic Stats box for any port. Only HP devices support the monitoring of X-RMON statistics. If you check the X-RMON box for a port, the Traffic Stats box for that port is automatically checked as well. Even if X-RMON data cannot be collected for some reason, traffic statistics will be collected.

After selecting the ports to monitor, click on the **Restart Collector** button. The Traffic Data Collector restarts with the new information.

Removing Selected Devices

To remove devices from the table, click on the **Remove Device(s)** button at the bottom of the Configuration page. The Remove Device dialog box displays a list of devices currently being monitored. Select the device(s) to be removed, then click on the **Remove** button. Data is no longer collected from these devices, and they are removed from the Traffic Data Manual Configuration table.

After selecting the devices to remove, click on the **Restart Collector** button. The Traffic Data Collector restarts without these devices.

Remove All Devices

To remove all devices from the table, click on the **Remove All Devices** button at the bottom of the page. All devices are removed from the Traffic Data Manual Configuration table.

Traffic Data Storage

You can specify some criteria to control how much data is collected. Select **Traffic Data Collector Settings** from the **Performance** button in the navigation frame, then select the **Storage** tab. Your current settings are displayed in the **Current Storage Status on Server** area. The **Historic Traffic Data** collection area displays the following choices:

- Storing data up to a maximum number of days of data or a maximum amount of data, whichever occurs first. The default is 31 days, up to 100 MB. You can click the **Default Values** button to set these values.
- Storing data up to a maximum amount of data (in Megabytes).
- Stopping collection of historical traffic data for analysis by the Network Performance Advisor.

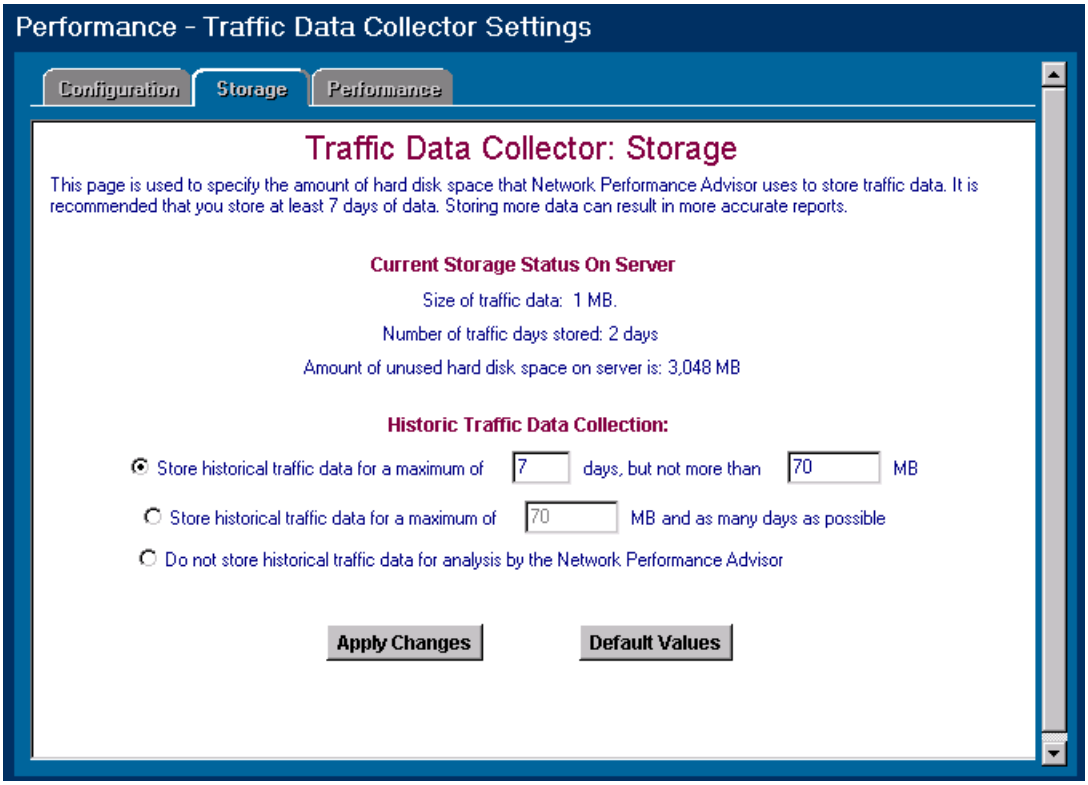


Figure 9-5. The Traffic Data Collector - Storage Settings Page

Note

To stop data collection, you must stop all of the HP TopTools services. Click on the **Settings** tab in the navigation frame and select **TopTools Services**. On the Services page click on the **Stop Services** button.

Traffic Data Collector Performance

You can specify the amount of system resources that the data collector can use. A more detailed network analysis requires more availability of system resources. The selections are:

- High Resource Availability—Recommended for systems dedicated to network management.
- Medium Resource Availability—Recommended for systems that run other less performance-sensitive applications.
- Low Resource Availability—Recommended for systems that run performance-sensitive applications.

Note

If system resource availability is set too low, some EASE segments will be dropped from monitoring. This could affect the data available for the Top 5 view of traffic as well as the accuracy of Network Advisor reports. Traffic statistics are always monitored.

Note

You cannot specify the availability of system resources when you are in manual mode. The **Apply changes** button will be grayed out.

Until you select one of the above settings and click on the **Apply** button, the resources dedicated to the Traffic Data Collector are assigned by HP TopTools.

To access this page, select the **Performance** button in the HP TopTools navigation frame, then select **Traffic Data Collector Settings.** The Configuration page displays. Select the **Performance** tab.

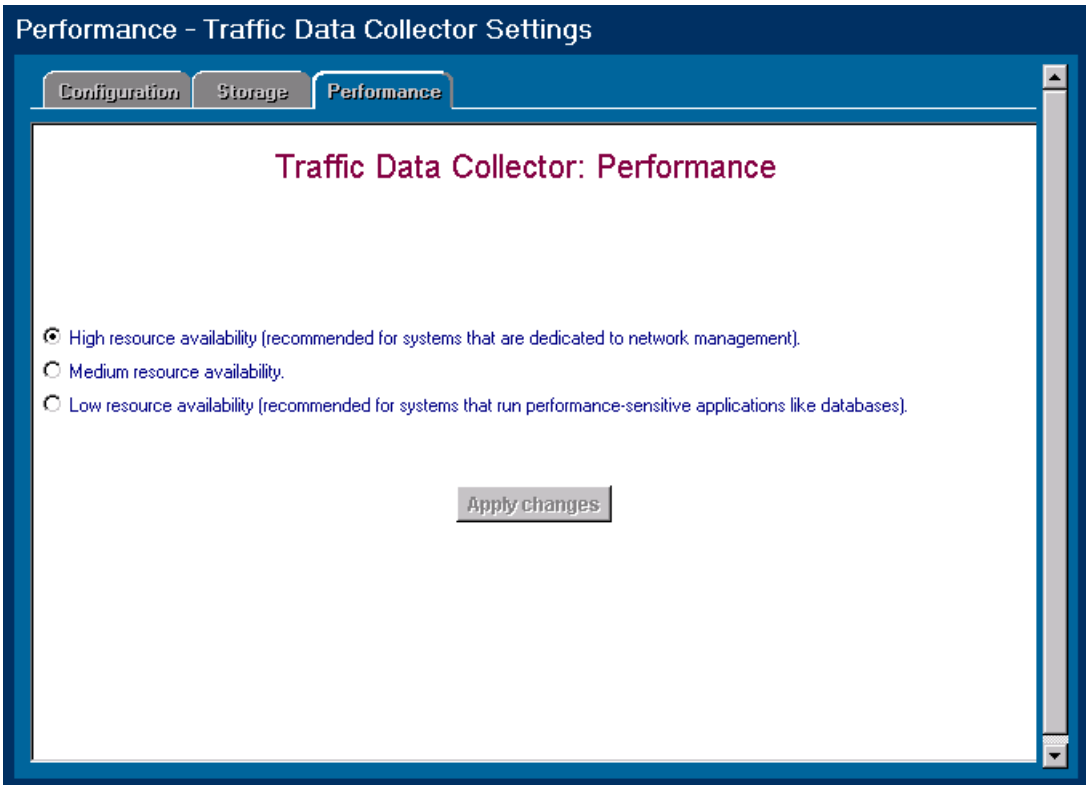


Figure 9-6. Traffic Data Collector - Performance Page

The data collector must examine your management station's capabilities to determine what is appropriate for the resource setting that you select. The capabilities test begins when you click on the **Apply changes** button. You will see a screen listing some statistics about the test. Data collection will stop during the test, and your management station may run slowly When the test is complete (approximately four minutes), your resource settings will be in effect.

Troubleshooting Traffic Monitor

There may be times when your Traffic Monitor gauges are not registering any data (you see no gauge needles), or one or more segments in the histogram may go gray. Some of the reasons this may occur are:

- No Known Segments—If there are no known segments for the selected network, the gauges will not have needles or threshold indicator colors. The Selected Segment list box will be empty.
- Data Not Current—If the data is not current, the gauges will not have needles, the attribute values are grayed out, and the segment bars in the histogram are shades of gray. Darker shades of gray indicate more serious problems with that segment.

- Too Little Traffic on Network—If your network is carrying very little traffic at this time, the gauges will not indicate any traffic.
- One Segment is Gray—There may be a problem with this particular segment. The data sampler may not be working, there may not be enough traffic on that segment, or a device may have been disconnected from that segment.
- Machine is Very Busy—The CPU may not be able to process the data because it is too busy.

Connection to Server Lost

If you see a message in the Traffic Monitor page stating that the connection to the server is lost, you can try the following:

- Check the server to see if it is still running.
- Verify that the Data Collector is running. Go to the HP TopTools home page and select **Settings - TopTools Services**.
- Click on the browser **Refresh** button, or use **Ctrl-Refresh** to have the browser reload the applet.
- Close the browser and reopen it.

10

Planning for Network Growth

This chapter includes the following topics:

Meeting the Challenges

The rapid increase in the number and size of networks has created new challenges in network administration. Companies depend on efficiently functioning networks to stay competitive, maintain productivity, and control costs. Network administrators must perform network optimization activities to use the available bandwidth efficiently and maintain acceptable response times for the users. Additionally, network administrators must meet the conflicting demands of providing continuous network operation and planning for long-term growth and advances in technology.

Most network administrators manage networks that have grown over time, using the technologies that were available. As networks grow, problems also increase. The feedback mechanism to the administrator is an irate phone call. Few planning processes exist, often because administrators do not have the time or the expertise required to plan for network growth.

Network administrators must be able to take some proactive steps to improve the performance of the network or they will have networks characterized by congestion and unavailability to users. Planning, optimization, and having the tools to effect changes quickly are vital as the network grows.

Using Network Tools

Current network analysis tools provide data about network activity in tabular or graphic form that must be laboriously analyzed and interpreted by a knowledgeable system administrator. This approach is time-consuming and does not provide the proactive analysis that allows for future planning. System administrators require tools that analyze data and present it in an easily understood format. The data must help the administrator prioritize the network problems and suggest solutions, as well as allowing him or her to anticipate possible future problems.

Network planning and optimization tools must be accurate and cost-effective. The impact on network usage should be minimal. The tool must collect the correct data efficiently and provide intelligent analysis of the data to the administrator.

Planning with the Network Performance Advisor

One of the major challenges facing network administrators is the increasing amount of traffic on the network. It is important to manage the available bandwidth as efficiently as possible. The HP TopTools Network Performance Advisor is an intuitive, intelligent interpretation tool that provides you with information about the entire network. The Advisor performs automatic traffic analysis and displays the results in easy-to-understand tables and charts. The reports created by the Advisor make useful recommendations on how to improve network performance. The Advisor also provides an **inventory report** about the end nodes for each segment in the network (excludes hubs, switches and routers). The analysis and data provided by the Advisor assists the system consultant in making a sound business case for changes to the network.

The Network Performance Advisor creates reports that make recommendations about reducing utilization on the network segments to increase network performance. The Advisor provides proactive analysis of a network, in contrast to the real-time, reactive analysis provided by Traffic Monitor.

The Network Performance Advisor makes its recommendations by analyzing the network monitored by HP TopTools. There are two planning reports:

- *Reorganize Your Current Equipment Report*—suggests ways to improve network performance by rearranging the existing nodes.
- *Add or Upgrade Equipment Report*—suggests ways to improve performance by dividing segments or upgrading segments with a switch. It will also tell you if you have any nodes that need to be on a dedicated segment.

Advisor can also include the following information in the reports:

- Show **Top Conversations** per segment- creates a list of the Top Conversations for each segment during the time period selected

- Include **Inventory** in Report—creates a listing of your end nodes by segment.

Use the **Modify Report Settings** page in the **How to Improve Performance** tab.

The reports are HTML documents and must be viewed with a frames-capable browser such as Microsoft Internet Explorer (MSIE) 4.01 or later. For information on how to interpret the display, see "How to Interpret this Report" in each report's Table of Contents.

Starting the Network Performance Advisor

You can start the Network Performance Advisor by clicking on the **Network Performance Advisor** button in the HP TopTools home page. The Welcome page provides you with a brief description of the purpose of the two reports. Click on the **How to Improve Performance** tab to begin creating a report.

Note

If no historical data is available, a report cannot be generated. Selecting the **How to Improve Performance** tab in this situation displays an error message and all buttons are grayed out.

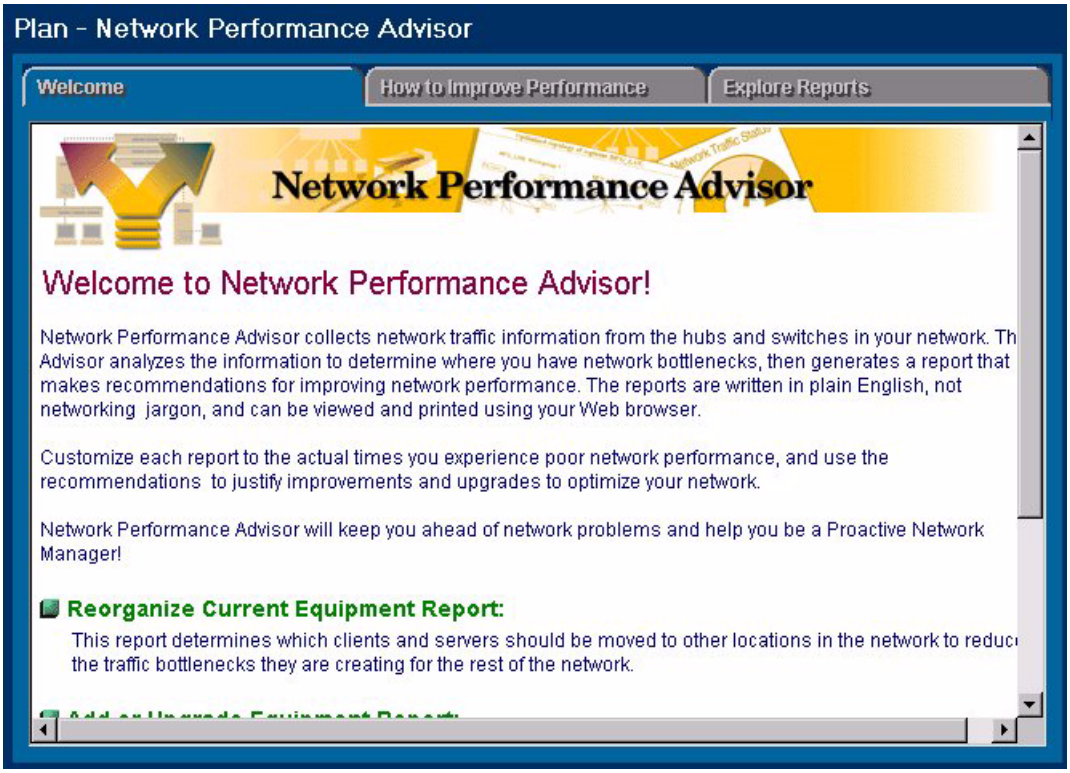


Figure 10-1. Welcome Page for Network Performance Advisor

Creating a New Report

Start creating your report by selecting the type of report you would like. Enter a name for your report or accept the default name.

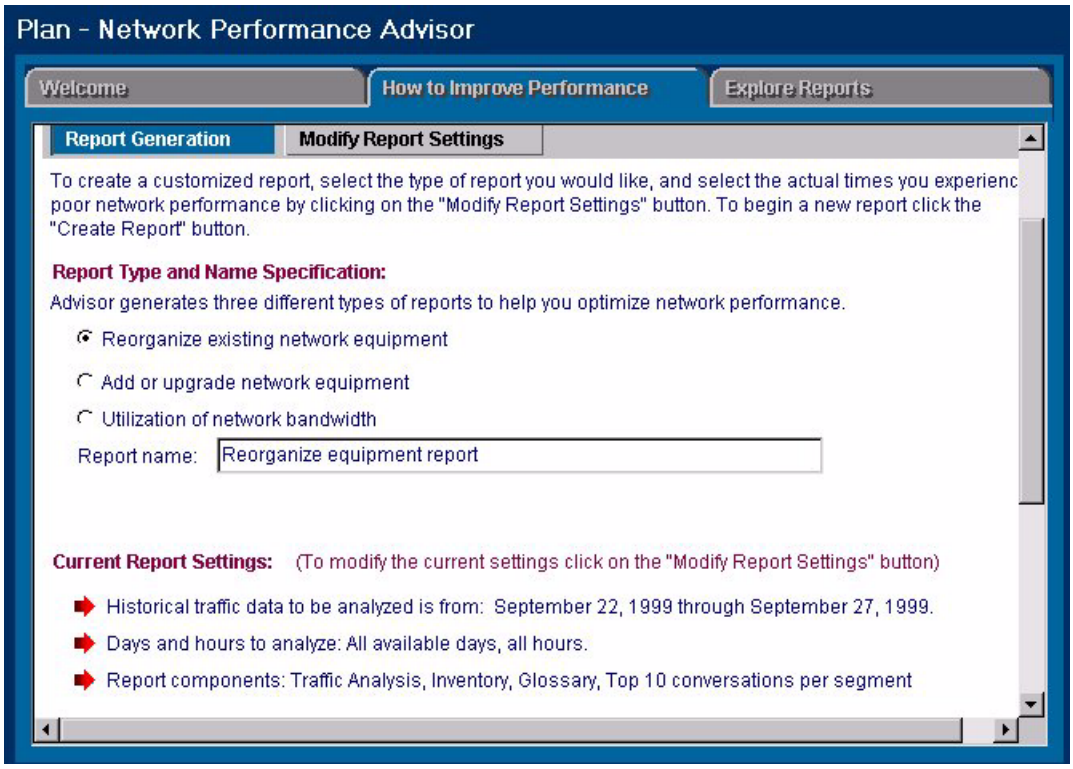


Figure 10-2. Report Generation Page of Network Performance Advisor

The page will display your current report settings. If you would like to change your settings, click on the **Modify Report Settings** tab.If you are happy with your settings, click on the **Create Report** button at the bottom of the Report Generation page to start your report.

Modifying Your Settings

Select the **Modify Report Settings** button to enter the date and time parameters for a report.

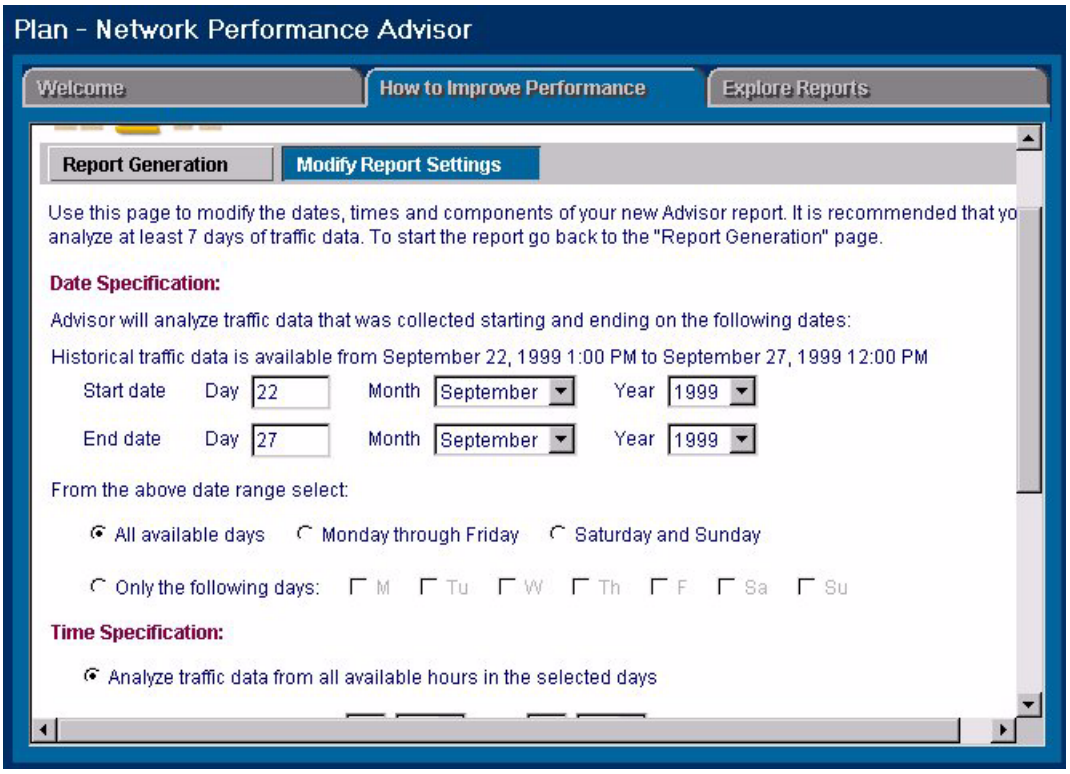


Figure 10-3. Modify Report Setting Page

If you select a report period that has no available historical data, an error message appears during report execution. There must be at least 1 hour of historical traffic data available. Try changing your criteria to generate a report.

Note

Choose periods of time that represent the type of network utilization you wish to analyze, for example, only Monday through Friday. Acting on recommendations made for a data sampling period of atypical network usage could worsen network performance during periods of normal use.

When you are finished with your selections, click on the **Generate Report** button to go back to the Report Generation page. At the bottom of this page, click the **Create Report** button. The report will begin generating. Statistics about the report, such as the percent completed and time elapsed, will display on the page.

You can only create one report at a time.

To cancel a report, click on the **Cancel analysis** button.

The new report displays automatically when it is completed. If there aren't enough hours of historical data in the selected time period to successfully generate a report, or if there is insufficient disk space or memory, an error

message stating the problem displays during report generation. When the report completes successfully, information about the report execution, including any errors that occurred, is displayed in the Summary page of the report.

Viewing a Report

To view a report, click on the **Explore Reports** tab and select a report from the list. The reports are listed chronologically with the most recent report at the top of the list. New reports that have not been read have a **New** icon next to them. Each report displays in its own browser window, so you can look at more than one report at a time.

The button functions are:

- View Report—To view the selected report click on the **View Report** tab at the bottom of the page.
- Rename Report—Select the **Rename report** button to choose a new name for the selected report.
- Delete report—To delete the selected report, select the **Delete report** button. The report will be erased from the disk.

Note

If you rename a report after viewing it, then view the report again, the report name is not updated if caching is enabled on your browser. This is because you are seeing the old, cached version of the report. Use **Ctrl-Refresh** to load a new copy of the report.

Report Properties Section

The Report Properties section lists the values for several characteristics of the report. Report properties can be viewed for completed reports by selecting the report, then clicking on **Report Properties** in the Table of Contents.

The report characteristics are described in the following table.

Characteristic	Description
Name	The user-defined name of the report.
Number of Recommendations	The number of recommendations produced by this report for possible network changes.
Data Availability	Provides a measure of how much data was available during the time period specified for the Network Performance Advisor to analyze. For example, if you selected a Time Spanned of 9/1/96 through 9/14/96, the actual data available to the Network Performance Advisor might be 92% of the total hours for the Time Spanned.
Number of Hours Requested	The time span in hours requested for the report.

Characteristic	Description
Number of Requested Hours with Data Available	The actual number of hours that have data available. This is used with the Number of Hours Requested to obtain the Data Availability. For example, if you requested 10 hours of data, but two of the hours in the time period requested had no data, the Data Availability would be 80%.
Networks Analyzed	Data was collected by HP TopTools for the networks listed here.
Time Spanned	The data being reported on was collected during this time period (non-inclusive, for example, a time period of 1 p.m. to 5 p.m. would include data through 4:59 p.m.).
Days Included	You can choose to only report on data collected on weekdays, the entire week, weekend, or a "custom" set of days during the week.
Hours Included	You can choose to only report on data collected during selected hours. For example, you may only want to include data collected during the busiest hours of the day.
Time Initiated	The time the report began running.
Time Completed	The time the report completed.
Report Size	The total size (in kilobytes) of the report.

Summary of Recommendations Section

The Summary of Recommendations section of the report lists in tabular form the recommendations for network changes without any supporting detail. The format for the *Reorganize Your Current Equipment Report* is:

- Move node A from Segment 1 to Segment 2

The formats for the *Add or Upgrade Equipment Report* are:

- Divide Segment 1 into the New Workgroups listed. The bandwidth required for the workgroups and the nodes comprising the workgroups are also listed.
- Convert Segment 1 to a desktop switch, listing those nodes that require 10 Mbps ports and those that require 100Mbps ports.
- Dedicating bandwidth to a "top talker" by moving the top talker to a dedicated 10 Mbps or 100 Mbps segment.
- Upgrade Segment 1 to a faster speed shared media.

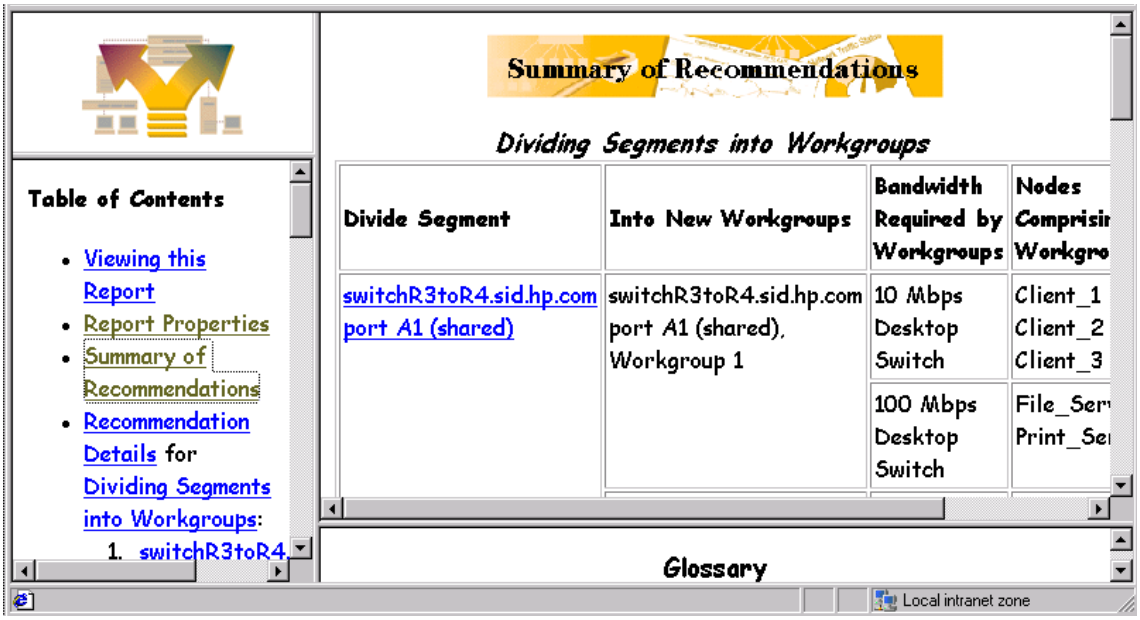


Figure 10-4. Summary Report

A priority of low, medium or high is given to help you determine the urgency of each recommendation. The priorities are defined as follows:

- **Low**: Implementing this recommendation will result in a small reduction in network utilization. A low priority recommendation may be regarded as advance warning of a marginal condition on the network. These conditions often evolve into situations that produce medium or high priority recommendations in future reports.
- **Medium**: Implementing this recommendation will result in a measurable reduction in network utilization.
- **High**: Implementing this recommendation will result in a significant reduction in overall network utilization.

The Summary page may also provide explanations when no recommendations are made. Possible reasons for no recommendations are:

- The network is already optimized.
- An error condition occurred because of bad data.

Reorganize Your Current Equipment

The report titled *Reorganize Your Current Equipment* makes recommendations about which nodes you can move to another location in the network in order to reduce the amount of traffic forwarded through network devices such as bridges, switches and routers.

Recommendation Details Section

The Recommendation Details section of the report supplies the supporting information for the recommendations made by the Network Performance Advisor. It includes a textual explanation and the "before" and "after" graphical representations of the affected network. The recommendations are in priority order, starting with High Priority.

A "before" representation of the network might look like the following figure:

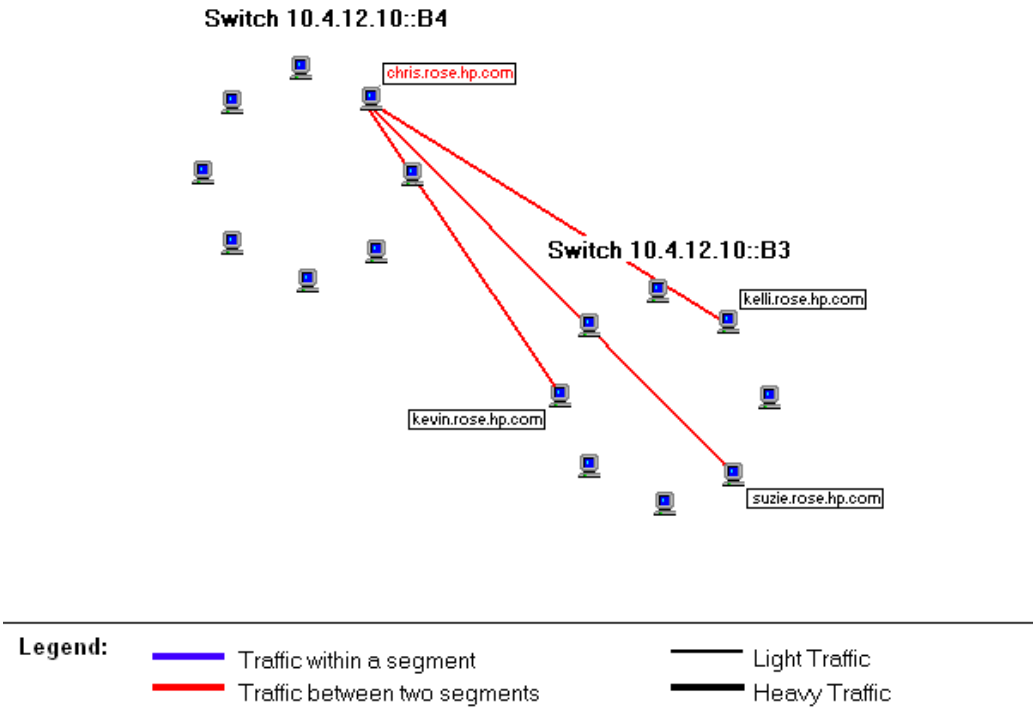


Figure 10-5. The traffic pattern before implementing reorganization recommendations

In this situation, the node **chris.rose.hp.com** communicates most frequently with nodes on another segment. Network utilization can be improved by moving **chris.rose.hp.com** to the switch segment **10.4.12.10::B3**. This is a High Priority recommendation because it will significantly decrease network utilization for switch segment **10.4.12.10::B4**.

The "after" representation would look like the following figure:

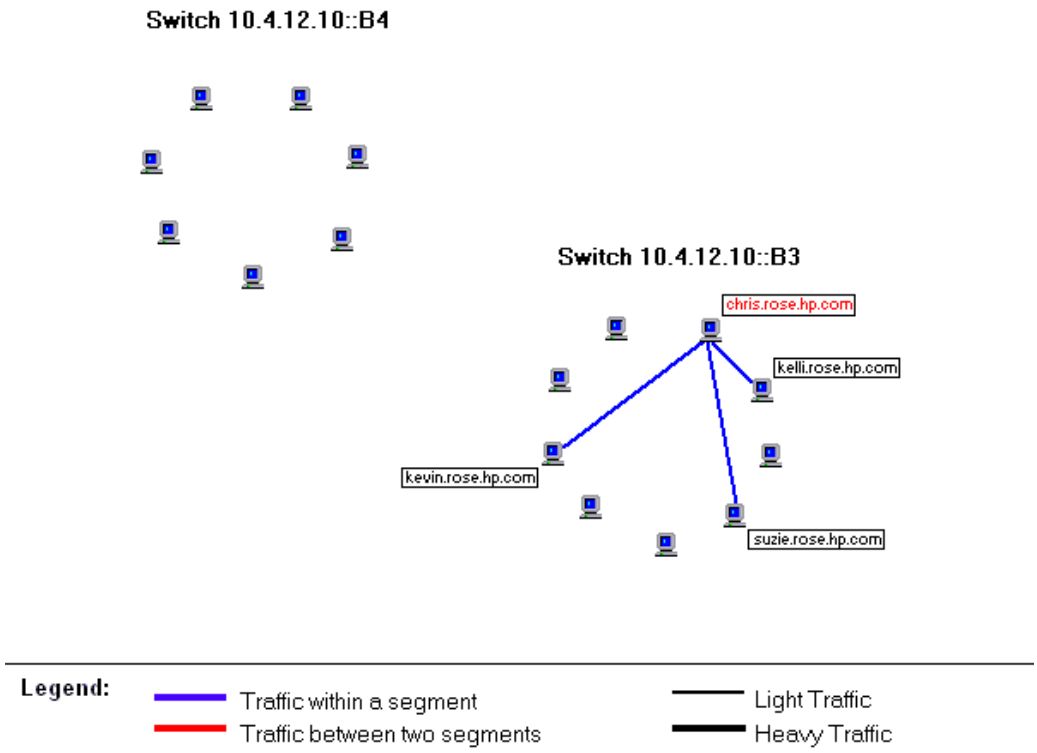


Figure 10-6. The traffic pattern after implementing reorganization recommendations

The network utilization for switch segment **10.4.12.10::B4** is reduced. The network utilization on switch segment **10.4.12.10::B3** is unchanged.

It is recommended that you run this type of report before the *Add or Upgrade Equipment* report to obtain recommendations for reorganizing your existing equipment.

Note

If you move a node to a segment that has a different subnet address, you need to change the IP address of the node so that its subnet address is the same as the subnet address of the destination segment.

Note

If you are moving a node that is a member of a VLAN, and your VLANs are configured by MAC address, you do not need to change any addresses. If your VLAN is configured by port and you move a node from one port to another,

you must decide if you want the new port to be a member of the VLAN if it isn't already. For example, if a node is on Port 1 in VLAN A, and you move the node to Port 6, you may want to include Port 6 in VLAN A.

How the Data is Analyzed

The Network Performance Advisor analyzes historical traffic data for the time period specified to determine which nodes on the network converse. These nodes then are examined to determine if they have conversed frequently with nodes on other segments. The Network Performance Advisor will recommend moving a node to a different segment if: it is not on a desktop switch and the move will reduce network traffic through networking devices that add latency to each packet.

Add or Upgrade Equipment

The *Add or Upgrade Equipment Report* makes recommendations about which segments can be divided into two or more segments to optimize network performance. If the segment utilization is high, but segment division will not reduce network utilization enough to improve network performance, the report will recommend upgrading each segment to desktop switching or a higher speed shared media. This will result in shorter response times for software applications that are accessed across the network because each node has its own dedicated network segment. The extraneous traffic that each node hears in a shared-media environment is eliminated. Each node can use the full capacity of the network.

If desktop switching is not feasible, an alternate option is to upgrade the shared segment's speed.

Recommendation Details Section

The Recommendation Details section of the report supplies the supporting information for the recommendations made by the Network Performance Advisor. It include a textual explanation and the "before" and "after" graphical representations of the affected network. The recommendations are in priority order, starting with High Priority.

Dividing Segments into Workgroups

The Network Performance Advisor may determine that network performance can be enhanced by dividing a segment into two or more groups of nodes. The nodes in each group, often called a "workgroup", converse among themselves most of the time. The workgroups are physically divided using a switch, bridge or router.

A "before division" representation of the network traffic might look like the following figure:

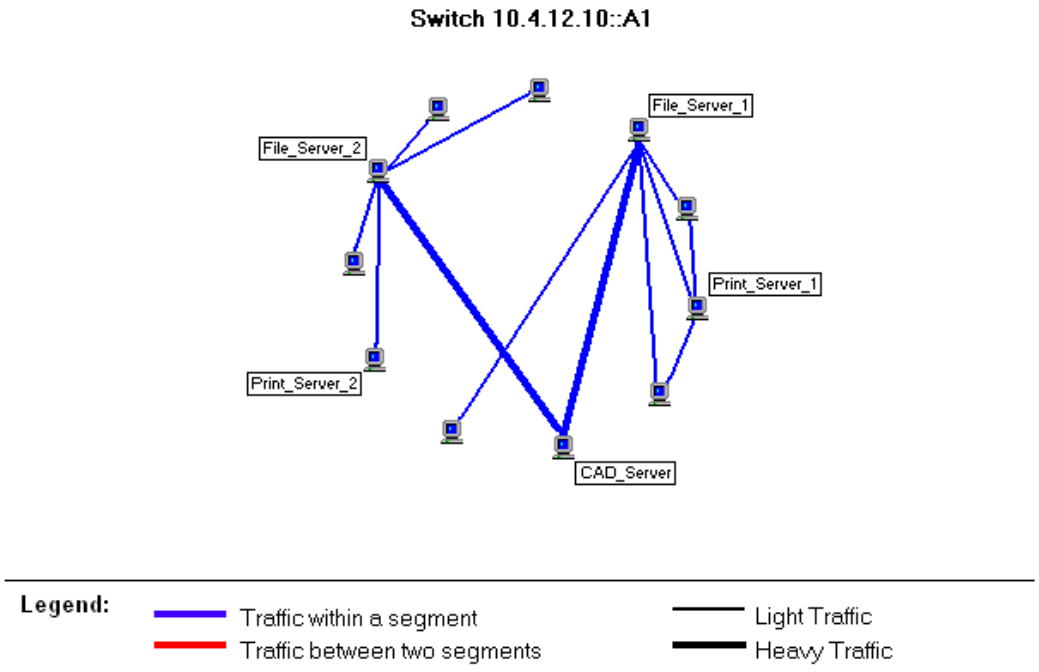


Figure 10-7. The traffic pattern before dividing into workgroups

After the segment was divided into three workgroups, the traffic could be represented as shown in the following figure:

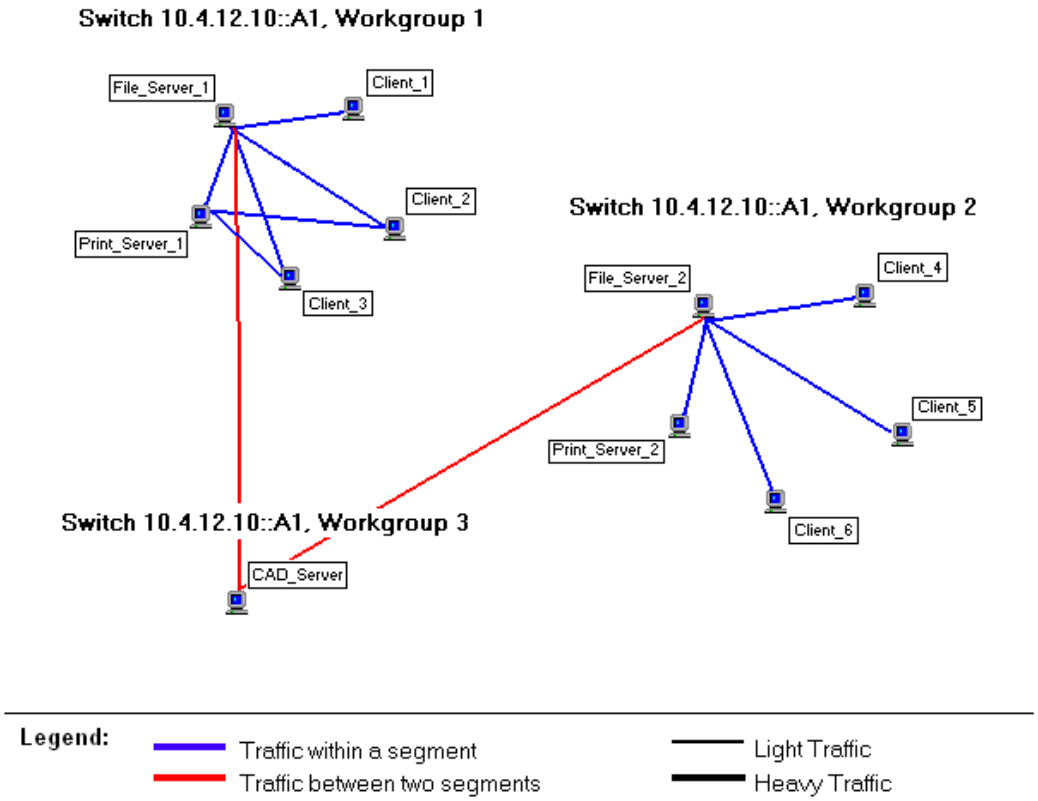


Figure 10-8. The Traffic Pattern after Dividing into Workgroups

A table shows the nodes included in each workgroup, the projected utilization of the workgroup, and the recommended segment bandwidth for each workgroup.

The Network Performance Advisor analyzes segments that have historical traffic data exceeding a maximum threshold to determine how to create separate workgroups that would reduce utilization. The newly formed workgroups are analyzed to determine if any further division is recommended. If a newly formed workgroup does not have enough traffic to exceed a minimum threshold, it is merged back into the original segment.

Note

A recommendation to divide a segment is made only if the amount of traffic within a workgroup exceeds the amount of traffic between workgroups.

Converting Segments to Desktop Switching

If a workgroup has high network utilization and cannot be divided, the Network Performance Advisor may recommend converting the segment's topology to desktop switching, giving each node a dedicated port.When two nodes need to exchange data, the switch makes a connection with the dedicated segments of each node. Extraneous traffic to the nodes is eliminated and each node uses the full capacity of the network. Converting a segment to desktop switching is most effective when the nodes can be placed on higher speed ports to offset the latency of the switch.

Note

If your network has a lot of multimedia or multicast traffic, or if you have configured VLANS, a desktop switching environment is the recommended solution.

Upgrading Segments to Faster Speed Media

The Advisor may recommend that a shared segment's speed be increased when:

1. The segment is capable of being upgraded to a faster speed, and
2. There are no nodes that can be placed on higher speed ports of a desktop switch. Higher speed ports help offset the switch's latency.

Dedicating Bandwidth to Top Talkers

Nodes that create a large amount of traffic on a segment are referred to as "top talkers". Network performance can be improved by dedicating bandwidth to a top talker. A switch allows the top talker to use the full capacity of the network. Other nodes on the network will not have to contend for bandwidth with the top talker, improving their access to applications accessed across the network.

If a segment with high utilization has a node that talks equally among all segments, the Network Performance Advisor will recommend that the node be on a dedicated port in a desktop switching environment. If utilization for that segment continues to be high, the Network Performance Advisor will recommend that the segment with that node be upgraded to 100 Mbps or a Gigabit, depending on the segment's current speed.

Top Conversations

The Top Conversations section of the report displays a table listing the most active nodes during the time period examined. The table is sorted by utilization percent. This section only appears if you have checked it in the **Modify Report Settings** page (checked by default). Enter the number of top conversations that you would like to see.

The right column of the table shows the percent that this conversation contributed to the total traffic on this segment.

Possible reasons that a conversation may not be listed in the table when a conversation has occurred on the segment are:

- The conversation was not in the top number of conversations (for example, the Top 10 conversations) selected for display for each segment
- One end of the conversation is a device (hub, switch or router). Only conversations between end nodes are shown.
- One or more of the end nodes was not found by the discovery/topology process.
- The segment does not contain either of the end nodes of the conversation but the conversation traverses the segment. For example, a conversation traverses Segment 1, Segment 2, and Segment 3, but the conversation is only reported on Segment 1 and Segment 3, where the end nodes reside. (Conversations in which the end nodes are in different segments will be listed in both segments.)
- Conversations involving nodes that utilize less than .1% of the segment bandwidth are not reported.
- The segment was not discovered by HP TopTools.

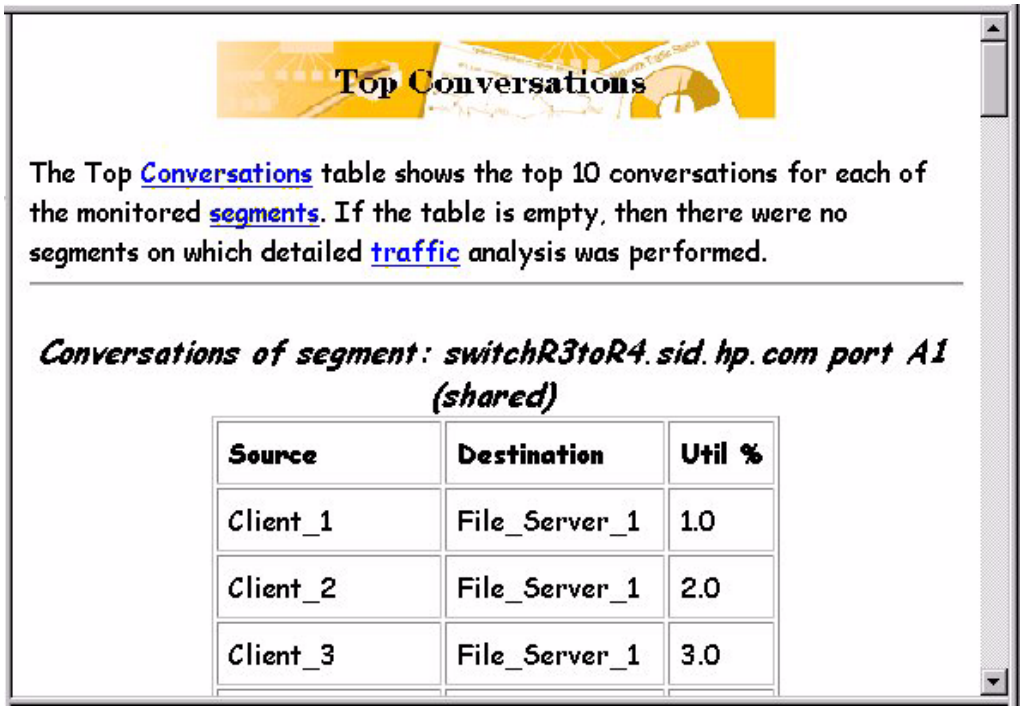


Figure 10-9. Top Conversations Page

You can use the Top Conversations table to determine who is using the bandwidth when utilization is high for a segment.

Inventory of End Nodes

The Inventory section shows the end nodes for each segment with the IP address, IPX address, and MAC address for each node. The table is in alphabetical order by “Friendly Name”. This section only appears if you have checked it in the Modify Report Settings page (checked by default). Click on a segment in the Table of Contents frame to jump to the table listing the end nodes for that segment.

Note

Networking devices such as hubs, bridges, switches and routers are not reported in the inventory list.

Note

HP TopTools provides an inventory list of devices by type of device, for example, a list of all hubs in the network. The HP TopTools inventory list is not organized by segment. Select the Inventory button in the HP TopTools home page.

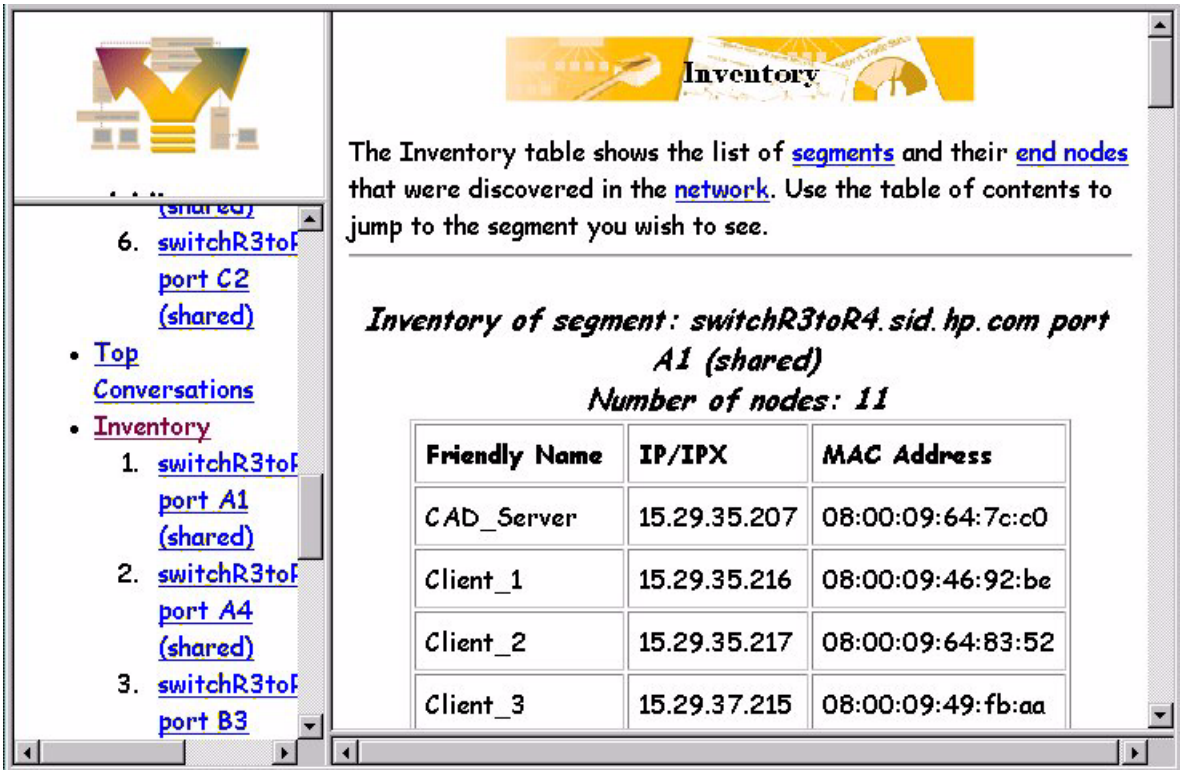


Figure 10-10.Inventory Report

When There Are No Recommendations

If the *Add and Upgrade Equipment Report* determines that, based on the historical data for the time period you specified, there are no advantageous ways to optimize the network, the Summary section of the report states that there are no recommendations for changes to your network configuration at this time. If you think that your network may need performance improvements, try selecting a more representative time period. Verify that your traffic data has been collected for the minimum time period, or the recommendations may not be valid.

Looking at the Top Conversations table may help you determine where the network traffic is occurring so that you can anticipate future growth needs.

Note

Adding devices that can sample data to high traffic segments that do not already have them allows the Advisor to perform a more detailed analysis of those segments.

Controlling Data Storage—Administration

You can specify some criteria to control how much data is collected. Select **Traffic Data Collector Settings** from the **Performance** button in the navigation frame, then select the **Storage** tab. Your current settings are displayed in the **Current Storage Status on Serve**r area. The **Historic Traffic Data** collection area displays the following choices:

- Storing data up to a maximum number of days of data or a maximum amount of data, whichever occurs first. The default is 31 days, up to 100 MB. You can click the **Default Values** button to set these values.
- Storing data up to a maximum amount of data (in Megabytes).
- Stopping collection of historical traffic data for analysis by the Network Performance Advisor.

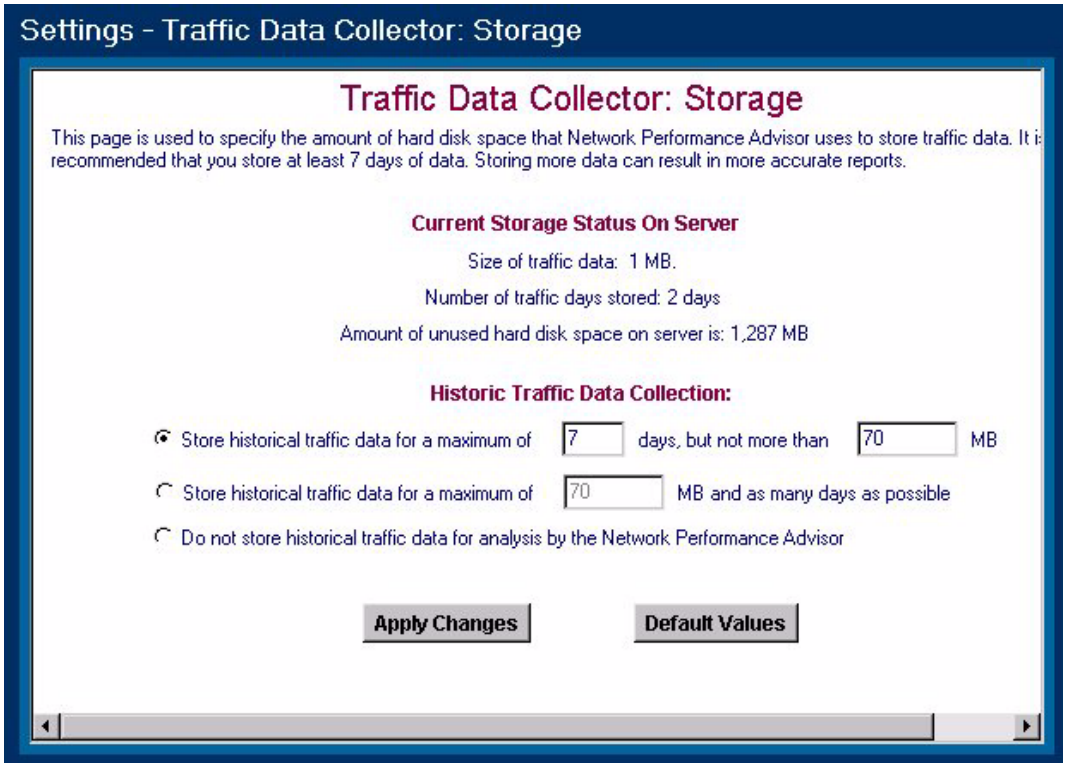


Figure 10-11.The Traffic Data Collector - Storage Settings Page

Note

To stop data collection, you must stop all of the HP TopTools services. Go to the **Settings** tab in the home page and select **TopTools Services**. On the Services page click on the **Stop Services** button.

How the Network Performance Advisor Collects Data

If you have data collection enabled in the Settings - Top Tools Services page, the Data Collector begins automatically when you start your PC. The historical traffic data is written to disk once per hour. It reflects activity on the network during the past hour.

Understanding HP Sampling

The Network Performance Advisor analyzes network traffic data over time, allowing the Advisor to detect long-term trends and problems on the network. When you run a report, recommendations are made that will improve your network performance.

Keeping the historical data about each conversation on a network requires a large amount of disk space. HP has developed a patented technique for greatly reducing the amount of data collected by using a statistical sampling of network traffic. Statistical sampling is the appropriate method for detecting the major contributors to traffic on the network because most network problems are caused by a few nodes that generate the most packets, the most errors, or use a large portion of the available bandwidth. Information about *interesting* traffic can easily be separated from the *noise* or traffic coming from the majority of nodes that only send small amounts of data.

HP's sampling method is based on randomly sampling network traffic and has been mathematically proven to work under **all** network conditions. The traffic is correctly attributed to the nodes that are creating it. Because of this random sampling method you don't need to provide a sampling interval to the Network Performance Advisor.

Traffic Data Collector Performance

You can specify the amount of system resources that the data collector can use. A more detailed network analysis requires more availability of system resources. The selections are:

- High Resource Availability—Recommended for systems dedicated to network management. The default setting.
- Medium Resource Availability—Recommended for systems that run other less performance-sensitive applications.
- Low Resource Availability—Recommended for systems that run performance-sensitive applications.

To access this page, select the **Performance** button in the HP TopTools navigation frame, then click on **Traffic Data Collector Settings**. Select the **Performance** tab.

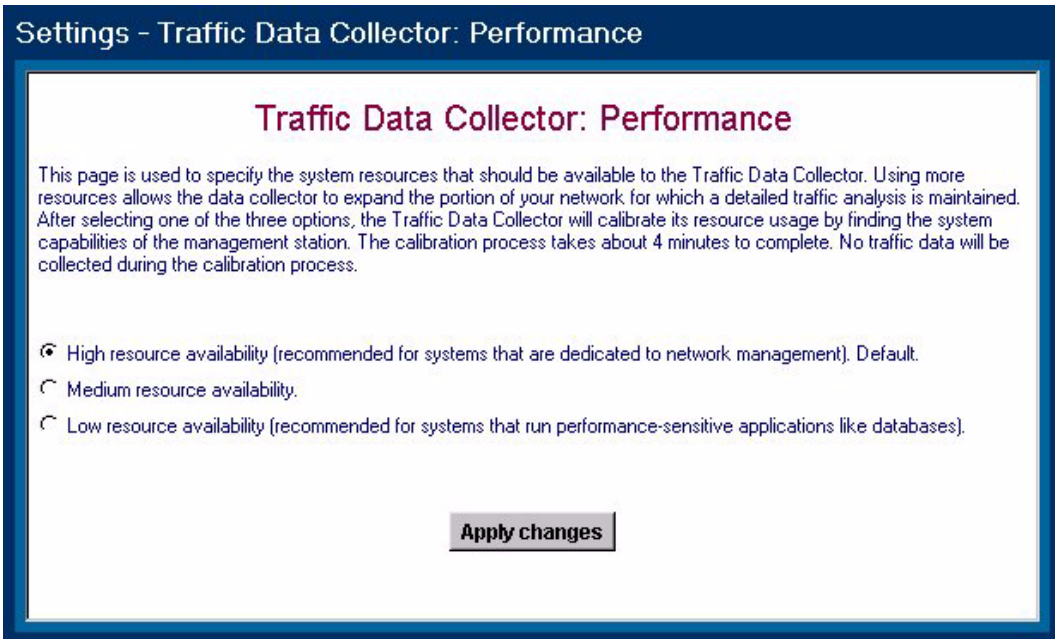


Figure 10-12.

The data collector must examine your management station's capabilities to determine what is appropriate for the resource setting that you select. The capabilities test begins when you click on the **Apply Changes** button. You will see a screen listing some statistics about the test. Data collection will stop during the test, and your management station may run slowly When the test is complete (approximately four minutes), your resource settings will be in effect.

Potential Problems with Data Collection

The existing historical traffic data becomes invalid when certain events occur, for example:

- When segments are split.
- When a node is moved to another segment.
- When you load a new topology file for a different network.

The Data Collector will reinitialize automatically after Discovery runs, in case new devices or segments were discovered or devices were moved.

Data collection must take place for at least an hour before the Network Planning report recommendations are valid. If changes to the network are frequent, it will be difficult to accumulate a sufficient amount of traffic data to generate accurate recommendations.

Segments Excluded from Analysis

Analysis of network traffic is possible for all segments with HP devices attached to them that have Extended RMON sampling capability, but may be performed for only a subset of the segments. This strategy best utilizes system resources for gathering information about the segments most likely to have traffic flow problems.

Segments that do not have Devices with Sampling Capability

When no HP devices with Extended RMON sampling capability are attached to a segment, only SNMP data is incorporated into the analysis. These segments are listed as Overutilized Segments in the "Segments Excluded from Analysis" section of the *Add or Upgrade Equipment Report.* A recommendation may be made to upgrade the segment to a faster speed if there is only one end node on the segment.

Segments not Selected for Analysis

If a segment is not considered a likely source of traffic problems, it may be excluded from analysis. If the segment traffic increases significantly, it will be included in future analyses of the network.

11

Quality of Service

This chapter discusses the benefits of the Quality of Service features available in HP TopTools for Hubs & Switches. It includes:

Overview

Quality of Service (QoS) is a general term for classifying and prioritizing traffic throughout a network. QoS enables you to establish a traffic priority policy to improve control and throughput of important data.

There will always be points in the network where multiple traffic streams merge or where network links will change speed and capacity, so it is important to move traffic on the basis of relative importance. Without QoS prioritization, less important traffic can consume network bandwidth and slow down or halt the delivery of more important traffic. For example, without QoS, most traffic received by a switch is forwarded with the same priority it had when entering the switch. In many cases, such traffic is “normal” priority and competes for bandwidth with all other normal-priority traffic, regardless of its relative importance to your organization’s mission. QoS keeps the most important network traffic moving at an acceptable speed regardless of current bandwidth usage. This means you can manage available bandwidth so that the most important traffic goes first.

As of Summer 1999, HP TopTools for Hubs & Switches can configure a QoS policy in your network for the following HP ProCurve Switches running the C.07.XX (or later) software release:

- HP ProCurve Switch 1600M
- HP ProCurve Switch 2400M
- HP ProCurve Switch 2424M
- HP ProCurve Switch 4000M

- HP ProCurve Switch 8000M
- HP Procurve Routing Switch 9308M and 9304M
- HP ProCurve Routing Switch 6308M-SX and 6208M-SX

Note

The Quality of Service features available in HP TopTools for Hubs & Switches includes the ability to set up consistent traffic prioritization (Class of Service) policies across the ProCurve switches in your network. The Class of Service features can also be configured on an individual switch using the switch's console or web browser interface. HP ProCurve documentation uses Quality of Service (QoS) to refer to HP TopTools network-wide prioritization, and Class of Service (CoS) to refer to prioritization configured on an individual switch using the switch's web browser or console interface.

At release P.01 of HP TopTools for Hubs & Switches (October, 1999), the HP ProCurve Switches 1600M, 2400M, 2424M, 4000M, and 8000M support QoS in HP TopTools for Hubs & Switches when upgraded to software release C.07.01 or later. You can download software upgrades free from HP's ProCurve website at **http://www.hp.com/go/procurve.**

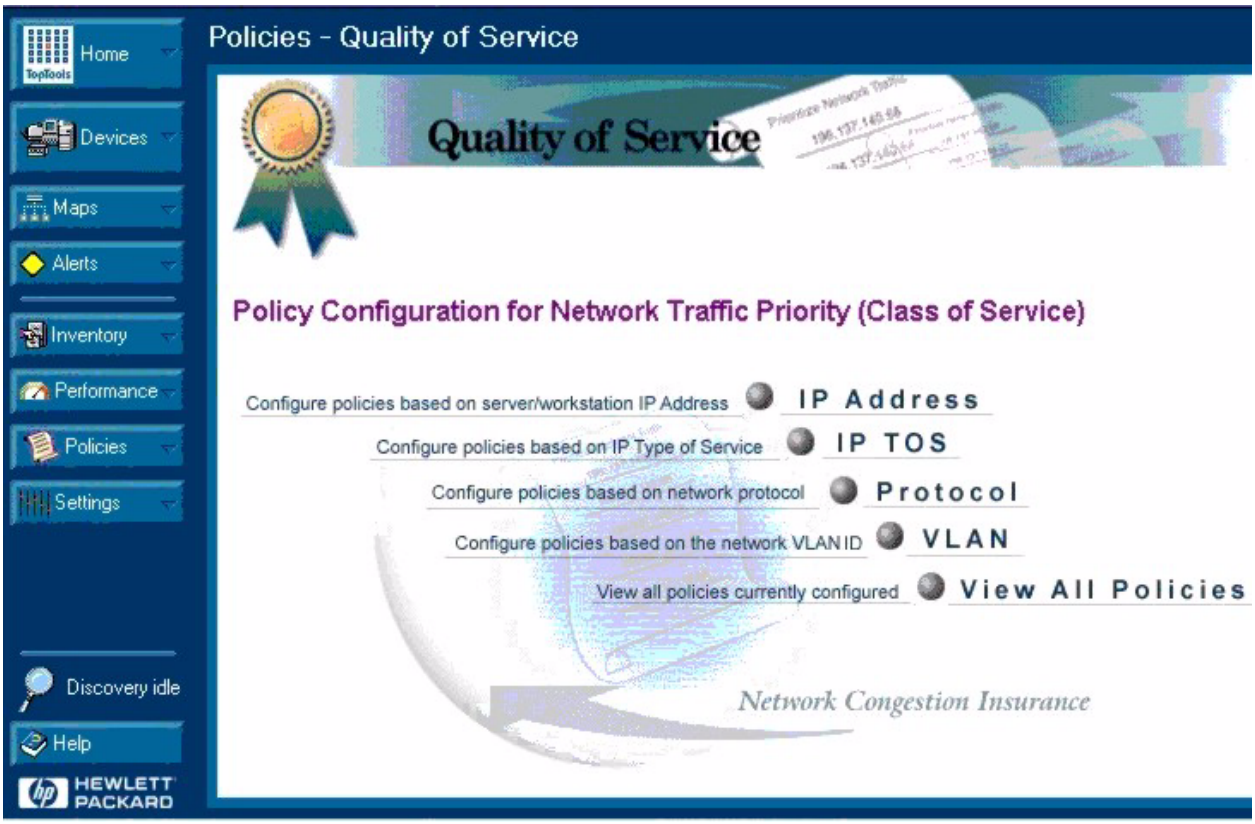


Figure 11-1. Quality of Service Main Page

Basic Operation

HP TopTools QoS operates on two levels as described below.

Controlling the priority of outbound packets. ProCurve switch ports have two outbound traffic queues; “normal” priority and “high” priority. High-priority packets leave a port first. Normal-priority packets leave the port after the port’s high-priority queue is emptied.

With no QoS control, all traffic (except IGMP traffic configured for high priority) goes through the “normal” outbound port queues. However, with a QoS configuration, you can determine the outbound priority queue to which a packet is sent. In an 802.1Q tagged VLAN environment, if QoS is not configured on a switch, but is configured on an upstream device, high priority traffic received by the switch is forwarded through high priority queues.

Configuring the 802.1p priority of outbound packets in a tagged VLAN environment for use by downstream devices. If an outbound packet is in an 802.1Q tagged VLAN environment, that is, if the packet is assigned to a tagged VLAN on the outbound port, then the packet carries an 802.1p priority setting that was configured in a switch implementing the QoS policy. This priority setting can range from 0 to 7, and can be used by downstream devices having up to eight queues. While packets within a switch move only at high or normal priority, they still can carry the 802.1p priority that can be used by downstream devices having more than two priority levels. If the packet enters a switch with an 802.1p priority setting, QoS can override this setting if configured to do so, giving you more control over traffic generated by various devices and applications in your network.

Note

If you are not using multiple tagged VLANs in your network, you can still use the tagged VLAN feature by configuring the default VLAN as a tagged VLAN.

The criteria for prioritizing traffic, in order of precedence, is:

1. Device Priority (destination or source IP address)
2. IP Type of Service (ToS) field
   - IP Precedence
   - Differentiated Services
3. Protocol Priority (IP, IPX, ARP, DEC LAT, AppleTalk, SNA, and NetBeui)
4. VLAN Priority
5. Incoming 802.1p Priority (present in tagged VLAN environments)

If more than one criteria is present in a packet, the above precedence scheme determines which criteria to use for prioritizing the packet. For example, if QoS assigns high priority to “red” VLAN packets, but normal priority to IP packets, since Protocol Priority (3) has precedence over VLAN priority (4), IP packets on the “red” VLAN will be set to normal priority.

Viewing All Currently Configured QoS Policies

This feature lists all prioritization policies you have configured using QoS in HP TopTools for Hubs & Switches.

The Policy List page provides a listing of all currently configured HP TopTools QoS policies. If the policy list exceeds the length of the list box, use the scroll bar on the right side of the list box to view all policy listings.

- Policy—Lists the type of policy and any identifying data, such as device name (for IP address policies) and VLAN ID number (for VLAN policies).
- Priority—Lists the priority setting (0 - 7) for the corresponding policy.
- Return button—Returns you to the main QoS page.

How To View the Policy List Page:

1. In the HP TopTools navigation frame, click on the **Policies** button.
2. Click on **Quality of Service** to display the Main QoS page.
3. In the Main QoS page, select a group, then click on **View All Policies**.

Configuring QoS for Specific Devices (IP Addresses)

This feature prioritizes network traffic to or from specific devices, using either the IP device name or the device IP address. Up to 30 device policies can be configured.

IP Device Address features:

- Node—Lists IP devices by device name or IP address.
- Priority—The priority assigned to traffic for a given policy. For example, assigning a priority of 7 (high priority) to a given IP address or IP device name means that all traffic to or from that device has the highest priority level.
- Add New Policy button—Displays the page used for adding a new IP address policy.
- Modify Selected Policy button—Displays the page used for changing the priority level for the selected IP address or device name.
- Delete Selected Policy button—Deletes the existing priority policy for the selected IP address or IP device name.
- Apply All IP Address Policies button—Configures the IP address policies on the QoS-capable, discovered HP switches on the network. If you have added, deleted, or changed any IP address policies, you must click on this button before proceeding.
- Return button—Returns you to the main QoS page.

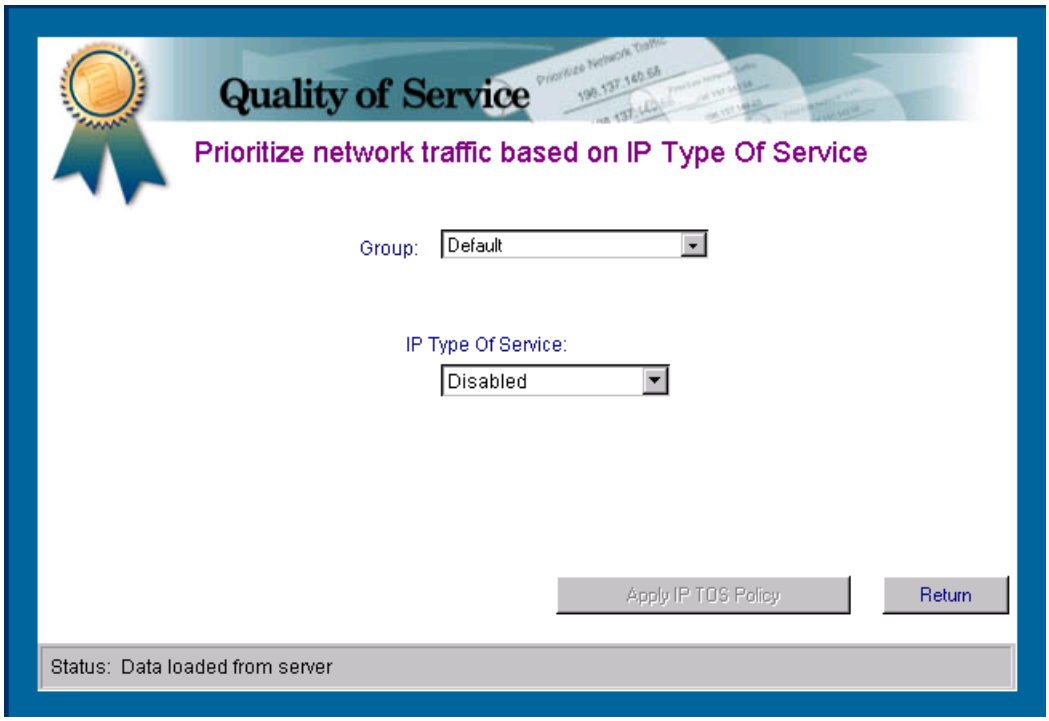


Figure 11-2. Adding a Policy for an IP Address

Adding a Policy for a Specific IP Address

1. In the HP TopTools navigation frame, click on the **Policies** button.
2. Click on **Quality of Service** to display the Main QoS page.
3. In the Main QoS page click on **IP Address** to display the device address page. This page lists any device-based policies already configured for the network, along with their priority settings.
4. To configure a priority policy for traffic to or from a specific device, select a group, then click on **Add New Policy** to display the page for adding IP address policies.
5. Select a device for which you want to configure an IP address policy:
   - For a Discovered Server: Ensure that the **Show servers only** radio button is selected, then use the menu to locate and select the server.
   - For any Discovered Device: Select the **Show all nodes** radio button, then use the menu to locate and select the device.
   - To Manually Enter a Device: Select the **Enter Manual Address** radio button, then type the device name or IP address in the Manual Entry field.
6. Use the Priority menu to select the priority level you want for the device you are adding.

7. Click on **OK**. This returns you to the IP Device Address page.

Repeat steps 4 through 7 for up to 30 IP Address policies.

Click on the **Apply All IP Address Policies** button. All buttons will appear temporarily grayed-out. When the Add New Policy button re-activates, any new IP address policies you entered have been configured on the QoS-enabled switches that HP TopTools has discovered in your network.

Configuring a QoS Policy for IP Type of Service (ToS)

Every IP packet includes a ToS field. This field carries priority settings that are read and used, but not altered by HP ProCurve switches. When an HP TopTools prioritization policy is configured for ToS criteria, the ProCurve switches in the network read the content of the ToS field in packets received from upstream devices and applications and take actions based on whether the policy applies to the packets. To use ToS to configure priority, you need to anticipate the ToS field settings in IP packets entering ProCurve switches from upstream devices. This involves having knowledge of how an upstream device or application will set the bits in the ToS field of IP packets transmitted onto the network. A ToS policy can prioritize IP packets in either of two ways:

- Use the Differentiated Services bits to select the packets to prioritize (ToS Differentiated Services option)
- Use the Precedence bits to prioritize a packet (ToS IP precedence option)

ToS Configuration Options

ToS policy configuration includes three options:

- Disabled (the default) -- ToS is disabled and is not a factor in prioritizing packets. (Priority settings in the ToS fields of IP packets are ignored by the HP ProCurve switches in the network.)
- IP Precedence -- ToS is enabled, and ProCurve switches will use ToS precedence bits (the upper three bits in the ToS field of packets received from upstream devices) to determine packet priority. The value of these bits is in the range of 0 through 7.
- Differential Services -- ToS is enabled and ProCurve switches will use the Differentiated Services bits (the upper six bits of the ToS field). Each possible setting is termed a codepoint, and there are 64 possible codepoints. This means that you can configure a priority (0 - 7) for up to 64 ToS codepoints. If No override (the default) is specified for a codepoint, then differentiated services prioritization is not used for packets carrying that codepoint. Using HP TopTools for Hubs & Switches, you can enable or disable the Differentiated Services option. To configure the priority policy corresponding to the codepoints in the ToS fields for IP packets, telnet to the console interface of the individual ProCurve switches in your

network. (Information on how to use the console interface to configure ToS Differentiated Services is included on your HP TopTools for Hubs & Switches CD.)

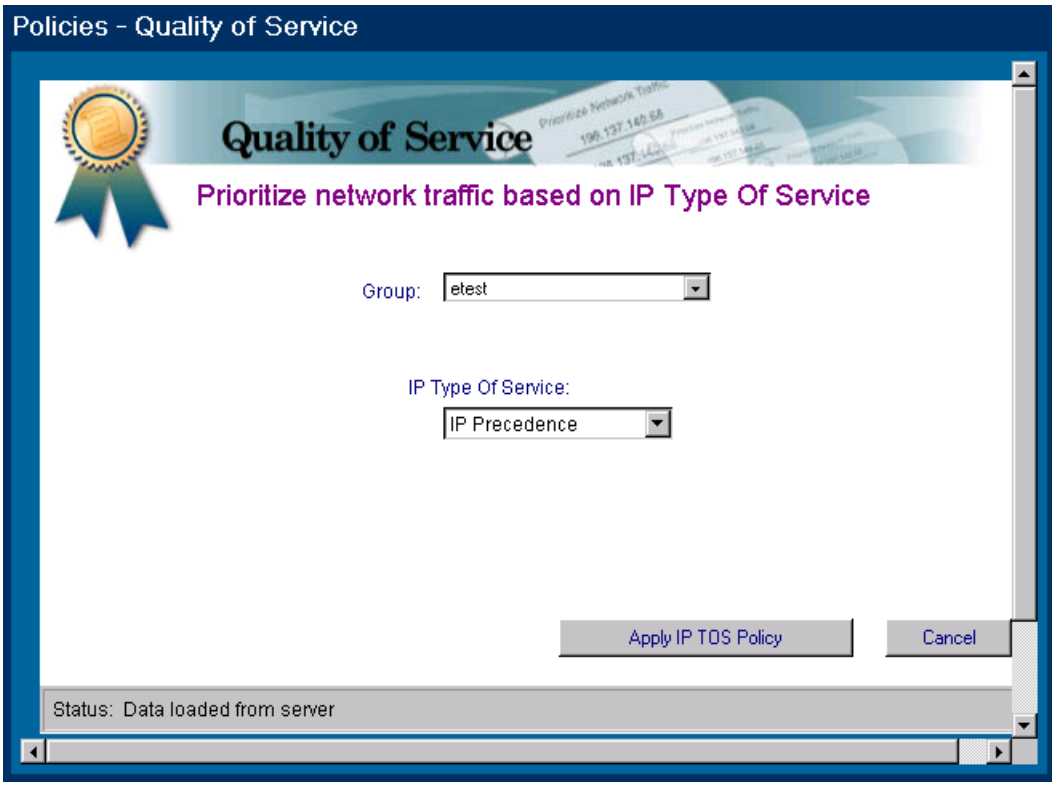


Figure 11-3. Qos Policy for IP Type of Service (ToS)

The following table describes how a ToS prioritization policy can affect IP packet priority:

For a given packet carrying a given codepoint in the ToS field:

Outbound ProCurve Switch Ports	ToS Option	
	IP Precedence (Value = 0-7)	Differentiated Services

IP Packet in an Untagged VLAN or No VLAN	Depending on the value of the IP Precedence bits in the packet's ToS field, the packet will go to either the high or normal priority outbound port queue of ProCurve switches: 0 - 3 = normal priority 4 - 7 = high priority	For a given packet carrying a given codepoint in the ToS field: • If a priority (0 - 7) has been configured for that codepoint, the ToS policy sends the packet to either the high or normal priority outbound port queue in the network's ProCurve switches. • If No override (the default) has been configured for that codepoint, then the packet is not prioritized by a ToS policy.
IP Packet in a Tagged VLAN	Same as above, plus the IP Precedence value (0 - 7) will be used to set a corresponding 802.1p priority in the VLAN tag carried by the packet when it exits from a ProCurve switch.	Same as above, plus the user-configured Priority value (0 - 7) will be used to set a corresponding 802.1p priority in the VLAN tag carried by the packet when it exits from a ProCurve switch.

How To Configure a ToS Policy

1. In the HP TopTools navigation frame, click on the **Policies** button.
2. In the resulting pull down menu, click on **Quality of Service** to display the Main QoS window.
3. In the Main QoS window click on **IP ToS** to display the IP ToS window.
4. Select a group, then using the **IP Type of Service** pull down menu, select a ToS option:
   - Disabled -- Disables IP ToS prioritization policy in your network.
   - IP Precedence -- Enables IP Precedence as the ToS policy in your network.
   - Differential Services --Enables Differential Services as the ToS policy in your network.
5. Click on the **Apply IP ToS Policy** button to configure the ToS policy on the QoS-capable, discovered HP switches on the network.
6. Click on the **Return** button to return to the main ToS screen.
7. Do one of the following:
   - If you selected IP Precedence (in step 4, above) for your ToS policy, you are finished configuring ToS prioritization policy and can go on to other HP TopTools activities.
   - If you selected Differential Services (in step 3, above) for your ToS policy:
     a. Open a window in which you can Telnet to the console interface in each of the individual ProCurve switches in your network.

b. Configure the priority for each codepoint for which you want a ToS prioritization policy. (Refer to the further information available on the HP TopTools CD and also on HP's ProCurve website.)

Configuring a QoS Policy for Specific Protocols

This feature prioritizes network traffic on the basis of these specific protocol types:

- IP
- IPX
- ARP
- DECNet
- AppleTalk
- SNA
- NetBEUI

The Protocol page displays the following:

- Protocol—Lists the network protocols for which you can configure a prioritization policy.
- Priority—The priority assigned to traffic for a given protocol policy. For example, assigning a priority of 7 (high priority) to a given protocol means that all packets implementing that protocol have the highest priority level. The default setting for any protocol is No override, which means that no prioritizing policy exists for that protocol type.
- Modify Selected Policy button—Displays the page used for changing the priority setting for the selected protocol.
- Apply All Protocol Policies button—Configures the protocol policy on the QoS-capable, discovered HP switches on the network. If you have added, deleted, or changed any protocol policies, you must click on this button before proceeding.
- Return button—Returns you to the Main QoS page.

Figure 11-4. QoS Policy for a Specific Protocol

To modify a protocol:

1. In the HP TopTools navigation frame, click on the **Policies** button.
2. Click on **Quality of Service** to display the Main QoS page.
3. In the Main QoS page click on **Protocol** to display the Protocol Policy page. This page displays the protocol policy options and the priority setting for any protocol policies already configured for the network.
4. To configure a priority policy for a specific protocol, select a group, then highlight the protocol and click on the **Modify Selected Policy** button.
5. Use the Priority pull-down menu to select the priority level you want for the selected protocol.
6. Click on **OK** to return to the Protocol Policy page.

Repeat steps 4 through 6 for any additional protocol policy changes.

Click on the **Apply All Protocol Policies** button. All buttons will appear temporarily grayed-out. When the Return button re-activates, any new protocol policies you entered are configured on the QoS-capable, discovered HP switches on the network.

Click on the **Return** button to return to the Main QoS page.

Configuring a QoS Policy for a Specific VLAN

This feature prioritizes network traffic on the basis of the priorities assigned to the ID number for specific VLANs.

The VLAN page features:

- VLAN ID—Lists the ID number(s) for any 802.1Q VLAN(s) that are configured on your ProCurve switches.
- Priority—The priority assigned to traffic for a given VLAN policy. For example, assigning a priority of 7 (high priority) to a given VLAN ID means that all traffic on that VLAN has the highest priority level.
- Modify Selected Policy button—Displays the page used for changing the priority setting for the selected VLAN ID.
- Delete Selected Policy button—Deletes the existing policy for the selected VLAN.
- Apply All VLAN Policies button—Configures the VLAN policy on the QoS-capable, discovered HP switches on the network. If you have added, deleted, or changed any VLAN ID policies, you must click on this button before proceeding.
- Return button—Returns you to the Main QoS page.

How To Add a VLAN Policy

1. In the HP TopTools navigation frame, click on the **Policies** button.
2. Click on **Quality of Service** to display the Main QoS page.
3. In the Main QoS page click on **VLAN** to display the VLAN Policy page. This page displays any currently configured VLAN policies.
4. To configure a policy for a specific VLAN, select a group, then click on the **Add New Policy** button. Configure a new VLAN policy in the VLAN Policy Configuration page.

12

Accessing Hub Features

HP TopTools for Hubs & Switches lets you manage your HP devices with your browser from anywhere in your network. Several features provide information about the status of your device, alert you to problems in your network, and give you the ability to configure settings for proactive network management.

This chapter includes information on:

See the chapter **Setting Up Security for a Device** for information about device security.

See the chapter **Performing Diagnostics** for information about resetting devices and performing Link and Ping tests.

See the chapter **Alerts** for information about the Alert Log and Automatic Fault Finding.

Device Management Features

To launch the device management interface, double-click on a device in the Devices list or in a topology map. You can also click on a device (one click) in the list, then click on the **Actions** button and select **Properties (Device View)**. The Status - Overview page for the device displays.

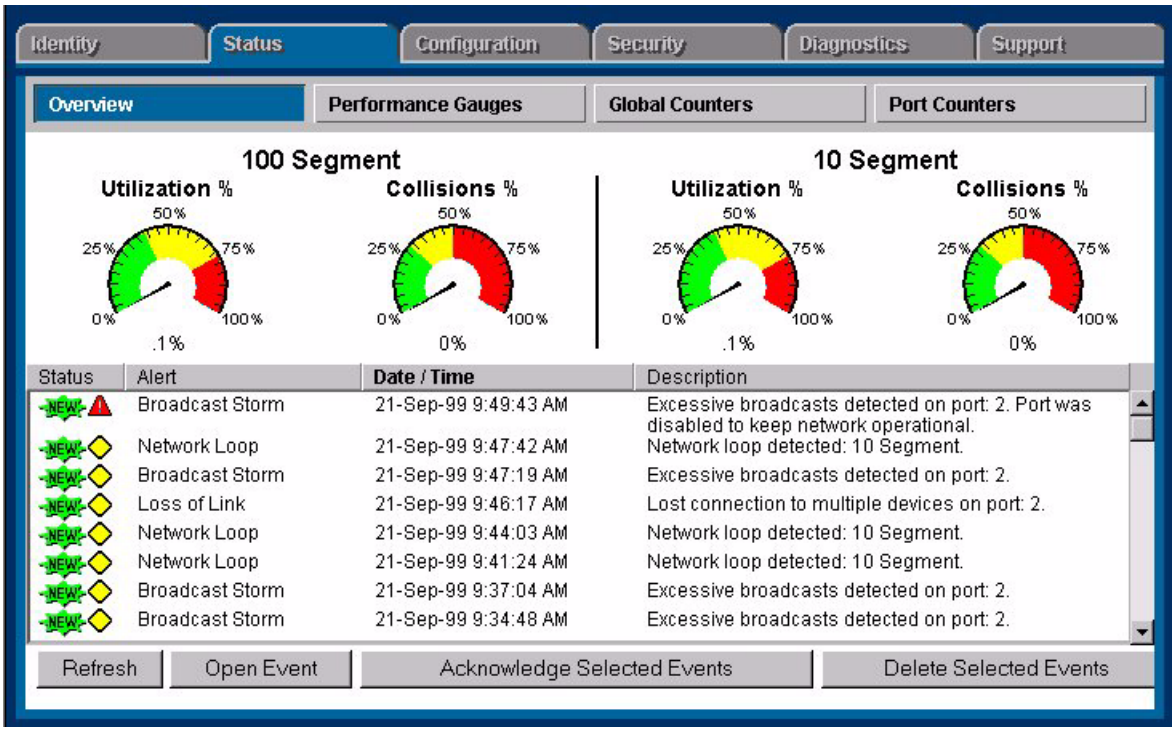


Figure 12-1. Hub Status Overview Page

Viewing Device Identity Information

You can view some basic information about the device by selecting the **Identity** tab. You can change the information by selecting the **Configuration** tab and clicking on the **System Information** button.

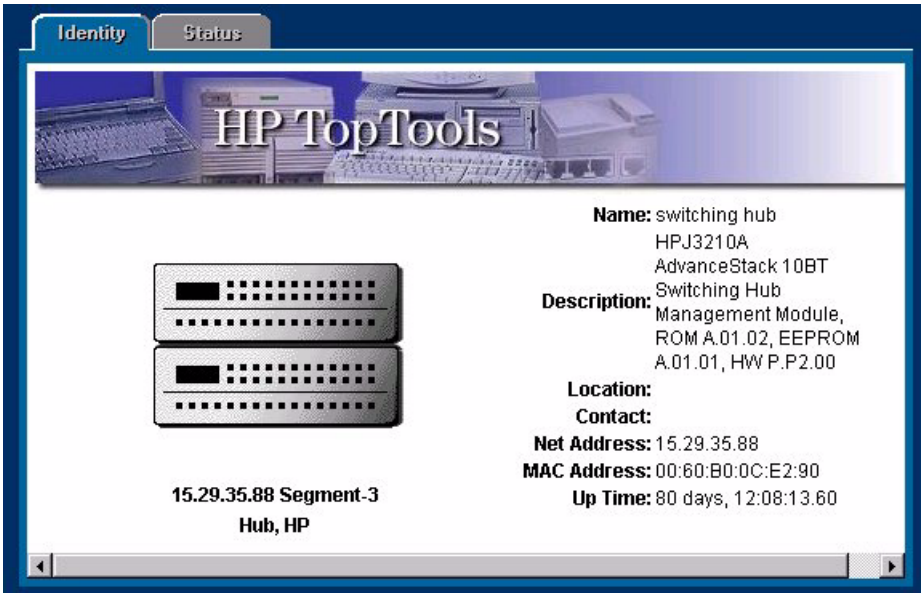


Figure 12-2. Identity Page for a Switching Hub (when "Properties" is selected from menu)

See the online help for information about setting or changing these values.

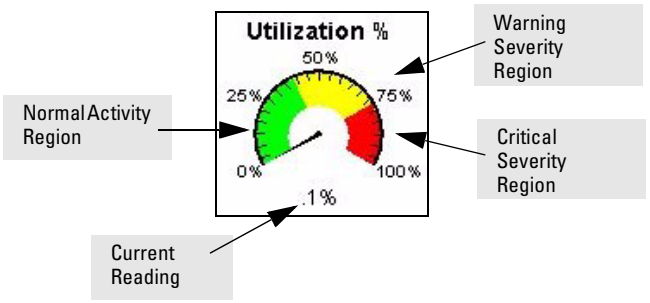
Interpreting Device Status

The Status - Overview page for the hubs displays the Performance Gauges and any alerts that have occurred. For switching hubs, the Status - Overview page displays gauges by segment instead of by attribute.

See the chapter **Alerts** for more information on the Alert Log.

Reading the Performance Gauges

The performance gauges display statistical information about the selected device. By looking at the gauges, you can quickly determine if there are problems with the network utilization, collisions, the number of broadcasts per second, or the number of error packets. The gauges are refreshed every five seconds.



The information shown for hubs is for all ports on the device. You can obtain information for each port by selecting the **Performance Gauges** button (Status tab), then selecting an individual port from the drop down list. If you want to monitor a different attribute for that port, just select the desired attribute from the drop down list below the port number.

You can also obtain information for all 100Base-T ports or all 10Base-T ports.

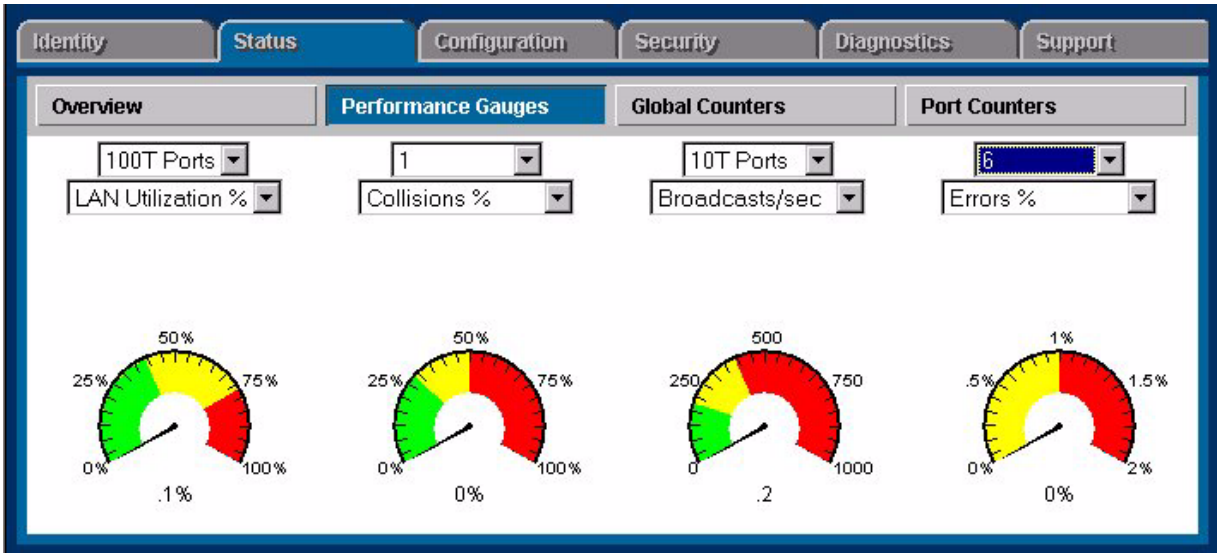


Figure 12-3. Performance Gauges for a Hub

The following table explains the attributes and gives their threshold settings on a per port basis for hubs. These settings cannot be changed. You can view an attribute value for all the ports of a device by selecting **All Ports** from the drop down list above the attribute. For the switching hubs, you can also select a segment from the drop down list.

Table 12-1. Gauge Attributes

Attribute	Description	Severity Values
Utilization%	Represents the traffic on the port as a percentage of the port's bandwidth.	Warning: 40% Critical: 75%
Collisions%	Represents the number of collisions that have occurred expressed as a percentage of the packets transmitted through the port.	Warning: 30% Critical: 50%
Broadcasts/sec	Represents the number of broadcast packets being transmitted through the port per second.	Warning: 150/sec Critical: 400/sec
Errors%	Represents the number of errors that have occurred expressed as a percentage of the total number of packets received through the port.	Warning: 0%-1% Critical: 1%
Multicasts/sec	Represents the number of multicast packets being transmitted through the port per second.	Warning: 1500/sec Critical: 4000/sec

Global Counters

Hub Global Counters

Selecting the **Global Counters** button displays a page listing eight counters and their values since the last device reset. The counters are totals for the device. To view counters by port, select the **Port Counters** button.

Switching Hub Global Counters

The switching hubs display the counters as shown in the following figure.

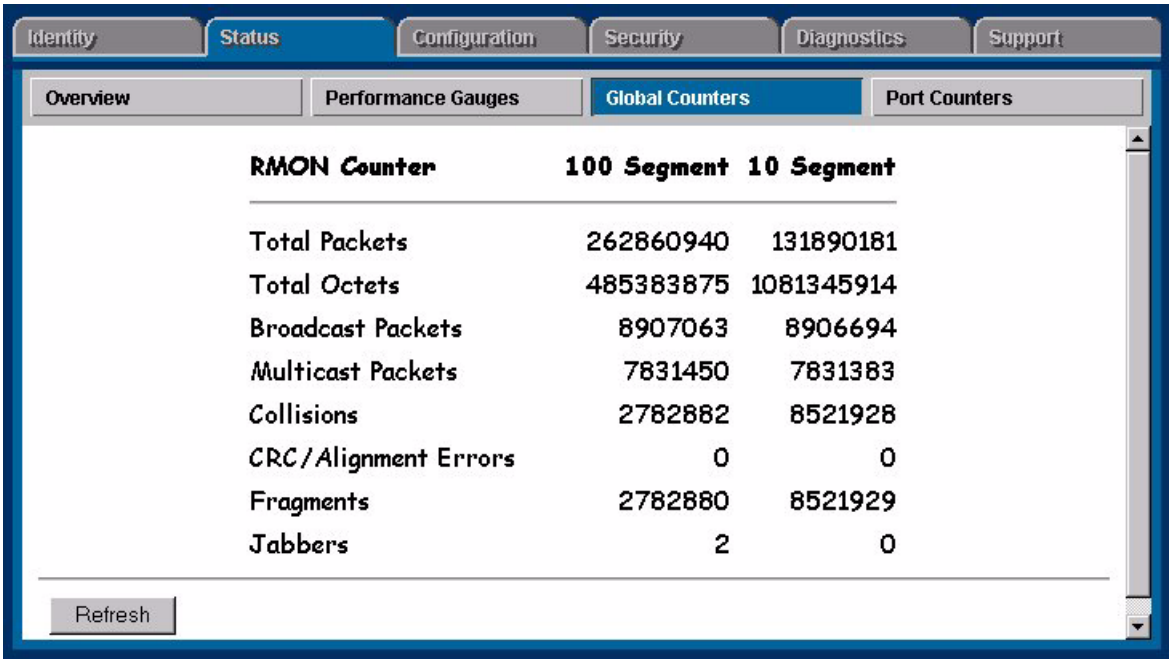


Figure 12-4. Hub Global Counters

The counters are described in the following table.

Table 12-2. Global Counters

Counter	Description
Total Packets	Total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Total Octets	Total number of octets of data (including bad packets) received on the network. This object can be used to estimate Ethernet utilization.
Broadcast Packets	Messages sent to all users on the network.
Multicast Packets	Multicast packets are delivered to a subset of users on the network, as opposed to Broadcast packets, which are sent to all users.
Collisions	When two or more devices attempt to transmit a message on a cable at the same time, interfering with one another's transmissions. The number of collisions should be proportional to the number of packets transmitted over time and the number of nodes operating on the network.
CRC/Alignment Errors	The Cyclic Redundancy Check (CRC) is a code typically placed at the end of the frame or packet to ensure the integrity of the data within the frame. Alignment Errors are the number of instances where the CRC method was used to correct a packet whose bits were misaligned because of timing errors.
Fragments	Total number of packets received that were less than 64 octets in length and had a bad Frame Check Sequence (FCS).

Counter	Description
Jabbers	Total number of packets received that were longer than 1518 octets and had a bad Frame Check Sequence (FCS). High levels indicate too many packet transmissions.

Port Counters

The **Port Counters** button displays a page with information about important counters for each port.

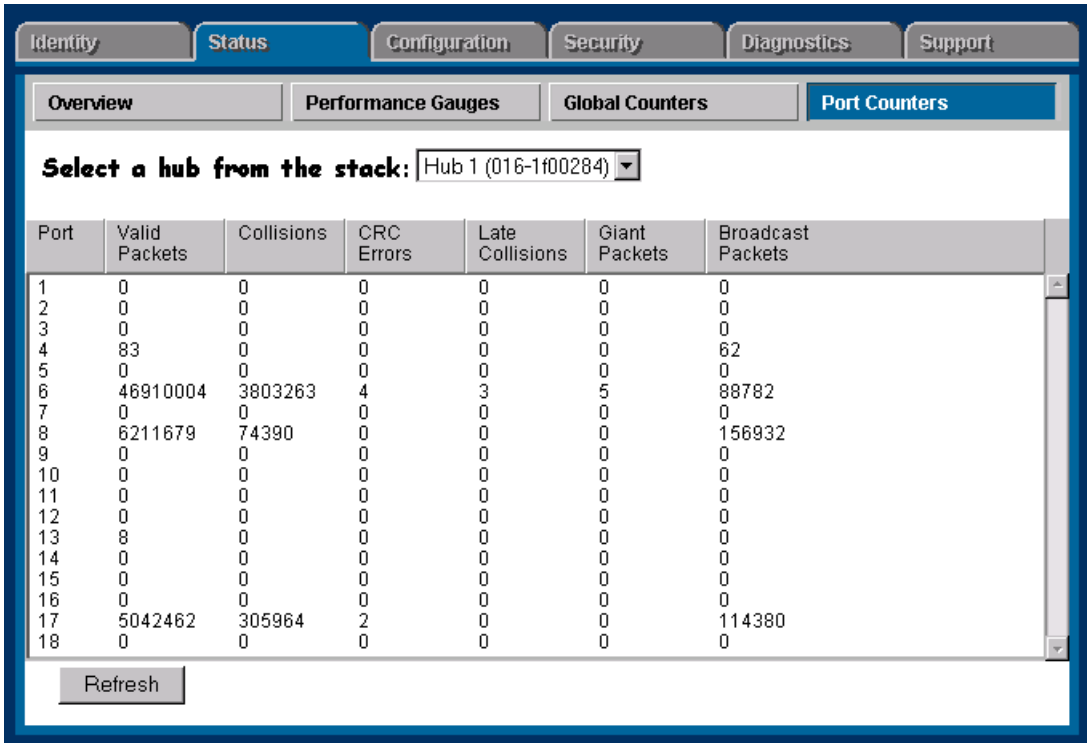


Figure 12-5. Hub Port Counters

See the online help for information on each counter.

Configuring Your Device

Select the **Configuration** tab to display the Device View (formerly a Closeup View). The other buttons in this page provide access to various configuration features for that device.

If the device you selected is not manageable by browser, you can only manage it from the HP TopTools Management Workstation. To obtain generic SNMP information about non-HP devices, select **Properties** from the **Actions** button menu. To establish a telnet session to this device (if the device supports telnet), select **Telnet** from the **Actions** button menu.

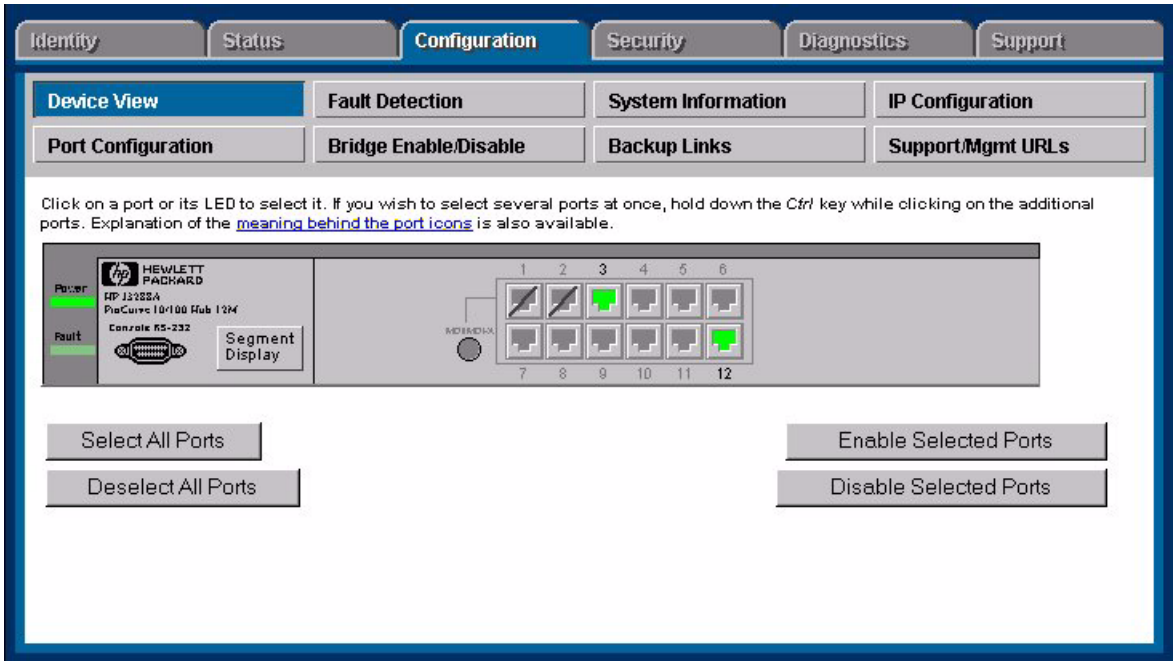


Figure 12-6. Hub Device View

You can enable and disable individual ports (click on the port to select it), or click on the **Select All Ports** button to enable or disable all the ports of a device in one step.

Click on the link "**meaning behind the port icons**" above the Device View to view the port indicator legend.

Fault Detection

The automatic fault detection feature protects your network from failing because of problems such as network loops, defective cables, transceivers and faulty network interface cards. The Fault Detection page lets you set the sensitivity and actions that occur when a fault is detected on a port in your network. For hubs, you can set the sensitivity for logging network problems and disabling ports. The sensitivity settings are:

High Sensitivity: The device will act when a network problem of any severity occurs. Network problems are automatically detected and entered into the Alert Log.

Medium Sensitivity: The device will act when serious network problems occur.

Low Sensitivity: The device will act only when severe network problems occur. These are problems that may bring the network down.

Never: The device will never take any actions regardless of the severity of the problem.

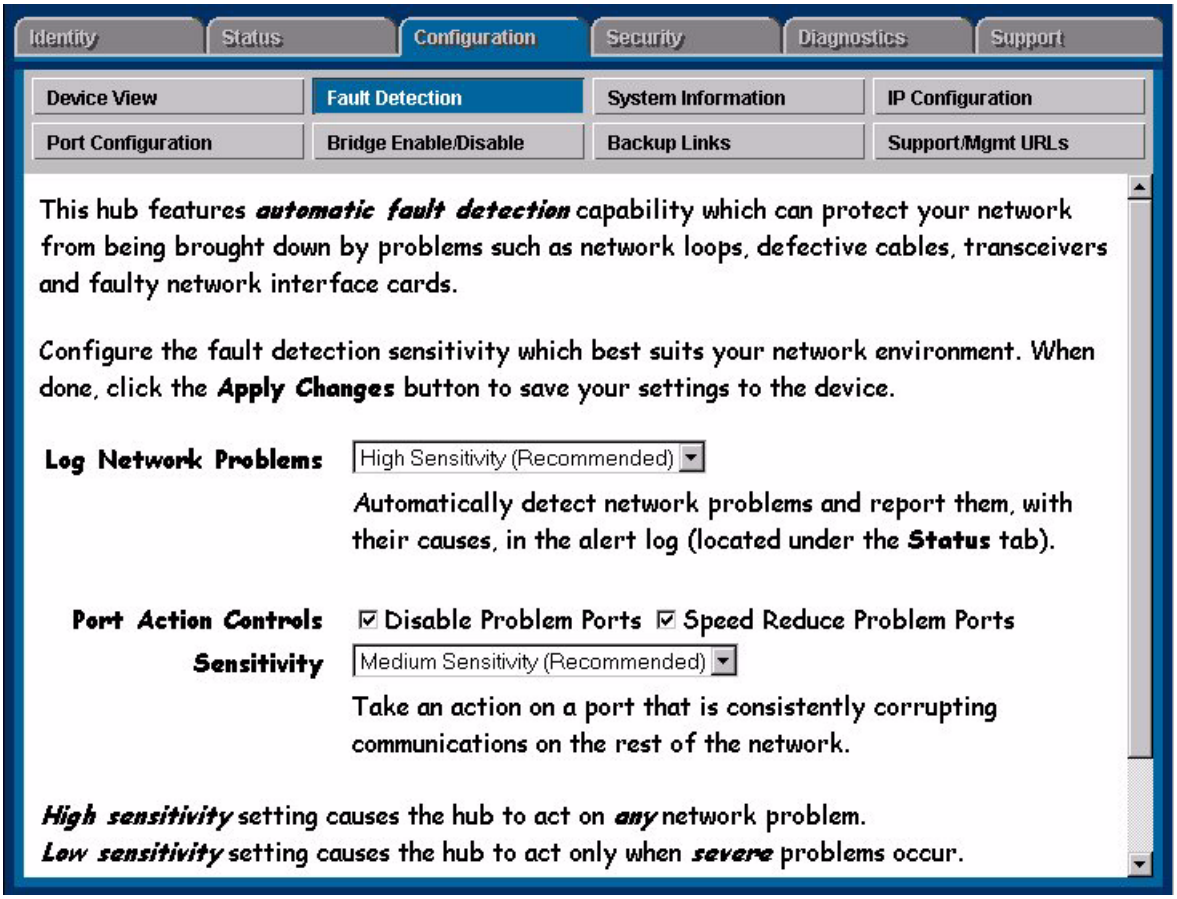


Figure 12-7. Fault Detection Sensitivity Settings

System Information

The System Information page lets you enter a system name for the device, the location of the device, and whom to contact in the event of a problem.

Configuring IP

Select the way that you want IP addresses configured for your network:

- Manual—Set the IP address through the console.

- Disabled—IP is disabled, there is no access to management or telnet. **Not Recommended**.
- Use Bootp—The Bootp protocol sets the IP address automatically.

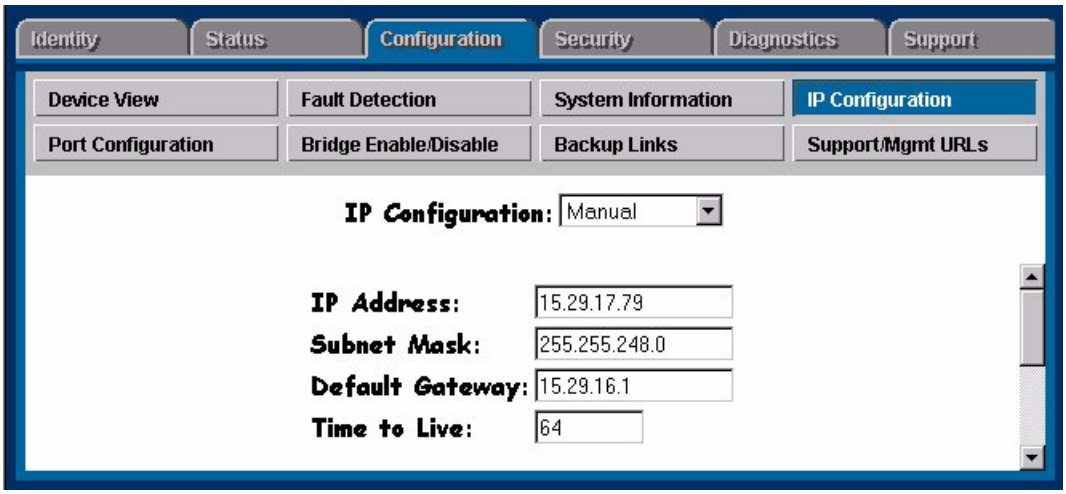


Figure 12-8. Hub IP Configuration

Hub IP Configuration

If you select **Manual**, you must then enter an IP Address, Subnet Mask, Default Gateway, and Time to Live for the device. If you select **Bootp/DHCP**, the IP address will be assigned automatically.

Switching Hub IP Configuration

For the switching hubs, you must select a segment to configure before you select Manual or Bootp/DHCP. If you select **Manual**, you must then enter an IP Address, Subnet Mask, Default Gateway, and Time to Live for the device. If you select **Bootp/DHCP**, the IP address will be assigned automatically.

Characteristics of Bootp and DCHP. The Bootp protocol is designed for a network in which each host has a permanent network connection. It is not adaptable to a mobile computing environment.

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 only need the address for an hour, while another device may use the same address for several days. DHCP is more suitable in environments where the number of IP addresses needed exceeds the number available. It also allows a device to obtain its configuration information, such as the IP Address and Subnet Mask, in one message, reducing the demand on the network.

A static IP address is a unique address that is assigned to one client only. Static addresses are used for an extended time period.

Port Configuration

The Port Configuration page displays information about the hub ports. To enable a port, select the port number in the page, then click **Enable Selected Ports**. Use the **Disable Selected Ports** button to disable a port or group of ports.

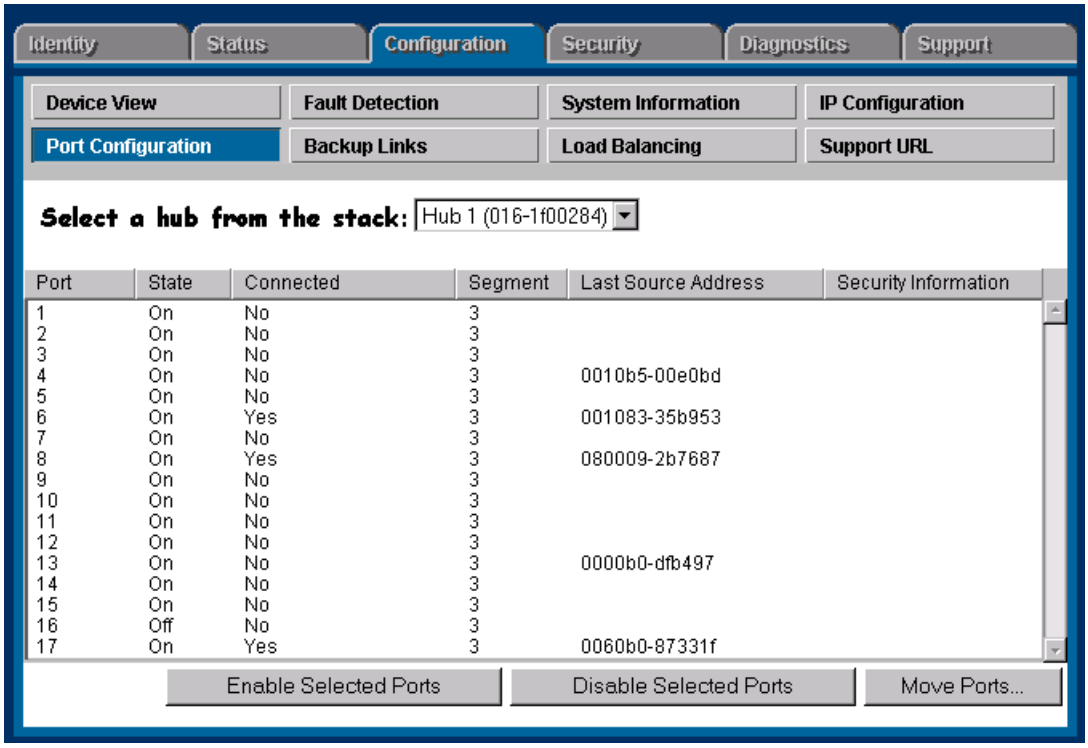


Figure 12-9. Hub Port Configuration

The information is described in the following table.

Table 12-3. Port Information

Setting	Description
Port	The port number.
State	The port can be on or off.
Connected	**Yes**: A device is connected to this port. **No**: There is nothing connected to this port. **Partitioned**: The node is disconnected from the network and the traffic that the port generates is lost. **Polarity Reversed**: Some signals in the cable are reversed due to a miswired cable.

Setting	Description
Segment	For switching hubs, the segment that the port is on.
Last Source Address	The address of the last device that sent packets through this port.
Security Violation	States whether there is a security violation or no violation.

Bridge Enable/Disable

Select the **Bridge Enable/Disable** button to enable or disable the internal bridge between the 10 Mbps and 100 Mbps segments in the hub.

Note

It is recommended that this setting remain enabled for optimum connectivity. You may want to disable the bridge:

- To connect the segments via and external switch
- To simplify the network for troubleshooting.

Backup Links

A backup link (hubs only) configures two ports on one hub to create a redundant connection to another device. This provides a connection with fault-tolerant capability for highly reliable networking. One port is designated the primary port; the second port is the backup port. The backup port becomes active only if the primary port becomes inoperative. Any of the network ports (twisted-pair, ThinLAN, or AUI/Xcvr) can be used as the primary port or backup port.

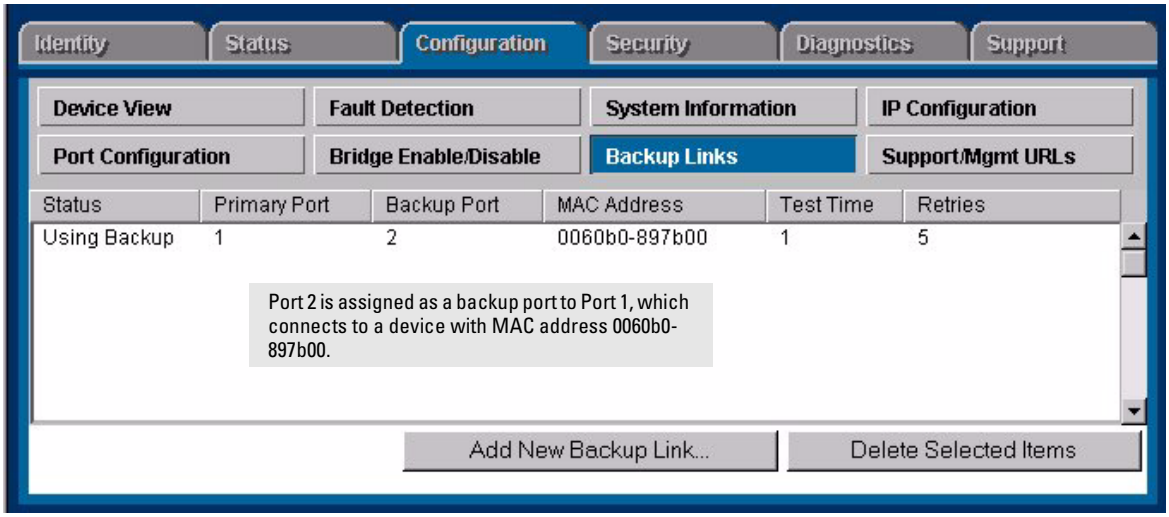


Figure 12-10.Adding a Backup Link

You can create one or more backup links by selecting the **Backup Links** button and clicking on the **Add New Backup Link...** button at the bottom of that page. The parameters are described in the following table.

Table 12-4. Backup Link Parameters

Parameter	Description
Status	Displays which port is currently being used, a primary port or a backup port.
Primary Port	A port that you can use as a primary port, or the port that will be used during standard connection of a hub and the connected device.
Backup Port	The backup port to be used if there is a failure on the primary port. If the primary port is active, the backup port is inactive.
MAC Address	The MAC address of the device to which you have a backup (redundant) path. It is the recipient of the 802.2 test packets, which are used to verify the primary path.
Test Time	The interval in seconds between test packets sent between the primary port and the receiving device.This checks the integrity of the link to determine whether to initiate a backup link. The number can be between 1 and 15.
Retries	The maximum number of times the test packets from the primary port fail to return from the other device before the backup port becomes the active port.

Configuring Load Balancing—Switching Hubs

Only the switching hubs provide a load balancing feature to automatically distribute the switching hub ports among the four segments to optimize performance. This feature requires a switch module.

To access this feature, select the **Load Balancing** button. Click on the **Perform Automatic Load Balancing** button. If you want to undo the load balancing, select the **Undo Last Load Balancing** button.

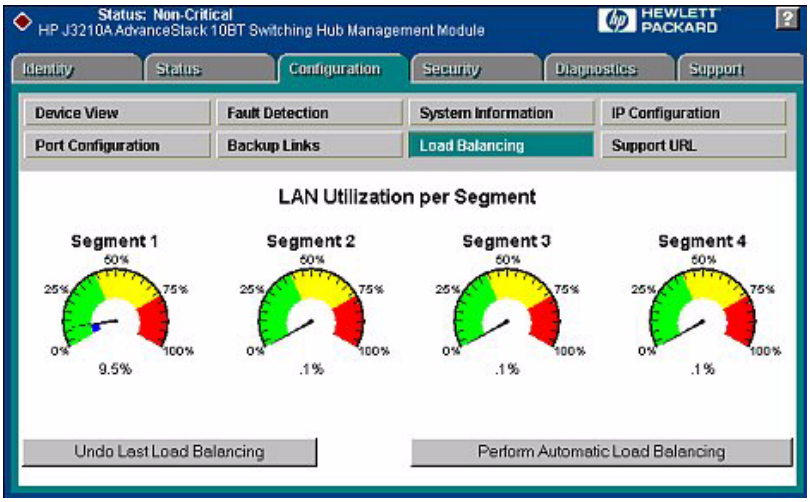


Figure 12-11.Load Balancing in a Switching Hub

Support URL

You can obtain support information by going to the HP Support site on the World Wide Web. The URL is:

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

Select **Technical Support.**

If you want to change the URL that is accessed when the Support tab is selected, type in the new address and click on the **Apply Changes** button. For example, you could change the URL to launch your site home page.

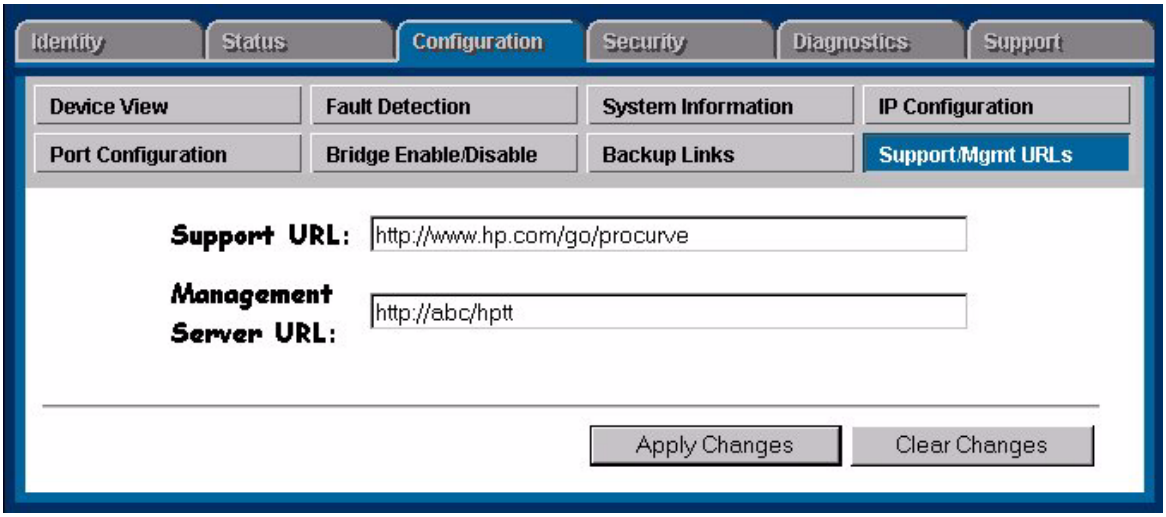


Figure 12-12.The Support Page

13

Managing Switches

This chapter has information on:

- **Displaying Switch Status**
- **Switch Identity Information**
- **Configuring Switch Features**
- **HP ProCurve Stack Management**
- **VLAN Configuration**
- **Support/Mgmt URLs**

For more information on switches:

See the chapter **Alerts** for more information on handling alerts.

See the chapter **Setting Up Security for a Device** for information on device security.

See the chapter **Performing Diagnostics** for information on resetting devices and performing Link and Ping tests.

Displaying Switch Status

Status - Overview Page

To launch the Status - Overview page for a device that is manageable by browser, double-click on a device in the Devices list or in a topology map, or right mouse-click on a device and select **Properties (Device View)**. If the device is not manageable by browser you will see the Closeup View in a separate window (you must launch the Closeup View from the management station). The Status - Overview page is divided into two areas, the Graph area and the Alert Log area.

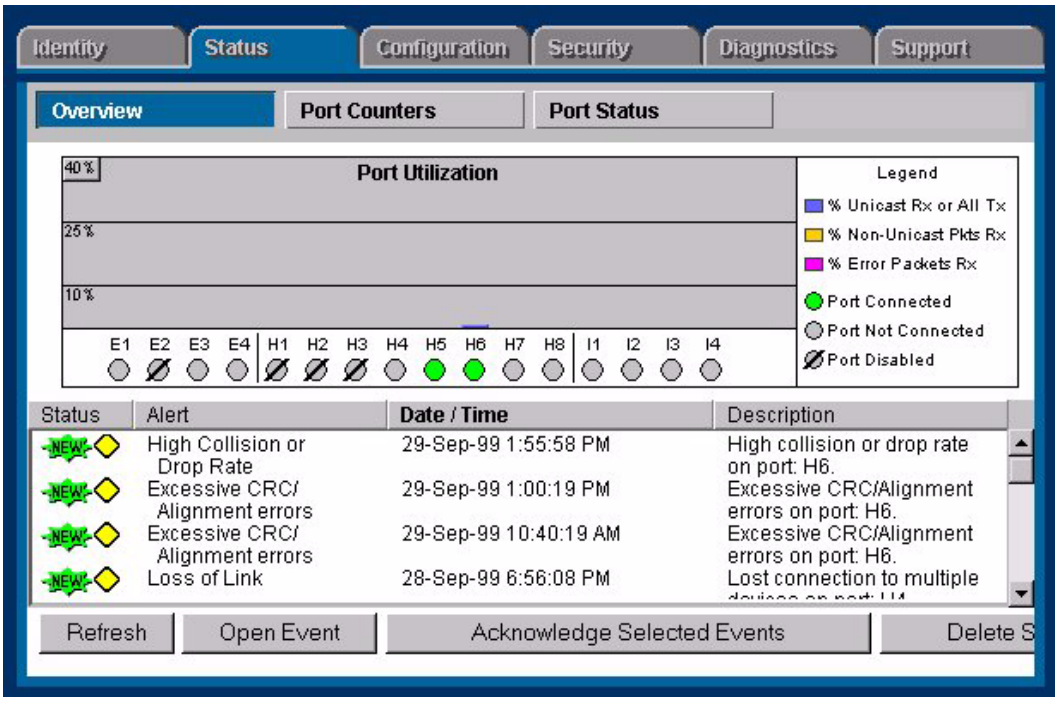


Figure 13-1. Status Overview Page

Graph Area

The bar graph gives a quick overview of the performance of the switch. Each bar shows the highest percentage of transmitted (TX) or received (RX) traffic utilization for that port in the last five seconds.

The graph area proportionally depicts three attributes for each port:

- Unicast packets—The percent utilization for packets that were not addressed to a multicast or broadcast address.
- Non-Unicast packets—The percent utilization of received non-unicast packets (both broadcast and multicast). If there is a broadcast storm, only the port receiving these packets shows high utilization, letting you quickly pinpoint the problem.
- Errors—The percent utilization for error packets received. A high percentage may indicate possible network problems.

Place the cursor over a bar in the graph to display the exact percentages for each attribute and to display the speed of that port.

The graph only scales to 40% utilization. Network utilization above this level indicates serious performance problems.

The graph also shows you if a port is active, disabled, or not connected.

Alert Log Area

The “Find/Fix/Inform” capability of a device helps you proactively manage your network by displaying network traps and problem conditions in one easily accessible browser page. The device itself monitors counters, internal hardware information, and network traffic. When a problem is discovered, such as loss of link, a problem cable, or a broadcast storm, the Alert Log displays clear messages about the problem. When you click on an alert in the Alert Log (or select the alert and click on the Open Event button), the Alerts page displays more information about the alert as well as some suggestions for fixing the problem.

For example, the Alert Log may display the alert “Cable Length”. The following information is available:

- **Description**:

Packet loss detected on port 4. This may be due to an overextended LAN topology or faulty hardware. The loss was detected on this port, but the actual problem can be occurring elsewhere on this segment.

- **Solution**:
  - Verify the network topology is within IEEE 802.3 topology standards. All ThinLan coaxial cabling must be 185 meters or shorter. No more than 4 repeaters are allowed between any two stations in the network.
  - Insert bridges or switches between repeaters to extend network topology if needed.
  - Also, check for faulty cabling, transceivers, and NICs.

Using the Find/Fix/Inform capability, the device can isolate a problem that occurs on one port, preventing it from affecting the entire network.

See the chapter **Alerts** for information on reading and acknowledging alerts, setting filters, and configuring Action on Events.

Port Counters

The Port Counters information for switches displays specific network conditions or traffic. See the online help for more information about each counter.

Port Status

The Port Status page (switches only) displays the operational status of each switch port. The settings can be changed in the **Configuration - Port Configuration** page.

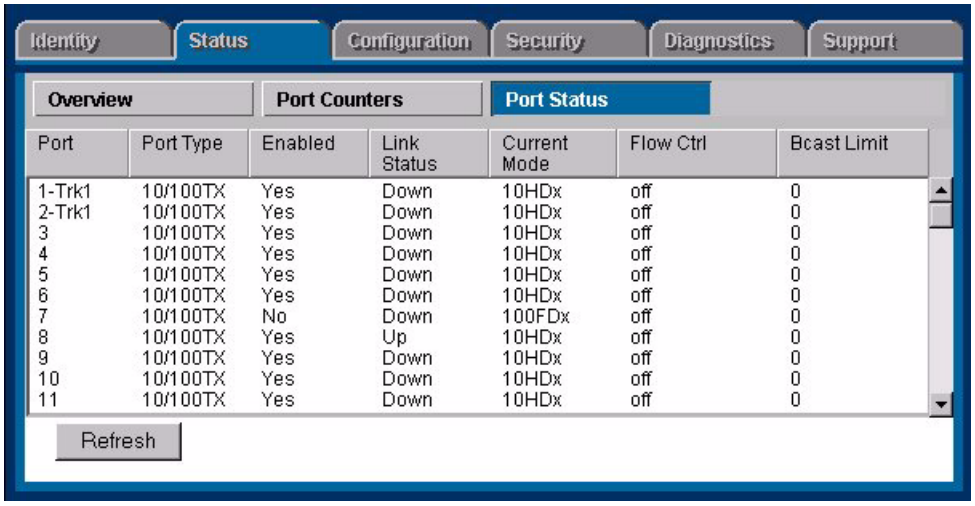


Figure 13-2. Switch Port Status

The Port Status settings are described in the following table.

Table 13-1. Port Status Settings

Setting	Description
Port	The port number.
Port Type	The network type of each switch port, for example, 100TX.
Enabled	Whether the port is enabled or disabled.
Link Status	The port's current operational status. Up means the port is working correctly. Down means the port is disabled.
Current Mode	The operational mode of the port. • 10/100 Base TX—Can be 10 Mbits half or full duplex or 100 Mbits half or full duplex. • 100 Base FX—Can be 100/full duplex or 100/half duplex. • Gigabit—Can only be 1000 full duplex.
Flow Control (not available on the HP J3298 A or HP J3299A)	Indicates the current state of flow control for this port. • 10/100TX, 10 FL, 100 FX: – On—Flow control is enabled. – Off—Flow control is disabled (default). • Gigabit: – On (TX, RX)—Flow control is enabled on transmit and receive. – On (RX)—Flow control on receive only. – Off (default)—Flow control is disabled.
Bcast Limit (not available on the HP J3298 A or HP J3299A)	The Broadcast Limit, expressed as a percentage of broadcast packets relative to the theoretical limit. Any broadcast or multicast traffic exceeding this limit will be dropped. A value of zero indicates that no limit is to be applied. Values range from 0-99.

Switch Identity Information

The Identity tab (**Properties** menu item in the **Actions** menu) displays some basic information about the switch. You can also display this information in the Identity page of the Device View.

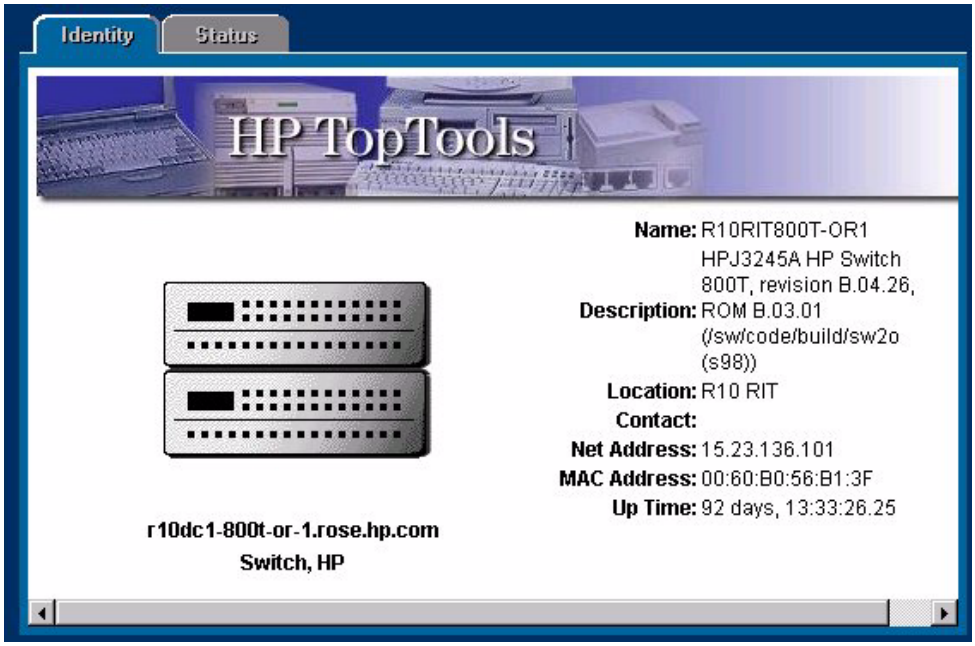


Figure 13-3. Identity Page for HP Switch 800T

The Status tab (**Properties** menu item in the **Actions** menu) shows the network interfaces and ping status for the switch.

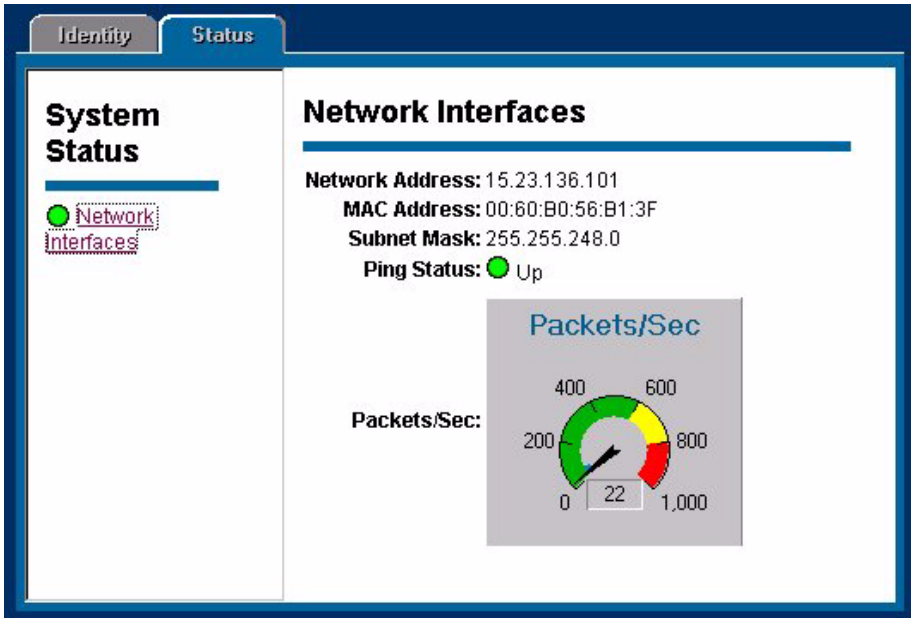


Figure 13-4. Switch Status Page with Network Interfaces

Configuring Switch Features

The Configuration page lets you configure many switch features, for example, the sensitivity levels for Fault Detection. Click on a device in the Devices page and select **Properties (Device View)** from the **Actions** menu. Click on the **Configuration** tab.

Device View

There is a Device View for every managed HP switch. The Device View for the HP ProCurve Switch 2424M looks like the following graphic. Use the online help to obtain information about specific switch modules.

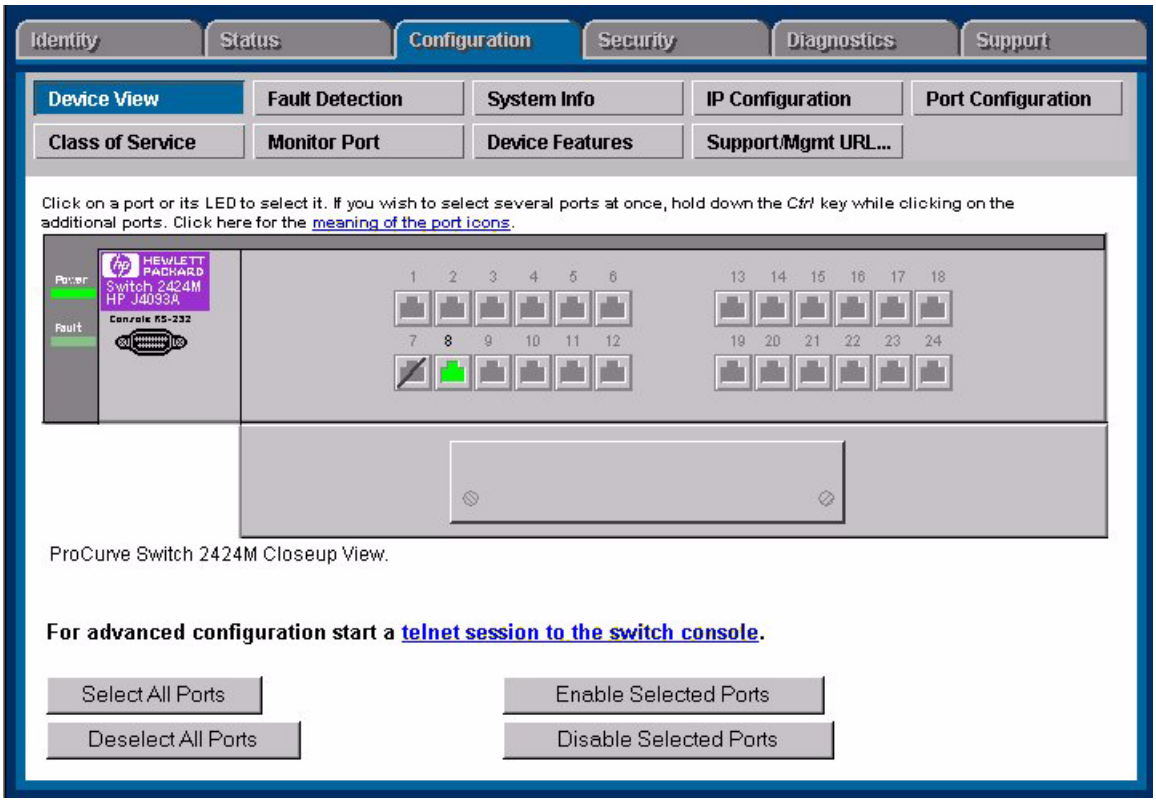


Figure 13-5. Device View for the HP ProCurve Switch 2424M

Fault Detection

The automatic fault detection feature protects your network from failing because of problems such as network loops, defective cables, transceivers and faulty network interface cards. Network problems are automatically detected and entered in the Alert Log. The Fault Detection page lets you set the sensitivity levels for the actions to be taken when a fault is detected on a port in your network. Switches only have a sensitivity setting for logging network problems. The sensitivity settings are:

High Sensitivity: The device will make an entry in the Alert Log (located in the Status tab) when a network problem of any severity occurs.

Medium Sensitivity: The device will make an entry in the Alert Log when serious network problems occur.

Low Sensitivity: The device will make an entry in the Alert Log only when severe network problems occur. These are problems that may bring the network down.

Never: The device will never make any entries in the Alert Log regardless of the severity of the problem.

System Information

The System Information page lets you enter a system name for the device, the location of the device, and whom to contact in the event of a problem.

IP Configuration

Select the way that you want IP addresses configured for your network:

- Manual—Set the IP address through the console.
- Disabled—IP is disabled, there is no access to management or telnet. **Not Recommended**.
- Use Bootp—The Bootp (or DHCP) protocol sets the IP address automatically.

If you select Manual configuration, you can change the IP address, a subnet mask, and a default gateway for the device.

Some switches let you configure an IP address for every VLAN you have created.

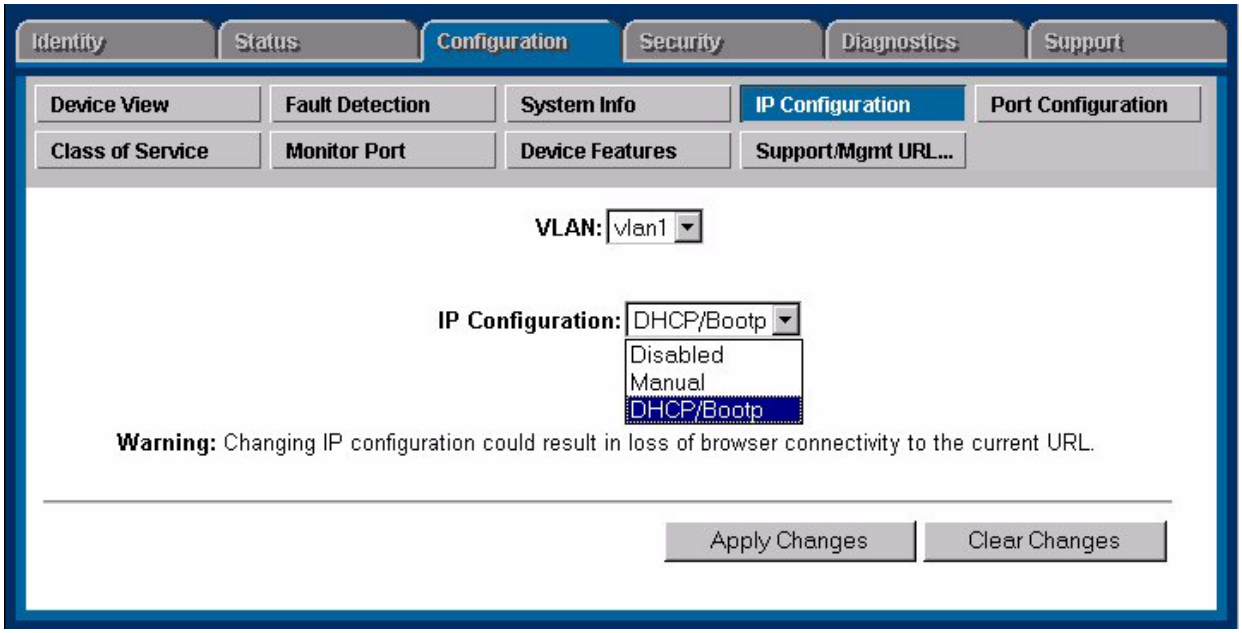


Figure 13-6. Switch IP Configuration

Characteristics of Bootp and DHCP

The Bootp protocol is designed for a network in which each host has a permanent network location. It is not adaptable to a mobile computing environment.

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 only need the address for an hour, while another device may use the same address for several days. DHCP is more suitable in environments where the number of IP addresses needed exceeds the number available. It also allows a device to obtain its configuration information, such as the IP Address and Subnet Mask, in one message, reducing the demand on the network.

A static IP address is a unique address that is assigned to one client only. Static addresses are used for an extended time period.

Port Configuration

The Port Configuration page displays information about the switch ports. The settings are explained in the following table. To modify a port setting, click on a port then select the **Modify Selected Ports** button. Modify multiple ports at one time by using Ctrl-Click to select the desired ports.

Note

Some switches support trunking. For information on trunking, see the online help for that device.

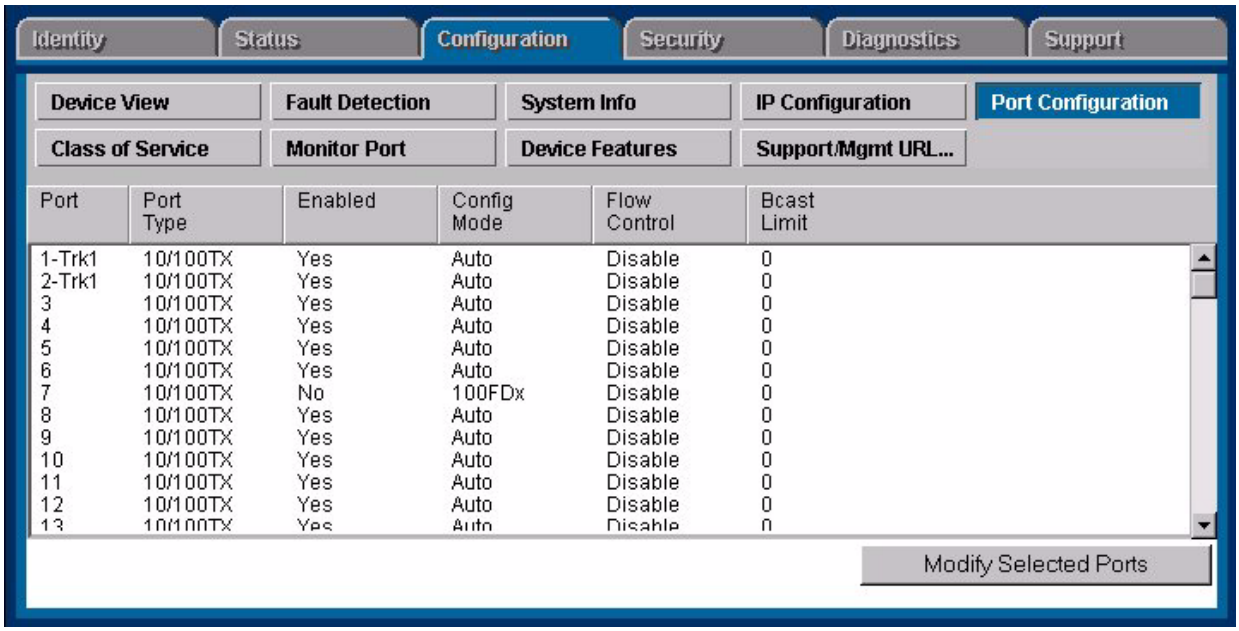


Figure 13-7. Switch Port Configuration

Table 13-2. Port Settings

Setting	Description
Port	The port number. The port may be appended with one of the following: • Trkx—The port trunk to which this port belongs • Mesh—The port has been assigned to a switch mesh domain • MP—The port is a Monitor Port
Port Type	The MAC layer type, for example, 100VG or FDDI.
Enabled	Whether the port is enabled or disabled.
Config Mode	The speed and duplexing for the port. Auto mode will negotiate with the device on that port to determine the mode. Click on **Modify Selected Ports** to change the mode.
Flow Control (not available on the HP J3298 A or HP J3299A)	Indicates the current state of flow control for this port. When disabled, the port does not generate flow control packets and drops any flow control packets it receives. • 10/100TX, 10FL, 100FX: – On—Flow control is enabled. – Off—Flow control is disabled (default). • Gigabit: – On (TX, RX)—Flow control is enabled on transmit and receive. – On (RX)—Flow control on receive only. – Off (default)—Flow control is disabled.
Bcast Limit (not available on the HP J3298 A or HP J3299A)	The Broadcast Limit, expressed as a percentage of broadcast packets relative to the theoretical limit. Any broadcast or multicast traffic exceeding this limit will be dropped. A value of zero indicates that no limit is to be applied.Values range from 0-99.

Class of Service

There will always be points in the network where multiple traffic streams merge or where network links will change speed and capacity. It is important to move traffic on the basis of relative importance. Without CoS prioritization, less important traffic can consume network bandwidth and slow down or halt the delivery of more important traffic. For example, without CoS, most traffic received by a switch is forwarded with the same priority it had when entering the switch. In many cases, such traffic is “normal” priority and competes for bandwidth with all other normal-priority traffic, regardless of its relative importance to your organization’s mission. CoS keeps the most important network traffic moving at an acceptable speed, regardless of current bandwidth usage. This means you can manage available bandwidth so that the switch transmits the most important traffic first.

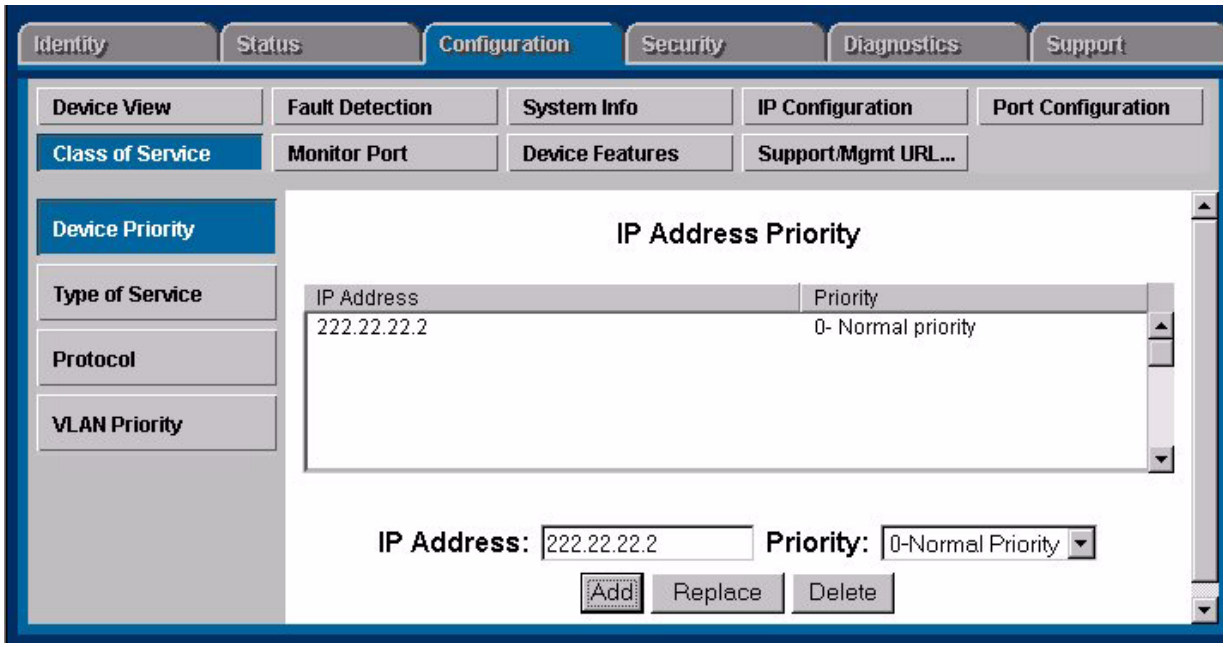


Figure 13-8. Class of Service showing the IP Address Priority Page

Note

The Quality of Service features available in HP TopTools for Hubs & Switches includes the ability to set up consistent traffic prioritization (Class of Service) policies across the ProCurve switches in your network. The Class of Service features can also be configured on an individual switch using the switch's console or web browser interface. HP ProCurve documentation uses Quality of Service (QoS) to refer to HP TopTools (network-wide) prioritization, and Class of Service (CoS) to refer to prioritization configured on an individual switch (using the switch's web browser or console interface).

Using VLANs to Maximize the CoS Benefit

Without an 802.1Q tagged VLAN environment, CoS can prioritize only the movement of outbound traffic through individual ProCurve switches in your network. Using 802.1Q tagged VLANs provides the maximum advantage by allowing CoS to set priorities that are supported by downstream devices. This means that CoS can support improved performance for present traffic levels as well as future traffic growth while optimizing the use of existing resources and delaying the need for further investments in equipment and services. That is, CoS enables you to:

- Specify which traffic in the switch has higher or lower priority, regardless of current network bandwidth or the relative priority setting of the traffic when it is received on the switch.
- Change (upgrade or downgrade) the priority of outbound traffic.

- Override “illegal” packet priorities set by upstream devices or applications that use 802.1Q VLAN tagging with 802.1p priority tags.
- Avoid or delay the need to add higher-cost NICs (network interface cards) to implement prioritizing. Instead, control priority through network policy administered by HP TopTools for Hubs & Switches.

Definitions

The following terms are used frequently with policy configuration.

- Differentiated services bits: The upper 6 bits of the Type of Service (ToS) field (the DS field) of an IP packet
- Downstream device: A device linked directly or indirectly to an outbound switch port. The switch sends traffic to downstream devices.
- Inbound port: Any port on a switch through which traffic enters the switch
- Outbound port: Any port on a switch through which traffic leaves the switch
- Outbound port queue: For any port, a buffer that holds outbound traffic until it can leave the switch through that port. There is a “high priority” queue and a “normal priority” queue for each port in the HP ProCurve switches supporting this feature. Traffic in a port’s high priority queue leaves the switch before any traffic in the port’s normal priority queue.
- Precedence bits: The upper three bits in the Type of Service (ToS) field of an IP packet
- Upstream device: A device linked directly or indirectly to an inbound switch port. The switch receives traffic from upstream devices.
- 802.1p priority: A traffic priority setting carried only in packets in 802.1Q tagged VLANs. This setting can be from 0 to 7.
- 802.1Q tagged VLAN: A virtual LAN (VLAN) that complies with the 802.1Q standard and is configured as “tagged”. (For more on VLANS, see the Management and Configuration Guide you received with your HP ProCurve switch.)

Basic Operation

Configuring a CoS policy in the switch affects switch internal traffic priorities at the outbound port and, if 802.1Q VLANs are configured in your network, the priority settings in traffic leaving the switch. This enables control over traffic movement within the switch as well as control over the priority settings in packets going to downstream devices and applications that can use those settings.

Policy Option for Controlling Traffic Priorities at the Outbound Port.

Each port in the switch has two outbound traffic queues; “normal” priority and “high” priority. (High-priority packets leave the switch port first. Normal-priority packets leave the switch port after the port’s high-priority queue is emptied.) With no CoS control, all traffic (with two exceptions) goes through

the “normal” outbound port queues. However, with a CoS policy operating in your network, you can determine the outbound priority queue to which a packet is sent.

Policy Options for Extending Traffic Priority Control to Outbound Packets Traveling to Downstream Devices.

If an outbound packet is in an 802.1Q tagged VLAN environment, that is, if the packet is assigned to a tagged VLAN on the outbound port, then the packet carries an 802.1p priority setting that was configured in the switch. This priority setting can range from 0 to 7, and can be used by downstream devices that have up to eight queues. While packets within a switch move only at high or normal priority, they still can carry the 802.1p priority that can be used by downstream devices that have more than two priority levels. Also, if the packet enters the switch with an 802.1p priority setting, CoS can override this setting if configured appropriately.

Note

If you are not using multiple tagged VLANs in your network, you can still use the tagged VLAN feature available in HP ProCurve switches by configuring the default VLAN as a tagged VLAN.

Priority Settings for Outbound Packets. You can configure a CoS priority of 0 through 7 for an outbound packet. When the packet is sent to a port, the CoS priority determines which outbound queue the packet uses.

Table 13-3. CoS Priority

QoS Setting	Outbound Port Queue	Operation
0*-3	normal	Packets in this queue leave the port after the high-priority queue is emptied.
4-7	high priority	Packets in this queue leave the port first.
* Note that in compliance with the 802.1p standard, “0” is ranked as “normal” and is a higher priority than “1” and “2”.		

If a packet is not in an 802.1Q tagged VLAN environment, the above settings control only to which outbound queue the packet goes, and no 802.1p priority is added to the packet. However, if the packet is in an 802.1Q tagged VLAN environment, then the above setting is also added to the packet as an 802.1p priority that can be used by downstream devices and applications, as shown in the Priority Mapping Table. For each priority policy setting this table shows:

- The corresponding outbound port queue a packet will use when exiting from any switch covered by the policy
- The corresponding 802.1p priority setting the packet will carry when it leaves the switch

- The priority queue assignment that the packet will receive in a downstream device that uses 802.1p priority settings.

Table 13-4. Priority Mapping Table

Priority Policy Set in HP TopTools	Outbound Port Queue in the ProCurve Switches	802.1p Priority Setting Added to Tagged VLAN Packet Leaving the Switch	Queue Assignment Downstream		
			8 Queues	4 Queues	2 Queues
1	Normal	1 (low priority)	Queue 1	Queue 1	Queue 1
2		2	Queue 2		
0		0 (normal priority)	Queue 3	Queue 2	
3		3	Queue 4		
4	High	4	Queue 5	Queue 3	Queue 2
5		5	Queue 6		
6		6	Queue 7	Queue 4	
7		7 (high priority)	Queue 8		

Criteria for Prioritizing Outbound Packets

You can configure CoS prioritization on the basis of five criteria ranked as follows:

1. Device Priority (destination or source IP address)
2. IP Type of Service (ToS) field
3. Protocol Priority (IP, IPX, ARP, DEC LAT, AppleTalk, SNA, and NetBeui)
4. VLAN Priority
5. Incoming 802.1p Priority (present in tagged VLAN environments)

If more than one criteria is present in a packet, the highest ranked of the criteria is used to prioritize the packet; all lower-ranked criteria are ignored. For example, if CoS assigns high priority to “red” VLAN packets and normal priority to IP packets, IP packets on the “red” VLAN will be set to normal priority since Protocol Priority (third in precedence) has precedence over VLAN priority (fourth in precedence).

The “Priority Criteria and Precedence” table provides a more detailed description of how this works.

Guidelines for Configuring CoS Priorities

Using CoS in a tagged VLAN environment controls the following:

- Outbound port queue—The queue to which a high or normal packet will be sent
- Outbound 802.1p priority—The new 802.1p priority setting in an outbound packet or the packet's existing 802.1p setting. This enables the packet to carry an 802.1p priority to the next downstream device.

Using CoS without a tagged VLAN environment affects only the outbound port queue to which a packet is sent. It prioritizes traffic flow only within the switch. However, without a tagged VLAN environment, an outbound packet cannot carry an 802.1p priority setting to a downstream device.

Note

If you use HP TopTools for Hubs & Switches to configure Quality of Service (QoS) policy in a network, it overrides any CoS settings configured through the console or the web browser interface in any individual HP ProCurve switch.

Steps for Configuring CoS Priority

The following table shows the Priority Criteria and their precedence.

Table 13-5. Priority Criteria and Precedence

Precedence	Criteria	Description
1	Device Priority (IP Address	You can specify a priority for any packet having a particular destination or source IP address. It is recommended that you prioritize server addresses instead of client addresses in order to include the widest possible range of traffic in your device priority policy. If an outbound packet has an IP address as the destination, it takes precedence over another outbound packet that has the same IP address as a source. (This can occur, for example, on an outbound port in a switch mesh environment.) Default state: No IP address prioritization. If a packet does not meet the criteria for device priority, then precedence defaults to IP Type of Service (ToS) criteria, below.
2	IP Type-of-Service (ToS)	Applies only to IP packets. The ToS field in an IP packet is configured by an upstream device or application before the incoming packet enters the switch, and is not altered by the switch. The switch reads the packet's Type of Service (ToS) field and prioritizes the packet (if specified in the CoS configuration) for outbound transmission. The default state is Disabled. If a packet does not meet the criteria for ToS priority, then precedence defaults to Protocol criteria, below.

3	Protocol Priority	The switch can prioritize outbound packets for one or more of these network protocols: IP, IPX, ARP, DECNet, AppleTalk, SNA, and NetBEUI. Default state: No override for any protocol. If a packet does not meet the criteria for Protocol priority, then precedence defaults to VLAN criteria, below.
4	VLAN Priority	Enables packet priority based on the name of the VLAN in which the packet exists. For example, if the default VLAN (DEFAULT_VLAN) and the "Blue" VLAN are both assigned to a port, and Blue VLAN traffic is more important, you can configure CoS to give Blue VLAN traffic a higher priority than DEFAULT_VLAN traffic. (Priority is applied on the outbound port.) Default state: No override. If a packet does not meet the criteria for VLAN priority, then precedence defaults to Incoming 802.1p criteria, below.
5	Incoming 802.1p Priority	When a packet enters the switch on a tagged VLAN, if CoS is not configured to apply to the packet's priority setting, the switch uses the packet's existing 802.1p priority (assigned by an upstream device or application) to determine which outbound port queue to use. If the packet leaves the switch on a tagged VLAN, then there is no change to its 802.1p priority setting. If the packet leaves the switch on an undated VLAN, the 802.1p priority is dropped. **Entering** (Inbound) 802.1pPriority 0-3 4-7 Outbound Port Queue Normal High Exiting (Outbound 802.1p Priority) 0-3 4-7 If a packet does not meet the criteria for Incoming 802.1p priority, then the packet is sent to the "normal" outbound queue of the appropriate port. If the packet did not enter the switch on a tagged VLAN, but exits from the switch on a tagged VLAN, then a tagged VLAN field, including an 802.1p priority of 0 (normal), is added to the packet.

Assigning a Monitoring Port

The Monitor Port tab (only found on switches) lets you select a "Monitoring Port" that you can use with a network analyzer to monitor other ports on the switch. For the HP J3298A and HP J3299A you can only choose the Monitoring port and the port to be monitored. For other switches you can choose to have all the ports for one VLAN monitored, or you can select individual ports to be monitored. See the online help for information on specific switches.

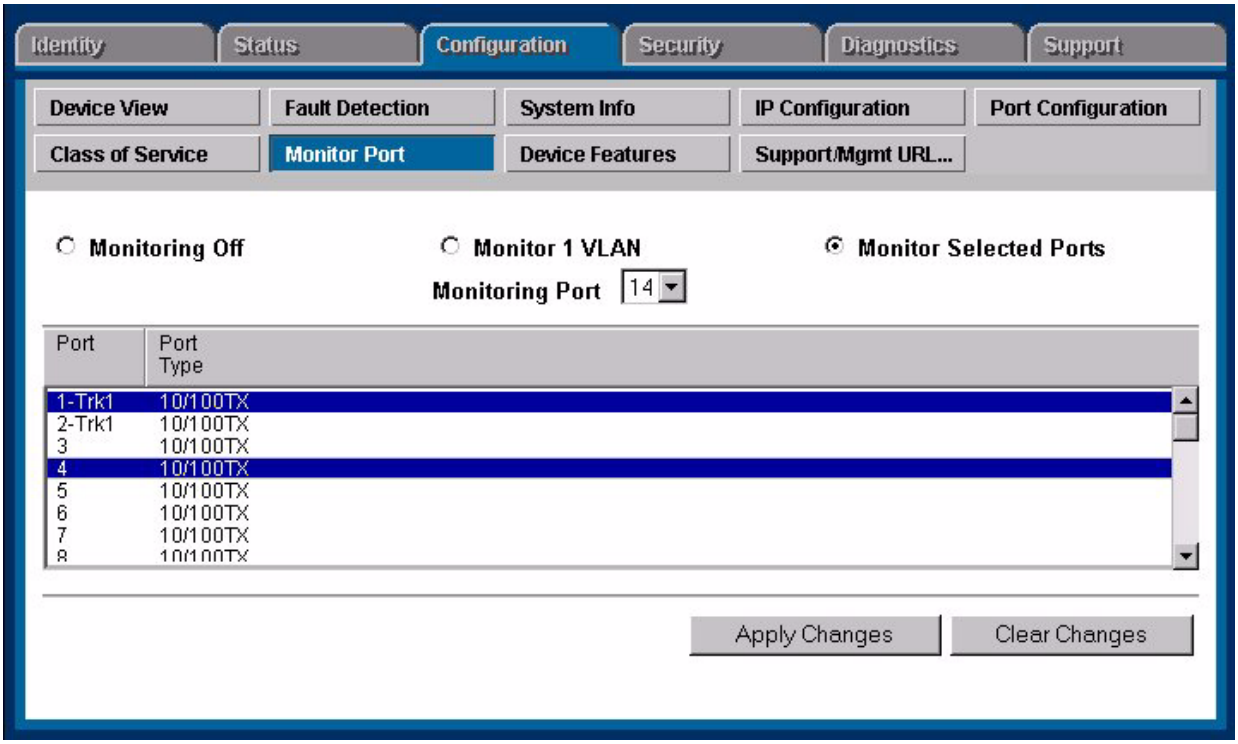


Figure 13-9. Monitoring Selected Ports on a Switch

Setting Device Features

The Device Features page (only found on switches) lets you set some or all of these features:

- Automatic Broadcast Control (ABC)—ABC reduces the number of broadcasts propagated through the network. See **Automatic Broadcast Control** for further discussion of this feature.
- Multicast Filtering (IGMP)—The Internet Group Management Protocol is a method for automatically controlling multicast traffic through the network. Using multicasting, applications can send one copy of a packet addressed to a group of computers that wish to receive it. This method is more efficient than sending a separate copy to each node, and saves bandwidth when large transmissions such as video are sent across the network. See **Internet Group Management Protocol** for further discussion of this feature.
- Spanning Tree—Spanning Tree is used to detect and break circular traffic patterns by disabling certain links. It prevents loops in redundant switches by maintaining the secondary switch as a backup.

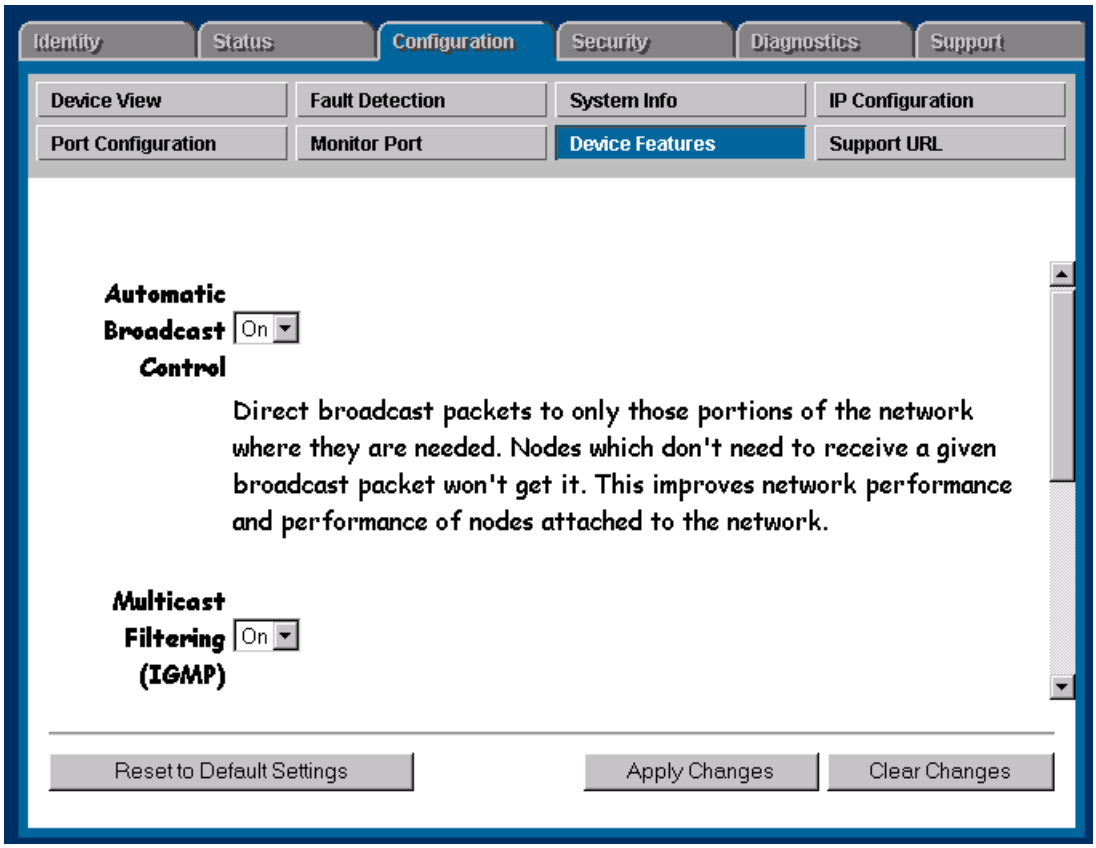


Figure 13-10.Switch Device Features Page

If you have configured VLANs for the switch (you must do this with the device console), select a VLAN for which the features will apply.

Note

It is recommended that you use the Group Policies feature (accessed in the Top Tools for Hubs & Switches home page) to set these features for all your switches. Setting features individually, for example, Spanning Tree, could create problems with your network.

HP ProCurve Stack Management

If an HP switch has been updated to software release C.08.XX, you can configure switches for stack management. The switches that support this feature are the HP ProCurve Switches 8000M, 4000M, 1600M, 2424M and 2400M.

If the switch has been configured as a Commander for the stack, the Device view has an additional header above the tabs.

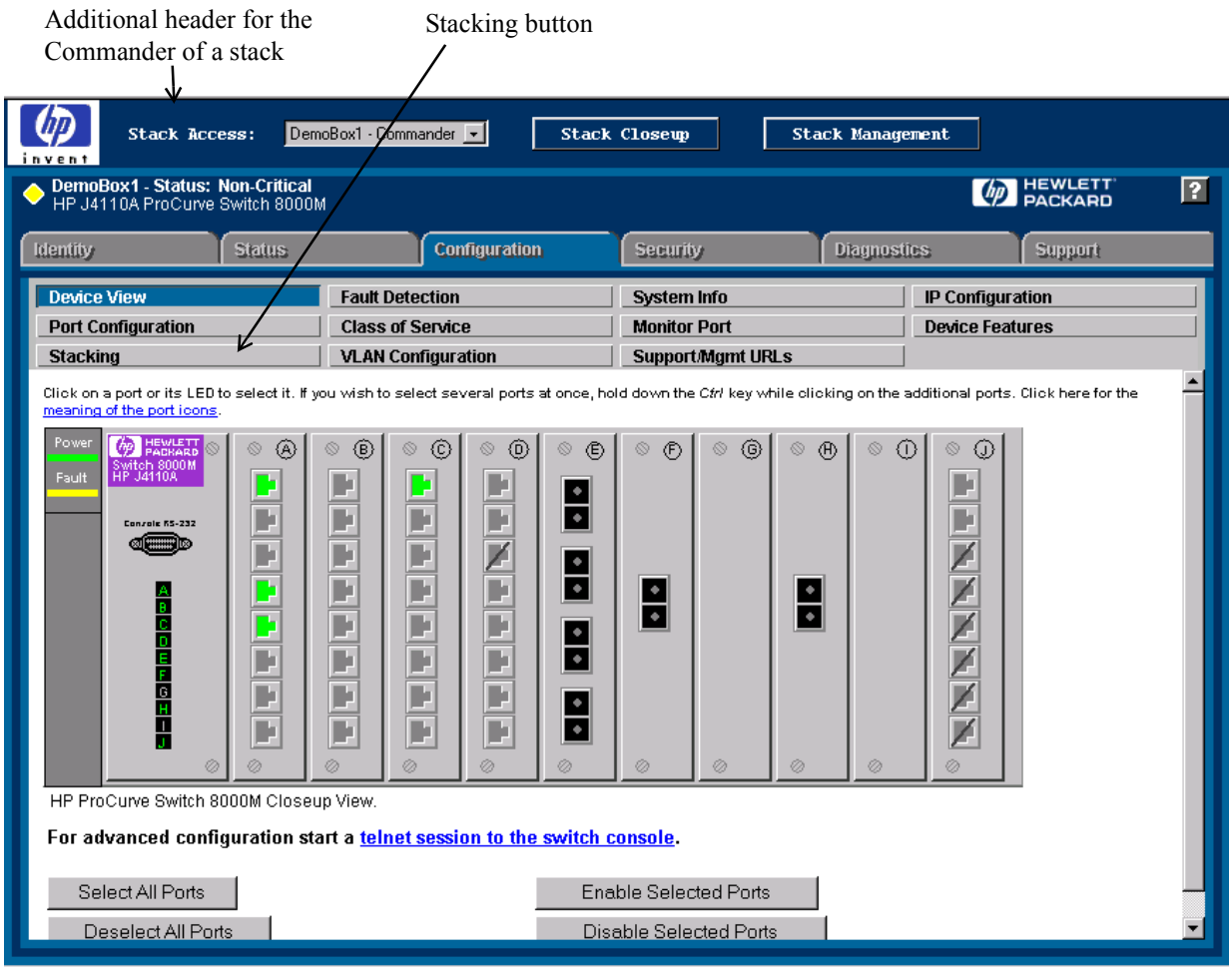


Figure 13-11.Configuration Page for HP 8000M as Commander of a Stack

Stacking allows the configuration of a group of switches so that they appear as one unit with one IP address. This provides a single point of IP management for all switches in the stack and allows the configuration of multiple ports or switches at one time. All members of the stack must be on the same subnet; the stack cannot cross a router. There is no limit on the number of stacks you can create.

A stack can have up to 16 switches; one switch must be the Commander, the other fifteen switches are Members.

Stack Management with VLANs

You can use stacks in a VLAN environment. Each switch in the stack (Commander and Members) uses only the default VLAN configured in that switch for stack links. In the Web browser interface, this is the VLAN labeled Default <VLAN ID>. All VLANs in the stack need to be interconnected through the default VLAN.

The VLAN ID for the default VLAN must be the same for all switches in the stack. The default VLAN name can differ among switches in the stack. For example, if the VLAN ID (VID) for the default VLAN in Switch A is "1" and the default VID for Commander Switch B is "5", then Switch A can't be a Candidate or a Member of Commander Switch B's stack, even though you may have connectivity to Switch A from Commander Switch B through other tagged VLANs.

Benefits of Stack Management

Stacking benefits include:

- Reducing the number of IP addresses required for managing your switches
- Increasing the scalability of your network to handle more traffic when used with switch meshing
- Simplifying network management for small groups

See the online help for more information about stack management.

VLAN Configuration

VLANs are a method for segmenting a network into related groups, improving the efficiency of traffic flow and limiting the propagation of multicast and broadcast messages. Traffic between VLANs is blocked unless the VLANs are connected by a router, increasing security.

A VLAN is a group of ports designated by the switch as belonging to the same broadcast domain. That is, all ports carrying traffic for a particular subnet address would belong to the same VLAN. Using a VLAN, you can group users by logical function instead of physical location. This helps to control bandwidth usage by allowing you to group high-bandwidth users on low-traffic segments and to organize users from different LAN segments according to their need for common resources. Beginning with release C.06.01 of the switch software (operating system, or "OS") you can use the switch's console interface to configure up to 30 port-based, IEEE 802.1Q-compliant VLANs. (Earlier releases of the OS allow up to eight port-based, IEEE 802.1Q-compliant VLANs.) This enables you to use the same port for two or more VLANs and still allows interoperation with older switches that require a separate port for each VLAN.

The benefits of VLANs include:

- Grouping users into logical networks for increased performance

- Providing an easy, flexible, less costly way to modify logical groups in changing environments
- Preserving current investment in equipment and cabling
- Allowing administrators to “fine tune” the network
- Providing independence from the physical topology of the network

If an HP switch has been updated to software release C.08.xx, you can configure VLANs with the Web browser. The switches that support this feature are the HP ProCurve Switches 8000M, 4000M, 1600M, 2424M and 2400M.

Enabling VLANs

To enable VLANs, click the **VLANS Enabled** radio button at the bottom left of the table in the **VLAN Configuration** page.

Note

If you change a setting, you must reboot the switch for the change to take effect.

Adding a VLAN

If you want to add another VLAN to your switch:

1. Click on the **Add/Remove VLANs** button at the bottom of the table in the VLAN Configuration page. The **Add/Remove VLANS** page displays. Two fields appear below the Current VLAN Definitions box.
2. Enter a name for the new VLAN in the **VLAN Name** field.
3. Enter the **802.1Q ID** (an unused number between 1 and 4094) in the field labeled **802.1Q VLAN ID**.
4. Click on the **Add VLAN** button. The VLAN appears in the Current VLAN Definitions box.

Renaming a VLAN

1. Click on the Add/Remove VLANs button at the bottom of the table in the VLAN Configuration page. The Add/Remove VLAN page displays.
2. Select the VLAN to be renamed from the Current VLAN Definitions list.
3. Enter a name for the selected VLAN in the New VLAN Name field.
4. Click on the Rename Selected VLAN button to save the new name.

Removing a VLAN

1. Click on the Add/Remove VLANs button at the bottom of the table in the VLAN Configuration page. The Add/Remove VLAN page displays.
2. Select the VLAN to remove from the Current VLANS box.
3. Click on the Remove Selected VLAN button.

4. Confirm removal of the VLAN.

Modifying Port VLAN Configuration

There are three modes a port in a VLAN can be in:

- Tagged—When a port is tagged, it allows communication among the different VLANs to which it is assigned.
- Untagged—When a port is untagged, it can only be a member on one VLAN.
- No—the port is not a member of that VLAN.

To modify a port in a VLAN:

1. In the VLAN table, click on the **Modify** button for the VLAN whose ports you want to modify. The **Modify Port VLAN Configuration** page displays.
2. Select the port to be modified.
3. Select the mode, for example, **Tagged**.
4. Click on the **Apply** button.

Enabling GVRP Security

The Generic Attribute Registration Protocol (GARP) propagates topology information by using tags. The GARP VLAN Registration Protocol (GVRP) is an 802.1Q-compliant method for facilitating automatic VLAN membership configuration. GVRP-enable switches can exchange VLAN configuration information with other GVRP-enabled switches. Unnecessary broadcast traffic and unicast traffic also can be reduced.

Policy rules or other network management methods can determine who is admitted to a VLAN. When a node requests admission to a specific VLAN, GVRP handles the registration of the node with GVRP-enabled switches and maintains that information.

The GVRP protocol allows switches to tell each other which ports carry the traffic for a particular VLAN. For example, Switch A tells all other switches that it is connected to VLAN1. Any other switch connected to Switch A can also connect to a member of VLAN1. This is easier than manually configuring the ports of each switch to belong to a particular VLAN.

To enable GVRP Security for a port in a VLAN:

1. First make sure that the **GVRP Enabled** radio button at the bottom of the table in the VLAN Configuration page is checked.
2. Click on the **GVRP Security** button. The GVRP Security page displays.
3. Select the ports for which you want to assign a different security mode.
4. In the **Security Mode** drop-down list box, select the mode. The choices are:
   - Learn—The port will join the advertised VLAN and propagate a VLAN join request through all other forwarding ports that are participating in GVRP.

- Disable—GVRP is disabled for this port.
- Block—The port will not join the advertised VLAN and will not propagate any VLAN joins for the advertised VLAN. GVRP is totally blocked for this port; it will never learn it.

5. Click on the **Apply** button.

Support/Management URLs

Support URL

To go directly to the HP Support Site on the World Wide Web, click on the **Support** tab. You will launch the site indicated by the URL that has been entered in the Configure - Support/Mgmt URLs page. By default this is the HP ProCurve support site. The ProCurve site has information about HP devices, FAQs, firmware upgrades, white papers on current technologies, and much more. This URL is:

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

If you want to change the URL that is accessed when the Support tab is selected, type in the new address and click on the **Apply Changes** button. For example, you could change the URL to launch your site home page.

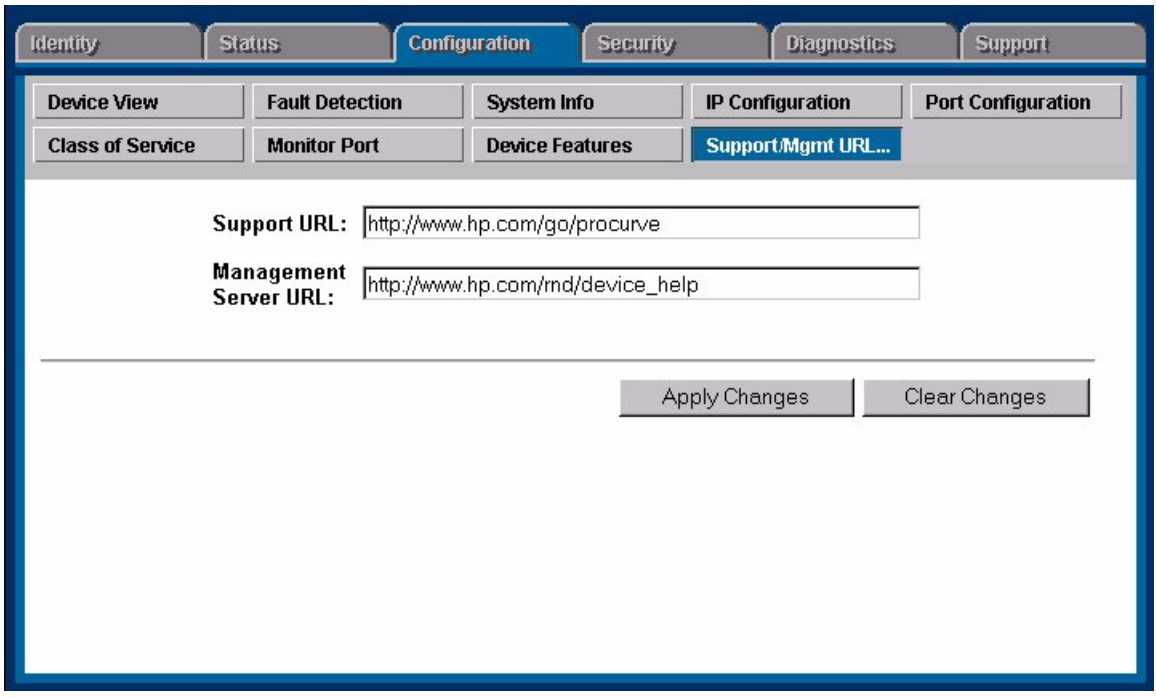


Figure 13-12.Support URL Page

Management Server URL

Enter the URL for your management server. This will let you display the online help at any client in the network.

Note

This field will contain the address for the HP ProCurve web site by default. If you do not change it, the online help will be loaded from the HP ProCurve site.

14

Setting Up Security for a Device

It is advisable to set up security for your devices to prevent unauthorized access to the device or the network. You can configure device security to prevent unauthorized use of certain parts of the network by certain nodes, and to keep unwanted traffic out of certain parts of the network. This chapter contains information on:

Device Passwords

Assigning passwords to devices helps limit access to authorized persons. In the Security page, select the **Device Passwords** button to assign passwords for the device.

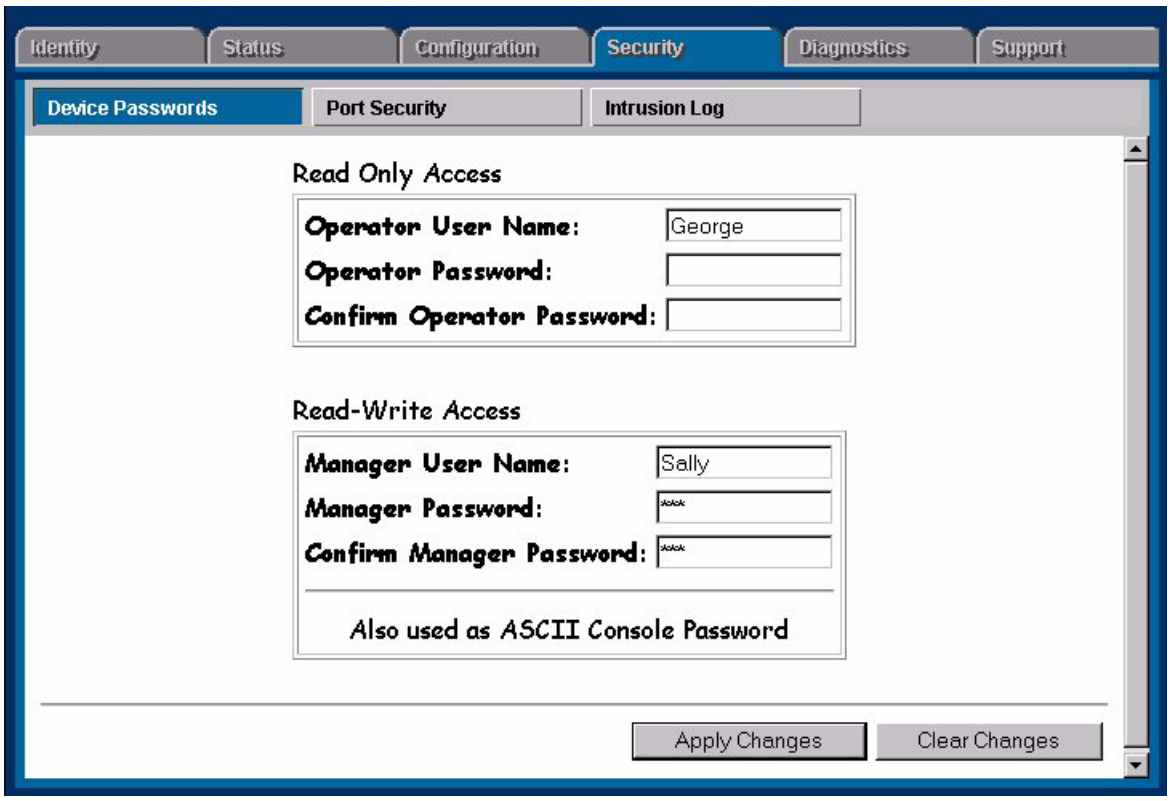


Figure 14-1. Device Passwords Page

There are two categories of passwords:

- Operator (Read only)—The Operator can view all pages except the Security pages. For switches, this password is the same as the console password.
- Manager (Full Read and Write permissions)—The Manager can view all pages and make any changes in any page. The Manager name and password are the same as the name and password used in accessing the device through the console or a telnet session. If you change the password in this page, the console password is overwritten and becomes this password.

Enter the desired names and passwords. The minimum recommended setup is to have one Manager password. Click on the **Apply Changes** button. If you want to clear these changes select the **Clear Changes** button. This will not clear any changes that you have already applied to the device.

Manager/Operator Password Combinations

The level of protection and the access granted to the device depends on what passwords are set at what levels. The table below describes the settings and their consequences.

Table 14-1. Password Settings

Passwords	Read Protected	Write Protected	Results
Manager password set Operator password not set	N/A	Yes	Anyone can get Read Access, but only the Manager can read and write to the device. Recommended minimum setting.
Manager password set Operator password set	Yes	Yes	Both the Manager and the Operator have Read Access, but only the Manager has Write Access. Everyone else is shut out of the device. Recommended setting.
Manager password not set Operator password set	Yes	Yes	The Operator has both Read and Write Access because Write Access has not been reserved for the Manager.
Manager password not set Operator password not set	N/A	N/A	Anyone can get Read and Write Access to the device. Not recommended.

See the online help for information about devices without a web agent.

The Function of Community Names

A community defines authentication and access control between an SNMP agent and a management station. The community name functions as a password in that management stations must use the community name for all Get and Set operations. This is different and separate from the Operator and Manager passwords, which protect access to the browser interface and console settings.

For information about configuring Communities by Policy, see the section **Security Configuration Policies**.

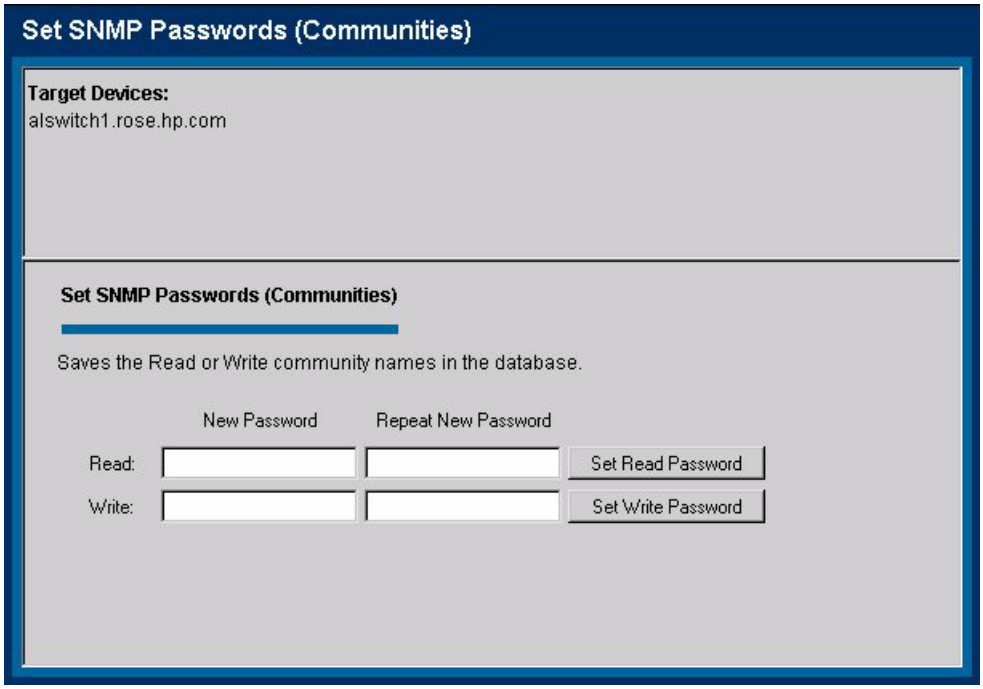


Figure 14-2. Set SNMP Community Names Page

A device must have a community name of "public" to be identified by HP TopTools for Hubs & Switches. If a device does not have a community name of "public", it will be discovered but not identified.

For HP bridges and older hubs (See Note 1) there is only one community name, which has both "read" and "write" access. The "public" community name exists, but is hidden. It has "read" access. You can use the "public" community name for "read" access in HP TopTools for Hubs & Switches.

Newer hubs and switches (See Note 2) allow you to specify multiple community names with different access levels. Only the "read" and "write" community names can be used by HP TopTools for Hubs & Switches. There is no hidden "public" community name. Use the device console to configure the community names as follows:

- For hubs:

1. From the main menu of the device console, select "2. Management Access configuration..." [or "5. Managers/Password Change...",]
2. Select "2. Community Name" [or "2. Configure community name"].
3. For the "read" Community, set Read View = User; Write View = Discovery.
4. For the "write" Community, set Read View = Full; Write View = Full.

- For Switches:

1. From the main menu on the device console, select "Configuration...".

2. Select “SNMP Communities...”.
3. For the “read” Community, set MIB View = Operator; Write Access = Restricted.
4. For the “write” Community, set MIB View = Manager; Write Access = Unrestricted.

For greater security you can specify the addresses of those stations from which SNMP requests are allowed. These addresses are specified in the list of Authorized Managers associated with each community name. Include the station on which HP TopTools is installed.

Configuring for Community Names

If running Discovery does not discover all of your devices, make sure that Ping Discovery and Web Server Discovery are checked. If some devices are still not being discovered, you need to add them manually as follows:

1. Point the browser at the HP TopTools home page.
2. In the navigation frame on the left, click **Settings** and select **Discovery** from the menu.
3. Select the **Additional Devices** tab.
4. Type in the address of the device and click the **Add Device** button.

Perform the following steps to let HP TopTools know the community names for each device:

1. Point the browser at the HP TopTools home page.
2. In the navigation frame on the left, click **Devices** and select **Device Types** from the menu.
3. Select the **All Devices** tab.
4. Select the devices in the list at the right. You can select multiple devices if they are going to have the same community name.
5. Click the right mouse button on one of the selected devices.
6. Select the **Security** menu item and **Set SNMP Passwords (Communities)**.
7. Type in the “read” community name (twice) for the selected devices and click **Set Read Password**.
8. Type in the “write” community name (twice) for the selected devices and click **Set Write Password**.
9. Run Discovery again.

Note

You may want to add routers manually and define their community names. This improves the Discovery process.

All of the features of HP TopTools for Hubs & Switches should now work correctly for all devices, with the following exceptions:

1. The topology of some older devices may not display correctly.
2. The Update Firmware... option may not work.
3. The Closeup View for devices J3100A, J3125A, J3175A, and J3177A cannot be invoked.
4. The SNMP Trap Configuration option in the Devices page will not work.

To work around numbers 1, 2, and 4 above, keep the "public" community name for these devices, specifying "read" capability. Add security for the devices (except J3125A, J3126A, and J3233A) by specifying an Authorized Manager for each device.

Note 1

Hubs and bridges with the following model numbers: J2355A, J2410A, J2413A, J2415A, J2600A, J2601A/B, J2602A/B, J2610A/B, J2611A/B, J2612A, J2630A, J2631A, J2632A, 28692A, 28674B, 28682A, 28688A/B, 28699A, 28673A, 28674A

Note 2

Hubs with the following model numbers: J3200A, J3202A, J3204A, J3301A, J3303A

Note 3

Switches with the following model numbers: J3100A/B, J3245A, J3175A, J3177A, J3298A, J3299A, J4110A, J4120A, J4121A, J4122A

Hub Port Security

You can assign security levels on hubs port by port. Select the **Port Security** button to view the current settings for each port.

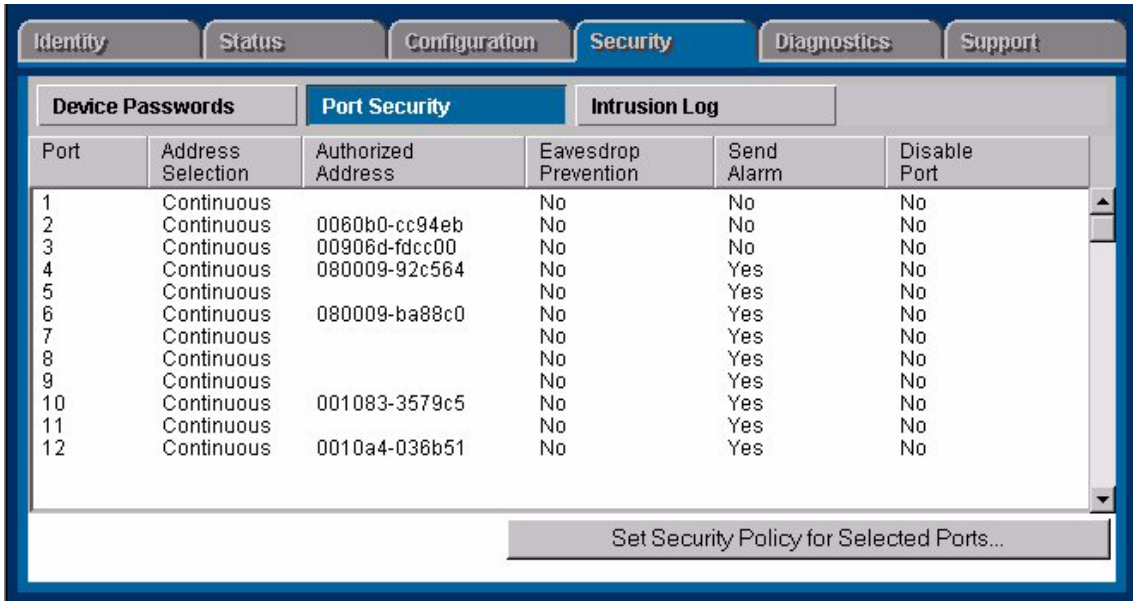


Figure 14-3. Hub Port Security Page

Address Selection

Address Selection refers to how the authorized address for a port is discovered. The three settings are explained in the table.

Table 14-2. How Authorized Addresses are Discovered

Setting	Description
Continuous	The device learns the address of the device attached to the port and makes it the authorized MAC address. If a different device is later attached to the port, the new address is learned and becomes the authorized address.
First Heard	The device learns the address of the device attached to the port and makes it the authorized MAC address. If a different device is later attached to the port, the new address is registered as an "intruder address"; a security violation has occurred and the port is automatically disabled.
Assigned	Enter the address of the device that is authorized to be attached to the port. If a different device is attached to the port, the new address is registered as an "intruder address"; a security violation has occurred and the port is disabled.

To set the Address Selection:

1. Click on the **Set Security Policy for Selected Ports** button.
2. Select a setting from the **Address Selection** drop down list.
3. Click on **Apply Settings**.

Authorized Address

The Authorized Address field contains the MAC address of the device that is authorized to be attached to the port.

Eavesdrop Prevention

Eavesdrop Prevention is a feature of several HP devices that 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 port's authorized MAC address is compared with the destination address of any outbound packets. If the addresses do not match, the bit pattern of the packet is scrambled, making it unreadable by any device on that port.

Set the Eavesdrop Prevention parameter for a port or group of ports by clicking on the **Set Security Policy for Selected Ports** button and selecting **yes** from the **Prevent Eavesdropping** drop down list.

Caution

Do not turn on Eavesdrop Prevention for a cascaded port.

Send Alarm

If you set the Send Alarm parameter to **yes**, a trap will be sent to the management station when an incoming packet from the connected node does not match the authorized address. Set the Send Alarm parameter for a port or group of ports by clicking on the **Set Security Policy for Selected Ports** button and selecting **yes** from the **Send Alarm** drop down list.

- Yes—Indicates that an alarm will be sent to a log when an incoming packet from the connected node does not match the authorized address.
- No—Indicates that no alarm will be sent to a log when an incoming packet from the connected node does not match the authorized address.

Note

In order for traps to function, you must also set the trap in the Thresholds dialog box, as follows:

1. Using the right mouse button, click on the device in the topology map.
2. Select **SNMP/Trap Configuration** from the drop down menu.
3. Select the **Thresholds** tab and set the thresholds for the traps you are interested in receiving.
4. Select the **Trap Receivers** tab and set the management stations that can capture traps.
5. Select the **Authorized Managers** tab and set the management stations that can send and receive SNMP requests for the device.

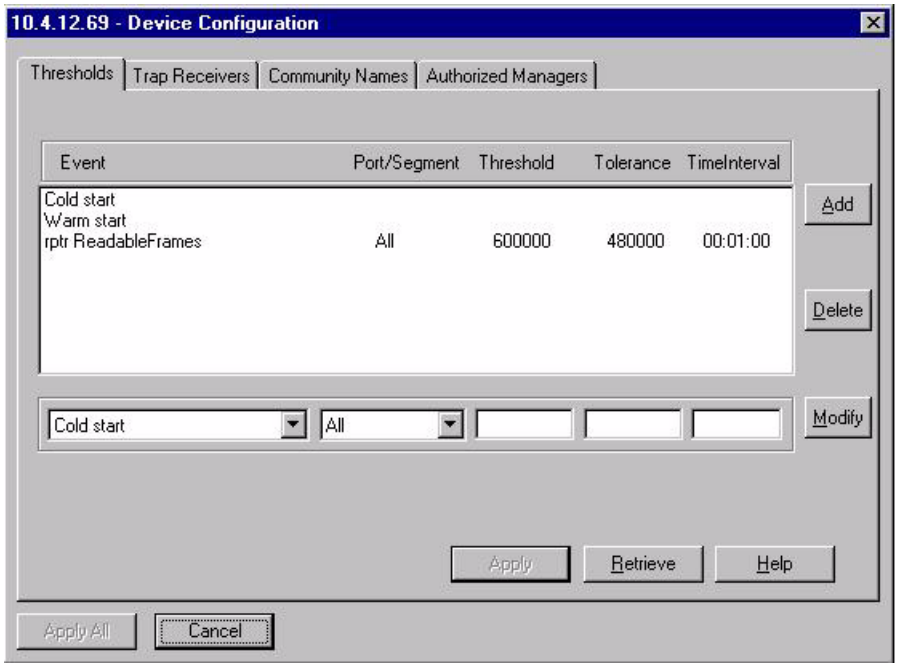


Figure 14-4. Setting the Thresholds for Trap Receivers

Disable Port

If the Disable Port parameter displays **yes**, the port may be disabled when an unrecognized address is received. Disabling the port depends on the Address Selection parameter that you have chosen. The settings **First Heard** and **Assigned** will disable the port if a new address is heard on that port. The port will not be disabled when a new address is learned if the setting is **Continuous**.

Setting Security Policy for Selected Ports

You can set the security policy port by port, or by selecting a group of ports. Select one port by clicking on the entry in the Port Security page. To select more than one port, you can Ctrl-click on each port you want to include, or to select a range of contiguous ports, click on the first port in the range, then shift-click on the last port to be included. Click the **Set Security Policy for Selected Ports** button. Select the parameters that you want to assign.

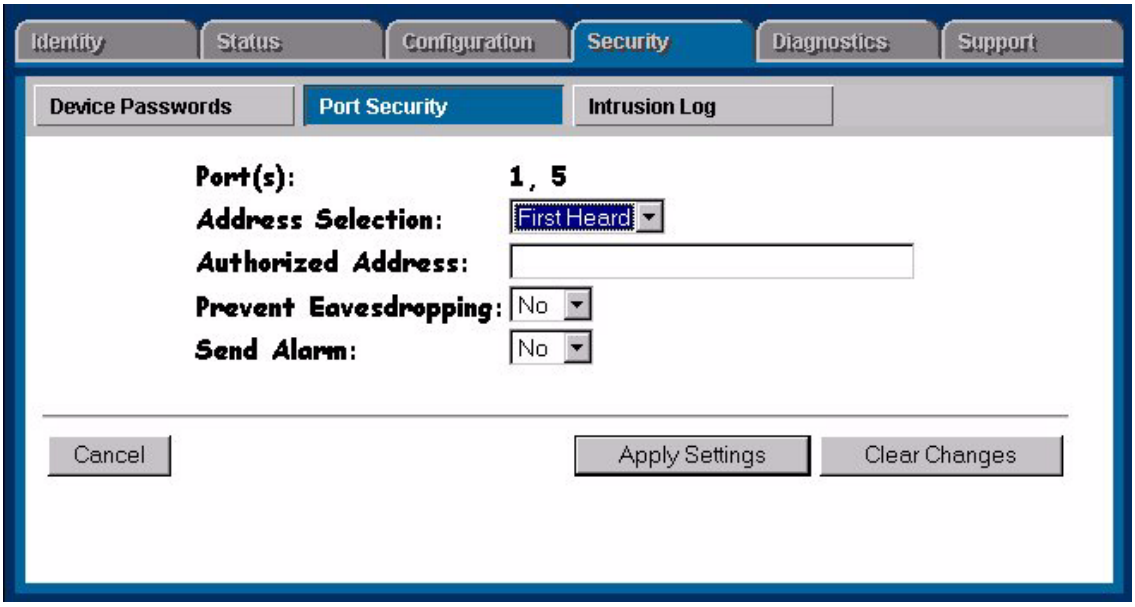


Figure 14-5. Setting the Security Policy for Selected Ports

The Hub Intrusion Log

The Intrusion Log page lets you view security intrusions (violations) of a device. The information displayed includes:

- Port—The ports that have detected attempts of unauthorized access.
- Intruder Address—The address of the intruder. The IP address is displayed for SNMP agent violations. The MAC address is displayed for port violations. The port violation must be cleared before another port violation will display.
- Date/Time—Date and time the security intrusion occurred.

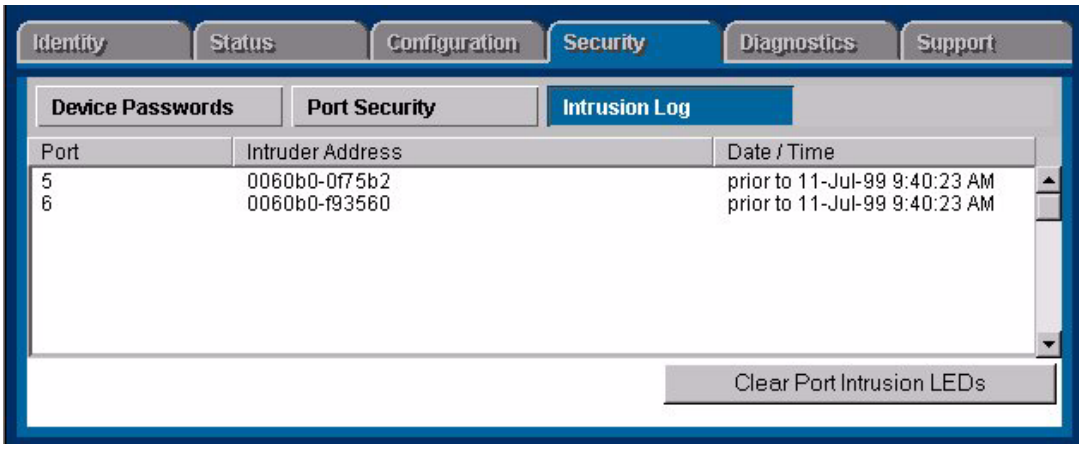


Figure 14-6. Hub Intrusion Log

Switch Port Security

Using Port Security, you can configure each switch port with a unique list of the MAC addresses of devices that are authorized to access the network through that port. This enables individual ports to detect, prevent, and log attempts by unauthorized devices to communicate through the switch.

Basic Operation

The default port security setting for each port is **off**. That is, any device can access a port without causing a security reaction. However, on a per-port basis, you can configure security measures to block unauthorized connections or "listening", and to send notice of security violations. Once you have configured port security, you can then monitor the network for security violations through one or more of the following:

- Intrusion flags that are captured by network management tools such as HP TopTools for Hubs & Switches
- Alert log entries in the switch's web browser interface
- Event Log entries in the console interface
- Intrusion Log entries in either the switch's web browser interface or console interface

For any port you can configure the following:

- Authorized Addresses: Specify up to eight devices (MAC addresses) that are allowed to send inbound traffic through the port. This feature does the following:
  - Closes the port to inbound traffic from any unauthorized devices that are connected to the port.

  - Automatically sends notice of an attempted security violation to the switch's Intrusion Log and to the Alert Log in the switch's web browser interface.
  - Sends an SNMP trap notifying of an attempted security violation to a network management station. For more information on configuring the switch for SNMP management, see the Management and Configuration Guide you received with the switch.
- Prevent Eavesdropping: Block outbound traffic with unknown destination addresses from exiting through the port. This prevents an unauthorized device on the port from eavesdropping on the flooded unicast traffic intended for other devices.

Note

The switch security measures block unauthorized traffic without disabling the port. This implementation enables you to apply the security configuration to ports on which hubs or other switches are connected, and to maintain security while also maintaining network access to authorized users.

Configuring Port Security—Planning

Plan your port security configuration and monitoring according to the following:

- On which ports do you want to configure intruder security?
- Which devices (MAC addresses) are authorized on each port?
- For each port, what security actions do you want:
  - Block intruders from transmitting to the network?
  - Prevent intruders from eavesdropping on network traffic?
- How do you want to learn of the security violation attempts the switch detects:
  - Through network management, that is, do you want an SNMP trap sent to a network management station when a port detects a security violation attempt?
  - Through the switch's web browser interface (Alert Log and Intrusion Log)?
  - Through the Event Log and the Intrusion Log in the switch console interface?

Use the web browser interface and/or the switch console to configure port security. The following table describes the parameters.

Table 14-3. Port Security Control Parameters

Parameter	Description
Port	Identifies the switch port to view or configure for port security

Parameter	Description
Learn Mode	Specifies how the port will acquire its list of authorized addresses. **Continuous** (the default): Allows the port to learn addresses from inbound traffic from any device(s) to which it is connected. In this state, the port accepts as authorized any device(s) to which it is connected. Addresses learned this way appear in the switch and port address tables and age out according to the Address Age interval in the System Information configuration screen. **Static**: Enables you to specify how many devices are authorized on the port and to enter the MAC addresses of the authorized devices. If you enter fewer MAC addresses than you authorized, the port learns the remaining addresses from the inbound traffic it receives. (See "Authorized Addresses" at the end of this table). **Note**: When you configure Learn Mode to Static, all devices (MAC addresses) in the port's address table are deleted from both the port's address table and the switch's address table and replaced by the authorized devices for this port.
Address Limit	When Learn Mode is set to Static, specifies how man authorized devices (MAC addresses) to allow. The range is 1 (the default) to 8.
Eavesdrop Prevention	Specifies whether the port will block outbound traffic addressed to devices unknown to the port, that is, flooded unicast traffic. This is recommended for use on secure port with known (static) MAC addresses, which makes it unnecessary for these ports to transmit flooded unicast traffic for unknown destinations. **Disabled**: (the default): Allow the port to transmit all outbound traffic it receives, regardless of whether the traffic is addressed to devices that are known to the port. **Enabled**: Allows the port to transmit only the outbound traffic addressed to devices that are known to the port. Outbound traffic to devices unknown to the port is dropped. Devices known to the port include all devices (MAC addresses) the port has detected and listed in its address table, and any devices configured in the Authorized Addresses table. You can view the port's address table from the console Status and Counters menu. The Authorized Addresses table appears if the Learn Mode parameter is set to Static. Note: This feature is not recommended for applications in which a port's Learn Mode is configured to Continuous.
Action	Specifies whether an SNMP trap is sent to a network management station when Learn Mode is configured to Static and the port detects an unauthorized device. **None** (the default): Prevents an SNMP trap from being sent. **Send Alarm**: Causes the switch to send an SNMP trap to a network management station. For information on configuring the switch for SNMP management, see the Management and Configuration Guide you received

Parameter	Description
Authorized Address	Appears when Learn Mode is set to Static. Enables you to enter up to eight authorized devices (MAC addresses) per port, depending on the value specified in the Address Limits field. If you enter fewer devices than you specified in the Address Limits field, the port learns the remaining addresses from the inbound traffic it receives. For example, if you specify four devices, but enter only two MAC addresses, the first two (non-specified) devices subsequently detected on the port will be added to the Authorized Address list, and all subsequent (non-specified) devices detected on the port will be handled as "unauthorized". **Caution**: If you enter fewer devices (MAC addresses) than specified in the Address Limits parameter, it is possible to unintentionally allow a device to become "authorized" that you do not want to include in your Authorized Address list. This can occur because the port, in order to fulfill the number of devices allowed by the Address Limits parameter, will automatically add devices it detects until the specified limit is reached. For this reason it is recommended that you configure the Address Limit to allow only as many devices as you plan to type in to the Authorized Addresses list.

Configuring Authorized IP Managers

This feature enables you to enhance security on the switch by using IP addresses to authorize which stations (PCs or workstations) are allowed to:

- Access the switch's web browser interface
- Telnet into the switch's console interface
- Perform TFTP transfers of configurations and software updates into the switch

Note

This feature does not affect SNMP access to the switch by SNMP-authorized managements stations. SNMP access is protected by community names and an independent SNMP Authorized Manager list.

You can configure up to 10 authorized manager addresses, where each address applies to a single management station or a group of stations, or a Manager or Operator access level.

Note

This feature does not protect access to the switch through a modem or direct Console (RS-232) port connection. Also, if the IP address assigned to an authorized management station is configured in another station, the other station can gain management access to the switch even though a duplicate IP address condition exists. For these reasons, you should enhance your network's security by keeping physical access to the switch restricted to authorized personnel, using the password features built into the switch, and preventing unauthorized access to data on your management stations.

Access Levels

For each authorized manager address, you can configure either one of these access levels:

- Manager—Enables full access to all web browser and console interface screens for viewing, configuration, and all other operations available in these interfaces
- Operator—Allows view-only access from the web browser and console interfaces. This is the same access that is allowed by the switch's operator-level password feature

Defining Authorized Management Stations

Authorizing Single Stations. Enable only one station per Authorized Manager IP parameter to access the switch (the default). To use this method, just enter the IP address of an authorized management station in the Authorized Manager IP parameter, and leave the IP Mask set to 255.255.255.255. This is the easiest way to use the Authorized Managers feature.

Authorizing Multiple Stations. Using one Authorized Manager IP parameter, enable a defined group of stations to access the switch. This is useful if you want to authorize several stations for either manager- or operator-level access to the switch. All stations in a group defined by one Authorized Manager IP parameter and its associated IP mask will have the same access level—Manager or Operator.

To configure the switch for authorized manager access, enter the appropriate Authorized Manager IP parameter, specify an IP Mask, and select either Manager or Operator for the Access Level. The IP Mask determines how the Authorized Manager IP parameter is used to define authorized IP addresses for management station access.

Overview of IP Mask Operation

The default IP Mask is 255.255.255.255 and allows switch access only to a station having an IP address that is identical to the Authorized Manager IP parameter. ("255" in an octet of the mask means that only the exact value in the corresponding octet of the Authorized Manager IP parameter is allowed in the IP address of an authorized management station.) However, you can alter the mask and the Authorized Manager IP parameter to specify ranges of authorized IP addresses. For example, a mask of 255.255.255.0 and any value for the Authorized Manager IP parameter allows a range of 0 through 255 in the 4th octet of the authorized IP address, which enables a block of up to 256 IP addresses for IP management access. A mask of 255.255.255.252 uses the 4th octet of a given Authorized Manager IP address to authorize four IP addresses for management station access.

Note

The IP Mask is a method for recognizing whether a given IP address is authorized for management access to the switch. This mask serves a different purpose than IP subnet masks and is applied in a different manner.

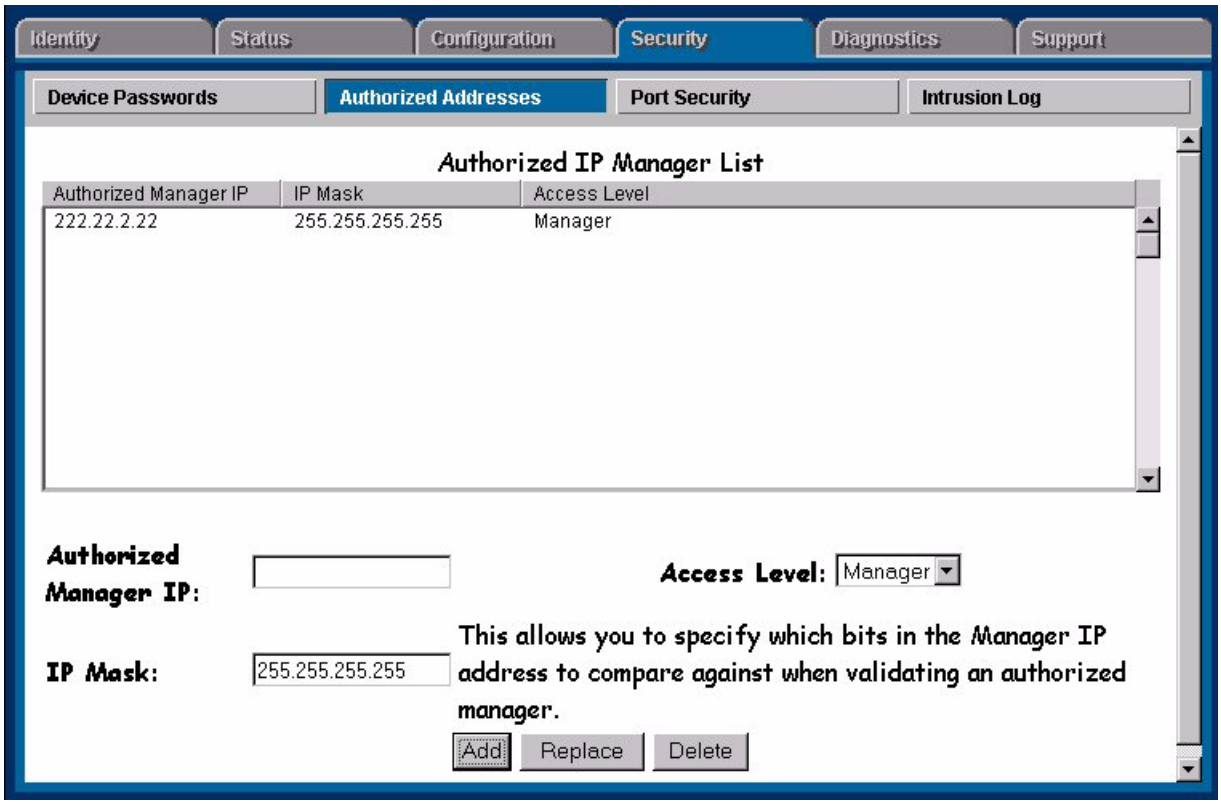


Figure 14-7. Switch Authorized Addresses List

To configure IP Authorized Managers:

1. Select the **Authorized Addresses** button in the Security screen.
2. Enter an **Authorized Manager IP address**.
3. Select an **Access Level**.
4. Use the default mask to allow access by one management station, or edit the mask to allow access by a group of management stations.
5. Click on **Add** to add the entry to the list.

Configuring Port Security

To configure Port Security perform the following steps:

1. Double-click on the selected switch to display its web browser interface.
2. Click on the **Security** tab.

3. Click on the **Port Security** button.
4. Select a port to configure.
5. Click on the **Set Security Policy for Selected Ports** button at the bottom of the screen.

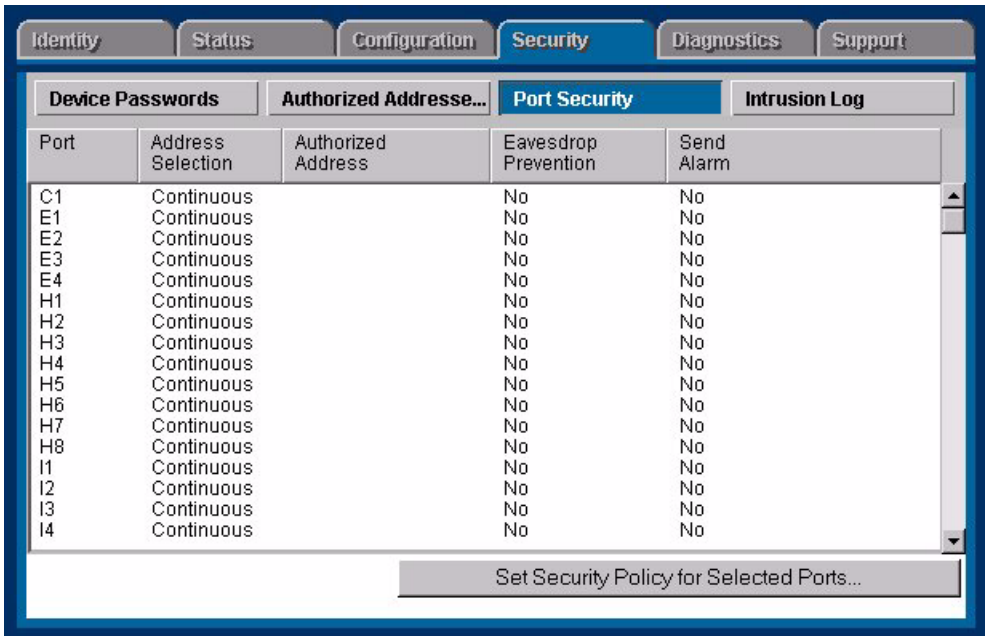


Figure 14-8. Port Security Overview Page

6. In the Security Policy page select the parameters for that port.

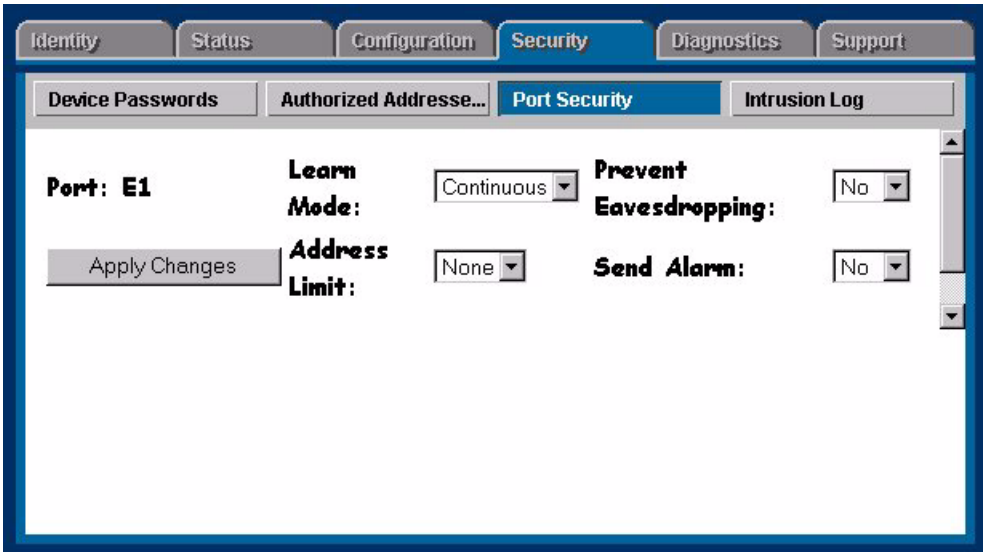


Figure 14-9. Security Policy Page for a Selected Port

If you want to configure authorized devices:

1. Select **Static** for the **Learn Mode** parameter.
2. Select the number of authorized addresses (devices) for the **Address Limit** parameter.
3. If you want to send SNMP traps notifying of attempted security violations, select **Yes** for the **Send Alarm** parameter.
4. Select **Yes** to **Prevent Eavesdropping**.
5. Click on the **Apply Changes** button.

Switch Intrusion Log

When an attempted security violation occurs on a port configured for Port Security, the port drops the packets it receives from the unauthorized device.

Notice of Security violations

When a security violation occurs on a port configured for Port Security, the switch responds in the following ways to notify you:

- The switch sets an intrusion flag for that port. This flag remains until:
  - You use either the console or web browser interface to reset the flag
  - The switch is reset to its factory default.
- The web browser and console interfaces notify you of the intrusion. In the browser:

- The Alert Log displays a Security Violation entry, with the system date and time, and the port on which the violation occurred
- The Intrusion Log lists the port number, the MAC address of the intruding device, and the system time and date when the intrusion occurred.

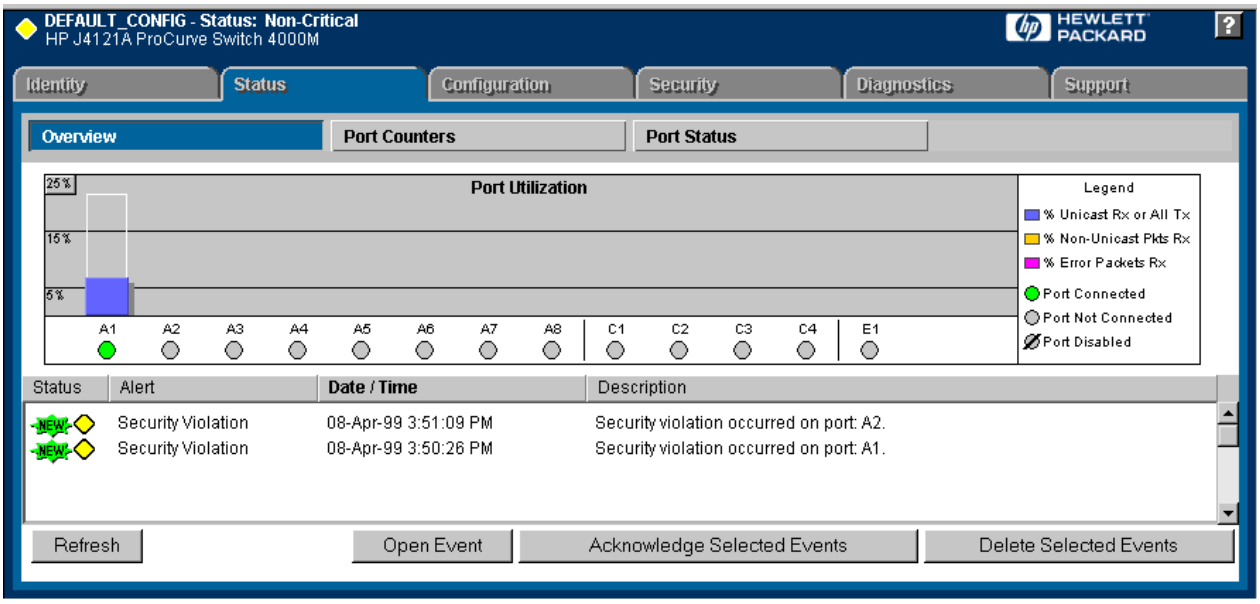


Figure 14-10.Security Violation Entries in the Alert Log

In the following figure, ports A1 and A2 have detected intrusions for which their intrusion flags have not been reset, as indicated by the Ports with Intrusion Flag entry. You must reset the intrusion flags for these ports before the log can indicate any new intrusions for them. Ports A3 and A5 are not listed, indicating that their intrusion flags have already been reset. These two ports are ready to log any new intrusions.

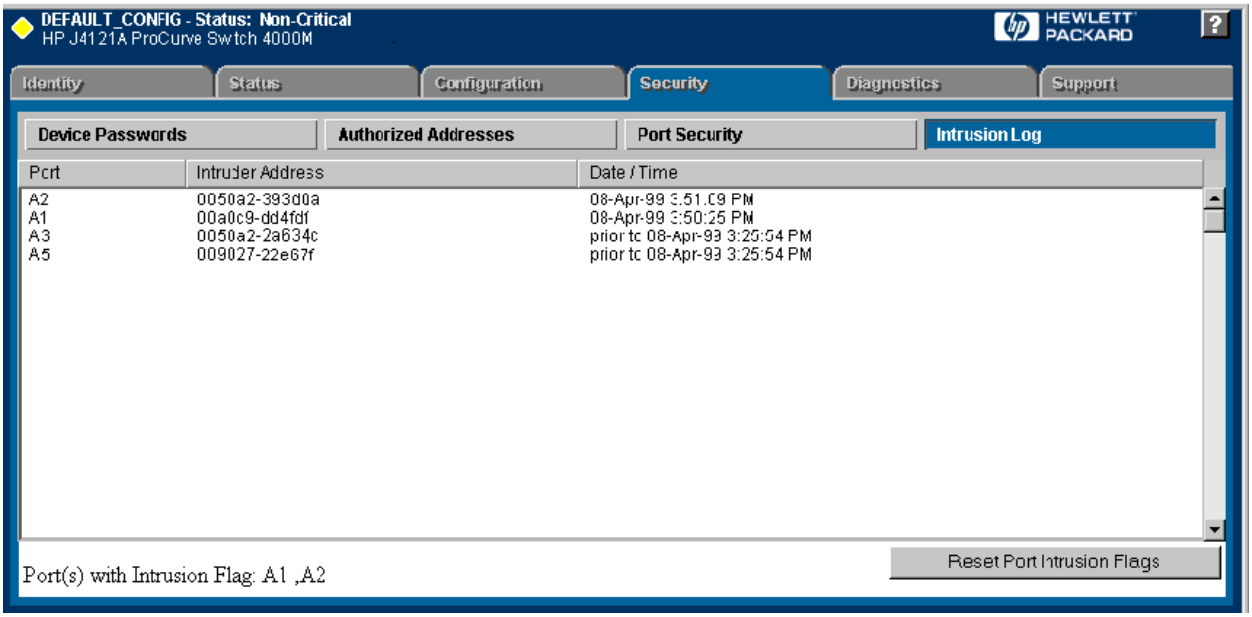


Figure 14-11.Intrusion Log with Intrusions Entered for Ports A1 and A2

How the Intrusion Log Operates

The Intrusion Log gives you a list of the 20 most recent security violation attempts, and appears in both the web browser interface and the switch console. The log shows the most recent intrusion at the top of the listing. You cannot delete Intrusion Log entries. Instead, if the log is filled when the switch detects a new intrusion, the oldest entry is dropped off the listing and the newest entry appears at the top of the listing.

Keeping the Intrusion Log Current by Resetting Flags

When a violation occurs on a port, an intrusion flag is set for that port and the violation is entered in the Intrusion Log. The switch can detect and handle subsequent intrusions on that port, but will not log another intrusion on the port until you go to the Intrusion Log and use the **Reset Port Intrusion Flags** button to reset the port's intrusion flag.

Operating Notes for Port Security

Identifying the IP Address of an Intruder

The Intrusion Log lists intruders by MAC address. If you are using HP TopTools for Hubs & Switches to manage your network, you can use the HP TopTools inventory reports to link MAC addresses to their corresponding IP addresses. (Inventory reports are organized by device type; hubs, switches, servers, etc.)

Proxy Web Servers

If you are using the switch's web browser interface through a switch port configured for Static port security, and your browser access is through a proxy web server, it is necessary to do the following:

- Enter your PC or workstation MAC address in the port's **Authorized Addresses** list.
- Enter your PC or workstation's IP address in the switch's **IP Authorized Managers** list.

Without both of the above configured, the switch detects only the proxy server's MAC address, and not your PC or workstation MAC address, and interprets your connection as unauthorized.

Security Violations

If you reset the switch (using the **Reset** button, **Device Reset**, or **Reboot Switch**), the Intrusion Log will list the time of all currently logged intrusions as "prior to" the time of the reset.

Intrusion Flag Status for Entries Forced Off of the Intrusion Log

If the Intrusion Log is full of entries for which the intrusion flags have not been reset, a new intrusion will cause the oldest entry to drop off the list, but will not change the intrusion flag status for the port referenced in the dropped entry. This means that even if an entry is forced off of the Intrusion Log, no new intrusions can be logged on the port referenced in that entry until you reset the intrusion flags.

15

Performing Diagnostics

Using HP TopTools, you can help isolate faults by running device self-tests, Link tests, and Ping tests (IP networks).

This section includes information on:

- **Performing a Ping/Link Test**
- **Rebooting a Device**
- **Resetting a Hub to Factory Default Settings**
- **Producing a Configuration Report**

Performing a Ping/Link Test

You can isolate faults by running Link tests or Ping tests (IP networks). Select the **Diagnostics** tab and click on the **Ping/Link Test** button. Choose a test for sending test packets to, or through, a device in order to verify the path between two network devices. In the **Destination MAC/IP Address** field enter the IP address or MAC address of the device for which you want to test the connection. Specify the number of packets to send and the timeout (in seconds) for each test. Click on the **Start** button to start the test. Click on the **Stop** button to stop the test.

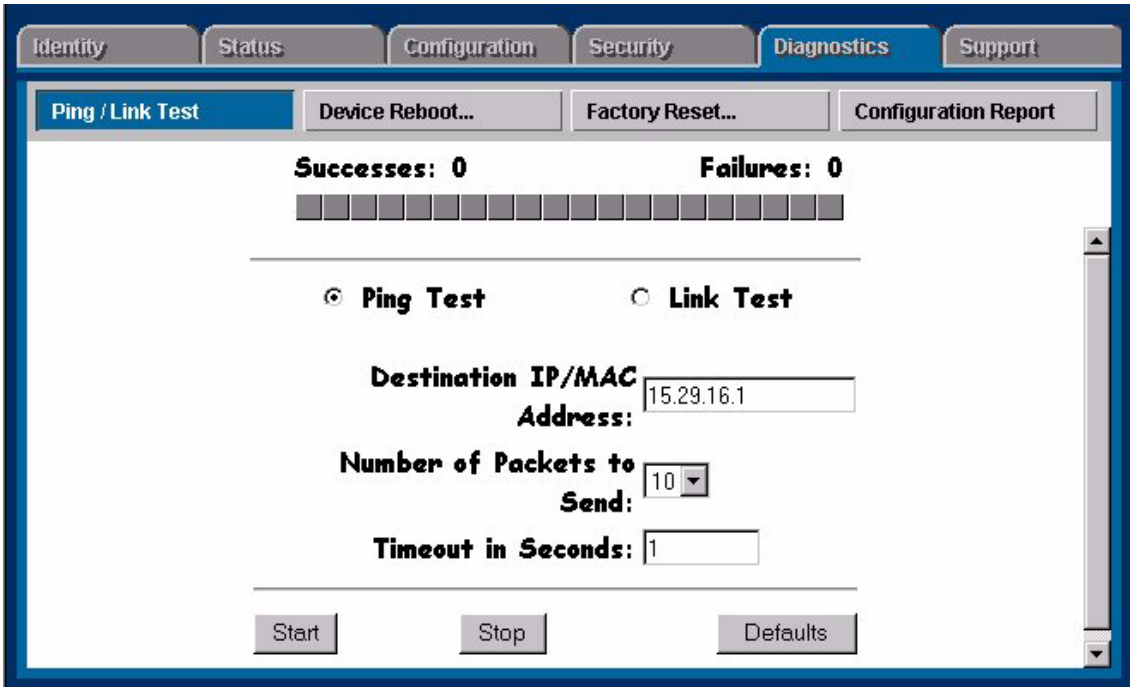


Figure 15-1. Ping/Link Test Page

The number of successes or failures of the test packets reaching the Destination IP or MAC Address are displayed at the top of the page. A failure means that either the device at the destination address did not respond within the timeout specified, or the data returned from the device indicated an error.

The Defaults button will reset the **Number of Packets to Send** and the **Timeout** value to the default values of 10 packets and 1 second, respectively.

Rebooting a Device

Some devices have a **Device Reboot...** button. Rebooting a device is the same as powering off. Network operation may be interrupted.

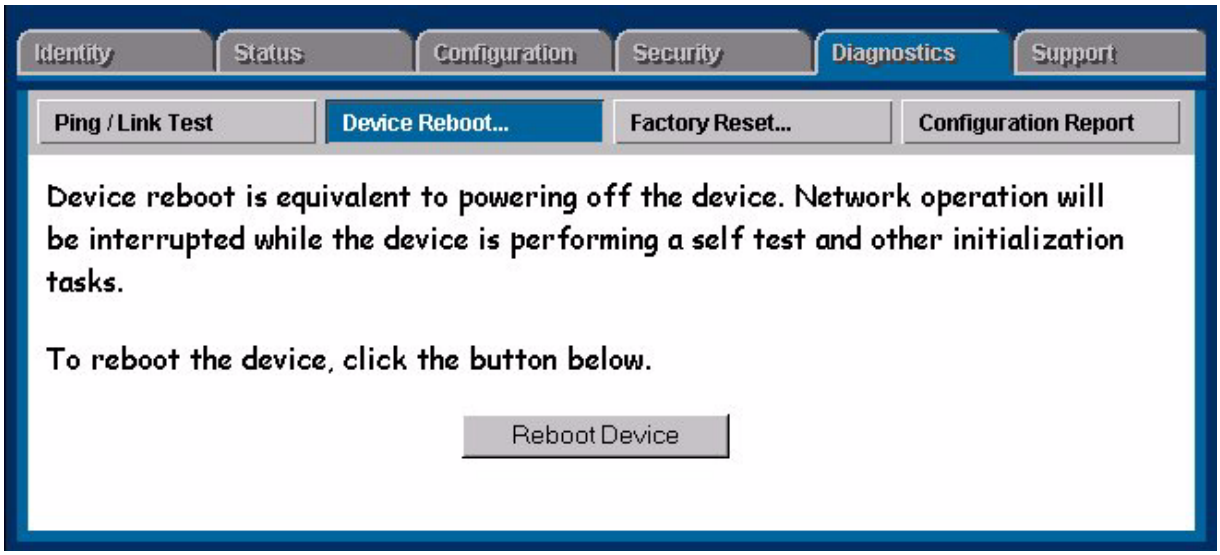


Figure 15-2. Device Reboot Page

Resetting a Hub to Factory Default Settings

Resetting the hub to the factory default settings removes any configuration changes that you have made since installing the device, and restores the factory defaults. The IP address is also removed; you must enter an IP address before the device will operate on your network, unless you have Bootp or DHCP.

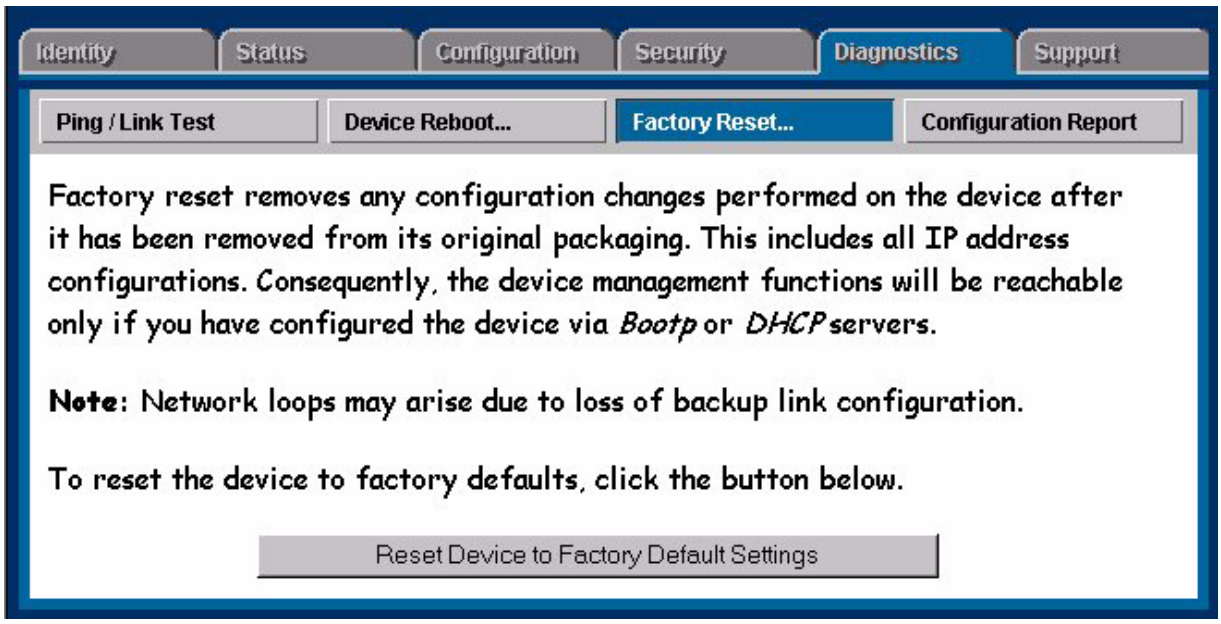


Figure 15-3. Factory Reset of a Hub

Resetting a Switch

Select the **Device Reset** button to reset a switch. Device reset is equivalent to powering off the device, then turning it on again. Network operation will be interrupted while the device is performing a self test and other initialization tasks. The switch's counters are cleared to zero during this reset.

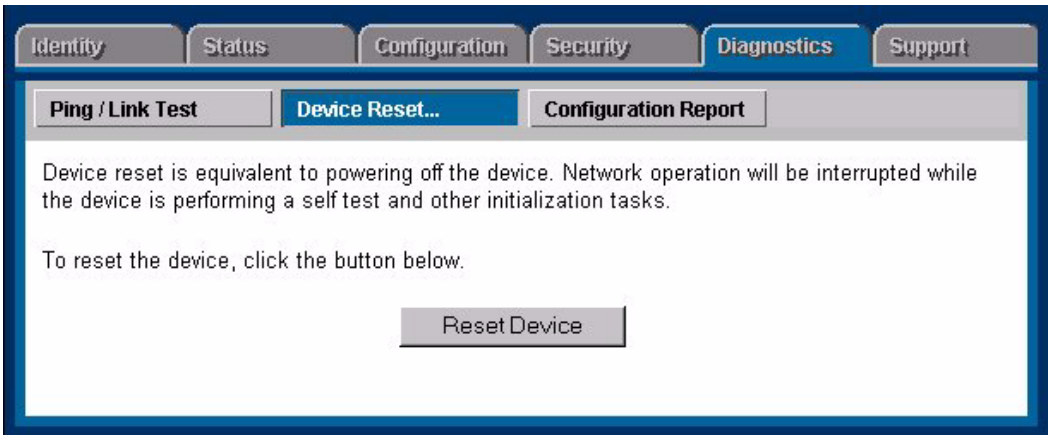


Figure 15-4. Resetting a Switch

Producing a Configuration Report

The Configuration Report displays information about the current settings on your device. You can use your browser's capabilities to print a copy of the report or save it to a file. See the online help for a more detailed explanation of this report.

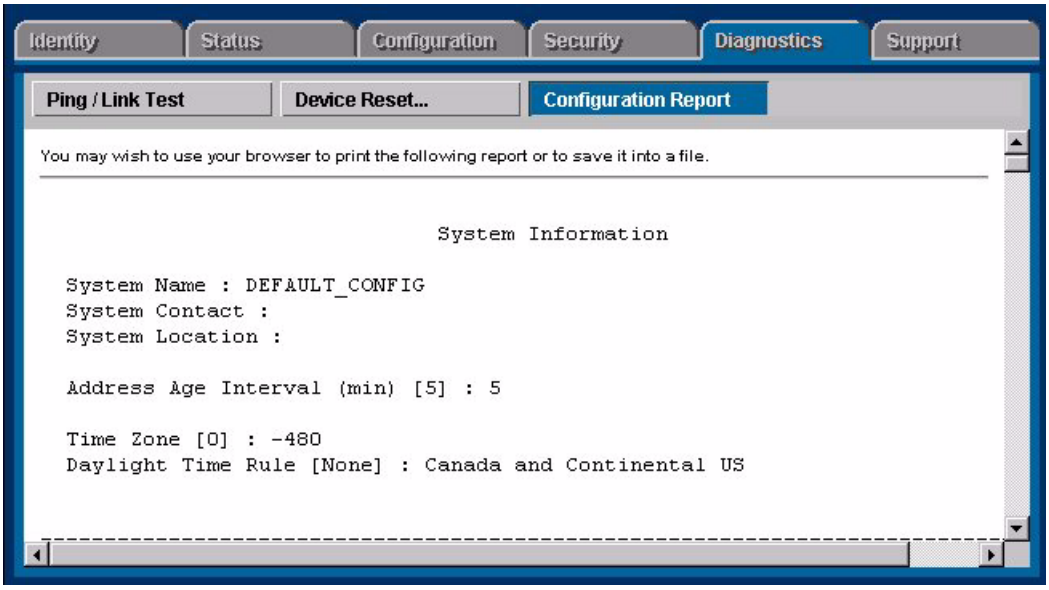


Figure 15-5. Configuration Report

16

Downloading Software

Software is the operating system running on the network device. The operating system manages all internal processes, including those that allow you to configure, diagnose, and troubleshoot that device and the network. From time to time Hewlett-Packard releases updated versions of software for certain networking devices. Using the HP Download Manager for older HP devices, and the browser-based Software Update Utility for newer HP devices, you can install new software on a device without physically replacing hardware memory modules (such as EEPROMs or flash SIMMs) in the device. This provides an easy and convenient way of upgrading or changing device features.

This section contains information on:

The Software Update Utility

The Software Update Utility is a browser-based utility for updating network device software. Features of the Software Update Utility include:

- Accessing the Web for information about the latest versions of device software
- Downloading the latest software from the HP Web page to the local HP TopTools server
- Updating more than one device at a time
- Scheduling updates within a one-week period

The Software Update utility can be used for the following devices:

Table 1. Devices Supported by the Software Update Utility

HP ProCurve Switches	HP ProCurve Hubs	Other HP Switches
HP ProCurve 212M	HP ProCurve 10-Base T Hub 12M	HP Switch 2000
HP ProCurve 224M	HP ProCurve 10-Base T Hub 24M	HP Switch 2000B
HP ProCurve 8000M	HP ProCurve 10/100 Hub 12M	HP Switch 800T
HP ProCurve 1600M	HP ProCurve 10/100 Hub 24M	

Table 1. Devices Supported by the Software Update Utility

HP ProCurve Switches	HP ProCurve Hubs	Other HP Switches
HP ProCurve 4000M		
HP ProCurve 2400M		
HP ProCurve 2424M		
HP ProCurve 2512M		
HP ProCurve 2524M		
HP ProCurve 6208M		
HP ProCurve 6308M		
HP ProCurve 9304M		
HP ProCurve 9308M		

See **The HP Download Manager** for updating all other HP devices.

Starting the Software Update Utility

To access the Software Update Utility, you must select a device from the device list. Display the device list by selecting the **Devices** button in the navigation frame, then clicking on **Device Types, Networking Devices**. A list of your switches, hubs, and routers displays.

Select a hub or switch to be updated and right-click on it. Select **Update Firmware** from the menu. You can also select the device, then click on the **Actions** button and select **Update Firmware**.

If this is the first time that you have used the Software Update Utility after installing HP TopTools for Hubs & Switches, there are no updates available on your server yet. You will see the following message:

> **"Your system has not been initialized with the latest support information for this type of device. This information is required to continue. OK to download it now?"**

Click on **Ok** to obtain the list of available software updates for the device you selected in the device list. After the information is downloaded, the next **Update System Software** page appears.

If this is not the first time that you have used the Software Update Utility, the **Update System Software** page appears immediately.

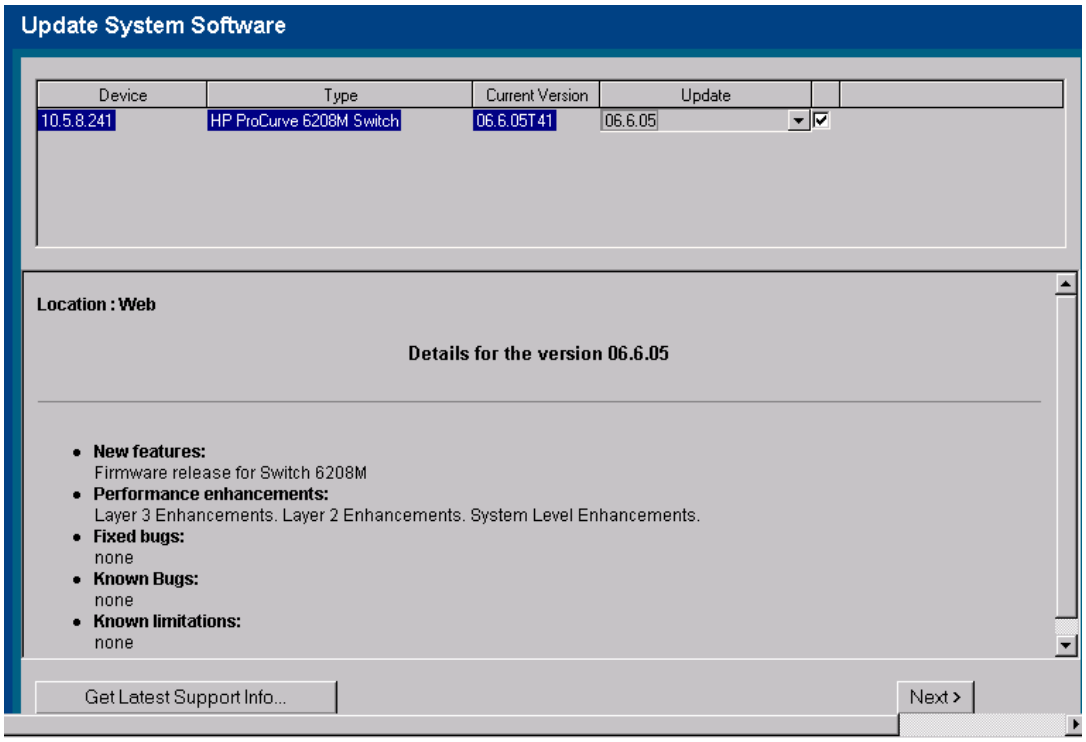


Figure 16-1. Browser-based Software Update Utility

This page of the Software Update Utility displays information about the current version of the software and the updates available for the device or devices that you selected from the device list.

Click on **Get Latest Support Info...** to download a list of the available software updates that are not already on your server. The displayed information includes:

- New features with this version of the software
- Performance enhancements
- Any bugs that were fixed
- Any existing known bugs in the new version
- Known limitations of the software

If there are multiple updates available for a device, select the version you want from the drop down list. Check the box to the right of the selection if it is not already checked. If no updates are available for the device you selected, the list box displays “no update available”.

Obtaining the Software from the Web

If the updates you have selected are not locally available on the TopTools server, that is, they need to be downloaded from the ftp server before they can be installed, a page appears that asks “Do you want to download them from

the HP website?" You can see what is locally available on the TopTools server by clicking on **Settings** in the navigation frame, then selecting **System Software**. See the section **Viewing the Software Updates Available on the TopTools Server** for more information.

If you are ready to download the updates, click on the **Download Now** button below the box listing the software versions that need to be downloaded. Another page appears detailing which software packages will be downloaded to your TopTools server from what location, for example,

Network device firmware C.07.26 ftp://rs51898w02/pub/RMDB_j4119726.exe

The software updates are downloaded to

```
c:\Program files\Hptt|Packages
```

Accepting the Licensing Agreement

Before you are allowed to download the software, you must accept the licensing agreement displayed on the page. Click on the radio button **I accept the agreement** to proceed with the download. Click on **I DO NOT accept the agreement** if you do not want to proceed. Click on **OK** to begin the download. Another page displays the software downloaded. Click on **Next** to continue with your updates.

When you have selected the software version, click on **Next**. The next page of the Software Update Utility appears.

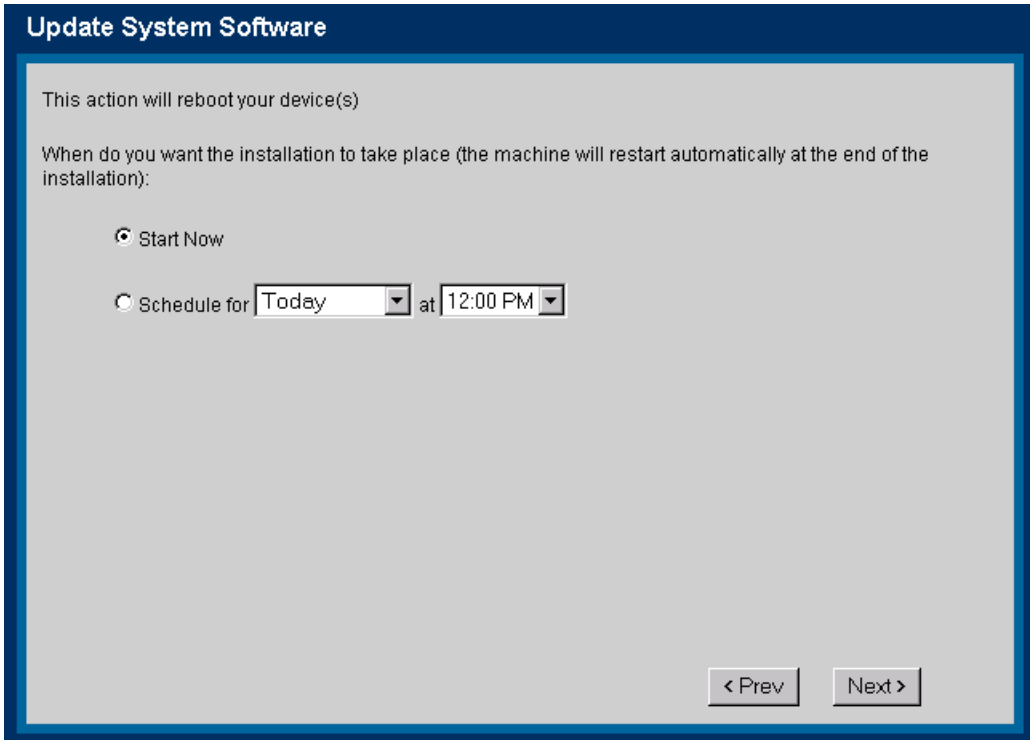


Figure 16-2. Scheduling the Software Update

Scheduling the Software Update

To update the device(s) immediately, click the radio button **Start Now**. The device update proceeds and the device is automatically rebooted when the update is finished. Alternatively, you can schedule a day and time within a one week period for the update to occur. Click on the **Schedule for** radio button and select Today, Tomorrow, or a day of the week, then select a time. Click on **Next**.

Your selections and schedule are displayed in the next page. Click on **Finish** to proceed with these selections. If you click on **Cancel** to cancel your selections you are returned to the first page of the Software Update Utility.

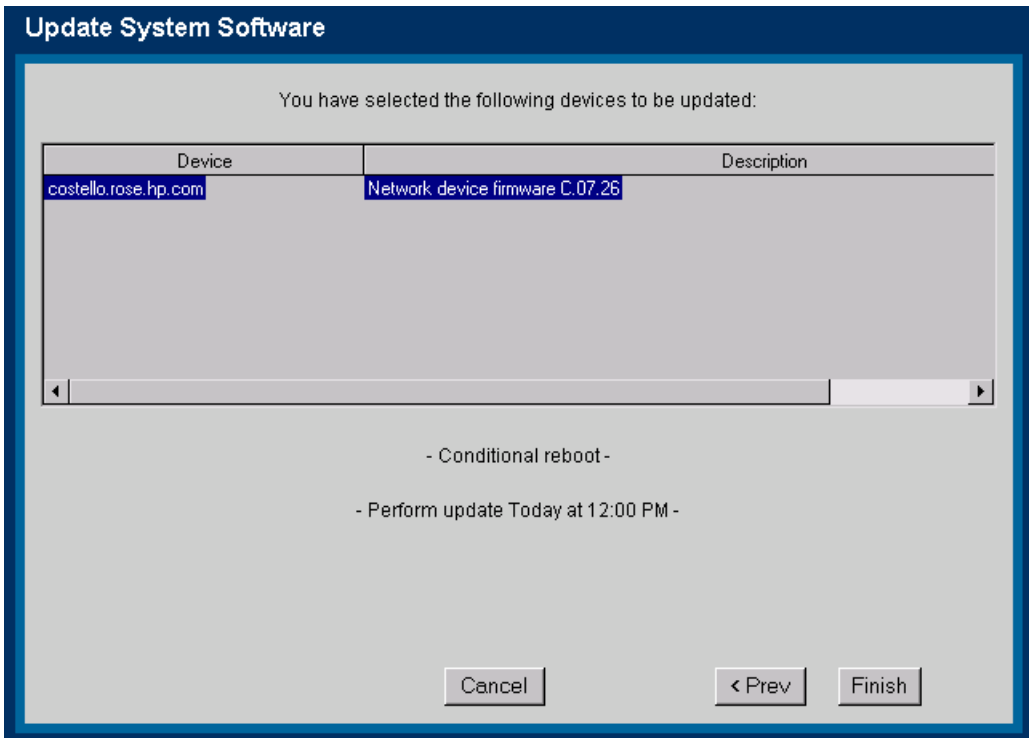


Figure 16-3. Devices Selected for Updating, Showing Scheduled Time of Update

The last screen informs you that the update action is scheduled, and that you can check the Alert Log (**Alerts** button in the navigation frame) for messages about the update.

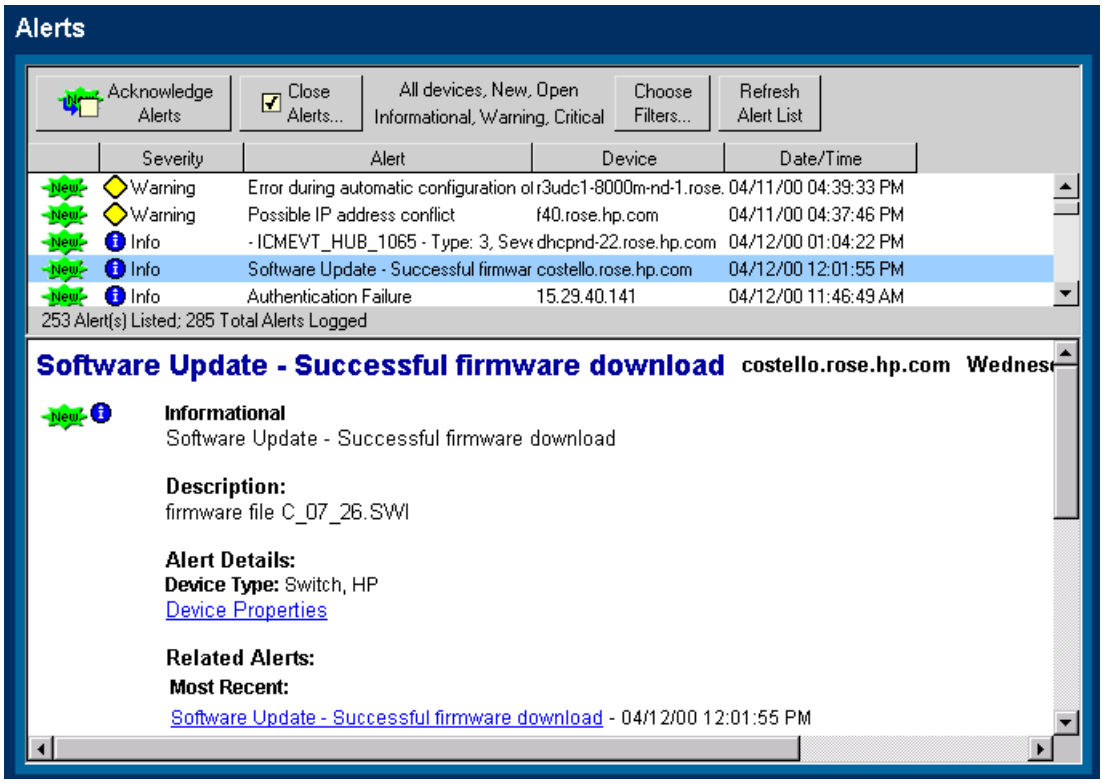


Figure 16-4. Alert Log Showing Successful Software Update

Viewing the Software Updates Available on the TopTools Server

Information about the available software updates can be viewed by clicking on **Settings** in the navigation frame, then selecting **System Software**. The **Settings - System Software Packages** page displays. Select the **Hubs & Switches** tab if it is not already selected.

Choose a device from the list at the top of the page. The software update packages available for that device will be listed in the middle of the page. Information provided includes:

- Location—If the update package is already on the server machine, **Local** is displayed. If you need to download it, **Web** is displayed.
- Type—The type will be System Firmware.
- Version—The version designation for the update package.
- Description—The HP devices that can be updated with this package.

To obtain a package with a **Web** location indicated, click on **Download package**. The update package is downloaded from the tftp server.

To delete a package from your server, click on **Delete package**.

To show a list of new software updates that may be available on the tftp server, click on the **Get Latest Support Info...** button.

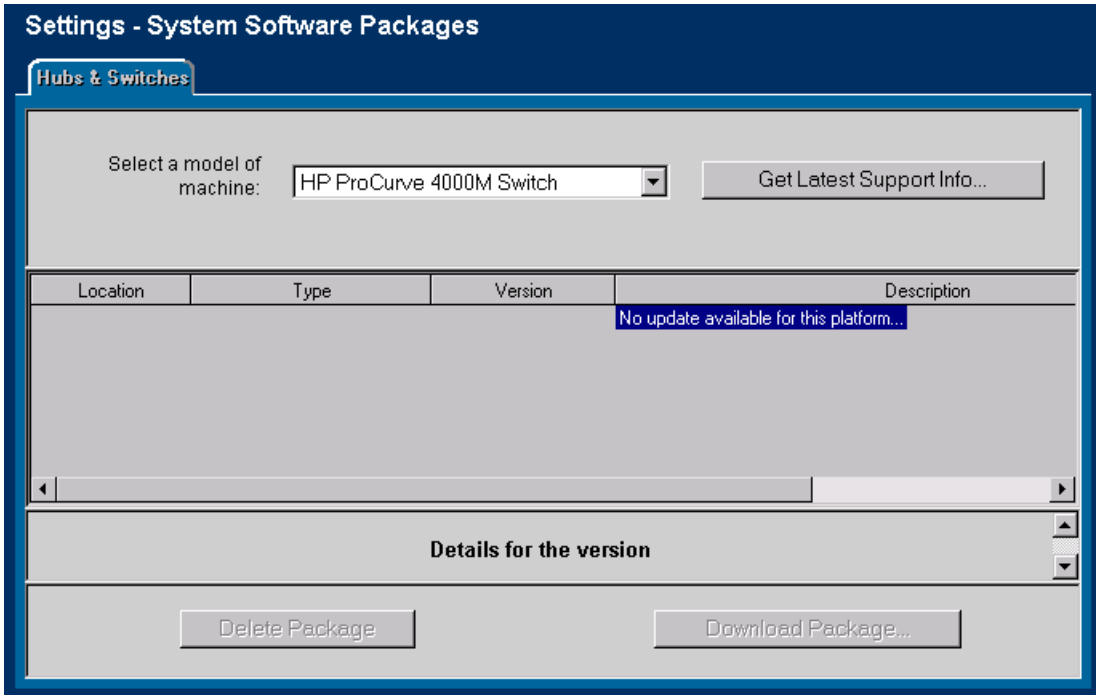


Figure 16-5. Available System Software Updates for Hubs and Switches

The HP Download Manager

Use the HP Download Manager for all devices not supported by the Software Update Utility.

Obtaining New Software from HP

There are three sources you can access for new software:

- The latest HP TopTools for Hubs & Switches CD-ROM
- The World Wide Web, at HP's ProCurve web site. The URL is:

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

- Your HP Customer Care Center or other authorized HP representative

Before you begin downloading, make sure your new software is accessible to your network. The most typical way is simply to place the HP TopTools for Hubs & Switches CD-ROM into the CD drive of the network management station on which HP TopTools is loaded. If you got the software files from the World Wide Web or HP Customer Care Center, copy the files to the hard drive of the computer running HP TopTools. Place all the files in this directory:

```
c:\Program files\Hptt\hpwnd\dld
```

Note

This assumes you are using the directories automatically set up during the HP TopTools installation. If you have changed "TopTools" to something else, change this pathname accordingly.

The Download Manager shows you which versions of software are currently on your devices, compares that information with the latest available software, and helps you download it onto as many devices as you wish.

Note

If the files are self-extracting, run the file as a program to extract the files. For example, if you retrieved the file `j4110510.exe`, put the file in the above subdirectory. Now run the program by typing `j4110510.exe` at a DOS prompt. The program will extract the files `c_05_10.swi, readc510.txt`, and `relnotes.txt` from itself. In this case the firmware file for the device is `c_05_10.swi`.

To use the Download Manager, you must first select the devices that will receive the software, as follows:

1. On the HP TopTools button bar, click the **Devices** button and then select **Device types**.
2. Under "Devices by Type" select **Networking Devices**. Highlight the device(s) you want to update. The devices you select must be all of the same type, i.e., all hubs or all switches.

3. Next, while holding the cursor over any selected item, click the right mouse button. Select the **Update Firmware...** option. The **Download Control** dialog box appears. Alternatively, you can click the **Actions** button and select **Update Firmware...** from the menu.

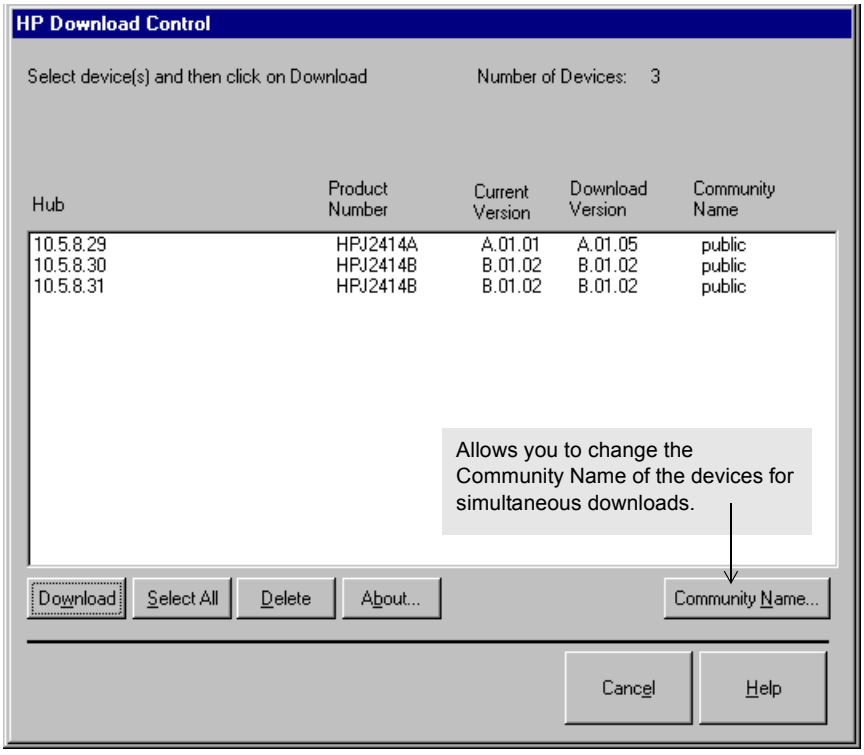


Figure 16-6. Download Control

When the Download Control dialog box appears, it lists the devices you selected along with the version numbers of the software currently loaded on each. Compare this version number with the version available for downloading. If the versions are the same, you need not proceed further. If the "Download Version" is older than the "Current Version" you probably have an outdated CD in your drive. Do not proceed; visit the HP ProCurve web page (http://www.hp.com/go/procurve) or call your authorized HP representative to obtain the latest files. If the "Download Version" is newer than the "Current Version" you can highlight the item(s) and proceed.

If you have to change the community names of the devices in order to download the file to all of them simultaneously, click the **Community Name...** button. This opens the **Change SET_COMMUNITY_NAME** dialog box. Enter the new community name in the "SET_COMMUNITY_NAME" field and click the **OK** button. Note, however, that if you selected more than one device, the community name you enter must be valid for all of them.

Click the **Download** button and, when prompted, enter the drive letter designation of the computer's CD drive. If the software files have already been copied to the correct directory on your hard drive, you will not be prompted. The Download Manager gives you an estimate of the length of time it will take to download the software for all the devices on the list. If you want to schedule the operation for another time, perhaps at night, click the **Schedule** button, set the time, and click **OK**.

Note

Make sure you leave the CD in the drive.

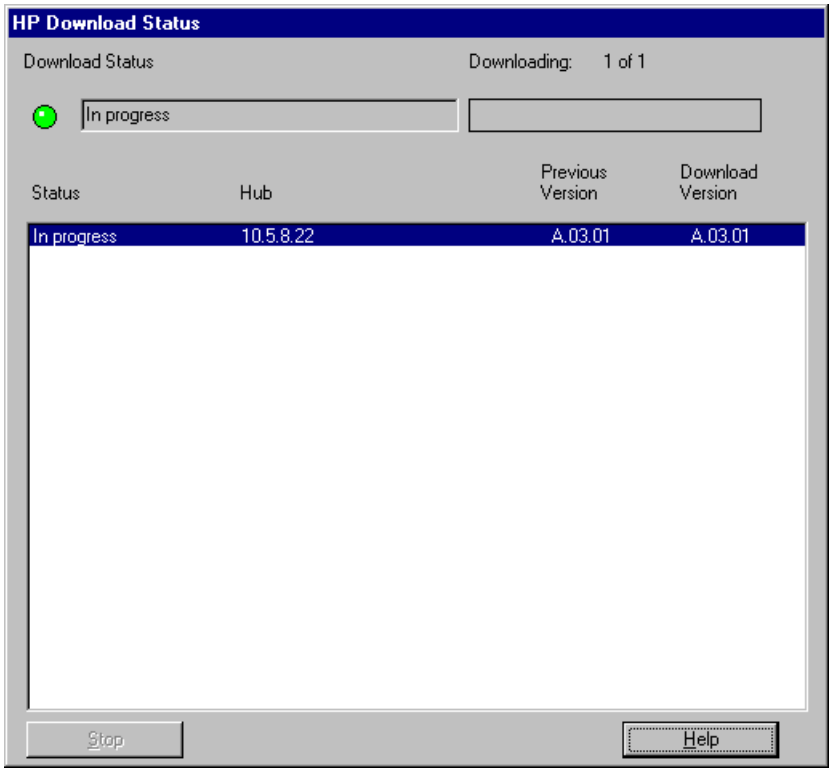


Figure 16-7. Download Status dialog box

As the Download Manager works, it displays a dialog box that shows the progress of the operation. If it encounters a problem, it will complete the downloading of the file in progress and then stop. If you want to stop the downloading at any time, you can click the **Stop** button.

When the download is finished, you can check the log file to see details of the operation and information about any problems that might have occurred. In the Download Done dialog box, click the **View Log** button.If there are no problems, click the **OK** button to finish.

How to Update the Map Files

The map file is used by the HP Download Manager to determine the supported product, the software file name for the supported product, and the version code for the product. Each record of the map file consists of four parts: product number, filename, version, and comment fields. For the Downloader to use the software files copied from the Web you will need to change the map file for that particular device located in the `\Program Files\hptt\hpwnd\dld` subdirectory.

Determine what device you want to update and get the file from the Support area of the HP ProCurve site on the HP World Wide Web. Make sure you make a note of the software version number for that device because you will need it later. Version numbers are expressed as A.01.01, for example.

Uncompress the file and copy the results (which will either be a .bin, .swi, or .fdd file) into the `\Program Files\Hptt\hpwnd\dld` directory.

Open either the hubs.map or switches.map file in a text-only editor like Notepad. You will be replacing the filename and version number in the line containing your device. (Note: DO NOT USE TABS between the columns. It will cause an error when you try to use the Downloader.)

Save the file and follow the instructions for using the Downloader program. You will need to edit the map file every time you pull down a newer versions of the software from the WEB.

Example: The hubs.map file before editing the J2603A entry for a new software version:

```
Product #   filename        version     ; comment
HPJ2414A    hpj2414a.dld    A.01.05     ; 100VG SNMP/Bridge Module
HPJ2603A    hpj2603a.dld    A.03.04     ; 10BaseT
HPJ2603B    hpj2603a.dld    A.03.04     ; 10BaseT
```

New software version data:

	Product Number	File Name	Version Number
Example	J2603A	j2603306.bin	A.03.06

Example: The hubs.map file after editing the J2603A entry to include the above data:

```
Product #   filename        version     ; comment
HPJ2414A    hpj2414a.dld    A.01.05     ; 100VG SNMP/Bridge Module
```

```
HPJ2603A   j2603306.bin   A.03.06    ; 10BaseT
HPJ2603B   j2603306.bin   A.03.06    ; 10BaseT
```

Appendix A

Appendix A contains the following topics:

Agent Firmware Versions

HP TopTools for Hubs & Switches communicates with network devices using SNMP (Simple Network Management Protocol). For HP TopTools to access device features, each network device must contain a compatible version of agent software or firmware.

Note

The latest firmware agents can be obtained from the Technical Support section of the HP ProCurve web page. The URL is:

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

Verifying Device Agent Versions

You can check the agent version on an HP device using one of the following methods:

- Use the device's console port interface (a ***non-network*** connection).
  - You can connect a terminal or computer directly to the device or through a modem. Refer to the device's *Installation and Reference Guide* for use of the device's RS-232 console port.
  - For HP devices, you can use an ASCII terminal or computer with VT 100 terminal emulation.
- Use an available network application (a ***network*** connection).
  - For HP devices, use an existing version of HP TopTools for Hubs & Switches or other device management utility.

Update the device's software or firmware to the current supported version.

Note

HP TopTools for Hubs & Switches may be able to discover devices that have previous versions of device agent firmware. However, the use of some functions may be limited.

Preparing Network Devices

For HP TopTools for Hubs & Switches to communicate with devices on your network, the network devices must:

- have SNMP agent firmware that is compatible with this version of HP TopTools.
- for IP networks, have a unique IP network address.

Note

Hubs and bridges shipped prior to July 1992 must be upgraded.

Basic hub management features are available for chained AdvanceStack hubs if they are connected to an SNMP-based hub of the same media type (10Base-T or 100VG) over a Distributed Management chain.

Device Network Addresses

IPX Networks

In IPX networks, each IPX-supporting device "self-configures" its IPX network address. The IPX address of each IPX device is generated automatically; you do not have to manually assign and configure IPX addresses.

Note

HP TopTools for Hubs & Switches does not support the discovery or management of the HP J2980A LAN Switch-16 on an IPX network.

IP Networks

On an IP network, each managed device must have an IP address. If you intend to run HP TopTools for Hubs & Switches on an IP network, you must configure the IP address for each device you want to manage.

IP addresses are normally configured when the device is installed. For HP hubs, bridges, and switches, IP addresses are configured using the console port interface. For more details on console port connection and available commands, see the device's *Installation and Reference Guide*.

Note

You can use HP TopTools for Hubs & Switches to change an IP address on a hub after it has been assigned, but not on a switch or a bridge.

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 been assigned to you. There is a formal process for assigning unique IP addresses to networks worldwide. Contact one of the following companies:

United States and countries not in Europe or Asia/Pacific	Network Solutions, Inc. Attn: InterNIC Registration Service 505 Huntmar Park Drive Herndon, VA 22070	1-703-742-4777 questions@internic.net http://rs.internic.net
Europe	RIPE NCC Kruislaan 409NL-1098 SJ Amsterdam The Netherlands	+31 20 592 5065 ncc@ripe.net http://www.ripe.net
Asia/Pacific	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	domreg@apnic.net http://www.apnic.net

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

Configuring IP Parameters

To run HP TopTools for Hubs & Switches on an IP network, you must configure the management station and all managed devices for IP.

The network management station is configured for IP using the TCP/IP stack utilities. To configure a device for IP, you typically connect to the device's console port and use the console port interface. (Refer to the device's installation manual for more information.)

Before you configure the network management station and manageable devices for IP, make a list of all the devices on the network and what their IP addresses will be.

Note: Make sure that every device has a unique IP address. Make sure that all devices on a given IP network number have the same subnet mask.

The IP configuration parameters are described below.

IP Address . The IP address of the hub, bridge, or switch 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.

The default value, 0.0.0.0, disables IP communications. Use the default value only if you are not going to manage the device with HP TopTools for Hubs & Switches and you want to disable IP communications for that device.

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 a given IP network number must use the same subnet mask address.

Primary Default Router. The routing IP address of the nearest router in your network. The default is 0.0.0.0.

Backup Default Router. The IP address of the router to use when the primary default router is inaccessible. The default value is 0.0.0.0. If there is no backup router and no primary default router, use the default.

Time To Live . 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, bridge, or switch is managed from a network management station that is more than 32 routers away. The maximum allowable value is 255.

Note For selected devices, such as the HP J2980A AdvanceStack 10/100 LAN Switch-16, you must preconfigure the SNMP community name “public” on the device to allow the device to be discovered and managed by HP TopTools for Hubs & Switches. Typically, the community name on HP hubs and bridges will automatically default to “public”.

To configure a device for IP networks, use the device's console port interface. Refer to the device's Installation and Reference Guide for use of the device's RS-232 console port.

Note For HP hubs, HP TopTools for Hubs & Switches can be used to *change* IP addresses after they have been initially assigned during installation.

Network Bootp Server

HP EtherTwist Hub Plus/24S and HP AdvanceStack 10Base-T hubs (with SNMP modules installed) support the use of Bootp (Bootstrap Protocol) to automatically retrieve their IP configuration from a server on the network. A device's IP configuration must be configured in a file on the Bootp server. When the device is powered on, Bootp is used to automatically download the IP configuration to the device.

- Each device that supports Bootp must have Bootp enabled to retrieve its IP configuration from the server. The factory default setting is for Bootp operation to be enabled. You can enable or disable Bootp operation through the device's console port, or from a network management application (such as HP TopTools for Hubs & Switches).
- For more information on IP configuration using Bootp, refer to your device's *Installation and Reference Guide*.

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X