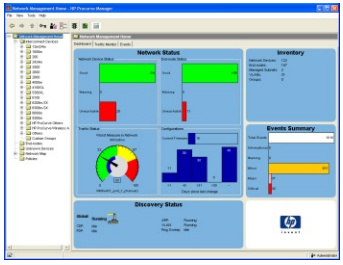
HP ProCurve Manager Plus

Network Administrator's Guide



The all-in-one solution for managing HP ProCurve networks

invent

HP ProCurve Manager

Software Release 1.5

Network Administrator's Guide

Publication Number

5990-6046
June, 2004
Edition 2.0

Trademark Credits

Microsoft, Windows, Windows 95, and Microsoft Windows NT are registered trademarks of Microsoft Corporation. Internet Explorer is a trademark of Microsoft Corporation. Ethernet is a registered trademark of Xerox Corporation. Netscape is a registered trademark of Netscape Corporation. Cisco® is a trademark of Cisco Systems, Inc.

Disclaimer

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

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

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

Warranty

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

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

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

Contents

1

About HP ProCurve Manager

Chapter Contents

Introduction

HP ProCurve Manager is a Windows-based network management solution for all manageable HP ProCurve devices. It provides network: mapping and polling capabilities, device auto-discovery and topology, tools for device configuration and management, monitoring network traffic, and alerts and troubleshooting data for HP ProCurve networks.

The graphical interface in HP ProCurve Manager Client provides at-a-glance summaries of network activity, with drill-downs for more detailed device information. It also provides a simplified interface for managing and configuring the network and devices, with access to device Web Agents and the Command Line Interface.

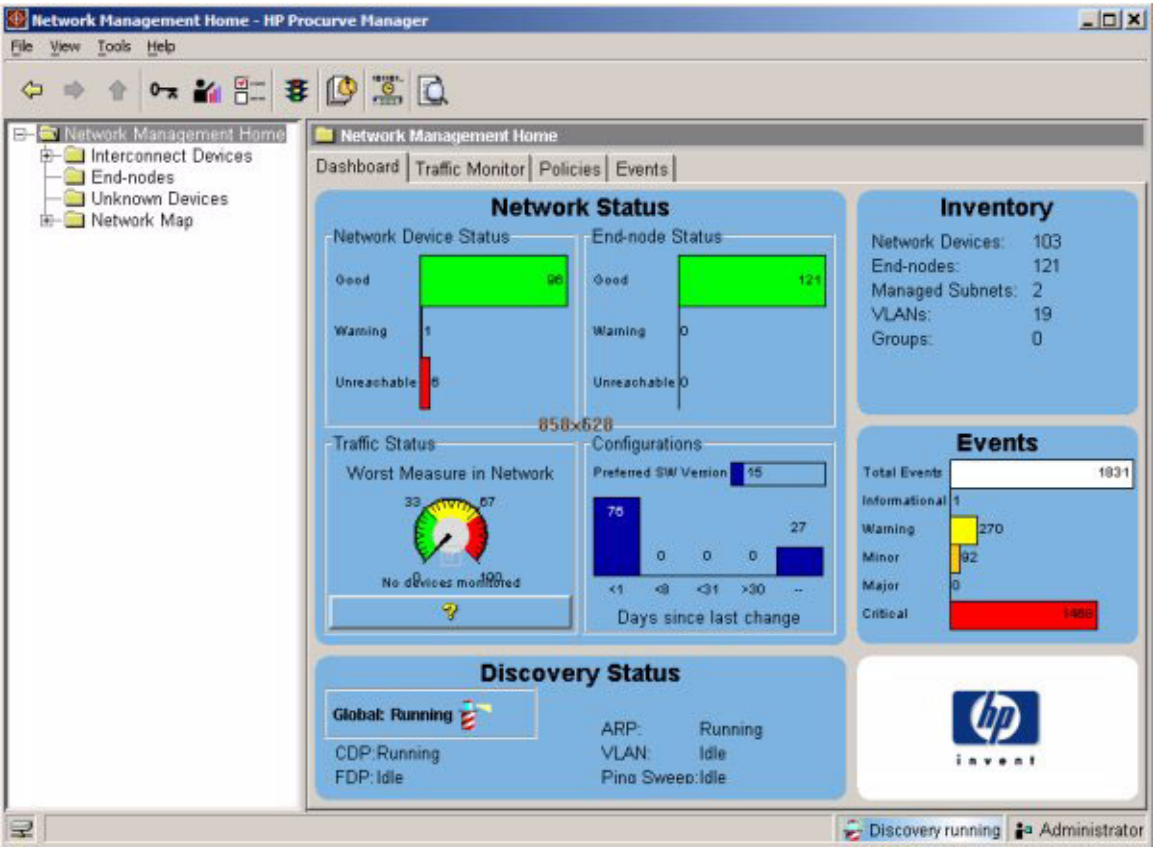


Figure 1-1. HP ProCurve Network Manager, Client Interface

HP ProCurve Manager Features

ProCurve Manager (PCM) offers the basic functionality required by most IT organizations for network management.

Network status summary: Upon boot-up, a Network Status screen displays high-level information on network devices, end nodes and events, all on one screen. From here, you can drill down on any one of these areas to get specific details.

Alerts and troubleshooting: An Events Summary displays alerts and categorizes them by severity, making it easier to track where bottlenecks and issues exist in the network. Alert details provides information on the problem, even down to the specific port.

Automatic device discovery: Customized for fast discovery of all HP ProCurve manageable network devices. You can also define specific IP subnets and VLANs on which to perform discovery.

Network Topology and mapping: Automatically creates a map of discovered network devices. Maps are color-coded to reflect device status and can be viewed at multiple levels (physical view, subnet view, or VLAN view).

Device management: Many device-focused tasks can be performed directly by the software, or you can access web and command-line interfaces with the click of a button to manage individual devices from inside the PCM Client.

HP ProCurve Manager Plus Features

The ProCurve Manager Plus (PCM+) package includes all of the functionality of PCM, along with advanced functionality that can dramatically improve the performance of an IT organization.

Network Traffic Analysis: The Traffic Monitor helps you collect, measure, and analyze data about enterprise network traffic. Traffic Monitor allows you to quickly identify issues, isolate problems, and optimize resource usage.

The Traffic Monitor interface provides detailed information on traffic throughout the network. Leveraging enhanced traffic analysis protocols such as extended RMON and SFlow, you can monitor overall traffic levels, network segments with the highest traffic, or even the top users within a network segment.

VLAN Management: The VLAN Manager in PCM+ provides a single tool to create, track, and manage VLANs on your network. The VLAN management interface lets you create and assign VLANs across the entire network, without having to access each network device individually. The VLAN Manager also provides Wizards for creating VLANs, and modifying VLAN configuration, significantly reducing the likelihood of error in working with VLANs.

Configuration Management: The Configuration Manager in PCM+ automatically tracks and logs configuration changes. You can archive configurations, then apply an archived configuration to one or many devices. Configurations can also be compared over time or between two devices, with differences automatically highlighted for you.

This functionality helps significantly decrease unplanned network downtime and reduce the number of repetitive, configuration tasks that consume hours of your valuable time.

Group and Policy Management: The PCM+ Group and Policy management features allow you to create device groups and set group policies for managing all devices in the group. In addition, you can use the Policy Manager to automatically apply pre-defined configurations across a group of devices, or to any new devices that are added to the network.

Device Software updates: The Software Version Update tool allows you to automatically update devices and obtain new HP ProCurve device software images from HP. You can also configure scheduled software version updates across large groups of devices--when it is most convenient for your network.

Client/Server Architecture

The HP ProCurve Manager software includes the PCM Server: A Windows host containing the HP ProCurve Manager server application software which you install on your primary network management device. The PCM Server is a Java-based application that uses a data repository to store and retrieve collected network management information.

The Client component included with HP ProCurve Manager software is automatically installed on the PCM management server (host). The PCM Client can be installed on other supported host (PCs) on the network, and used to access PCM and PCM+ features. In addition, you can configure additional users for a Client installation, with varying levels of access (Administrator, Operator, User-view only), then alternate between logins.

You can install both the Server and the Client on multiple systems, providing additional redundancy and user access for network management functions.

HP PCM and PCM+ Specifications

Devices Supported

HP ProCurve Manager supports network management functions on the following HP devices:

- HP ProCurve Routing Switches
  9315, 9308, 9304, 6308, 6304
- HP ProCurve Switches:
  5300xl Series (5304, 5308, 5348, 5372)
  4100gl Series (4104, 4108, 4124)
  2800 Series (2824, 2848)
  2600 Series (2650, 2626, and 6108)
  8000m, 4000m, 2424m, 2400m, 1600m
  2512, 2524
  212M, 224M
- HP Wireless Access Points (520wl, 420)
- HP ProCurve 10/100 Hubs (12M, 24M)

Operating Requirements

- Minimum Processor: 500 MHz Intel Pentium III or equivalent
- Recommended Processor: 800 MHz Intel Pentium III or equivalent
- Minimum Memory: 256 MB RAM
- Recommended Memory: 512 MB RAM
- Disk Space: 200 MB free hard disk space minimum, 500MB recommended.
- Operating System: MS Windows 2000, MS Windows XP, MS Windows 2003.

Installing PCM+ on a server with full terminal services is not supported.

Additional processing power and additional disk space may be required for larger networks, and to support extensive traffic monitoring.

Learning to Use HP ProCurve Manager

The following information is available for learning HP ProCurve Manager:

- This Network Administrator's Guide—helps you become familiar with using the application tools for network management.
- 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 ProCurve Manager, Installation Guide—provides details on installing the application and licensing, and an overview of HP ProCurve Manager functionality.

HP ProCurve Manager Support

Product support is 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:

- Product Manuals
- Software updates
- Frequently asked questions (FAQs)
- Links to Additional Support information.

You can also call your HP Authorized Dealer or the nearest HP Sales and Support Office.

2

Getting Started with HP ProCurve Manager

Chapter Contents

Starting PCM Client

Once you have installed the PCM Server and Client, you are ready to start the application. Select the ProCurve Manager option from the Windows Program menu to launch the PCM Client.

The PCM Client will start up and the Login dialogue will be launched.

If you did not enter a Username or Password during install, type in the default Username, *Administrator*, then Click Login to complete the login and startup.

If you have installed the PCM Server on more than one system, the first time you start up the PCM Client you will be prompted to select the primary server. You will also see the "Search for Servers" dialogue if the original primary server is unreachable.

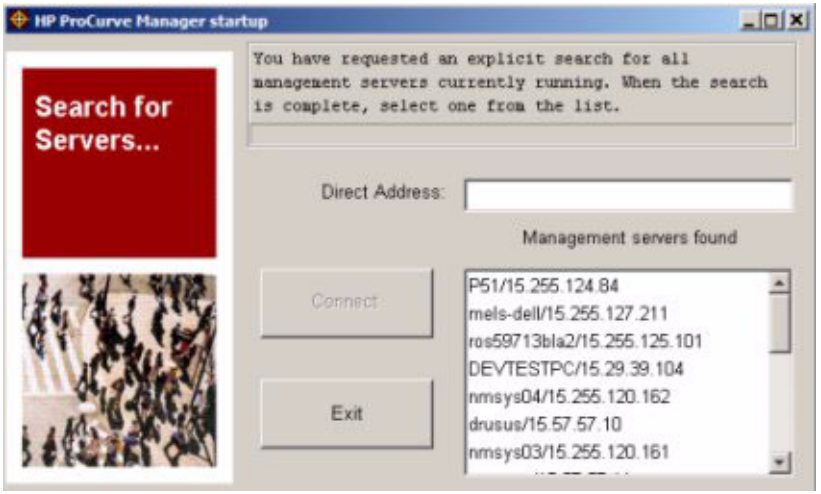


Figure 2-1. Search for servers

Select the server from the list on the right, then click Connect. The PCM Client will launch the HP ProCurve Manager home window.

NOTE: If you are unable to launch the PCM Client, check the IP Address in the **access.txt** file in the **config** directory on the PCM Server. See "Troubleshooting the PCM Application" on page 2-16 for more information.

License Registration

The HP ProCurve Manager installation CD includes a fully operable version of the PCM application, and a 30 day trial version of the PCM+ application. Until you have registered PCM and/or PCM+, an Expiring License warning will be displayed each time you log in, similar to the following.

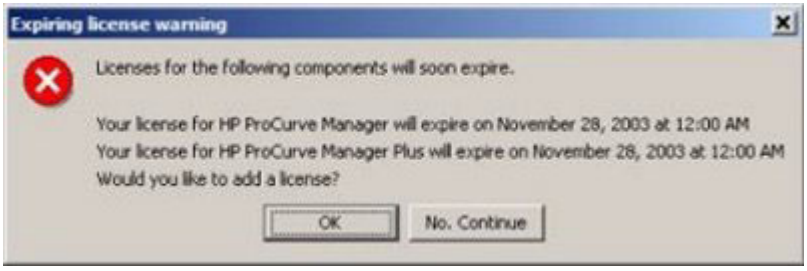


Figure 2-2. HP ProCurve Expiring License warning dialogue

Click No, Continue to close the dialogue. Click OK to launch the License Administration dialogue.

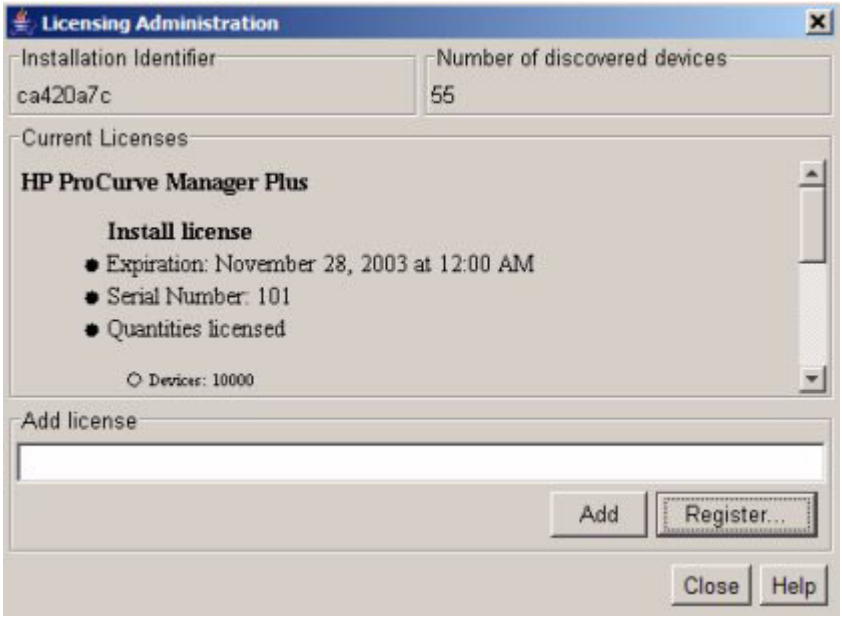


Figure 2-3. HP ProCurve License Administration dialogue

Click Register to go to the HP ProCurve Registration Web site. For details on registering PCM or purchasing PCM+, please refer to the *HP ProCurve Manager Installation Guide*.

HP ProCurve Manager Home

The Network Management Home display provides a quick view of your network status in the Dashboard tab, along with a navigation tree and access to menu and toolbar functions. You can resize the entire window, and/or resize the panes (sub-windows) within the Network Management window frame.

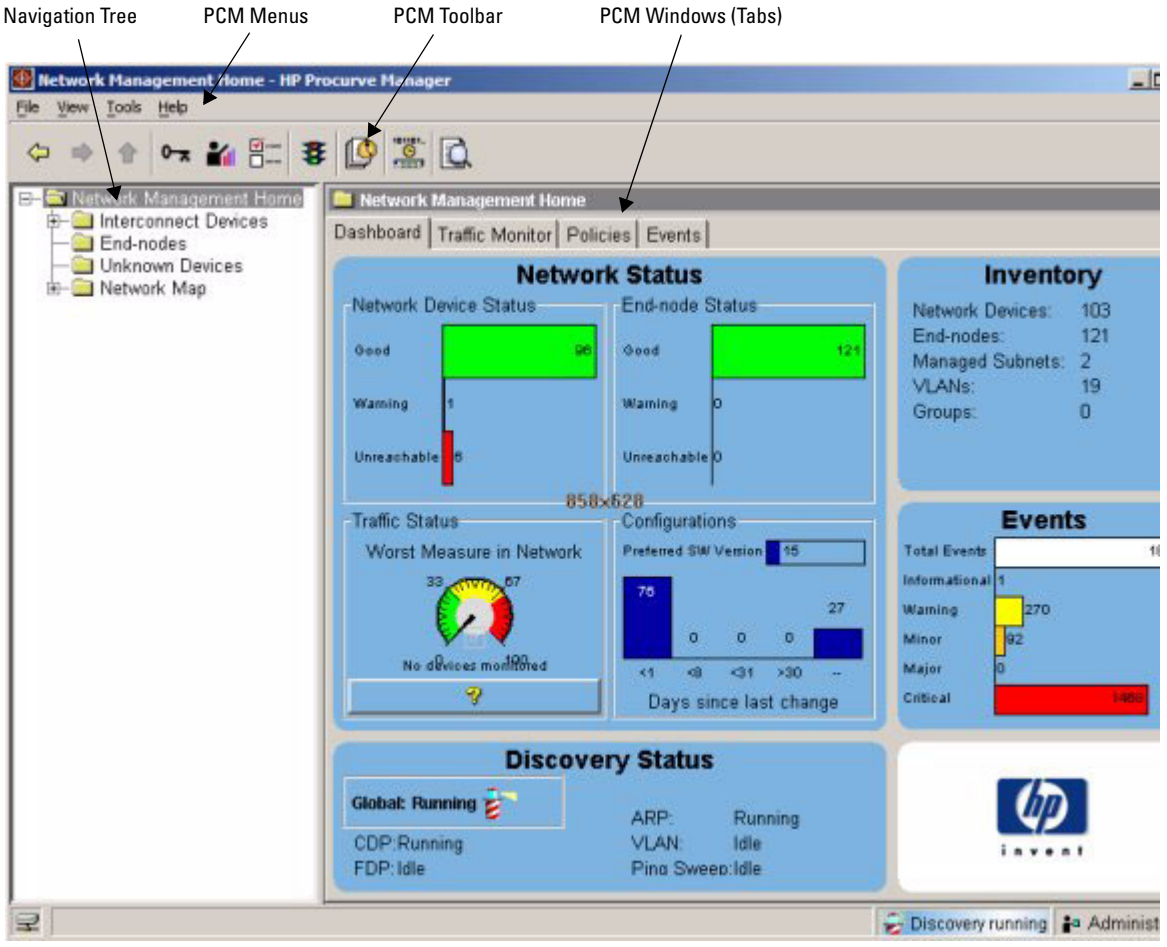


Figure 2-4. Home Page for HP ProCurve Manager

The basics of working within the PCM Client and the Network Management Home window are described in the following sections. The function descriptions assume you are familiar with using the Windows graphical user interface.

Network Management Home Window

The Dashboard tab (window) contains four separate panels, described below.

Network Status: This panel contains four sub-panel displays, described below.

- Network Device Status - A color coded histogram showing the number of devices by operational status. Clicking on this sub-panel will open the Device List window.
  - Good means the device is responding normally to discovery and status polling actions.
  - Warning means the device is responding to polling and discovery actions, but needs attention. Warnings can be triggered by events received from the device or by agents monitoring the device.
  - Unreachable means the device is not responding to discovery or polling actions.
- End-node Status - A color coded histogram, showing the number of end-nodes by operational status, similar to Network Device Status. Clicking on this sub-panel will open the Device List window.
- Traffic Status - A color-coded gauge indicating traffic measurement in the worst segment of the network based on threshold settings. If you do not have PCM+ installed, an "unavailable" message is displayed. The message "No devices monitored" is displayed if you do not have any devices configured in the Traffic Monitor.

  The color indicators used in the Traffic gauge are:
  - Green: indicates the values are within normal range.
  - Yellow: indicates threshold values have exceeded the normal range, but are not critical.
  - Red: indicates threshold values are in the critical range, and corrective action is needed.

  Clicking on this sub-panel will open the Traffic Monitor window.
- Configurations - A histogram indicating the number of devices with software configurations that differ from the preferred software version, and days since the configuration changed. If you do not have PCM+ installed, this section will not appear. Clicking on this sub-panel will open the Device Configuration window.

Inventory: This panel provides a count of the number of network devices, end-nodes, Subnets, VLANs, and Groups currently found on the network.

Events: This panel displays a summary of the outstanding (unacknowledged) events, including a count of the number of critical, major, minor, warning, and information events. Clicking on this panel will open the Events Monitor window.

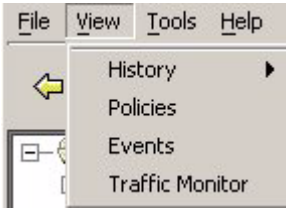
Discovery Status: This panel lists the status of the Device Discovery scans, running or idle.

Whenever you have changed the PCM window display, just select Network Management Home in the navigation tree to return to the Dashboard display.

PCM Status Bar

A Status bar at the bottom of the main PCM window lists the status of the Discovery process (running or idle), and indicates the login account currently in use. This status bar is visible at all times in the PCM client window frame.

PCM Main Menu Functions

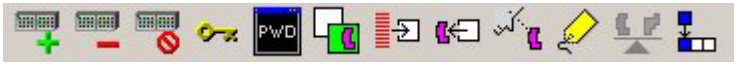


The application menus are available at all times in the PCM main window frame. The functions available in the menus will vary based on your login account type, and whether you are using PCM or PCM+. Disabled functions will be grayed out in the menus. Use of the application menu items is described later in this book under the process it supports.

Toolbar Functions

The PCM global toolbar functions are available at all times in the PCM main window.

A separate "components" toolbar appears in many of the device information and configuration windows.

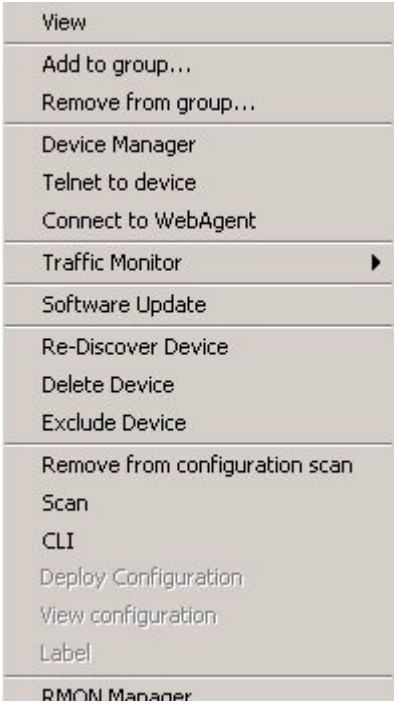


If you resize your window and reduce it's width, some component toolbar icons may be hidden due to size limitations. Increase the width of the window to restore all the toolbar icons.

The functions available in the toolbar will vary based on your login account type, and whether you are using PCM or PCM+. Disabled functions will be grayed out in the toolbar. The component toolbar icons are described later in this book under the process they support. You can hover with the mouse to display 'Tooltips' that describe the function of each of the toolbar icons.

Using the Right-Click Menu

You can also access most of the management tools and commands provided with PCM and PCM+ via the "right-click" menus. To use the right-click menu, select an object (node) in the navigation tree on the left of the screen, then right-click your mouse to display the menu. You can also access the right-click menus when a device is selected in the Devices List on the view panel.



The options enabled in the right-click menu will vary based on the node or device you have selected in the navigation tree, whether you are using PCM or PCM+, and your login account type. Disabled functions will be grayed out.

Using the Navigation Tree

The navigation tree in the left pane of the PCM window provides access to network device information using a standard Windows file navigation system. Information about groups of devices and each individual device or node discovered on the network by PCM can be accessed from the navigation tree. The tree is organized as follows:

Interconnect Devices: The top level of the tree provides access to information about every device in the network. Clicking the node displays the Devices List in the right panel of the window. Expanding the node displays the Device Group nodes, or HP ProCurve product line. The Device Group nodes can be expanded to access individual device information.

- The HP ProCurve Others node includes HP ProCurve devices that are SNMP accessible, but do not support CDP or FDP.
- The Others node includes network devices that are not part of the HP ProCurve family of products.
- The Custom Groups node is used to access information about devices in any Groups you have configured. See "Configuring Custom Groups" on page 10-3 for more details on creating Groups.

End Nodes: This node displays the Devices List for devices found on the network that are SNMP accessible, but do not support the bridge MIB, such as HP printers.

Unknown Devices: This node displays the Devices List for other devices found on the network that are not SNMP accessible, but have valid IP or IPX addresses.

Network Map: This node displays the Network Map for the entire network. The Network Map node can be expanded to access The Subnets and VLANs display listings and maps for the configured subnets and VLANs.

Viewing Device Information

There are several ways to view device information in HP ProCurve Manager.

- Select Interconnect Devices in the navigation tree to display the Devices List in the Interconnect Devices window. This will list all devices discovered on the network. If you are using PCM+ you will also see tabs for Traffic Devices and Configurations in the Interconnect Devices window.
- Click the "Network Device Status" panel in the Dashboard display to view the Devices List in the Interconnect Devices window.
- Select the Device Group (model) in the navigation tree to display the Devices List for the Device Group. This will list all devices of that type discovered on the network.

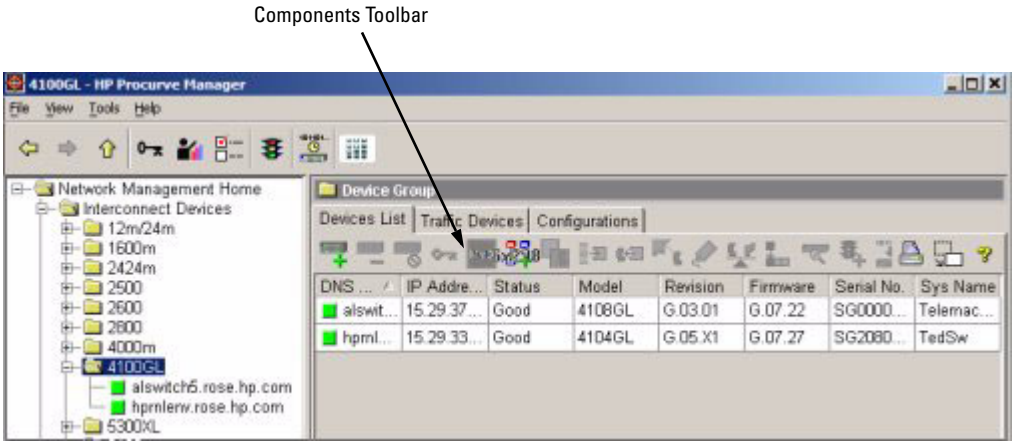


Figure 2-5. Example of the Devices List window

By default, the device lists are sorted on the first (left) column in descending order (1-10, a-z). You can click the column heading to change the sort order to ascending. You can also sort the data by any of the other columns contents by clicking on the column heading. An arrow indicates the sort column, and the sort order.

From the Devices Lists you can select individual devices to drill-down for additional information, or to manage network and device configuration. You can also use "Ctrl + click" and "Shift + click" to select multiple devices in the list for configuration and management tasks.

To review Device Properties, double-click the device entry in the Devices List window, or click the device node in the navigation tree.

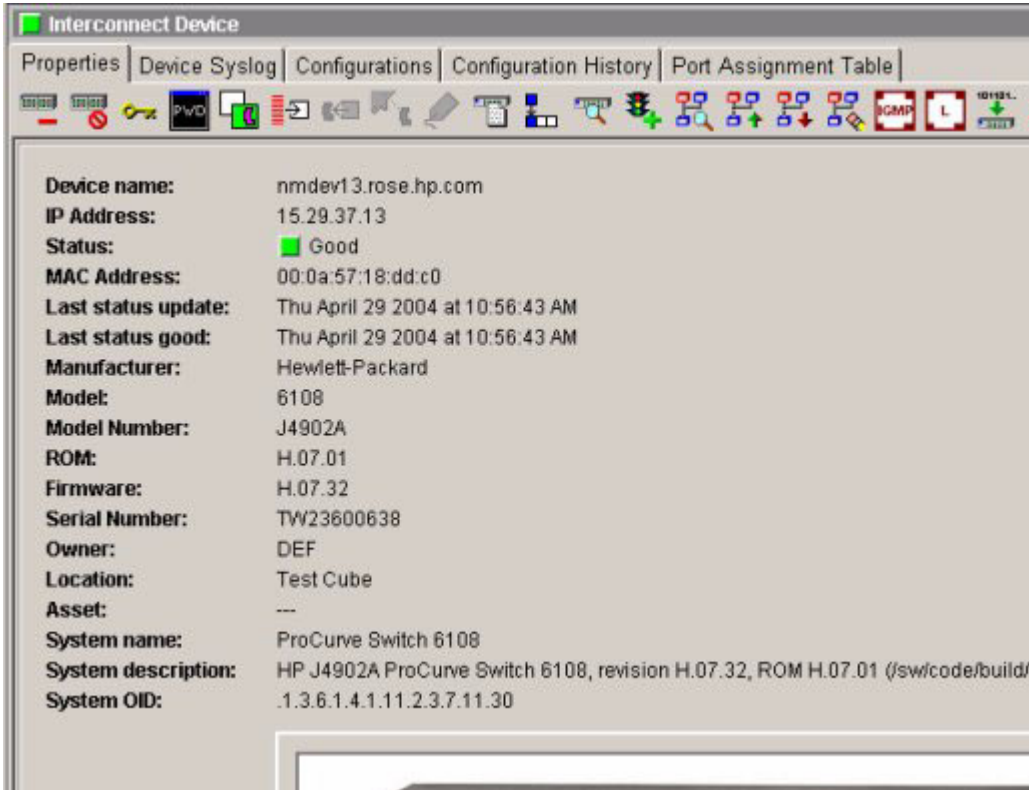


Figure 2-6. Device Properties window

Network Maps

HP ProCurve Manager also provides a map feature you can use to view your network topology.

- To view a map of the entire network structure, select the Network Map node in the navigation tree.

To view a subnet map, expand the Network Map node in the navigation tree to display the Subnets and VLANs nodes. Now you can:

- Select the Subnets node to display the Subnets List view, then double-click on the subnet in the list.

- Expand the Subnets node in the navigation tree to display the IP address for each of the subnets in the managed network, then select the IP address in the navigation tree.

For additional information on working with maps, see Chapter 4, “Using Network Maps”.

Floating Windows and Reports

There are two icons that appear in the components toolbar of most PCM and PCM+ windows.

The Show in New Window icon will copy the current tab or window display to a separate floating window on your desktop.

The Report icon displays the PCM tab window contents in a separate page layout window, formatted with a Company header, Report Title, and date. You can then print the report, or save it to a file.

Setting the Report Heading

To set the heading that will be printed on your PCM reports, click the Preferences icon in the PCM toolbar, then select the Reports option in the Global menu. This will launch the Global Preferences Reports settings window.

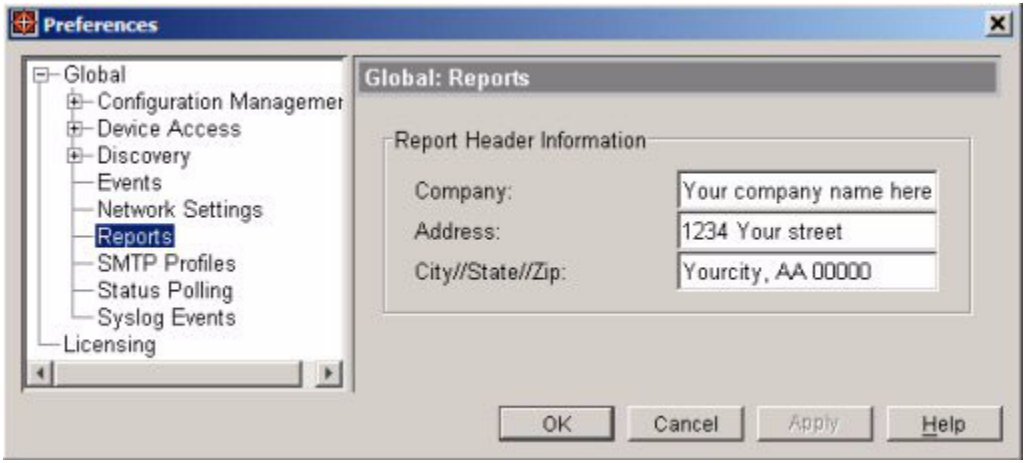


Figure 2-7. Preferences, Global:Reports window

Enter the information you want to appear in your reports, then click OK to save the changes and close the Preferences window.

Managing User Accounts

To manage login accounts for PCM, click the Add/edit/delete Users icon in the PCM toolbar, or select the Manage Users option from the File menu.

Changing Passwords

Use the Change Password option in the PCM File menu to change the default Administrator password or other login account passwords.

HP ProCurve Manager is configured with a default password for the Primary Administrator account. If you did not modify the password during installation, you should change this password after you first login.

The username requires at least two characters; the password at least three. For both the username and password, the maximum number of characters is 30.

A user name must begin with a letter or an underscore. Passwords can begin with any letter, underscore, or number. The password can contain lower and upper case letters from A to Z, the underscore character (_) and numbers from 0 to 9. It cannot contain any spaces, or any other "special" characters other than the underscore.

Adding User Accounts

The Manage Users function lets you add additional login accounts with access permissions set by the profile under which the user is added. The three profiles are:

- Administrator: This profile has permissions to all features included in HP ProCurve Manager, including adding and editing user accounts.
- Operator: This profile has permission for all administrative functions for configuring and monitoring devices, but does not have access to the user account management functions.
- Viewer: This profile has view-only access to HP ProCurve Manager screens. Users do not have access to any configuration or management functions.

To add a new user:

1. Click the User Manager icon to launch the Manage Users window.

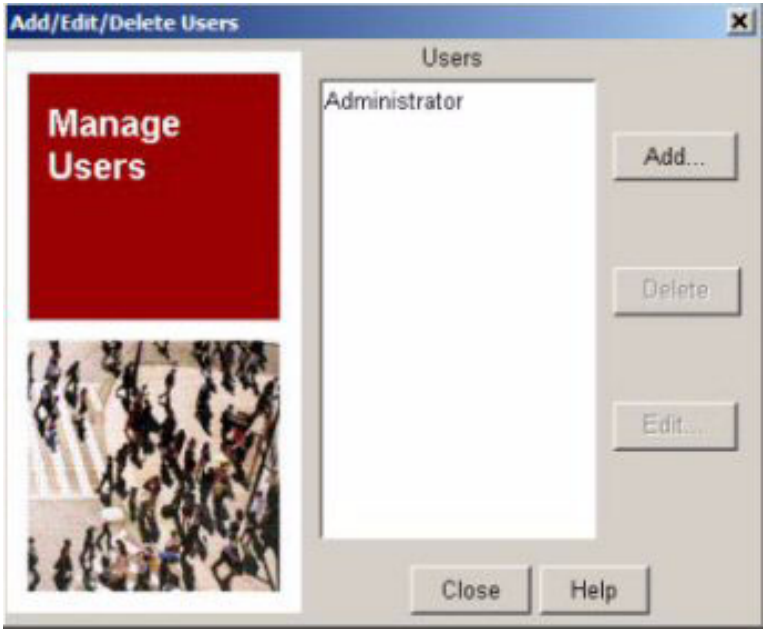


Figure 2-8. HP ProCurve Manage Users Wizard.

2. Click Add to Launch the Add Users window.

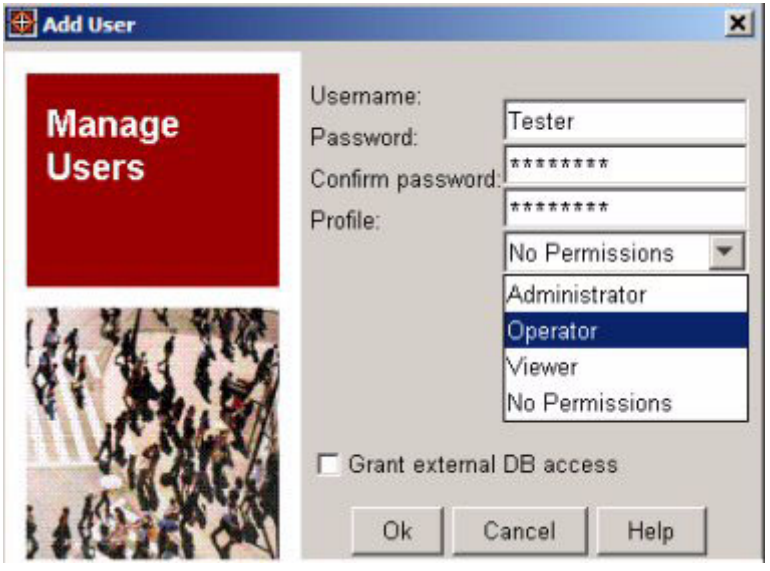


Figure 2-9. Add User dialog

3. Enter the Username and Password, then select the Profile for the account.

   Usernames must contain at least 2 characters, and cannot contain spaces. Passwords should conform to standard Password requirements (i.e., contain a combination of numbers, upper and lower case characters, etc.)

4. To allow user access to the PCM database from another application, such as HP OpenView Network Node Manager (OV_NNM), click to select Grant external DB access.

   The PCM database can be accessed directly through supported protocols. (JDBC, ODBC, solsql, etc.)

5. Click Ok. This will save the new user setup and close the Manage User Wizard.

Editing and Deleting User Accounts

Only Administrators can add, edit or delete users from the HP ProCurve application.

To edit a user account,

1. Select the account in the Manage Users window to enable the Edit and Delete option.
2. Select the Edit option to open the Edit Users window. It contains the same parameters as defined in the Add Users window.
3. Edit the user account parameters as desired, then click Ok.

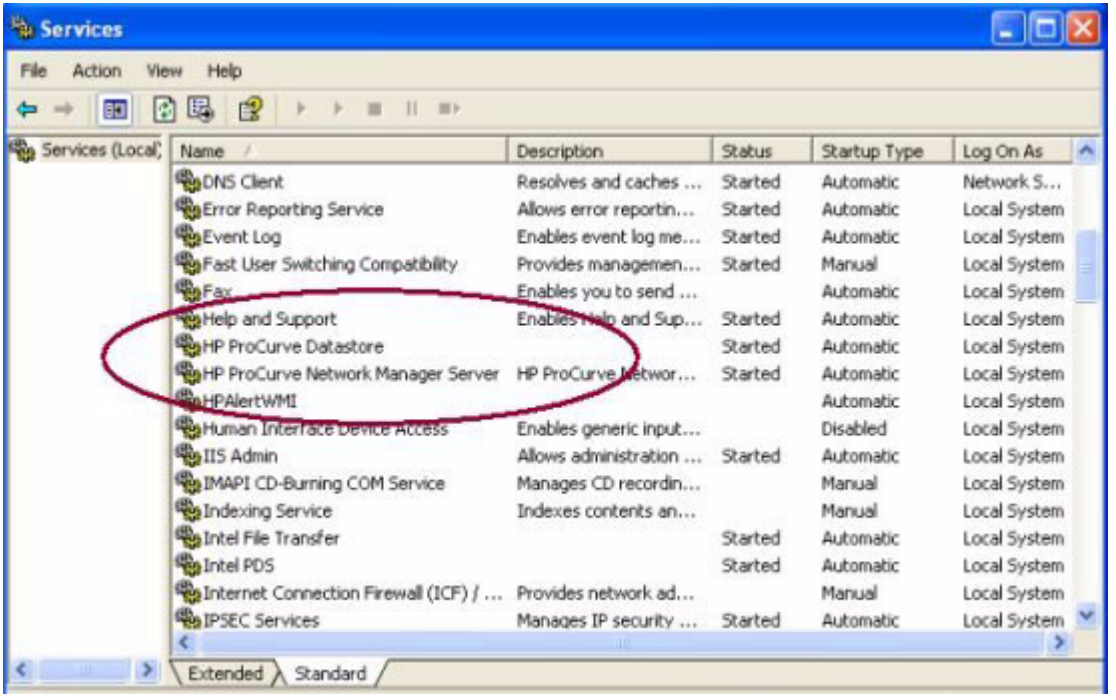
To delete a user account,

1. Select the account in the Manage Users window to enable the Edit and Delete options.
2. Click Delete.

Troubleshooting the PCM Application

PCM Services

If you are having trouble starting the PCM Client, or the application is not responding to commands, check to see that the PCM services are running on the PCM management server.



You may need to use the Windows Administrative tools option to restart one or more of the following services:

- HP ProCurve Datastore
- HP ProCurve Network Manager Server

PCM Client Permissions

If you can start the PCM Client, but there is no data, you may need to set the permissions for the client.

There are two files associated with HP ProCurve Manager client/server security.

- The **access.txt** file is located on the HP ProCurve Manager management server under the */Program Files/Hewlett-Packard/PNM/server/config* directory. This file contains a list of all IP addresses that are authorized to connect to the management server.

  There are situations where it is not possible to know ahead of time what IP address a potential client will have. This is particularly the case in situations where the client comes in through some sort of VPN, where the IP address of the client is assigned externally. To solve this problem it is possible to add client passwords to the **access.txt** file that correspond to specially configured clients. The file can contain a combination of IP addresses and passwords.

  For example, below is an example of a valid **access.txt** file:

  ```
  15.255.124.84
  15.29.37.*
  10.*.*.*
  *.rose.hp.com
  system1.hp.com
  ```

- The password in the **access.txt** file must match the password entered in the **riptide.cfg** file located on the PCM client under the */Program Files/Hewlett-Packard/PNM/client/* directory.

  To enable password access for a particular client:

1. First you need to you must change an entry in the **server\config\TyphoonServer.cfg file**.
   This file is a text file and can be edited with Notepad or Wordpad. Look for the entry that reads "AUTHENTICATION=10", and change it to read "AUTHENTICATION=100". Save the file and restart the server (listed as "HP ProCurve Network Manager Server" in the services list).
2. Edit the access.txt file as described above, but instead of entering an IP address, just enter the selected password (on a line by itself). Save the file. It is not necessary to restart the server. For example, if we set the password to "procurve":

   ```
   procurve
   *.rose.hp.com
   system1.hp.com
   ```

3. On the client (the client must already be installed), you must edit the **riptide.cfg** file. This file already has several entries in it. You must add a line similar to the following:

   PASSWORD = your password

   Do not change any of the other entries in the file, as they are necessary for the correct operation of the client.

A sample Riptide.cfg file, once edited with the password "procurve", would look like this:

```
LEASE_LENGTH = 40000
TRACING_PROPERTY_KEY = CoreServices.Main
MANUFACTURER = Hewlett-Packard
SERVICE_NAME = Typhoon
COMPONENT_DB = config/Components.prp
TRACING_DBFILE = config/Loggers.prp
NETWORK_DELAY = 25000
VERBOSE = true
PASSWORD = procurve
```

Once you have saved the riptide.cfg file, start the PCM Client and enter (select) the address of the PCM Server in the Direct address field of the "Search for Servers" dialog. The client should now connect successfully to the server.

3

Discovering Devices

Chapter Contents

How Discovery Works

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 List and Network Maps, and added to the device information database on the PCM server. HP ProCurve Manager can discover any devices within the managed network (subnet), that are SNMP accessible (with valid read community names). Such devices include:

- HP's ProCurve series of manageable switches and routers that support CDP (Cisco Discovery Protocol) or FDP (Foundry Discovery Protocol).
- Other HP ProCurve devices that are SNMP accessible, but do not support CDP or FDP.
- Other HP network devices that are SNMP accessible and support the bridge MIB.
- Devices on the network (end nodes) that are SNMP accessible, but do not support the bridge MIB, such as HP printers.
- Other devices on the network with valid IP addresses.

Discovery is a resource-intensive process and may take some time. It uses a four-phase process, working from the "starting device" IP address, and using the SNMP read community name specified during the installation process, to find and map devices in the network.

- In the first phase of the discovery process, PCM looks for all CDP and FDP enabled devices in the CDP/FDP Neighbor tables on the device. CDP is implemented on the following HP ProCurve devices: 8000, 1600, 4000, 2400, 2424, 5308, 2512, 2524, 5304, 4108, 4104, 2650, 6108, and 28xx. FDP is available on the 9300 devices with software version 7.6 or later. For a more complete discussion of CDP, refer to the "Management and Configuration Guide" for your HP ProCurve switch.
- In the second phase of the discovery process, ARP discovery is used to find any other active network devices (in ARP tables) that are not discovered via CDP or FDP. For a more complete discussion of ARP, refer to the "Advanced Traffic Management," or the "Management and Configuration Guide" for your HP ProCurve switch.

- The third phase of discovery is the ping sweep discovery. It is used to locate all devices connected to the network. This process will take the longest time to run due to timeouts because it will ping all addresses in a subnet.
- In the VLAN discovery phase, Discovery uses SNMP to collect information about VLANs configured on each device found on the network. If VLANs are not used in your network, it's recommended that you turn off VLAN discovery to reduce network traffic and resource usage.

From the starting device, specified during installation, Discovery will propagate through each of the devices listed in the CDP/FDP neighbors table and continue until it reaches a device without any CDP/FDP connections. Once the initial CDP/FDP phase is complete, Discovery will start the ARP, ping sweep, and VLAN discovery processes.

For each device found in the network during CDP/FDP, ARP, and Ping sweep, Discovery will perform the following process:

- Classify the device type for grouping in the "Tree" listing on the PCM Dashboard.
- Retrieve and update the device's properties, such as ports, VLAN configurations, software versions, sysContact, sysLocation, etc.
- Log an entry to the Device Log indicated the device has been created (an entry added to the PCM database)
- If AutoTrap is configured, add the management station as a trap receiver on the device, and log an entry to the Device Log and Events monitor table indicating either success or failure.

Initially, discovery works only for devices on the same subnet as the Discovery starting device. Discovery will poll the starting device for the subnet mask and compute the subnet address from the IP address. Discovery will then define the subnet as the default managed subnet. Once you have started PCM, you can add subnets and devices on your network to the Discovery list.

Discovery uses the default SNMP read community name specified during the install process to discover new devices on the network. Once a device is discovered, you can change the SNMP read community name for that device in PCM, but you will also need to add or change the specific community name on the device.

When Discovery is first started, it will launch the Status Polling component to poll the discovered network devices for operational status at prescribed intervals. The polling results are used to display device status in the Devices List. The interval for running each Discovery component can be altered in the Discovery Preferences settings. (See “Managing the Discovery Settings” on page 3-13.) Note that even if Discovery is stopped, status polling will continue to run and check the status of devices on the network.

You can review the current Discovery status in the Dashboard window. The Global indicator refers to the entire discovery process. That is, if any segment of discovery is running, Global status will be Running. Each of the segments is listed separately, with a status of Idle or Running. If Discovery is stopped, the Global status will report it is stopped.

Figure 3-1. Discovery Status panel of Dashboard window.

In addition, the Status bar in the bottom PCM window frame includes an indicator for Discovery status. This allows you to check the Discovery process status at all times.

Reviewing Discovery Data

The Dashboard window provides a summary of the items discovered on the network in the Inventory panel.

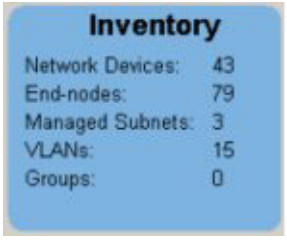


Figure 3-2. Inventory summary provided by Discovery

You can also click the Interconnect Devices node in the navigation tree to display a list of all devices discovered. The Subnets and VLANs nodes under the Network node in the navigation tree can be used to view a list of discovered Subnets or VLANs, and to access network topology map views.

If you change a device configuration, and do not want to wait until the next scheduled scan to see the changes in PCM, you can right-click on the device in the navigation tree, or the Devices List, then select the Re-Discover Device option in the right-click menu. If you do not find a device in the Devices List, use the Manual Discovery process to check for a device.

A device must be re-discovered to update PCM with changes due to any of the following:

- the device was disconnected, then reconnected to another port or device
- a "blade" has been removed or added to the device
- configuration changes are made to the device, such as STP, trunk connection, etc.
- connections shown for the device in the Network Maps are incorrect.

Note:

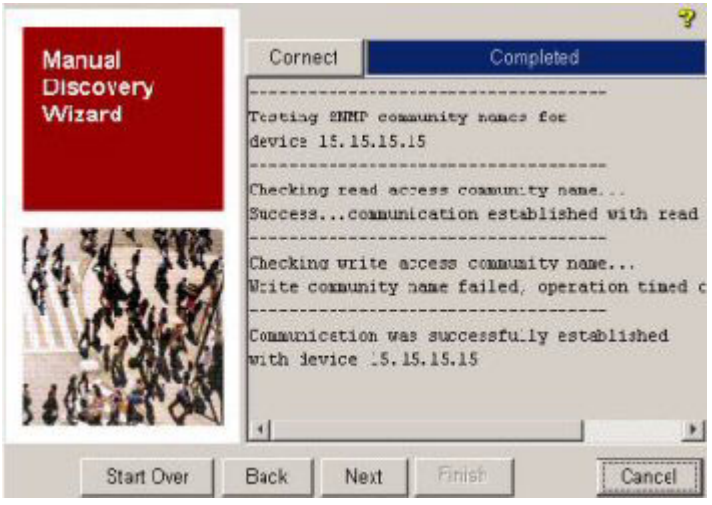
Discovery and Re-discover do not collect device configuration information. Discovery is used only to update the device's network properties and connections, as described on page 3-3. To get device configuration data, you must use the Configuration Manager Scan, described in Chapter 8, "Managing Device Configurations."

Using Manual Discovery

You can manually discover a device on the network at any time by clicking the "Manually discover device" icon in the Devices List toolbar, or by selecting the Manual Discovery Wizard option in the PCM Tools menu. If the device entered does not belong to a managed subnet, Discovery will automatically create a managed subnet for the device.

Enter the IP address and SNMP Read Community and Write Community names for the device you want to discover.

Once you have entered the device information and click Next, PCM will attempt to verify the device information and establish a connection with the device. If the IP address or SNMP community is not found, a failure message is displayed. In this case, go back and re-enter the device information and retry.



Click Next to complete the discovery process and view the device discovery summary, then click Finish to close the wizard.


Manual
Discovery
Wizard
Summary
Device: 15.15.15.15
Read Community Name: public (successful)
Write Community Name: unrestricted (failed)
Communication was successfully established
with device 15.15.15.15
Click the finish button to discover device
Start Over
Back
Next
Finish
Cancel

Managing the Discovery Process

You can manage the discovery process in PCM with the Discovery functions in the Preferences tool. Click the Preferences icon in the toolbar to display the Preferences Window and access the Discovery options.

When you select Discovery in the Preferences Global menu, the Global Discovery window is displayed.

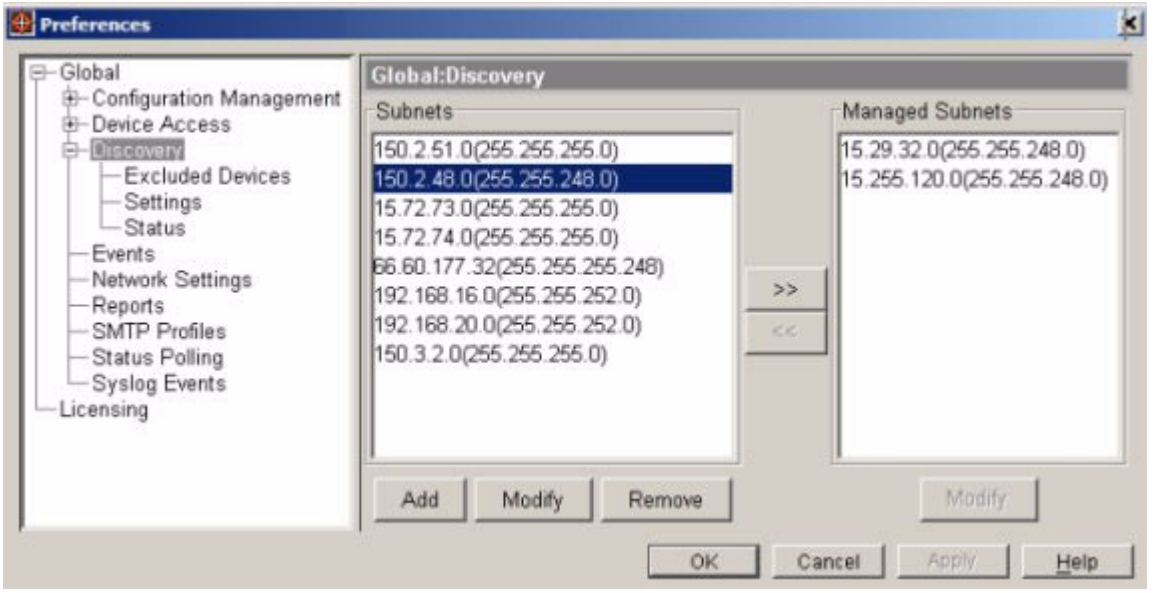


Figure 3-3. Global Discovery Window

Adding and Removing Subnets from Discovery

The Managed Subnets panel in the Global:Discovery window lists the subnets that are included in the Discovery process. The Subnets panel lists all other subnets found by Discovery.

To add a subnet to the Managed Subnets list, select the Subnet address and click >> to move it under Managed Subnets, then click OK or Apply. Click OK in the Restart Discovery pop-up dialogue to complete the process.

You will see a difference in the number of subnets listed in the Inventory panel in the Dashboard window.

Adding and Modifying Subnets

To add a new subnet to the list of subnets in the Global:Discovery window, click Add to launch the Add Remote Subnet dialogue.

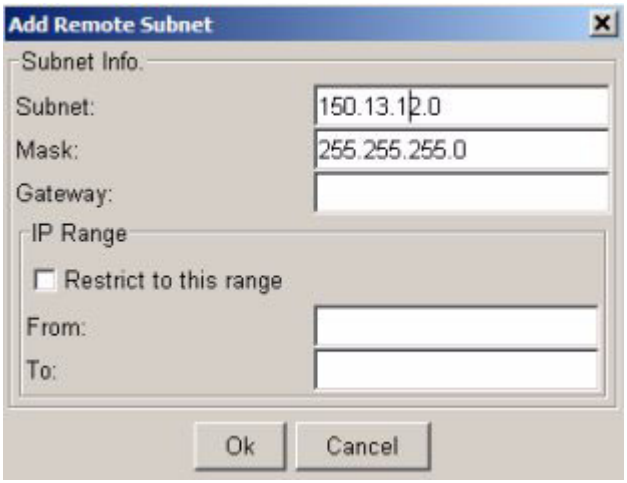


Figure 3-4. Add Remote Subnets dialogue

You must enter the Subnet IP Address, Subnet Mask address, and IP Address of the Gateway for the subnet. The IP Address section can be used to restrict discovery on the Subnet to a Range of IP addresses.

When you have entered the Subnet information click OK. The subnet information will be validated. If the IP address of the Subnet or Gateway is not found or invalid, you will get an error message. Otherwise, the Subnet Address will appear in the Subnets list on the Global:Discovery window.

To remove a Subnet from the listing, select the address in the Subnets list, then click Remove. The Subnet address will no longer appear in the Global:Discovery window.

To modify a Subnet, select the Subnet address in either the Subnets or Managed Subnets list in the Global:Discovery window, then click Modify button under the list. This will display the Modify Subnet dialogue, similar to the Add Remote Subnet dialogue. Make the desired changes, then click OK.

You need to restart the discovery process for the subnet changes to take effect.

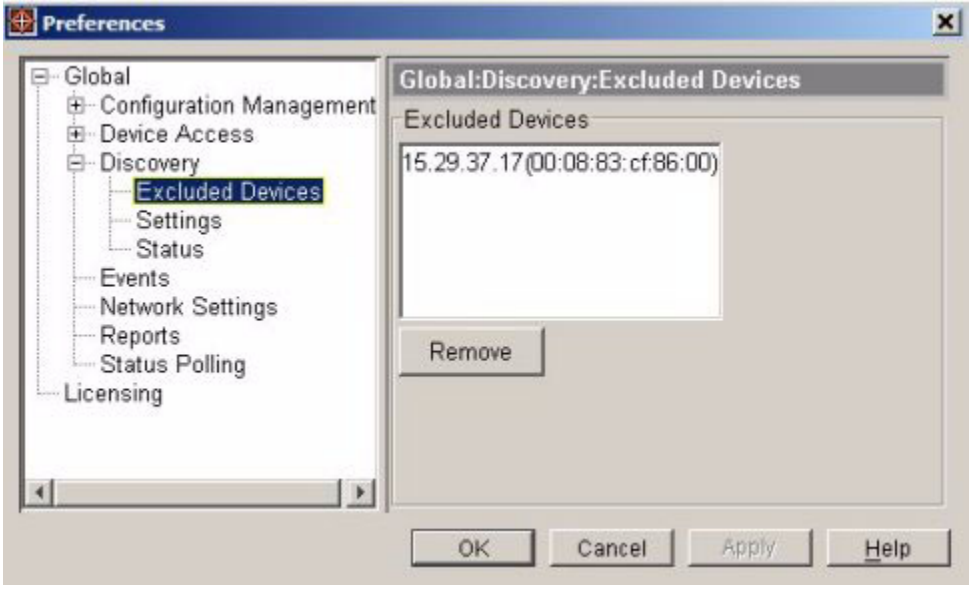
Excluding Devices from Discovery

A device can be excluded from all subsequent discoveries by adding it to the Excluded Devices list. Thereafter, the device can be included in discoveries by removing it from the Excluded Devices list.

To exclude a device from discovery, select the device in the Devices List, then click the Exclude Device icon in the toolbar. The device IP address will be added to the Excluded Devices list in the Global:Discovery:Excluded Devices window.

To include a device that was excluded from discovery:

Go to the Excluded Devices window [Preferences->Discovery->Excluded Devices].



Select the device in the Excluded Devices list, click Remove to remove it from the list, then click OK.

You need to restart Discovery for the change to take effect. If you do not click Yes in the Restart Discovery pop-up, you will need to use the manual discovery process to find and display the device in PCM.

If a device has been removed from the managed subnet or you no longer want to track the device, select the device in the Devices List, then click the "Delete selected device" icon in the toolbar.

Re-Classifying Unknown Devices

In some instances Discovery will be unable to classify an HP ProCurve device, generally due to a mismatch in the SNMP Management community name settings. You can reclassify the device so that the Discover process can determine the device type and configuration, and place the device into the correct group.

To reclassify an unknown device, click the Unknown node in the navigation tree to display the Devices List for unknown devices. Select the device to be reclassified and click the Reclassify Device icon in the toolbar to launch the Reclassify Device Wizard.

Click Next to continue the re-classification process.

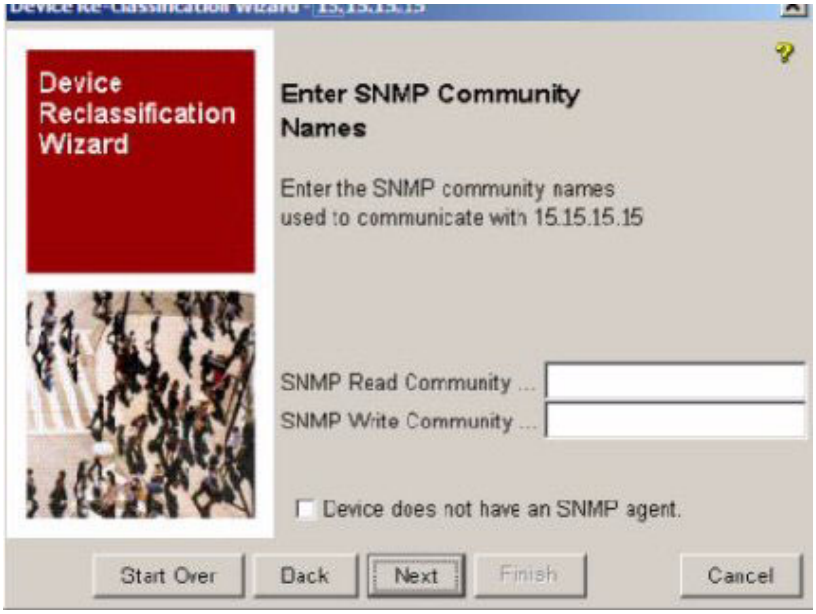
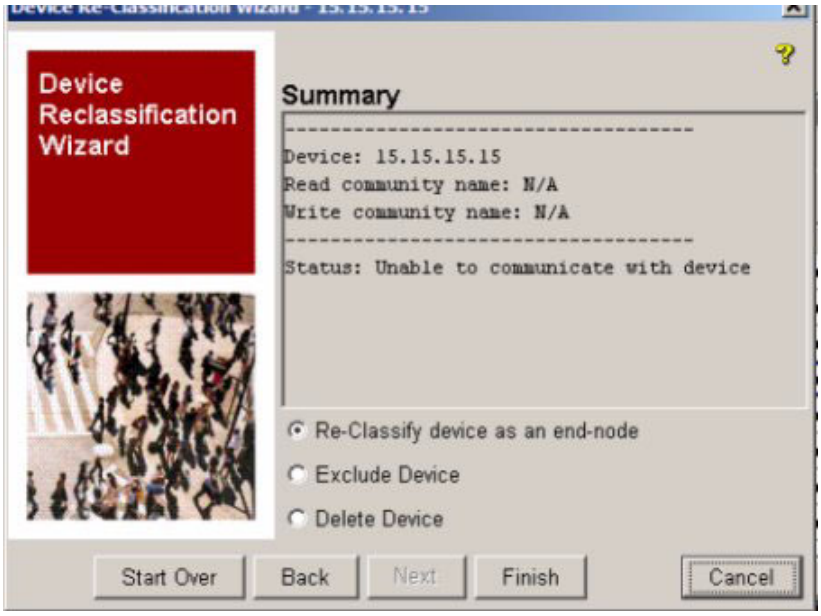


Figure 3-5. Device Re-Classification Wizard: SNMP Community Names

If the device does support SNMP, type in the SNMP Read Community name and Write Community name for the device, then click Next.

If the device does not support SNMP, check the Device does not have an SNMP agent option, then click Next.



If you entered the SNMP Community Names, the wizard will attempt to establish communication with the device. If the wizard cannot communicate with the device, or if the device does not have an SNMP agent, you can select one of the options from the bottom of the Summary dialogue:

- Re-classify device as an end-node: Move the device from the Unknown Devices group to the End-nodes device group.
- Exclude device: Exclude the device from future discovery scans.
- Delete device: Remove the device from the PCM devices list. The device will no longer be accessible in PCM.

If the wizard is able to communicate with the device, the device is moved to the appropriate group.

Click Finish to complete the process and exit the wizard.

NOTE: Once you re-classify a device as an end node, you cannot change the device classification.

Managing the Discovery Settings

You can change the Discovery starting device, and configure the frequency of discovery scans from the Discovery:Settings window.
[Preferences->Discovery->Settings]

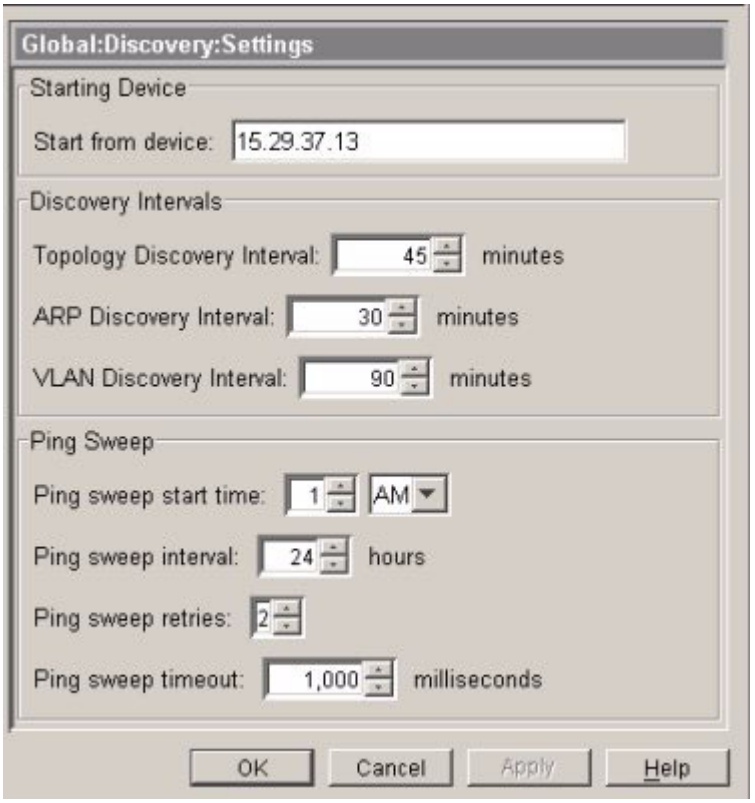


Figure 3-6. The Global Discovery Settings panel

When changing any of the discovery settings, click Apply to save the changes without leaving the Discovery:Settings window, or click OK to apply the changes and close the Discovery:Settings window.

To change the Starting Device: Delete the existing entry and type in the IP address of the Start from device (core HP ProCurve device or default gateway) for the discovery process. The starting point can be configured to be any SNMP network device that is reachable from the management server; however, discovery will work faster if an HP ProCurve device is used.

If the IP address entered is invalid or is not a legal IP address, PCM Discovery will ignore the entry and continue to use the last valid Discovery starting device. When you change the Discovery starting device, the previously specified starting device will be treated as a remote Subnet.

To change the Discovery Intervals: Type in the interval (minutes) or use the buttons to increase or decrease the interval time. Topology Discovery Interval is used to set the interval for CDP/FDP discovery.

Tip: *You can turn off any of the discovery scans by setting the interval to zero (0).*

To change the Ping Sweep settings: Type in the desired parameters, or use the button to increase or decrease the parameters. Use the pull-down menu to select AM or PM for the Start Time. Because the Ping Sweep takes the most time and resources, it is generally a good idea to run it when network traffic is minimal, such as late at night or early morning.

Changing the Status Polling interval.

You can change the interval at which device status polling using Status Polling option in the Global Preferences. [Preferences->Status Polling]

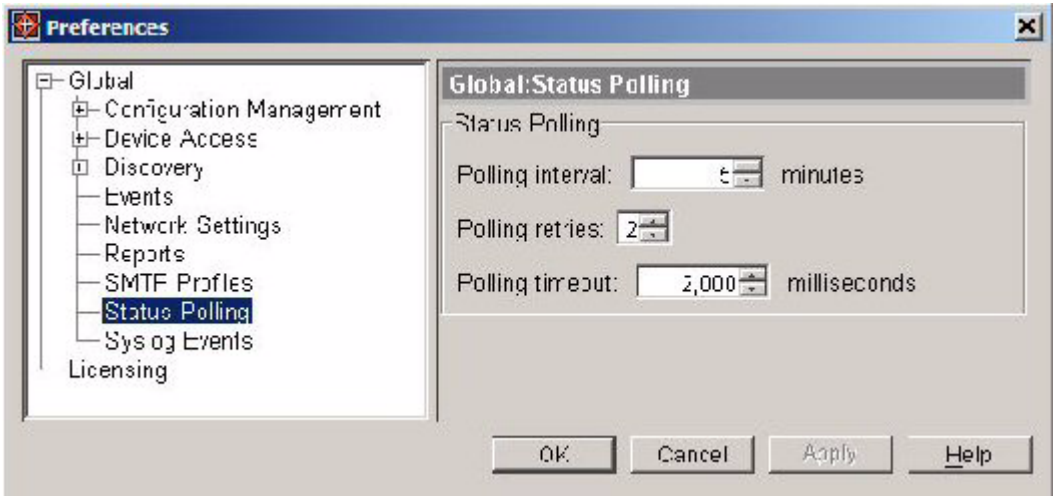


Figure 3-7. Global Preferences:Status Polling window

To change the Polling Status settings, type in the desired parameters, or use the button to increase or decrease the parameters. Click OK to complete the process.

Starting and Stopping Discovery

The Discovery process is set to run continuously. To stop the Discovery process, select the Status option under Discovery preferences to display the Global:Discovery:Status window. [Preferences->Discovery->Status]

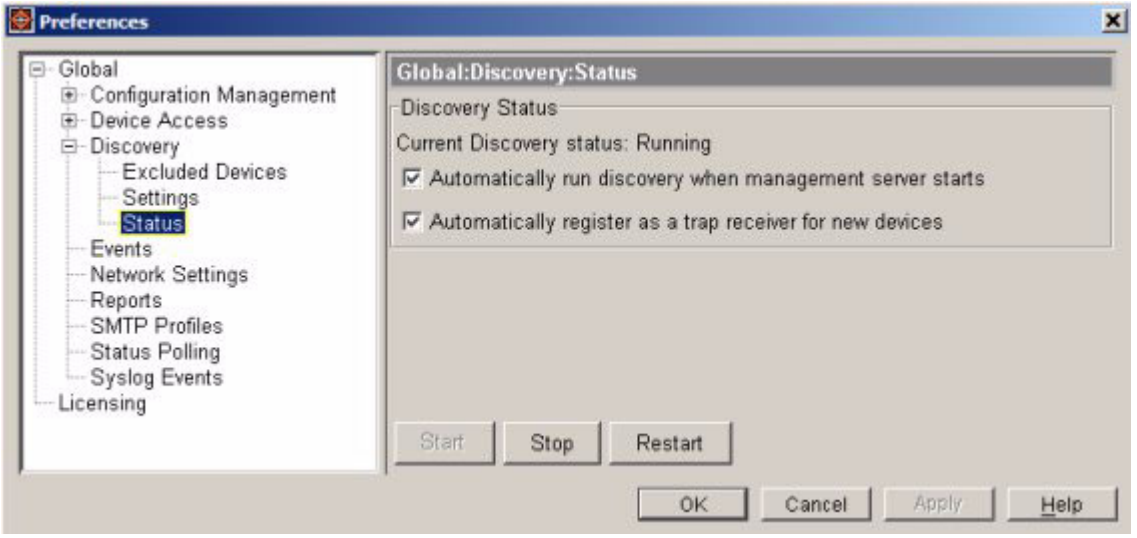


Figure 3-8. Discovery Status Panel

The default setting is to "Automatically run discovery when management server starts."

If the "Automatically register as a trap receiver" option is selected, when discovery is run, the management station will be set as a trap receiver for the selected device.

To stop the Discovery process, click Stop, then click OK. The discovery will remained "stopped" until you start it again in the Discovery:Status window. When all discovery processes are stopped, Current Discovery status will be Stopped.

To start the Discovery process, open the Global:Discovery:Status panel [Preferences->Discovery->Status], then click Start.

Restarting Discovery

When you click OK or Apply after changing any of the Discovery preferences, you will be prompted to restart discovery.

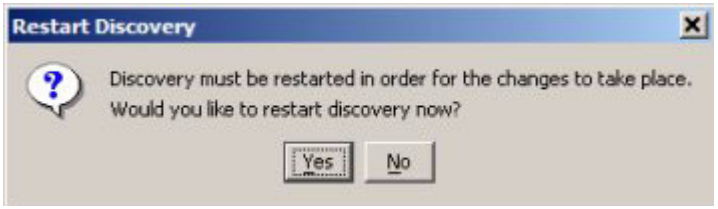


Figure 3-9. Restart Discovery pop-up dialogue

You can choose not to immediately restart discovery by clicking No. If you do, you must use the Restart button on the Preferences:Discovery Status window to restart Discovery at a later time and enable the changes you have made.

Troubleshooting Discovery

Because Discovery uses SNMP, if a device is not SNMP enabled, or if the SNMP community names are changed, Discovery may be unable to properly classify and map the device.

If Discovery is not finding or classifying a known device on the network, it may be due to temporary problems on the network or on the device. Try using Manual Discovery, or the Re-Discover function. If the Device is found, but is not classified in the correct product group, try using Device Reclassification.

The following CDP problems can result in Discovery and mapping errors:

- The switch does not appear in the CDP Neighbors table of an adjacent CDP device, which may be due to any of the following:
  - Either the port connecting the switch to the adjacent device is not a member of an untagged VLAN, or any untagged VLAN to which the port belongs does not have an IP address.
  - If there is more than one physical path between the switch and the other CDP device and STP (Spanning Tree Protocol) is running on the switch, then STP will block the redundant link(s). In this case, the switch port on the remaining open link may not be a member of an untagged VLAN, or any untagged VLANs to which the port belongs may not have an IP address.
  - The adjacent device's CDP Neighbors table may be full. View the device's Neighbors table to determine whether it is full.
- One or more CDP neighbors appear intermittently or not at all in the switch's CDP Neighbors table. This may be caused by more than 60 neighboring devices sending CDP packets to the switch. Exceeding the 60-neighbor limit can occur, for example, where multiple neighbors are connected to the switch through non-CDP devices such as hubs.
- The same CDP switch or router appears on more than one port in the CDP Neighbors table. Where CDP is running, a switch or router that is the STP root transmits outbound CDP packets over all links, including redundant links that STP may be blocking in non-root devices. In this case, the non-root device shows an entry in its CDP Neighbors table for every port on which it receives a CDP packet from the root device.

This page is intentionally unused.

Using Network Maps

Chapter Contents

How Network Maps Work

When HP ProCurve Manager is started, the Discovery process finds the devices on your network. The Mapping tool uses the information provided by Discovery to create network topology maps. The Mapping tool will automatically create a map of the entire network, and a separate map for any Subnets or VLANs you have configured.

During the CDP/FDP cycle, Discovery will generate or update network topology maps to reflect the physical layout of devices in the network, based on the connections found in the CDP/FDP Neighbor tables on devices in the network. Discovery also maps wireless devices such as the 420wl and 520wl Access Points, and the 700 series Access Control devices.

All forms of network topology mapping rely on CDP/FDP with the exception of HP ProCurve wireless devices, which rely on the Bridge MIB. Thus, discovery can only "map" CDP/FDP enabled devices and HP ProCurve wireless devices. All other devices will be shown as unmapped devices in the Network Map display.

Subnet maps and VLAN maps are subsets of the Network Map, and are created when the VLAN discovery cycle is completed.

To create the subnet map, Discovery extracts all the links (a connection between two devices) for all devices in the Network Map. For each link it determines if the connected devices belong to the subnet being mapped. If the devices for the link belong to the subnet being mapped, they are added to the Subnet map.

To create the VLAN map, for each link extracted from the Network Map, Discovery will determine if the connected ports for the link belong to the VLAN being mapped. If the ports for the link belong to the same VLAN ID, then Discovery add the link to the VLAN map.

Displaying Network Maps

Click on the Network node in the navigation tree to display the Network Map.

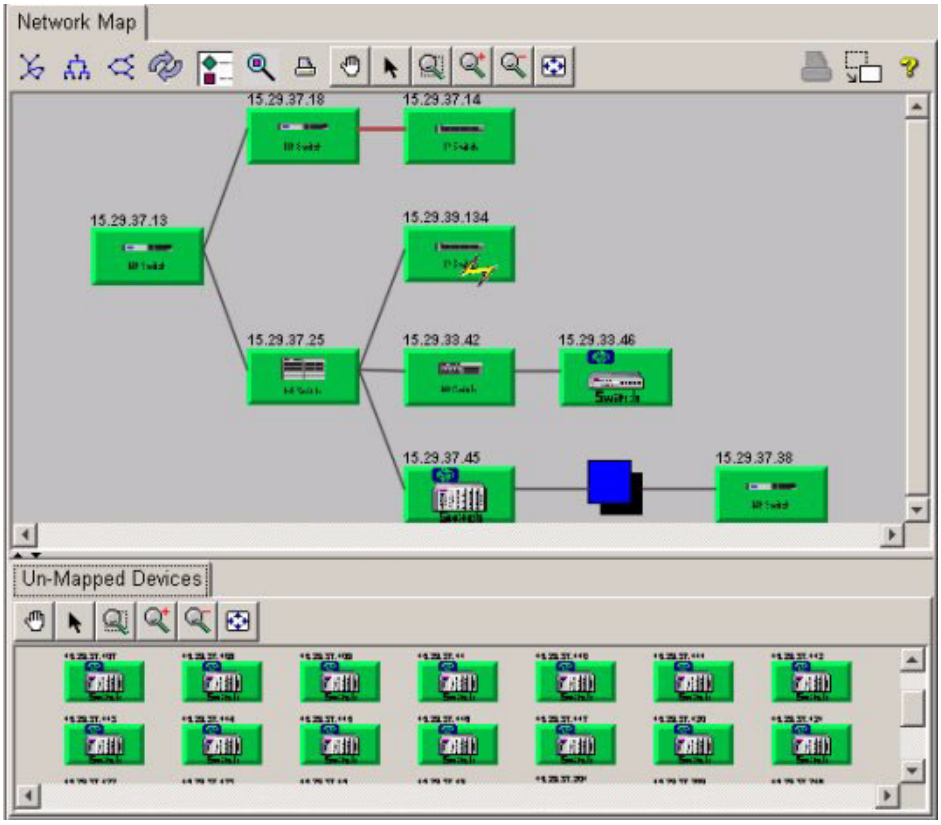


Figure 4-1. Network Map display.

To view the Network Map in a separate window, click the "Show in New Window" icon in the toolbar.

The Network Maps window provides a graphical view of the physical layout of a managed network. It displays the connectivity and status of all devices discovered in the network. Devices labels that appear in the map are based on the "Device Display Name" selected in the Preferences for Device Access. The example above shows devices using the IP address.

Devices that have been discovered, but that cannot be mapped (because they are not CDP/FDP enabled) are displayed in the Un-Mapped Devices section. You use the arrows in the border, or "drag" the border to resize or close the Unmapped Devices pane.

NOTE: Although you can resize the Mapped and Unmapped sections of the network map display, the resizing is not saved when you leave the window. When you return to the network map display it will revert to the default display size. Similarly, changes made to device location in the Unmapped display are not saved. If you go to another PCM window, when you return to the network map window the "unmapped devices" section will revert to the default display.

Map Layout Options

The default Network Map uses the "physical" map layout. That is, it reflects the physical wiring or layout of the network.

The Mapping tool provides four other options for map layout:

Radial Tree Layout- Arranges the nodes in a tree radially, with branches determined by device link. This is the PCM default map layout. The radial mode places the nodes of the same level on a circle around the root node. For large networks, the alternating radial mode is used, which places nodes of the same level at two alternating lengths around the root node to conserve space in the display.

Tree Layout - Arranges nodes at each level horizontally, connected vertically to other levels, starting from the root.

Hierarchical - Arranges the nodes hierarchically in horizontal or vertical levels, so that the majority of links point in the same direction.

Tools for Viewing Maps

In addition to map layout options, the Toolbar in the Maps windows includes buttons for map viewing functions. Each tool (button) is described below in the order in which it appears in the toolbar, reading from left to right.

Figure 4-2. Maps toolbar

Refresh Map: Refreshes the map display and includes any devices discovered manually since last CDP/FDP Discovery cycle.

Show Map Legend: Displays the conventions used to display device types and status in the maps. See below for details.

Find a node: Lets you locate the node (device) in the network map using the IP address. Click the icon to display the Find a Node dialogue. Enter the IP address of a device, then click OK. If the device exists on the map it will be selected. The Find function will also search through VLAN IP interfaces for a device.

Print Map: Provides standard print options for printing the displayed map.

Panner: Click and drag with the hand to center the network map in a different part of the window. This is useful for scrolling to view parts of the network that do not fit in the window.

Pointer Select: Click the 'pointer' button to select a device in the map, and to return the cursor to normal operation after using Panner or Zoom options.

Select Region to Zoom: Magnifies the selected region of the map.
Click this button and drag the crosshair to select the region of the map you want to magnify.

Zoom In: Magnifies the entire map.

Zoom Out: Reduces the magnification of the map.

Fit to View: Adjusts the map to display the entire network in the window.

Network Map Legend

Clicking the Map Legend icon will display the map legend.

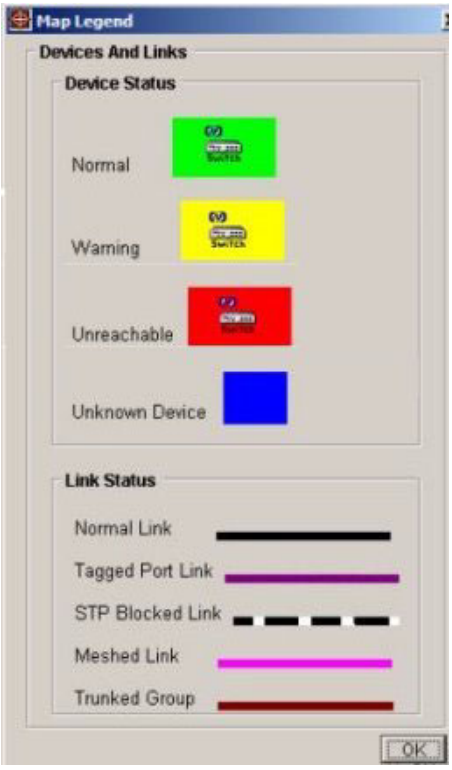


Figure 4-3. Network Map legend

The top half of the legend indicates the shapes used for device types and the device status indicator colors. Possible status indicators include:

- Green - Normal. The device is up.
- Yellow - Warning. The device is in warning state.
- Red - Unreachable. The device is down.
- Blue - unknown device type, no status available.

Possible link status types include:

- Normal link -A solid black line indicates the link between devices is up.
- Tagged Port Link - A solid purple line indicates a tagged port link. This appears only on VLAN maps. A tagged VLAN can combine several VLAN's on one link. (VLAN tagging enables traffic from more than one VLAN to use the same port.)

- STP Blocked Link - Identified on the map as a dashed line, an STP blocked link is any redundant physical path to serve as a backup (blocked) path in case the existing active path fails.
- Meshed Link - A solid magenta line on the map indicates a group of meshed switch ports exchanging meshing protocol packets.
- Trunked Group - A solid brown line indicates a trunked port connection. Refer to the configuration manuals that came with the switch for details on port trunking.

Viewing Network Device Information

The Network map provides 'mouse-over' functionality to provide access to network device information. Hovering with the cursor over a device in the map displays the device name and type. Hovering over a link in the map displays information about the link connections.

You can double-click devices in the Network Map to view the device properties and configuration, or you can select the device in the map and then use the right-click menu to view the device properties and access PCM functions.

NOTE: If you are running HP ProCurve 4100gl switches in router mode, the device will not appear in the network map.

If a device is excluded from the Discovery scans, it will still appear in the network map; however, you will not be able to select it in the map, or access the device properties.

Subnet and VLAN Maps

Maps are also available for managed Subnets and VLANs. All map types contain the same toolbar buttons and layout options as the main Network Map.

To view the map for a specific Subnet or VLAN, expand the Network Map node in the navigation tree, then expand the Subnets or VLANs node to display individual Subnet addresses and VLAN IDs. Click the Subnet address or VLAN ID to display the related map.

Definition:

Managed Subnet: A subnet within the Network Infrastructure that has been added to the ProCurve Manager's managed device list.

If you have installed PCM+, the VLANs map window also contains a Port Properties tab, which you can use to review the VLAN's port configurations. For more information on configuring and managing VLANs, refer to Chapter 9, "Using VLANs".

5

Alerts and Troubleshooting

Chapter Contents

Using the Events Browser

The Event Summary in the Dashboard helps you to quickly identify the number of problems in the network. For more detailed information, you can use the Events browser display to view and manage events generated by network devices and HP ProCurve Manager. You can perform the following functions from the Events window:

- View Event Detail Log
- Sort events
- Filter events
- Acknowledge events
- Delete events

To display the Events window:

- click the Events tab on the Network Manager Home window, or
- click the Events Summary panel in the Dashboard display, or
- click the Events icon on the PCM toolbar

Reviewing the Event Table

The Events table provides a listing of events currently contained in the database. The event detail is organized in five columns, described below.

Source: This column contains the name of the application component or device that generated the event. This column also contains either a green icon indicating the device is connected, a yellow icon indicating a warning, or a red icon indicating the device is unreachable.

Status: The Status column identifies whether the event has been acknowledged. A green asterisk indicates that the event has been acknowledged, and a red asterisk indicates that the event is new and has not been acknowledged.

If the Events browser configuration is set to auto-delete acknowledged events, the Status column will show only unacknowledged events. See “Customizing the Event Display” on page 5-7 for additional information.

Severity: The Severity column shows the severity of each event, one of:

- Informational - Routine events
- Warning - Unexpected service behavior
- Minor - Minor switch error that may impact performance

- Major - Switch error with potential of inhibiting switch operations
- Critical - Severe switch error with the potential of halting all switch operations

Date: The Date column identifies the date and time when the event occurred. The date is shown in the Day of Week-Month-Day-Time-Year format. Time is shown in the 24-hour clock format hh:mm:ss followed by the time zone.

Description: The Description column provides a short description of the event. The description is derived from a list of predefined event type descriptions included with the PCM application.

Sorting Events

You can click on any column heading to sort the table's contents by that column in descending order. Clicking the heading a second time will sort the data in ascending order. A pointer appears in to the column heading to indicate it is the sorting column. The down pointer indicates the sort is in descending order, and an up pointer indicates the sort is in ascending order.

Viewing Event Details

Clicking on an event in the table will display the Event Detail log for that event in the bottom section of the Events window. The Event Detail log provides the following additional information for an event:

Event Type: The Event Type identifies the event as a trap received from the switch or as an application event (such as Traffic Manager) issued by a component of the HP ProCurve Manager.

Trap Type: The Trap Type identifies the trap as a generic or enterprise specific trap.

Received on: Identifies the date and time when the event occurred. The date is shown in the Day of Week-Month-Day-Time-Year format. Time is shown in the 24-hour clock format hh:mm:ss followed by the time zone.

Acknowledged On: Indicates whether or not the event has been acknowledged, and the date and time of acknowledgement.

Received from: Lists the IP address and name (if available) of the device the event was received from, or the name of the PCM component that generated the event (e.g. Discovery, Traffic Monitor, etc.)

Action Taken: This line shows the action taken by the switch on "fault-finder" events. The action can be one of the following:

- Warning Issued - The switch has detected a problem and sent a warning to the HP ProCurve Manager.
- Warning Disabled - The switch disabled the port where the problem was detected and sent a warning to the HP ProCurve Manager.
- Warning Issued and Port Speed Reduced - The switch reduced the speed of the port where the problem was detected and sent a warning to the HP ProCurve Manager.
- Warning Issued, Port Speed Reduced, and Port Disabled - The switch reduced the speed of the port where the problem was detected, sent a warning to the HP ProCurve Manager, and then disabled the port.

Description: The Description column provides a short description of the event. this is the same description used in primary Events table display.

Acknowledging Events

Acknowledging an event indicates that you are aware of the event but it has not been resolved.

To acknowledge an event, select the event(s) to be acknowledged in the events table then click the Acknowledge button in the Events toolbar.

The "Acknowledge Event" action will set the selected event(s) as acknowledged, update the data store, and update the event status in the table to reflect the change. You can configure the Event Browser to automatically delete acknowledged events from the Events table, in which case the event will be removed from the list.

The "Hide Acknowledge Events" button in the Events toolbar works as a toggle to hide or show acknowledged events in the Events table.

Deleting Events

Deleting an event has the following effects:

- Removes the event from the Events window
- Removes the event from the count on the Event Summary subpanel in the Network Management Home window
- Moves the event to the Event Log.

The Event Log is located in the ~\PNM\server\logs\cs-ArchiveTraps.log

To delete an event select the events that you want to delete, the click the Delete Event icon in the Events toolbar.

Filtering Events

The listing in the Events table can be filtered to show only specific types of events. You can create up to four user-defined filters based on the device that generated the event, severity, date of occurrence, or description.

A toggle button is enabled on the Events window toolbar for each user-defined filter, with the name assigned to the filter. Simply click the associated toggle button to activate or deactivate a filter.

Click the Configure filters button in the Events toolbar to launch the Configure Filters window.

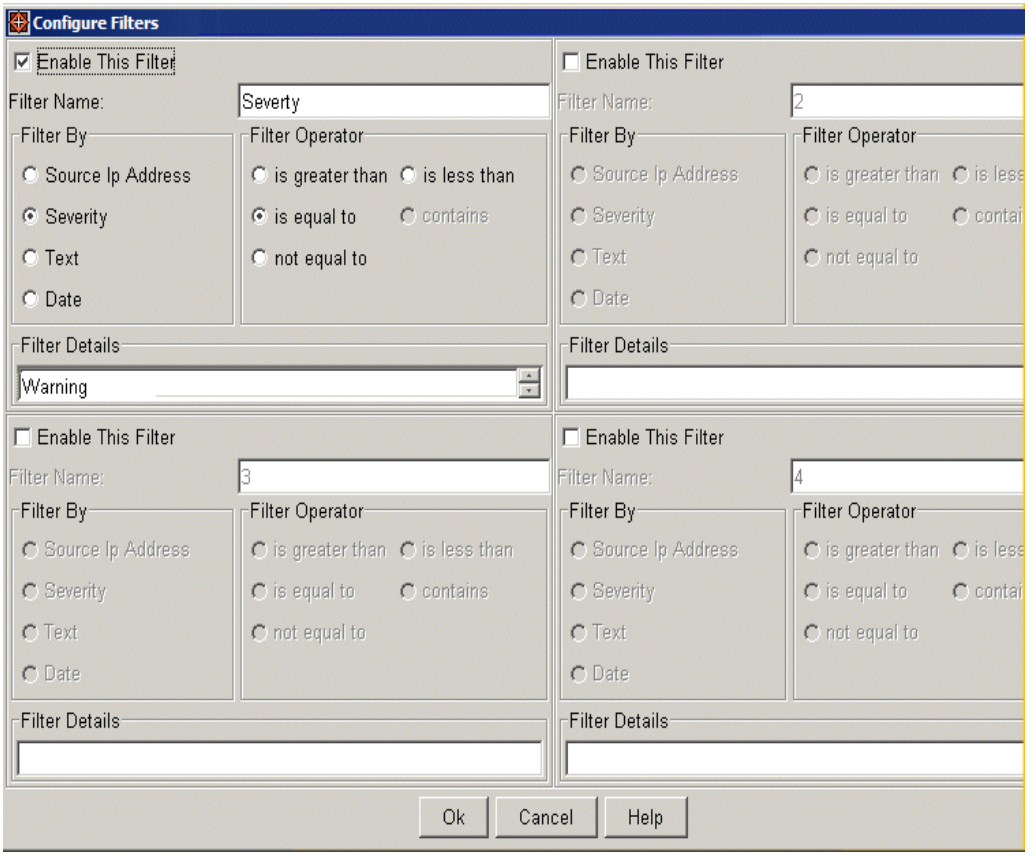


Figure 5-1. Event Filter Configuration window.

To configure the events filter(s):

1. Enable (check) the filter.
2. Type in a Filter Name, up to a maximum of 10 characters, including numbers and special characters.
3. Select a Filter By parameter. Each filter works with a single parameter:

   Source IP Address: Type the subnet IP address that you want to filter. Use this parameter to filter out events from a specific device or group of devices, or to filter out all events except for a single device.

   You can also use this option to filter for application event. In this case, enter a string for the application source into the Filter Details field. For example, "Software Update" or "Traffic Monitor."

   Severity: Select the severity level that you want to filter. Use this parameter to filter out lower or higher severity events, or to view events for only one severity level.

   Text: Type the text contained in events that you want to filter. Use this parameter to filter out events by specific text included in the event description.

   Date: Use this parameter to filter the events view for a specific date and time. When selected, the default (current) timestamp will appear in the Filter Details field. You can delete the default to enter a different date and time. Or you can click the portion of the date and time to be changed, then use the up or down arrows to increment or decrement the timestamp entry.
4. Select the Filter Operator. These are boolean operators that will be applied to the Filter By parameters. Operators that do not work with the selected filter parameter will be disabled.
5. Click OK
   The filters you defined will be validated. If there are errors, a message is displayed prompting you to check the filter configuration.

   If there are no errors, the Configure Filters window is closed, and you will be returned to the Events tab window. For each filter defined, the corresponding toggle button will be enabled with the name of the filter. You can then use the toggle button to enable or disable the filter as needed.

Customizing the Event Display

In addition to the event filters, you can use the Event Browser Configuration option in the Preferences menu to customize the Events tab display and event archiving attributes.

Open the Preferences window and select the Events option to display the Event Browser Configuration window.

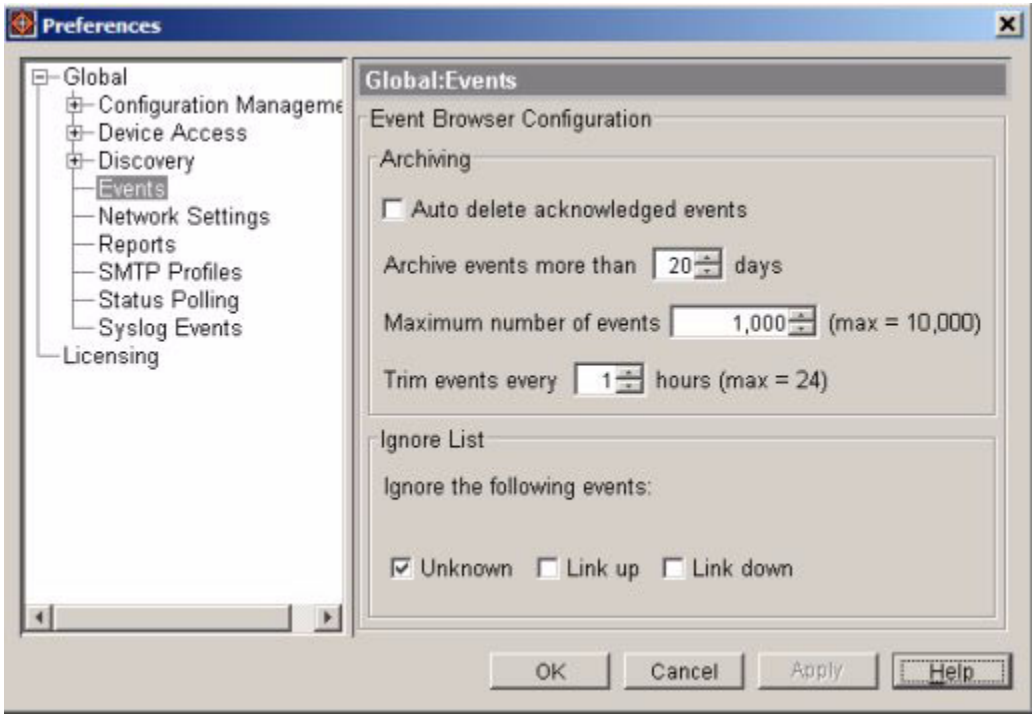


Figure 5-2. Event Browser Configuration preferences window.

Setting Archiving Attributes

1. To automatically remove acknowledged events from the Events table, click the Auto delete acknowledged events box.
2. Use the up or down arrow in the Archive events field to increase or decrease the number of days to display an event. Events older than the number days selected will be removed from the Events table and archived in the Event Log file.

3. Use the up or down arrow in the Maximum number of events field to increase or decrease the to the size of the events database. When the maximum number of events is exceeded, the oldest event is deleted to make room for the new event. The minimum number is 1000, and the maximum number is 10,000.
4. Set the trim interval (1-24 hours), which identifies how often the Event Log will be trimmed to the size specified in the preceding step.

Setting Ignore List Attributes

To exclude certain types of events from appearing on the Events list, click the box next to the event types:

- Unknown: The event type cannot be identified, and the event cannot be processed.
- Link Up: Communication with the device is possible.
- Link Down: The device cannot be accessed.

Click OK to save the Event Browser preferences and close the Event Browser Configuration window.

Using Alerts

You can use the PCM Client to create alerts based on incoming events. Alerts can be created in the form of an e-mail, forwarding of a trap, or tell the system to execute a predefined command.

Alerts Window

The Alerts window displays all configured alerts. Configure an alert if you want to be notified when certain types of events occur. You can configure several filters that issue alerts only when events occur that meet the filter criteria. You can select the action taken when an alert is issued. For example, you can be notified of alerts by email or popup dialog box, forward the alert as a trap to a specific device, or issue a CLI command.

The Alerts window contains the following information for each alert:

Enabled. A checkmark indicates that the alert is enabled. No checkmark means that the alert is disabled.

Alert Name. Name used to identify the alert (you will apply a name when you configure the alert).

Action. Action taken when an alert is triggered by the specified event. Possible actions are:

- Email - Displays the SMTP profile used to send Email alert messages
- Forward trap - Displays the IP address and port number to which the trap is forwarded when the alert condition occurs.
- Execute Command - Displays the command that is executed when the alert condition occurs.

To view alerts:

1. Go to the Events tab of the Network Management window.
2.  Click View alerts icon in the Events view toolbar.

   The Alerts dialogue will be displayed. (see figure 5-3)

   By default, the listing is sorted in alphabetic order by Name. You can sort on other attributes by clicking on the column heading.

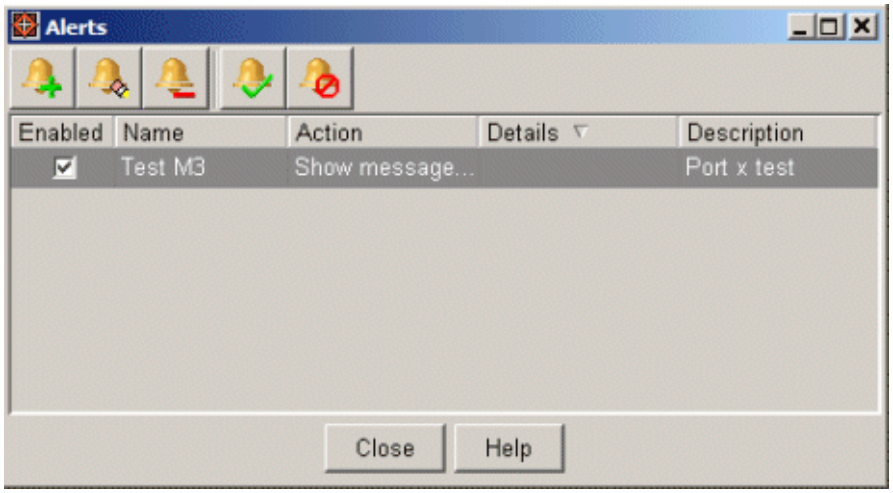


Figure 5-3. Alerts list window.

Creating Alerts

Before you can view an alert, you must create it using the Alert Configuration Wizard.

To create an Alert:

1. Click the Events tab in the Network Home window.
2. Click "View alerts" icon in the Events toolbar.

3. Click Click New alert on the Alerts dialog.

   The Alert Configuration Wizard will be launched.

Figure 5-4. Create Alert Wizard

4. In the Alert Name field, type the name you want to assign to the alert. Alert names are 1-15 characters in length, and must not contain the special characters / \ : * ? < > " and |.
5. Click Next.

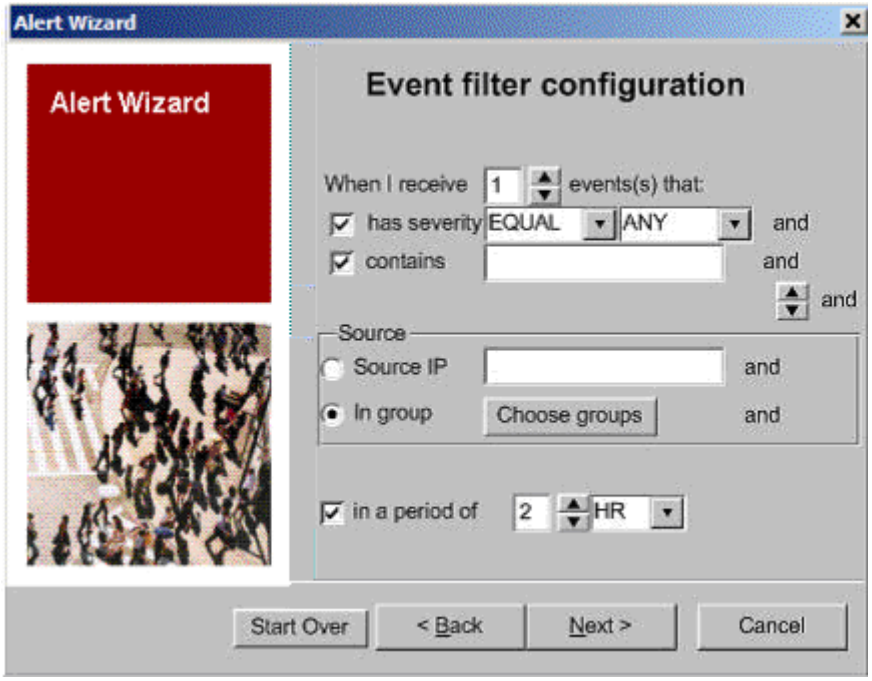


Figure 5-5. Alert Event Filter configuration

6. Configure the event filter, which defines one or more conditions required to issue an alert, similar to the events filtering described on page 5-5. At least one condition must be defined. You can also combine two or more filter types, for example severity, source IP, and group. Just enter the data for each filter to be applied for the alert condition.

   To configure the Event filter for an alert:

   a. Click the up and down arrows in the When I receive events field to set the minimum number of events (meeting all other filter criteria) that must occur before issuing an alert. You must set this to a number greater than 1 for the remaining filter settings to be applied.

      The number of events works in conjunction with the time period condition in the lower section of the dialog. For example, you can issue an alert when more than five events are issued within ten minutes. The default setting is one event within one millisecond, which will issue an alert for every event that occurs.

   b. Click the has severity checkbox to filter events by severity, then use the pull down menus to select the operator (equal, not equal, greater than, or less than), and the severity level (Any, Informational,

Warning, Minor, Major, and Critical). For example, to issue an alert when a Major or Critical event occurs, select "Greater Than" and "Minor."

c. Click the "Contains" checkbox to filter events by their content (text), and type the text (1-35 characters) that you want to use as a filter. For example, you can issue an alert when an event contains the phrase "Error occurred when" or "port number 12."

d. Click the Source IP checkbox to filter events by the IP address or DNS name of the device originating the event, and then type the IPv4 or IPv6 IP address (xxx.xxx.xxx.xxx) or DNS name of the device that generated the event.

e. To filter events by the device group originating the event, click the Choose groups button, and then select the source groups you want to use as a filter.

f. To set the window of time used to count the minimum number of events that must occur before an alert is issued, use the up and down arrows in the In a period of field to select the desired time period. This field is only activated when the number of events is set to more than 1.

7. Click Next to continue.

Figure 5-6. Alert Action Selection

8. Select the action to be taken when an alert is issued.

Send e-mail - Notify a user by email of the alert. For this option to work, you will be required to configure the SMTP profile, as described on page 5-20.

Forward trap - Forward a trap to the specified device.

Execute command - Execute a command when an alert is issued..

Display message dialog - Display a dialog containing the specified text when an alert is issued.

9. Click Next to continue.

   The next dialog displayed by the Wizard will vary, depending on the Action you selected.

   - Go to Step 10 (below) if you selected "Send e-mail"
   - Go to Step 11 (page 5-16) if you selected "Forward trap"
   - Go to Step 12 (page 5-17) if you selected "Execute Command"
   - Go to Step 13 (page 5-18) if you selected "Display a message dialog"

10. In the Choose SMTP profile dialog:
    a. Select the SMTP profile to use for issuing an e-mail alert.

Figure 5-7. SMTP Profile for E-mail Alert

See “Adding SMTP Profiles” on page 5-20, for details on configuring the SMTP profiles used for Alerts.

b. Click Next.

The Message settings dialog is displayed.

Figure 5-8. E-mail Alert Configuration

c. The To and From fields are initially set to the address configured for the SMTP profile you selected. The "From" email address should identify where the alert originated; however, you can override either of these addresses by entering a different, valid, e-mail address.

d. In the Subject field, type the e-mail subject line (0-35 characters) you want to use for the alert.

e. In the Body field, type any text you want to include in the body of the email (0-512 characters).

The "Substitution List" describes the variables you can use in the Subject and Body fields. The variables will be replaced (before the email is sent) by data from fields in the event evoking the alert.

NOTE: A subject and body text are recommended, but not required.

f. Click Finish to complete the alert configuration.

11. In the "Trap forward configuration" dialog, configure the trap forwarding information to be used for the alert.

Figure 5-9. Trap Receiver Alert configuration

a. In the Trap Receiver field, type the IP address of the device that you want to receive the trap. The IP address must be in the xxx.xxx.xxx.xxx format.

b. In the Port field, type the port number used to receive traps.

c. Use the Content field to enter any optional text you want to include in the trap.

   The Substitution List describes the variables you can use in the Content field. The variables will be replaced (before the trap is forwarded) by data from fields in the event that evokes the alert:

d. Click Finish to complete the alert configuration.

12. In the Command Configuration dialog, enter the command (string) that will be executed for the alert.

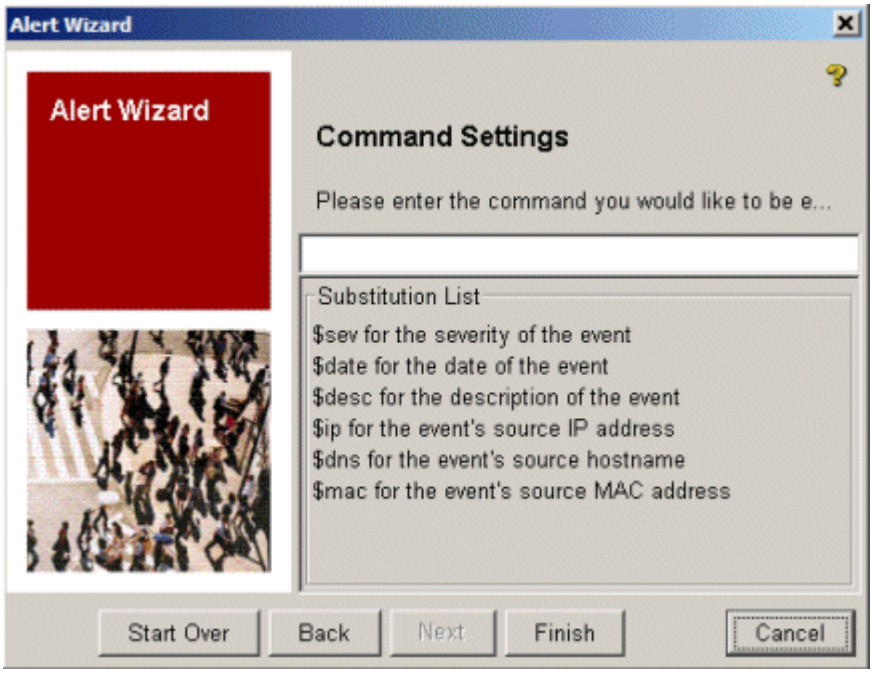


Figure 5-10. Command on Alert configuration

a. In the data entry field, type the name of the file or script (enter the full pathname, up to 75 characters in length) you want to execute when the alert is issued.

   The Substitution List describes the variables you can use in the Command field. The variables will be replaced (before the command is forwarded) by data from fields in the event that evokes the alert:

b. Click Finish to complete the alert configuration.

13. In the Display Message Settings dialog, configure the pop-up message that will be displayed for the alert.

Figure 5-11. Alert Message configuration

a. Type in the message (a string from 1-75 characters) you want to appear in a pop-up dialog when an alert is issued. The default is to include the variables described in the Substitution List. You can enter additional text, and/or delete any of the default message variables.

   The Substitution List describes the default variables included with the message, which will be replaced (before the message is displayed) by data from fields in the event evoking the alert:

b. Click Finish to complete the alert configuration.

Modifying Alerts

To modify an alert:

1. Go to the Events tab in the Network Management window.
2. Click the "Alerts" icon in the Events view toolbar.

3. Click "Modify alert" on the Alerts dialog to launch the Alert Configuration Wizard.

   The Modify Alert process has the same windows and uses the same procedures as used for creating an alert. (see page 5-10). The difference is that the data entry fields will display the current alert settings, which you can override with new entries.

Deleting or Disabling Alerts

To delete an alert:

1. Go to the Events tab in the Network Management window.

2. Click "Alerts" icon in the Events view toolbar.
3. Select the Alert in the table. Use "Ctrl+shift" to select multiple alerts.

4. Click the "Delete alert" button.
5. Click Yes in the confirmation pop-up to delete the selected alerts.

To disable an alert:

1. Ensure that the Enabled checkbox for the alert is NOT checked.
2. If it contains a check, select the alert to be disabled and click the "Enable/Disable alert" icon to clear the checkmark.

To enable an alert:

1. ensure that the Enabled checkbox for the alert is checked.
2. If not, select the alert in the table and click the "Enable/Disable alert" button to enter the checkmark.

SMTP Profiles for E-mail Alerts

In order to use the Alerts e-mail notification option, you need to configure an SMTP profile to be used for e-mailing the alerts. The SMTP profiles are accessed from the Preferences menu. {Preferences ->SMTP Profiles}

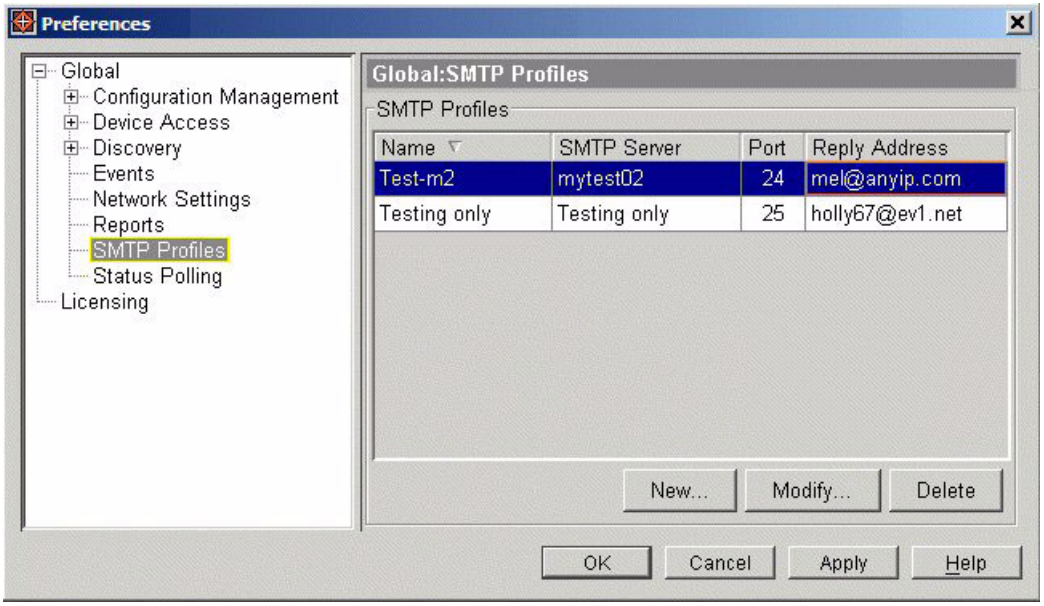


Figure 5-12. SMTP Profiles list

The SMTP Profiles window displays SMTP profiles that identify SMTP mail servers used for sending e-mail alert notifications.

Adding SMTP Profiles

To create a new SMTP profile:

1. Click New... in the SMTP Profiles window to launch the SMTP Profiles Wizard.

Figure 5-13. SMTP Profile configuration

2. In the Profile name field, enter a unique name for the SMTP profile: up to 35 characters, but not the special characters \ /) (* ? | : < > or #.
3. Click Next.

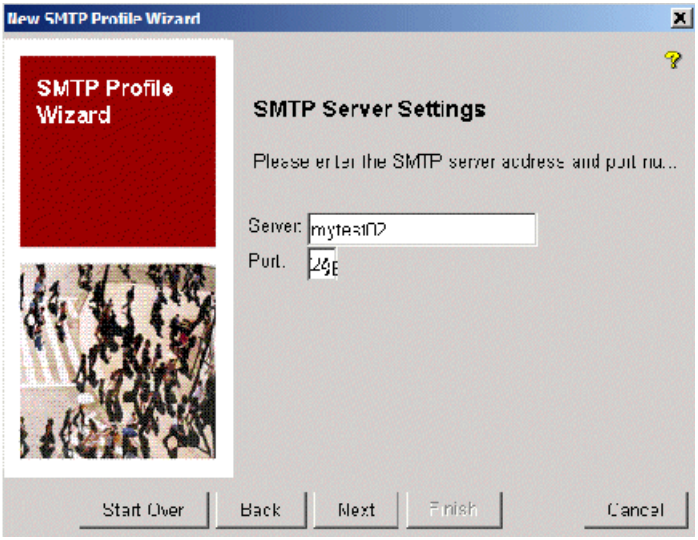


Figure 5-14. SMTP Profile configuration

4. To configure SMTP server settings:
   a. In the Server field, type the name of the SMTP server, from 1 to 35 characters. Note that this field will not be validated.
   b. In the Port field, type the port on the server that will be used for SMTP. It can be any number between 1 and 65353.
   c. Click Next.

      The system will verify that there is an entry in the Server (name) field, and that the Port is valid. If either of these conditions is not met, you will get an error message.

      If the SMTP server entries are verified, the SMTP Account Settings dialog is displayed.

Figure 5-15. SMTP Account: Reply Address setting

5. In the Reply address field, type the email address (up to 35 characters with no spaces).
6. Click Next.

   The system will validate the information. If an entry is invalid you will get an error message.

   If the entry is confirmed, the Summary dialog is displayed.

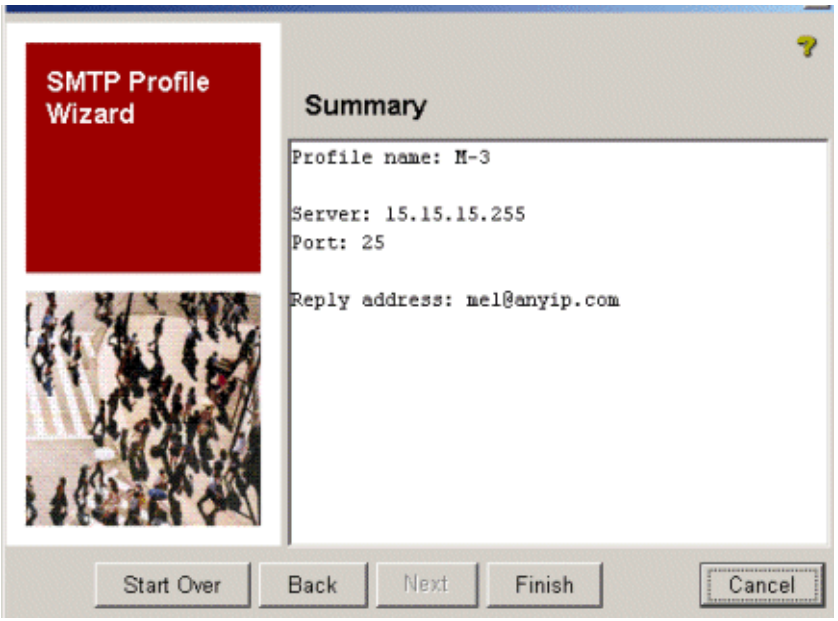


Figure 5-16. SMTP Profile Summary example

7. Click Finish to complete the SMTP Profile and close the wizard.

Modifying SMTP Profiles

To modify an SMTP profile:

1. Go to Preferences -> SMTP Profiles to view the SMTP profiles list.
2. Select the profile you want to change.
3. Click Modify to launch the SMTP Profile wizard.

   The SMTP Profile wizard has the same windows and uses the same procedures as the "Adding SMTP Profiles" (see page 5-20). The difference is that the data entry fields will display the current SMTP settings, which you can override with new entries.

Deleting SMTP Profiles

To delete an SMTP profile:

1. Go to Preferences -> SMTP Profiles to view the SMTP profiles list.

2. Select the profile you want to remove. You can use Ctrl+shift to select multiple entries from the list.
3. Click Delete.
4. Click Yes in the confirmation pop-up to remove the SMTP Profile from the list.

6

Managing Network Devices

Chapter Contents

Using the Device Manager

The Device Manager feature in PCM provides the basic functions to manage HP ProCurve network devices via SNMP, including:

- Configuring SNMP trap receivers on a device.
- Configuring SNMP community name strings on a device.
- Setting Authorized managers for a device.
- Ability to Telnet to a device to use the CLI.
- Ability to connect to a Device's Web Agent.

To access the Device Manager, select the device to be managed in the Devices List or the Navigation Tree then click the Device Manager button in the toolbar. Or, you can right click on the device and select Device Manager from the menu.

Figure 6-1. Device Manager window, default display.

The Device Manager window uses a tabbed display for the SNMP management functions supported. The default display shows the System Information tab, with the system name, contact, and location if available. The availability of the remaining tabs (Trap Receivers, Community Names, Authorized Manager) will vary based on the network device type and configuration.

Configuring Trap Receivers

To view the list of trap receivers configured for the device, select the Trap Receivers tab.

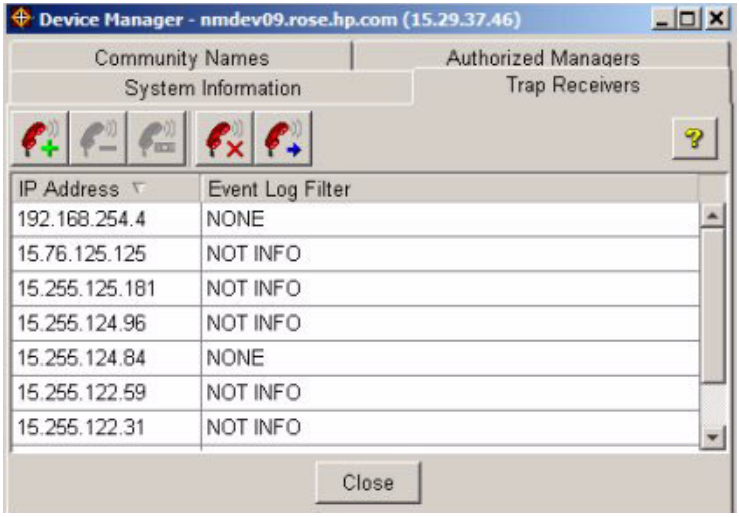


Figure 6-2. Device Manager: Trap Receivers tab.

The listing shows the IP Address of the trap receiver, and the filters in place for event types to be forwarded to the trap receiver.

You can refresh the display to check for changes in the Trap Receivers configuration by clicking the Retrieve button in the toolbar.

Adding Trap Receivers

The PCM management station is set as a default trap receiver for switches on the network. Use Device Manager to configure additional trap receivers.

1. Click the Add Trap Receiver icon in the toolbar to display the Add Trap Receiver dialogue.

2. Enter the IP Address of the device to receive traps.

   The IP address must be in the proper format. You cannot use 0.0.0.0, 255.255.255.255, the multicast address, loopback address, or subnet broadcast address of the device.

3. Use the Event Log Filter drop-down menu to select the type of events you want to include in the Event Log:

NONE	Do not use the Event Log
NOT INFO	Include all events except information events
CRITICAL	Include critical events only
ALL	Include all events
DEBUG	Include debug events only

4. Click Ok.

   A validity check will be performed on the IP address to ensure it is a valid IP address.

   - If it is a valid IP address the Add dialog is closed and the Trap Receivers list is updated with the new entry.
   - If the IP address is invalid you will get an "Invalid IP address" error, and the Add dialog remains open so you can edit the IP address.

NOTE:

When PCM (server) starts up, it binds to port number 162, which is the port that all incoming traps arrive on. If a previous process is already bound to that port, PCM will not be able to receive traps because the port is in use. Make sure no process is bound to port 162. Examples of applications that bind to port 162 are the Windows SNMP Trap Receiver Service, HP TopTools, HP OpenView, MG-Soft MIB Browser Trap Ringer, etc.

In the event that a process was bound to port 162, simply terminate the process and restart the PCM server. To restart the PCM server (in Windows):

- Go to Control Panel->Administrative Tools-> Services.
- Double click on the HP ProCurve Network Manager Server, click the Stop button, and then click the Start button.

Modifying Trap Receivers

To modify a Trap Receiver, select it from the list, then click the Modify Trap Receiver icon in the toolbar to display the Modify Trap Receiver dialogue.

The Modify Trap Receivers dialogue is displayed with the IP Address of the selected trap receiver. Edit the IP address as needed then click OK. The IP address will be validated (as described for adding a trap receiver).

Deleting Trap Receivers

To delete a Trap Receiver, select the entry from the list, then click the Delete Trap Receiver icon in the toolbar. A confirmation pop-up will be displayed.

Click Yes to complete the process.

You can delete all trap receivers at the same time by clicking on the "Delete All" icon in the toolbar.

Configuring SNMP Community Names

A community defines authentication and access control between an SNMP agent and a management station. A device must have a "Read" community name of that matches the one specified during installation in order to be properly identified by PCM. If not, it will be discovered, but may not be identified.

To view the list of SNMP community names configured for the device, select the Community Names tab.

Figure 6-3. Device Manger: Community Names tab.

The Community Names window lists all community names configured on the device and the following information about each community name:

Community Name: SNMP community name used to access the device.

Management: Check mark identifies the community name used by the HP ProCurve Manager to communicate with the device.

Read Access: Permissions that govern the community name's ability to read data on the device.

Write Access: Permissions that govern the community name's ability to write data on the device.

Click the Retrieve button in the Community Names toolbar to refresh the display and check for any changes to the device's Community Names settings.

Adding Community Names

To add a Community Name, click the Add Names button in the Community Names toolbar. This will display the Add Community Names dialogue. Up to five community names can be added to a device.

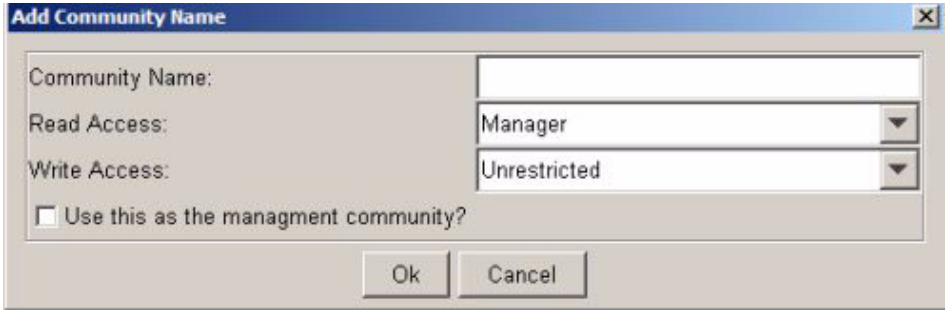


Figure 6-4. Device Manager: Add Community Name dialogue

Type in the SNMP community name to be added, up to 16 characters. The characters "<" and ">" cannot be used.

Select the Read Access permission from the menu: Manager provides full read permissions, Operator has restricted, read only permissions.

Select the Write Access permission from the menu, either Unrestricted or Restricted.

Click OK.

The entry will be validated that the community name value meets criteria (see above), and that the limit for community names on the device has not been exceeded. If the community name is invalid, you will get an error message. Otherwise, the Add dialogue is closed and the Community Names list is updated with the new entry.

Modifying Community Names

To modify a Community Name, select a community name in the list then click the Modify Names button in the Community Names toolbar. This will display the Modify Community Names dialogue, similar to the Add Community Names dialogue shown above.

If you select the Management Community Name, you will get an error message that you are not allowed to modify the Management Community Name.

Edit the community name entries as described in the Add process. When you click OK, a validity check on the community name will be performed. If it is valid, the Community Names list will be updated with the new entry.

Deleting Community Management Names

To delete a Community Name, select the name in the Community Names list then click the Delete Names button in the Community Names toolbar. A confirmation dialogue will be displayed.

Click OK to complete the delete process. If you have selected the Management Community Name, you will get an error notice telling you are not allowed to delete the Management Community Name.

To delete all the currently configured Community Names for the device, select the Delete All icon in the toolbar.

Modifying Management Community Access

The PCM Management Community Name is set at installation. If you do not specify one, PCM will use a default Management Community name of "public," with full read and write privileges to the device. This is used by PCM for auto-discovery, traffic monitoring, SNMP trap generation and threshold setting. If security for network management is a concern, it is recommended that you change the write access for the "public" community to "restricted."

In order to modify the Management Community, first you need to add a new community name, then select the (new) name in the Community Names list and click the "Set as Management Community" button in the Community Names toolbar.

The "Management" indicator (check mark) will now appear next to the new entry. Once you have changed the Management Community name, you can modify the original (public) Management Community name and change the Write access. When you have completed your changes, select the "public" Community Name, then click the "Set as Management Community" button to restore "public" as the management community.

Configuring Authorized Managers

For devices that support IP-based Authorized Managers, you can use the PCM Device manager to configure Authorized Managers. This allows you to enhance security on the switch by using IP addresses to authorize which stations can access the switch. An authorized manager is a management station that can send and receive SNMP requests for the device.

To review the authorized managers for a device, click the Authorized Managers tab in the Device Manager window.

Figure 6-5. Device Manager: Authorized Managers tab

The Authorized Managers list gives the IP address, IP Mask, and Access permissions for the device's authorized managers, with the date that the entry was last retrieved.

Click the Retrieve button in the toolbar to refresh the display and check for any changes to the device's Authorized Managers settings.

Adding Authorized Managers

To add an Authorized Manager, click the Add button in the Authorized Managers toolbar. This will display the Add Authorized Managers dialogue. Up to ten authorized managers can be added to the device.

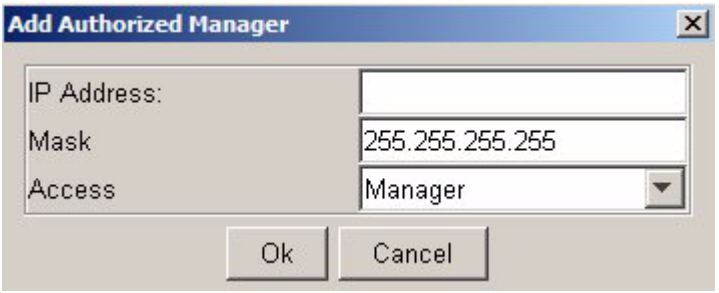


Figure 6-6. Add Authorized Manager dialog.

Enter the IP Address of the management station. The station must have the HP ProCurve Manager application installed.

Enter the IP Mask address.

- 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.)
- 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.

Select the Access level for the station.

- Manager: Enables full access (read and write) to device configuration functions.
- Operator: Enables read only functionality to device configurations.

Click Ok to complete the process. The IP address will be validated. You will get an error message if it is invalid. Otherwise, the Authorized Managers list will be updated with the new information.

Modifying Authorized Managers

To modify an Authorized Manager, click the Modify button on the Authorized Managers toolbar. This will open the Modify Authorized Manager dialogue, which has the same inputs as the Add Authorized Managers dialogue. Edit the existing entries, then click Ok.

Deleting Authorized Managers

To delete an Authorized Manager, select the entry in the Authorized Managers list, then click the Delete button in the Authorized Managers toolbar.

You can also use the Delete All button to delete all the authorized manager entries, without first having to select the entries.

Setting Device Access Preferences

In addition to the Device Manager functions, PCM lets you set Global SNMP and Telnet access information preferences. The Global SNMP preferences are used by PCM to access new devices found during Discovery scans, and Telnet Preferences are used to collect VLAN and device Configuration data on new devices.

To change the Global Device Access, click the Preferences icon in the PCM toolbar, then expand the Device Access node in the menu to display the SNMP and Telnet options.

Setting Device Display Names

The Device Access window is used to define the naming convention used to identify devices. You can select a standard naming convention or create a custom naming convention containing any combination of DNS name, IP address, and SNMP hostname.

To define the device display naming convention:

1. Select Device Access in the Preferences menu.

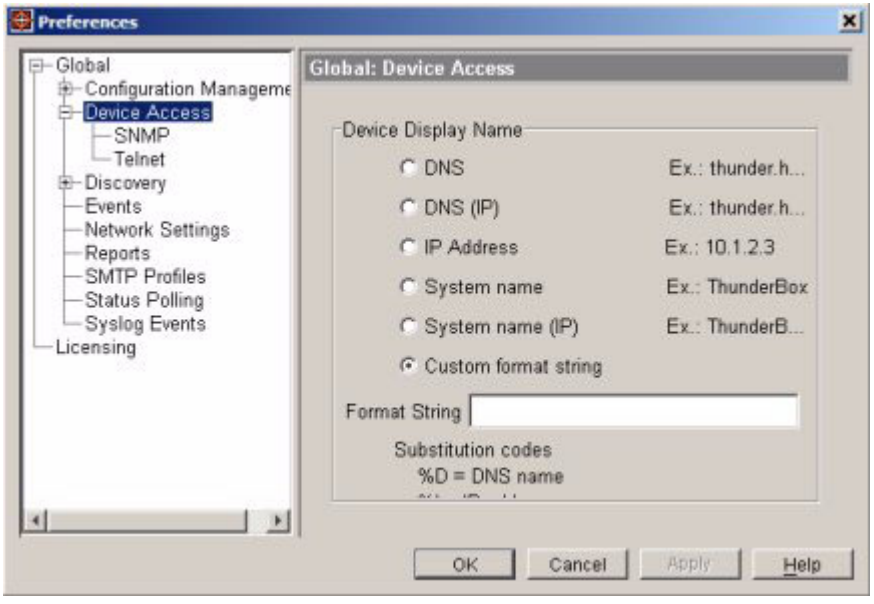


Figure 6-7. Preferences, Global:Device Access window

2. To use a standard naming convention, click the radio button next to the desired naming convention.
3. To create a custom naming convention, click the Custom format string radio button, and then type the text or codes you want to use for the device names in the Format String field,. Possible codes are:
   - %D - DNS name
   - %I - IP address
   - %S - SNMP hostname

   For example, type: `%S SNMP hostname`

   to display: Thunderbox SNMP hostname .
4. Click OK to save the Display Name settings and close the window.

Setting SNMP Preferences

Click the SNMP option to open the SNMP access preferences window.

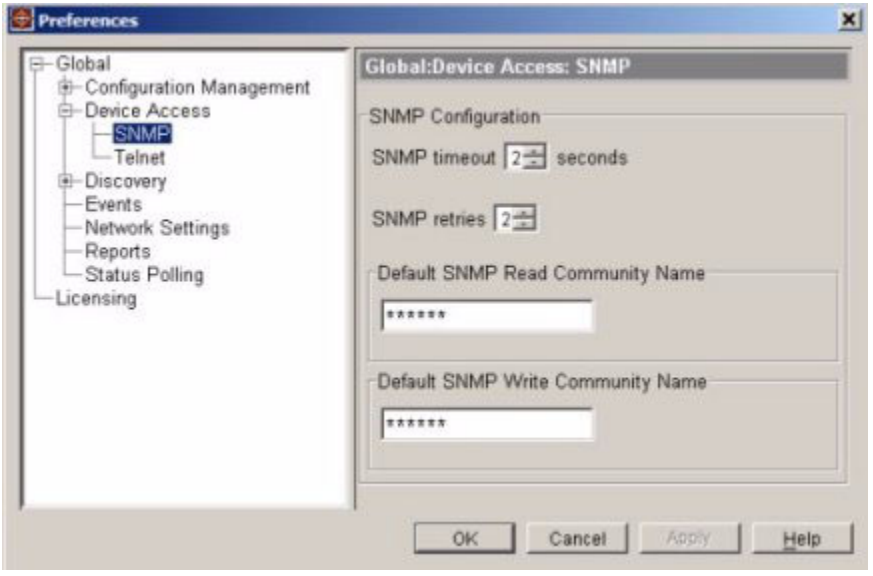


Figure 6-8. Preferences, Global:Device Access: SNMP window

Click the up or down arrows to set the SNMP timeout parameter. The maximum is 10 seconds.

Click the up or down arrows to set the SNMP retries parameter. The maximum is 5 retries.

The default SNMP Read and Write Community names are Public. However, they can be changed during installation.

To change the Default SNMP Read Community Name, type in the Community Name you want to use.

To change the Default SNMP Write Community Name, type in the Community Name you want to use.

Community names can consist of 1-16 characters including special characters except >, <, and spaces.

Click OK when you have completed your edits. This will apply your changes and close the SNMP preferences window.

NOTE:

The Global Preferences for SNMP Device Access are used to discover new devices on the managed subnet(s). If a device does not appear in the navigation tree or Devices List, try using the Manual Discovery wizard to discover the device. If Manual Discovery connects to the device, but cannot use SNMP to communicate, then you can either:

- Specify the current SNMP Read Community name for the device in Manual Discovery, or
- Use the device console to change the SNMP Read Community name on the device to match the SNMP Read Community name in PCM's Global SNMP (Device Access) preferences.

Setting Telnet Preferences

Click the Telnet option under Device Access in the Preferences menu to set the default Telnet access preferences.

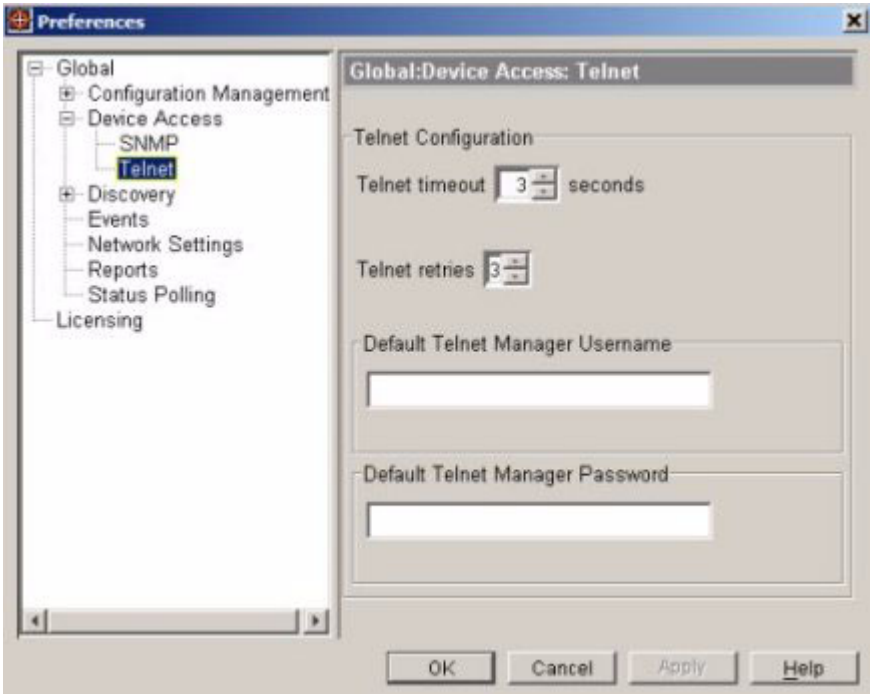


Figure 6-9. Preferences, Global:Device Access: Telnet window

Click the arrows to increase or decrease the Telnet timeout parameter. The maximum is 10 seconds.

Click the up or down arrows to increase or decrease the Telnet retries parameter. The maximum is 5 retries.

The default Telnet username and password is public.

To change the Default Telnet Manager Username, type in the username you want to use.

To change the Default Telnet Manager Password, type in the password you want to use.

Click OK when you have completed your edits. This will apply the changes and close the Telnet preferences window.

Setting the Telnet Password on a Device

When a new device is added to the network, Discovery uses the Global Device Access preferences for SNMP and Telnet to discover the device, and to collect VLAN and configuration information. If a new device has been discovered, but you are not getting configuration information, or VLAN information (if applicable) for the device, you may need to set the Telnet username and password for the device in PCM.

To set a Telnet Username and Password for individual devices, select the device (or devices) in the Devices List, then click the Set Telnet Password icon in the toolbar.

Figure 6-10. Set Telnet Password dialogue

The selected devices will be listed on the left side of the Set Telnet Password and Username dialogue.

Type in the Telnet Username and Password for the device, then click OK to apply the change, and close the dialogue.

The Telnet Username and Password will be saved to the device record in the PCM database. PCM should now collect and display configuration and VLAN information for the device.

Configuring Alarms using RMON

The RMON Manager (Remote Monitoring) feature in PCM provides an interface you can use to configure alarm thresholds for individual devices on the network. The RMON thresholds are used to monitor a variety of system variables. When an RMON threshold is exceeded on the device an alert (trap) is sent to all trap receivers configured for the device.

To review or configure the RMON alarm thresholds set for a device, select the device in the Devices List then click the "Launch RMON Manager" icon in the toolbar. The RMON Manager window will be displayed with a list of currently configured thresholds for the selected device.

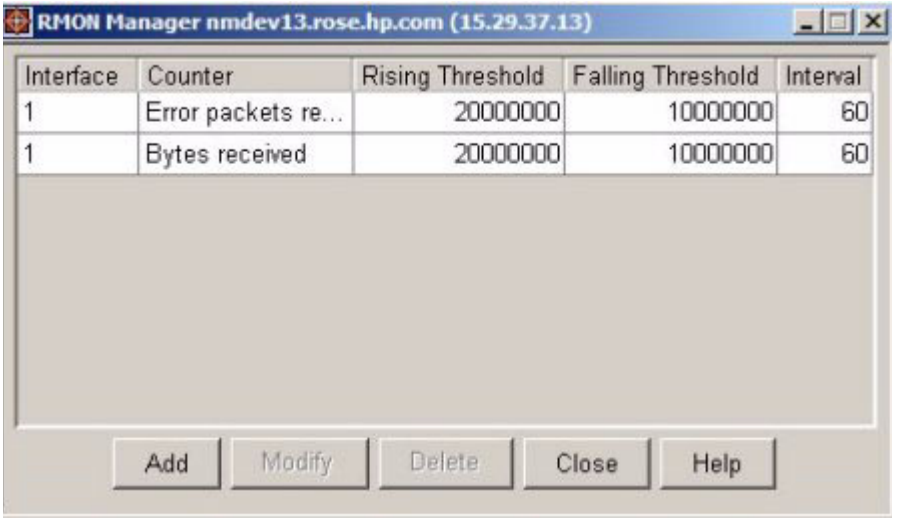


Figure 6-11. RMON Manager main window.

Adding and Modifying RMON Alerts

To set a new RMON alert, click Add to display the Add/Modify RMON Thresholds dialogue. To modify an existing alert, select it on the list of thresholds, then click Modify.

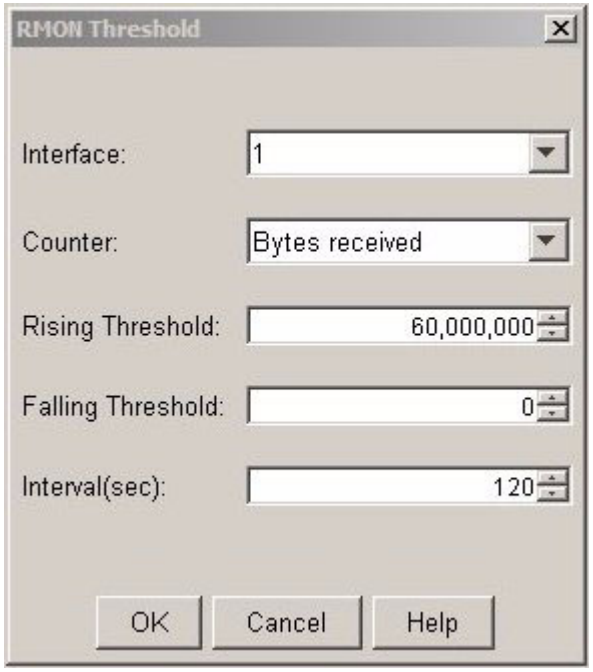


Figure 6-12. Add/Modify RMON Thresholds dialogue

RMON alarms are composed of five elements: interface, counter, rising threshold, falling threshold, and interval, defined as follows:

Interface: Specifies the port on the target device on which to set the RMON alarm. Select from the available ports using the drop down menu.

Counter: This defines the specific device variable to monitor. A trap is sent to all listed trap receivers if the alarm variable crosses the rising or falling threshold values. Select the Counter (alarm variable) from the drop down menu.

Rising Threshold: This numeric value defines the upper limit for the monitored variable. Should the variable exceed this limit a trap will be sent. Use the up and down buttons to increase or decrease the threshold value, or type in the desired value.

Falling Threshold: This value defines the lower limit for the monitored variable. Should the variable drop below this value a trap will be sent. Use the up and down buttons to increase or decrease the threshold value, or type in the desired value.

Interval: This value specifies the variable sample rate in seconds. Use the up and down buttons to increase or decrease the threshold value.

Click OK to complete the add or modify process and close the dialogue. The RMON Manager alarm threshold listing will be updated with the new settings.

The RMON Manager has a built in mechanism to prevent multiple events from being generated should the sampled value oscillate around one of the threshold values. Thus, in order for a rising threshold event to occur the sampled variable must first go below the falling threshold value. Conversely, before a falling threshold event can occur, the sampled variable must first exceed the rising threshold value.

For example, if the sampled variable exceeds the rising threshold value, a Rising Threshold Event will occur. If the sampled value drops back below the rising threshold and then rises above the rising threshold, an event will not occur. In order for another Rising Threshold Event to occur, a Falling Threshold Event must first occur. The process is reversed for falling thresholds - the rising threshold must be exceeded between generation of Falling Threshold Events.

Deleting RMON Alarms

To delete an RMON Alarm from the device, select the alarm in the list in the RMON Manager window, then click Delete. The alarm will be removed from the list in the RMON Manager window.

Other Device Management Tools

In addition to the functions provided by the PCM Device Manager, you can also access the Web Agent for the switch, or launch a telnet session to the Menu Interface for the switch from within the PCM display.

To access the Web Agent for a device, select the device in the Devices List or in the navigation tree, then open the "right click" menu and select the Connect to Web Agent option. This will launch the Web Agent browser, with the Status tab displayed.

To Telnet to a device, select the device in the Devices List or in the navigation tree, then open the "right click" menu and select the Telnet option. This will open a Telnet session to the device and launch the Main Menu Interface.

You can also select devices in the Devices List, then click the CLI icon in the toolbar to issue CLI commands.

For details on using the Web Agent, Menu Interface, and CLI, refer to the Configuration Management manuals that came with the switch device.

Troubleshooting Devices

This section describes the tools provided with this release of PCM that you can use to assist in finding and resolving problems that occur in individual devices on the network. For more detailed information on troubleshooting device problems, refer to the "Management and Configuration Guide" that came with your switch device.

Using the Device Log

The PCM application provides a Device Log viewer you can use to check the log entries created for a device by PCM. Select a device in the Devices List, then click the Device Log Viewer icon in the toolbar to display the Device Log Viewer window.

The Device Log Viewer shows a list of log entries for actions performed by PCM on the device. It will list the type of log entry, when it was created, and the log file name, along with additional details on data stored in the log file. You can drag the window pane separator to increase the detail section of the Device Log Viewer window. Double-click on an entry to see the device log details in a separate pop-up display. You can also copy and paste the device log entries to another application (such as notepad or MS Word) if desired.

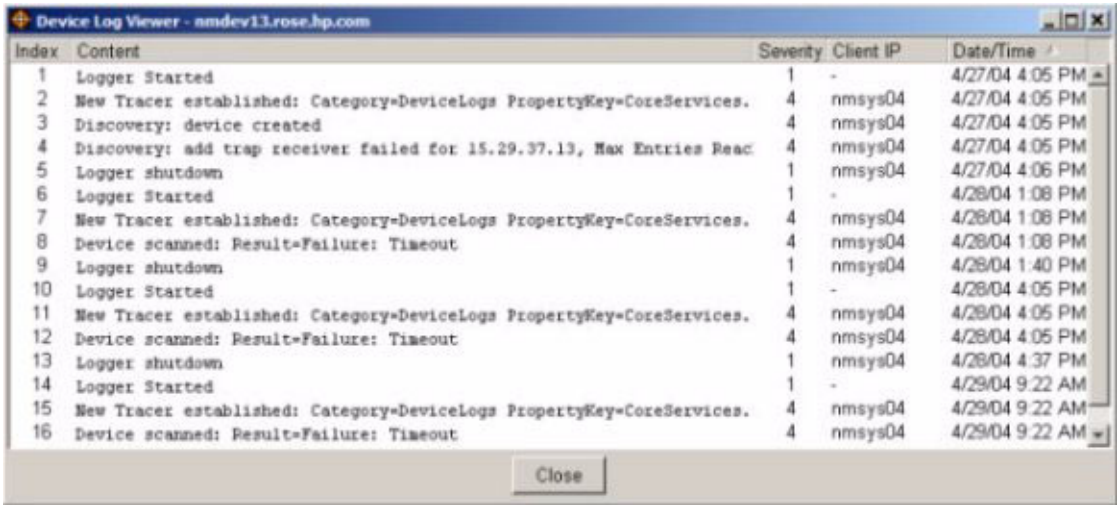


Figure 6-13. Device Log Viewer window

The Client IP is the address of the PCM console from which the action (command) was sent to the device.

Using Device Syslog

Syslog is a logging tool that allows a "client" switch to send event notification messages to a networked device operating with the Syslog Server software. HP ProCurve Devices that support Syslog Server software include:

- 28xx series, 26xx series, and 6108 on all software versions
- 25xx series with software version F.05.22 or newer
- 41xx series with software version G.07.21 or newer
- 51xx series with software version E.07.21 or newer

To enable the Device Syslog function in PCM, you need to set the PCM server as the Syslog server. You can use the CLI functionality in PCM to do this, entering the command:

set: logging <*syslog-ip-addr*>

where *syslog-ip-addr* is the IP address of the PCM server. For additional information refer to the section on "Syslog Operation" in the "Management and Configuration Guide" for your switch.

To review the Device Syslog in PCM, double-click on the device node in the tree or Devices List to display the Device Properties window, then click the Device Syslog tab.

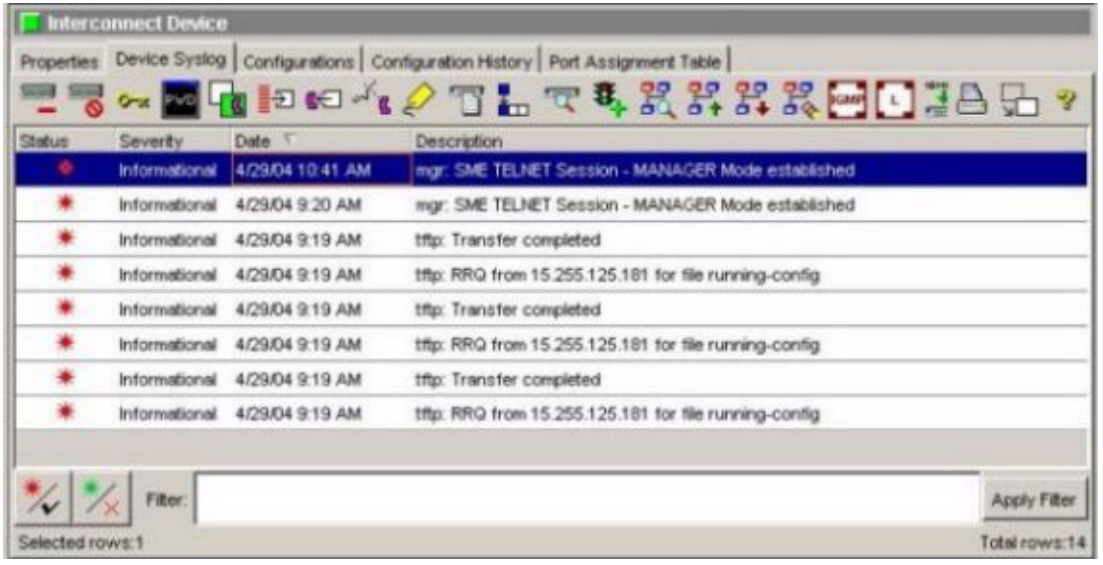


Figure 6-14. Device Syslog window.

The information in the Device syslog is similar to data found in the Events tab.

Status: The Status column identifies whether the event has been acknowledged. A green asterisk indicates that the event has been acknowledged, and a red asterisk indicates that the event is new and has not been acknowledged.

Severity: The Severity column shows the severity of each event, one of:

- Informational - Routine events
- Warning - Unexpected service behavior
- Minor - Minor switch error that may impact performance
- Major - Major switch error with potential of inhibiting some switch operations
- Critical - Severe switch error with the potential of halting all switch operations

Date: The Date column identifies the date and time when the event occurred. The date is shown in the Day of Week-Month-Day-Time-Year format. Time is shown in the 24-hour clock format hh:mm:ss followed by the time zone.

Description: The Description column provides a short description of the event. The description is derived from a list of predefined event type descriptions included with the PCM application.

Filtering Syslog Events

Use the Filter field at the bottom of Device Syslog window to enter text to search for within the event "Description". Just type in the word(s) you are searching for, then click Apply Filter. The listing will be resorted so that all events in which the filter text is found are at the top of the list.

Acknowledging Syslog Events

Acknowledging an event indicates that you are aware of the event but it has not been resolved.

To acknowledge an event, select the event(s) to be acknowledged in the list then click the Acknowledge button below the list.

The "Acknowledge Event" action will set the selected event(s) as acknowledged, update the Syslog file, and update the event status in the list to reflect the change.

Deleting Syslog Events

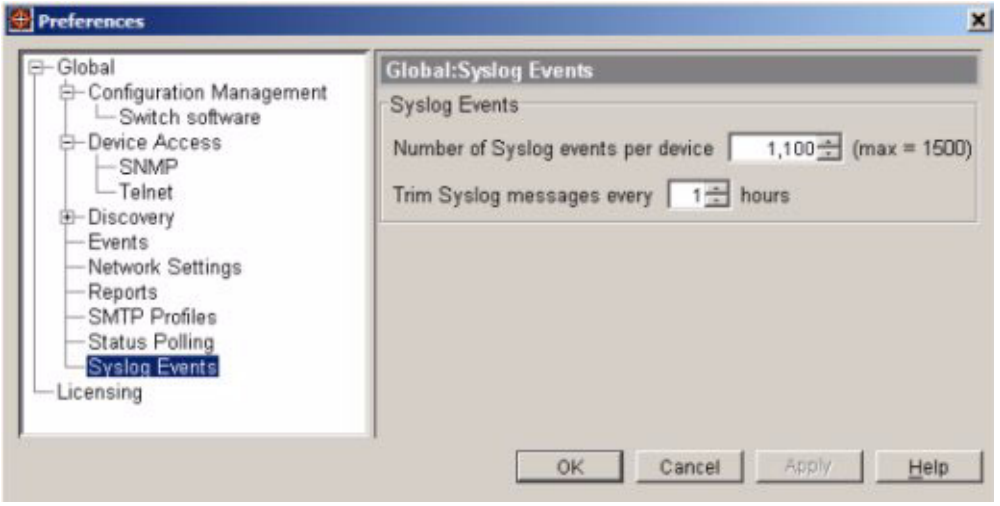
To delete an event select the events that you want to delete, the click the Delete Event icon below the events list..

Deleting a Syslog event will remove the event from the Syslog file and the Device Syslog display.

Managing Syslog Size

The PCM Syslog server can hold a maximum of 1500 events. You can use the Syslog Events option in the Global Preferences to reduce the number of events the Syslog will hold, and the rate at which the Syslog file will be automatically trimmed (cleared) of excess files.

1. Select the Syslog Events option in the Preferences menu to open the Global:Syslog Events window.



2. Type in the number of events you want the Syslog to hold, or use the buttons to increase or decrease the number of events.
3. Type in the interval (number of hours) that you want to wait before trimming the Syslog file to the maximum number of entries, or use the buttons to increase or decrease the trim interval.

   If a device is generating many events in the Syslog, the log will hold the events over maximum, but operations with Syslog will be impacted, and eventually the device operation may be impacted.
4. Click **OK** to apply the preferences and close the window.

This page is intentionally unused.

Monitoring Network Traffic

Chapter Contents

Using Traffic Monitor

The Traffic Monitor presents real-time information about the status of your network. When you select the Traffic Monitor tab on the home page, or click the Traffic Monitor button in the toolbar, 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.

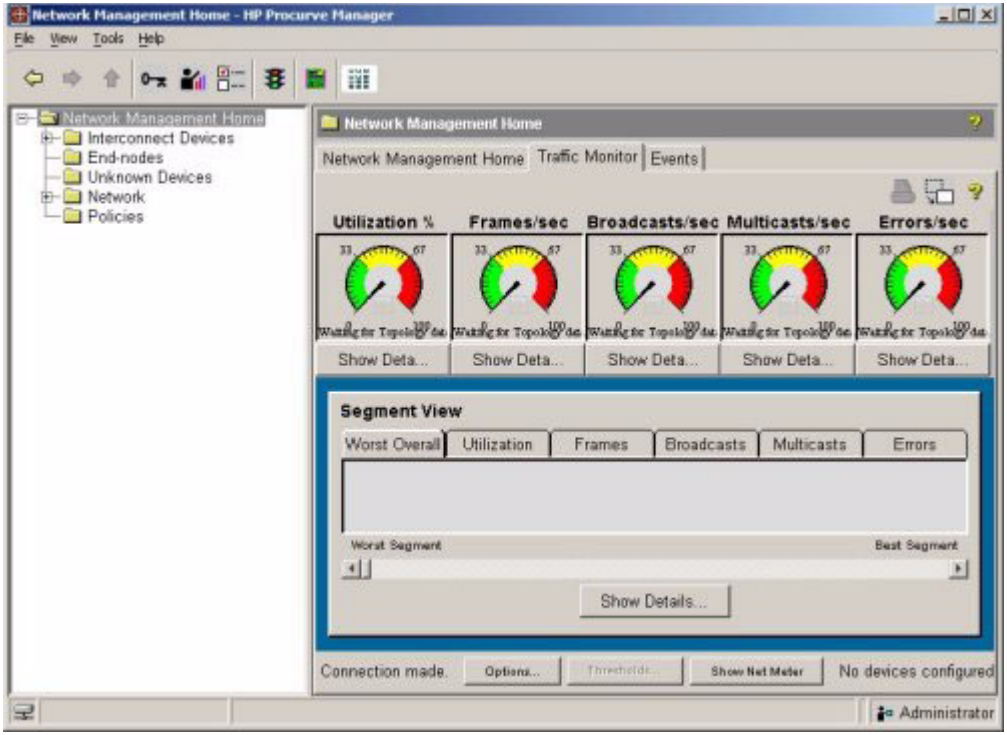


Figure 7-1. Traffic Monitor Main Page

The five statistical attributes sampled by Traffic Monitor are:

Utilization %: Represents the traffic on the selected 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 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 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 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 attribute value used for the ordering of the segments. The Worst Overall tab displays in sorted order left to right the segments that have the most problems. 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.

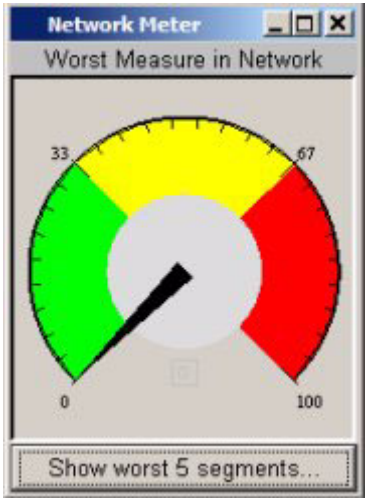
Comparing Segments Across Different Medias

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.

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. The Network Meter is similar to the Network Status panel of the Dashboard window.



To launch a separate instance of the Network Meter on your desktop click on the Net Meter button below the histogram on the Traffic Monitor page.

You can keep the Network Meter window anywhere on your PC desktop. It will continue to monitor the status of your network while you work at other tasks.

The Net Meter button works as a toggle, when it is "on" the button changes to Hide Net Meter in the Traffic Monitor window. Clicking it will close the Net Meter window and the button on the Traffic Monitor changes back to Net Meter.

Clicking on the Show Worst 5 Segments button displays a window showing the top five thresholds that have been exceeded, and the associated segments.

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. If you have "linked the gauges to the selected segment" (Options) the gauges in the Traffic Monitor page display the traffic only for the segment that you have selected. If the segments are not linked to the gauges (Options), the Network Meter and the gauges will reflect the same conditions.

Setting Thresholds

When you click on Thresholds at the bottom of the Traffic Monitor window, a separate Thresholds window appears.

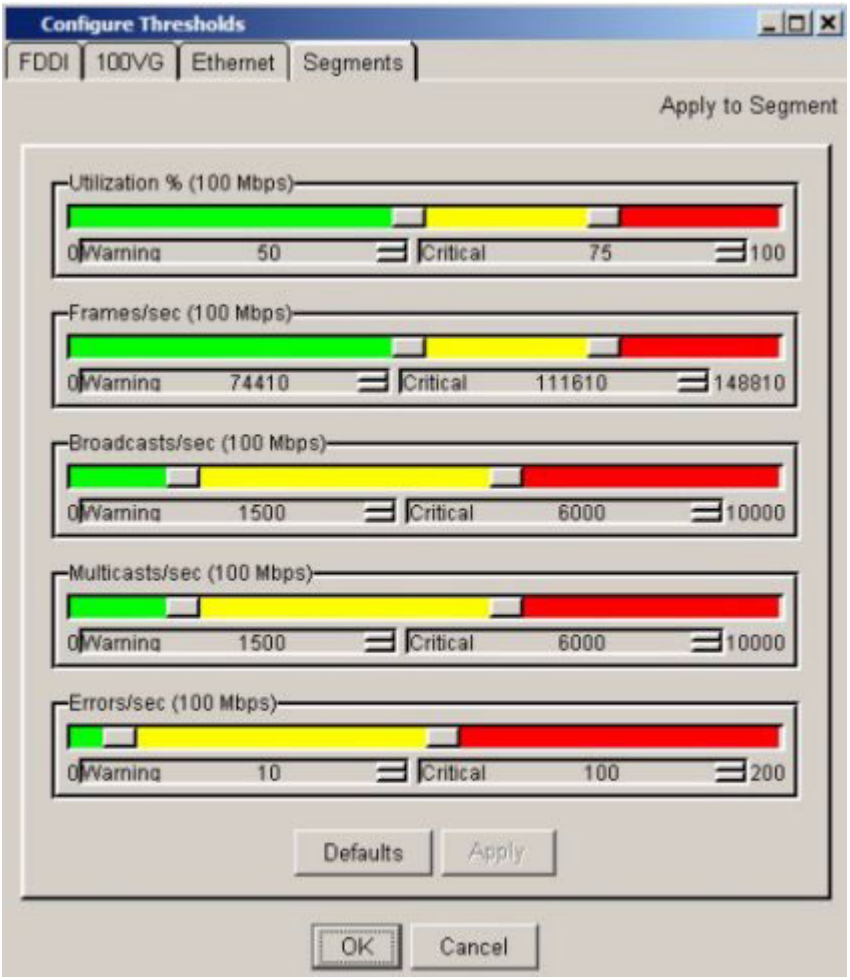


Figure 7-2. Traffic Monitor: Thresholds Window

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 appro-

priate, 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.

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.

Traffic Monitor thresholds will not generate alerts/events in the Event Browser, they appear only in the Traffic Thresholds display.

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 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 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've finished making changes, click 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.

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.

Click the Defaults button returns the threshold values for that segment or segment speed to the original default values.

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 (XRMON or SFlow) sampling-capable, the only data displayed is “Other”.

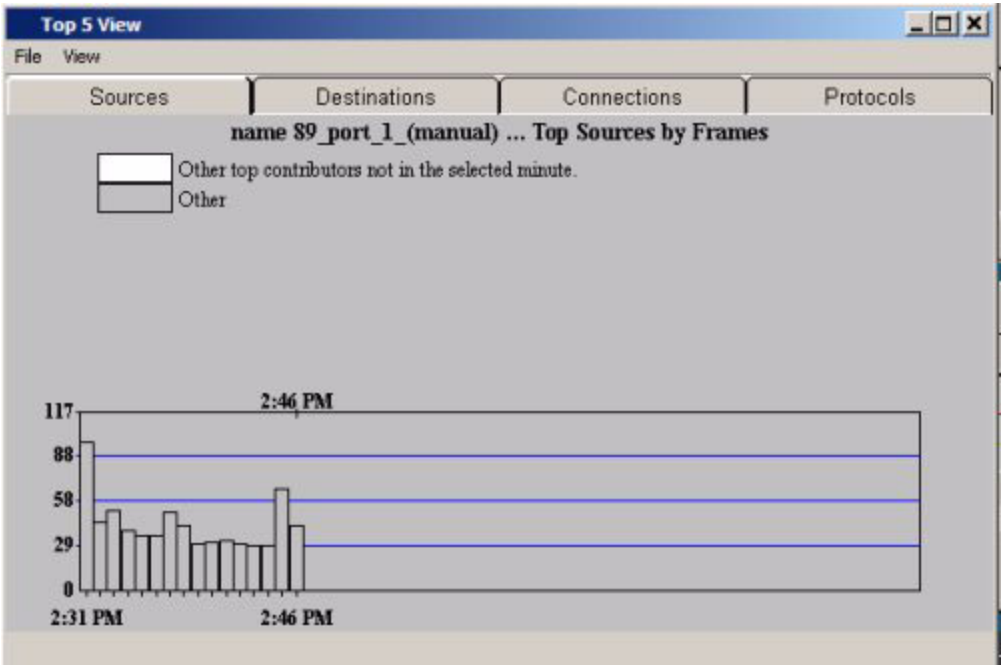


Figure 7-3. Traffic Monitor: Top 5 Talkers

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.

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”.

If your graph is only displaying “Other” data, there may be a problem with the data sampler for this segment, XRMON/SFlow data collection may be disabled, or the device is incapable of collecting XRMON/SFlow data.

Top5 View Menu Items

The Top5 View has two 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

Traffic Monitor Configuration

With HP ProCurve Manager Plus, you can collect traffic data from selected ports of devices. You can also choose the type of data to be collected, for example, Extended RMON (XRMON) or SFlow sampler data, or just traffic statistics.

Adding Devices to Traffic Monitor

When you first start PCM+, the Traffic Monitor is not set to collect data for any devices on the network. You need to add the devices to monitor to Traffic Monitor in order for traffic data to be collected. When a device is added to the Traffic Monitor, it is also added to the Traffic Devices tab.

You can add a single device at a time, or multiple devices. You may also modify the configuration of a device that has already been added to Traffic Monitor.

To collect traffic data for a device, add the device to the Traffic Monitor using one of the following methods.

To add devices to Traffic Monitor using the tree:

1. Right-click on the device, device group, or interconnect devices node to be added to the Traffic Monitor.
2. Select Traffic Monitor from the(right-click) menu.
3. Select one of the following:

   Add Device(s): Add the selected device(s) to traffic management but do not collect statistics for any ports on the devices (no statistics collected).

   Collect Statistics: Collect statistics (MIB-II SNMP counters) for all ports on selected device(s).

   Collect Sampler Data: Collect statistics and header samples based on the type of sampler (XRMON and sFlow) supported by the device. Collect Sampler Data configures the sFlow sampler if the device supports it. If the device supports XRMON but not sFlow, the XRMON sampler is configured for the device ports. If neither XRMON or sFlow is supported, only statistics are collected.

   NOTE: If the Stats checkbox is checked, XRMON (Ease) is configured.
4. When the Traffic Device Configuration window appears, configure the individual ports for the selected device.

To add devices to Traffic Monitor using the map:

1. Navigate to and select the Network, Subnet, or VLAN map in the tree.
2. In the map, right-click the device to be added to the Traffic Monitor
3. Select Traffic Monitor from the drop-down menu, and proceed as described for adding devices to Traffic Monitor using the tree.

To add devices to Traffic Monitor using the Devices List:

1. Click the device group or interconnect devices node in the tree.
2. Click the Devices List tab.
3. Select one or more devices from the Devices List.
4.  Click the "Add Device to Traffic Monitor" button. This launches the Traffic Device Configuration window that you will use to configure monitoring for ports on each device.

Configuring Ports for Traffic Monitoring

The Traffic Device Configuration window displays all devices from one or more selected device groups or individual devices. After the Traffic Device configuration window is displayed, you may continue to select additional devices or device groups and they will be added to the Traffic Devices Configuration window. When you are satisfied with the list of devices, you may then proceed to configure their ports.

The Traffice Device configuration window allows you to pick two monitoring options:

- Stats—Collects data using the MIB-II SNMP counters to measure traffic on the network.
- Sampler—Collect Statistics and SFLOW or XRMON (EASE) data. Selecting the check box in this column will enable the XRMON or SFLOW sampler for all ports on the device. The sampler data allows you to see the "Top 5" contributors to the network traffic segment.

  The "Sampler" option configures the device to collect both statistics and header samples based on the type of sampler that the interconnect device supports. Two types of samplers are supported; XRMON and SFLOW. SFLOW is the preferred sampler, and if the device supports both XRMON and SFLOW the SFLOW sampler will be enabled for the device. If the device does not support SFLOW but does support XRMON, then the

XRMON sampler is configured for the device. If the device does not support either sampler, N/A appears in the column and only Stats collection will be enabled.

You can tell which type of sampler is supported by noting whether the Stats column check box is selected. When SFLOW is supported, the statistics check box is blank because the SFLOW sampler has built in statistics data collection. If XRMON is supported, the Stats check box is always selected.

- The Last Arrival of Data column also indicates which devices are configured. The Unconfigured Device message indicates a device is not configured. A timestamp of the last time traffic monitor received data from a device, or any other message indicates a previously configured device.

  A message of "Device updated - no data" or "Port updated - no data" that appears for more than six minutes indicates there is a condition preventing Traffic Monitor from collecting data. You can look in the Event Browser for "Traffic Manager" error messages to get additional information.

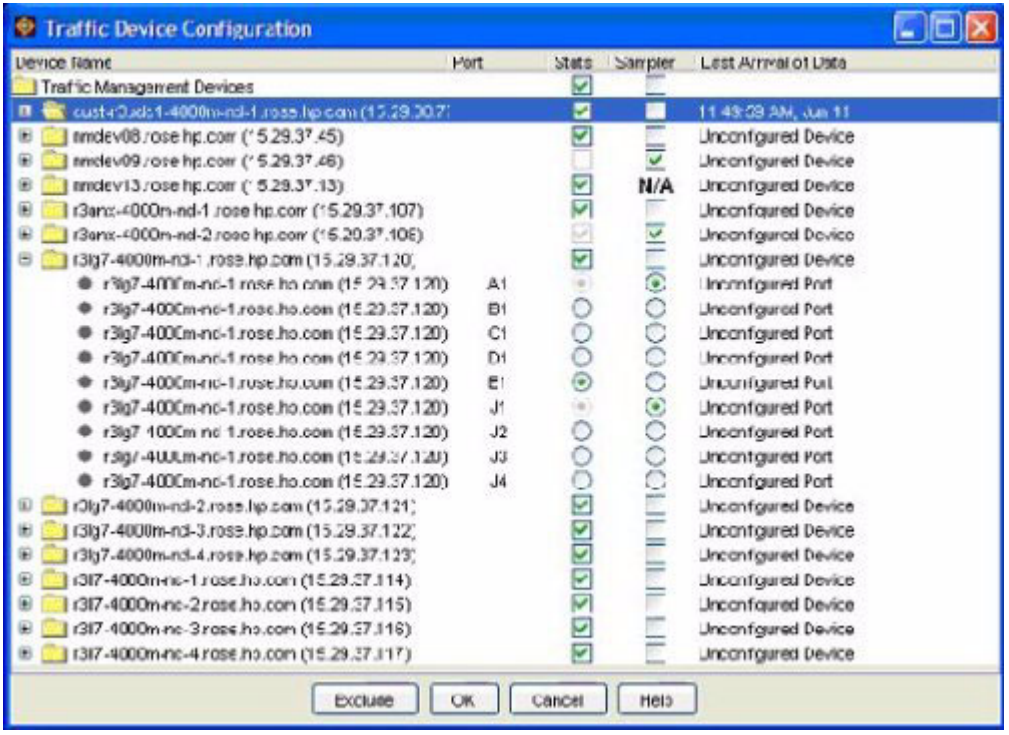


Figure 9-4. Traffic Device Configuration window

While it is simplest to configure all ports on a device at once, configuring a device on a port-by-port basis conserves network resources by allowing you to select the individual device ports that you want to monitor. For example, you might want to monitor only those ports that have traffic between your interconnect devices (switch-to-switch) and server end-nodes. In most cases you will want to omit all other end-node segments (PCs, printers, etc.). In addition, since every link (segment) between two devices has two ports (one on each side of the link), only one of the two ports needs to be monitored.

To configure ports on a port-by-port basis:

1. In the Traffic Device Configuration window, click the + next to the devices to be configured, which displays every port on the devices.
2. Click the Stats box next to each port that will be included in traffic statistics only.
3. Click the Sampler box next to each port that will be included in sampler data and traffic statistics. You cannot select Sampler for ports that do not support sFlow or Ease samplers.
   (Note that Ports configured for Sampler are automatically configured for traffic statistics.)

To configure all ports on a device:

1. In the Traffic Device Configuration window, select the device.
2. Click the Stats box next to the device that will be included in traffic statistics only.
3. Click the Sampler box next to each device that will be included in sampler data and traffic statistics. You cannot select Sampler for ports that do not support sFlow or Ease samplers.

To configure all ports for all devices in Traffic Monitor:

1. In the Traffic Device Configuration window, select the "Traffic Management Devices" row (top node).
2. To include all ports in traffic statistics only, click the Stats box.
3. To include all ports in sampler data and traffic statistics, click the Sampler box.
   (Note that Ports configured for Sampler are automatically configured for traffic statistics.)

When you are finished selecting the ports to monitor, click on the OK button. The Traffic Monitor restarts with the new device information.

Modifying Port Traffic Configurations

To modify the Port configurations on a traffic device, select Interconnect Devices in the navigation tree to display the Devices window, then select the Traffic Devices tab to display the list of configured Traffic devices.

Select the device in the Traffic Devices list, then click the "modify" icon in the toolbar. The Traffic Device Configuration window is displayed and you can modify your configuration using the same procedures as described above.

Excluding Devices from Traffic Monitoring

To exclude a device from the Traffic Device Manager, select the device in the Traffic Device Configuration list, then click on the Exclude button at the bottom of the window.

Excluding a device removes it from the current Traffic Device Configuration list, which is useful when you selected a group of devices and want to remove a device from the devices being added or modified. Excluding a device does not remove it from the Traffic Monitor or group, but simply removes it from the list of devices being configured.

Removing Devices from Traffic Monitor

To delete Traffic devices, select Interconnect Devices in the navigation tree to display the Devices window, then select the Traffic Devices tab to display the list of configured Traffic devices.

Select the device or devices in the Traffic Devices list, then click the "Delete" icon in the toolbar.

An alternate method for removing Traffic devices is to right click on the device in the navigation tree, and select the Traffic Monitor -> Remove Device(s) item from the menu. The selected device(s) will be removed from the Traffic Monitor and Traffic Device Configuration list.

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:

- 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.
- Switch is Very Busy—When an interconnect device becomes overloaded, it may stop responding to management requests in order to execute its primary function of handling network traffic.

You can also look in the Event Browser to get additional information on specific devices that may be having problems, or for "Traffic Manager" events indicating there is a problem with Traffic Monitor's ability to access the device.

Server Connection Lost

When you add, modify or delete a traffic device configuration, the "Attempting to re-establish connection" message is displayed in the lower left corner of the Traffic Monitor tab. Configuration changes can take up to five minutes, during which time the traffic monitor gauges will not show any traffic data.

If the message remains longer than five minutes and a connection is not established with the server, try the following:

- Check the Event browser window for Traffic errors.
- Use the Microsoft Task Manager to check that the TMServer and Trafficd are still running on the PCM Server.
- Restart the PCM Client.
- Restart the PCM Server Service
  (under Administrative Tools->Services)

8

Managing Device Configurations

Chapter Contents

About Configuration Manager

The Configuration Manager module in PCM+ allows you to scan HP ProCurve Switches in your network and store records of the switch configurations (SW, HW, and Switch Software [OS] configurations) in a database. This information can then be used to:

- Identify when a device configuration has been changed.
- Rollback or roll forward configurations on a single device or many devices.
- Send CLI command(s) to one or many devices.

The Configuration Manager scan process can be done on demand or as a scheduled process. This helps you manage device configurations in your network by providing notification whenever any configuration (software or hardware) changes on an HP ProCurve device in the network.

As a quick summary, the Configuration Manager component provides the following features:

- Automatic device configuration scans (manually or on set intervals)
- Viewing of device configurations
- Viewing configuration history for a device
- Comparison of any two device configurations
- Ability to restore or deploy a specific configuration to a device

Reviewing Device Configurations

The Configurations pane in the Network Management Dashboard display provides a quick review of overall network device configurations. For a more detailed display, click on the Configurations pane to display the device Configurations tab in the Interconnect Devices window.

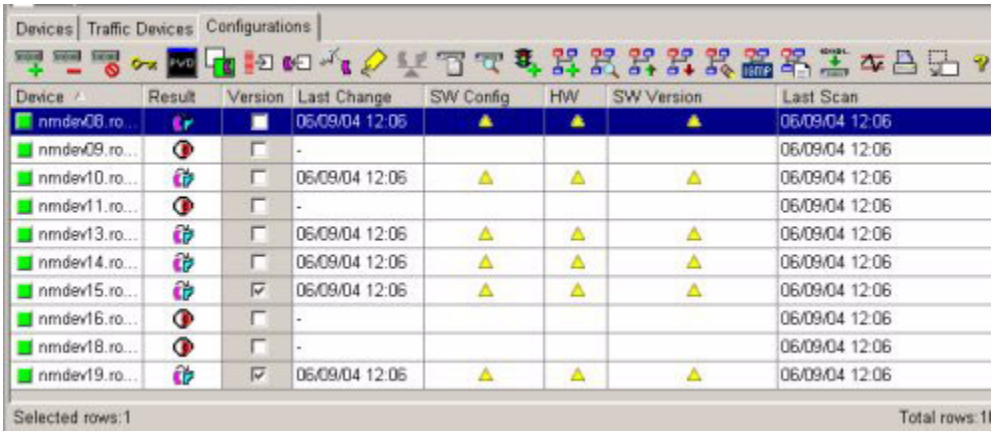


Figure 8-1. Device Configurations listing

The Configurations display provides a list of which devices have had configuration changes. It gives the following information for each device:

- **Device** - The DNS name or IP address of the device
- **Result** - Icons indicating the result of the last scan, one of:
  - Changed
  - Login failure
  - Device not supported
  - Scan timed out
  - Device never scanned
  - Network error prevented scan
- **Latest** - Whether the device has the latest software (operating system). Check indicates yes, blank indicates no.
- **Last Change** - Date of the most recent configuration change.

- **SW** - Yellow triangle indicates the software configuration changed on the date shown in the Last Change column.
- **HW** - Yellow triangle indicates the hardware configuration changed on the date shown in the Last Change column.
- **FW Ver** - Yellow triangle indicates the ProCurve Switch Software changed on the date shown in the Last Change column
- **Last Scan** - Most recent date that a device scan was attempted.
- **Scheduled** - Indicates the device is included for the next scheduled scan. A grayed out icon indicates the device has been removed from the next scheduled scan.

You can sort the list on any of the columns. For example, click the SW column and/or Last Change column heading. This will re-sort the list with devices that have software changes at the top.

Configurations Detail

To view detailed configuration information for a device, double-click on the device in the Configurations tab to display the Configurations detail.

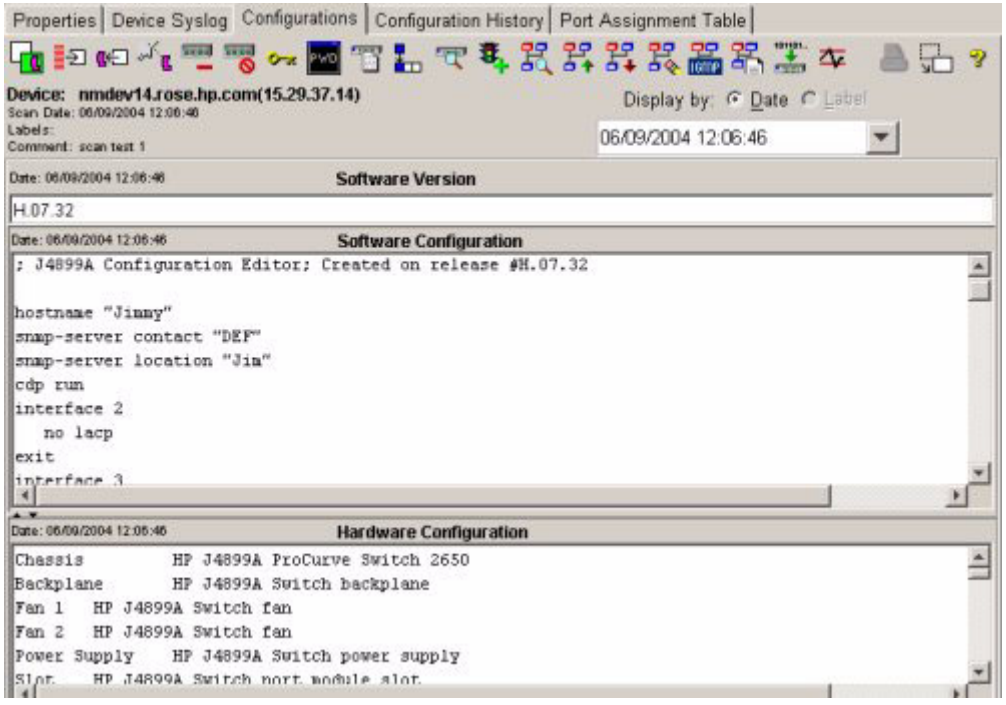


Figure 8-2. Device Configuration detail

If the configuration for the device has changed, you can use the "Display by" option to review the configuration details from previous scans, either by date of the scan, or by configuration label (if used).

Configurations are collected for the HP ProCurve Wireless access points (420wl, 520wl), but the format is binary proprietary (machine readable only). You can still label and re-deploy wireless configurations as needed.

VLAN Configuration Detail

To review the VLANs configurations for the device, click the "Show VLAN List" icon in the toolbar. (Or use the "Show VLAN" option in the right-click menu).

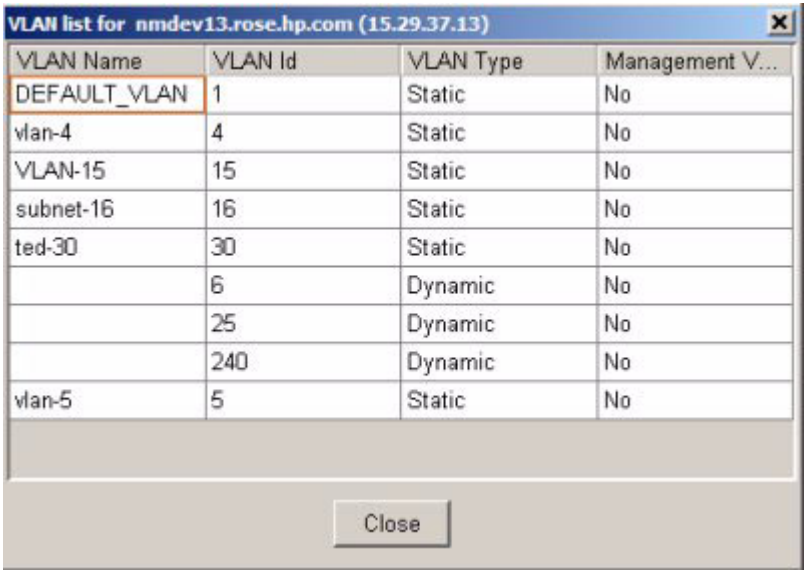


Figure 8-3. Show VLAN List for Device window.

The VLAN list includes the VLAN Name, ID, type, and management status for all VLANs configured on the device.

Refer to Chapter 9, “Using VLANs” for information on configuring VLANs.

Device Configuration History

Click the Configuration History tab to view a history of configuration changes for the device.

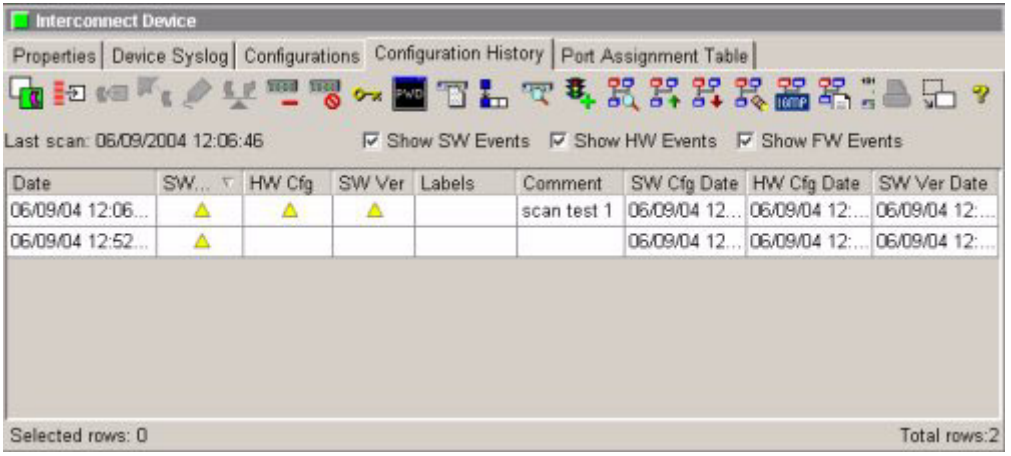


Figure 8-4. Device Configuration History display

The Configuration History window displays a list of every* past configuration stored for the device. This information can be used to determine when and how configurations have changed. The SwChg, HwChg, and OsChg columns are marked with a yellow triangle to indicate if the given configuration had changed when that configuration scan was stored. The Labels field lists any labels applied to a given configuration, and the Comments field lists comments entered on the scan event. The remaining Sw, Hw and Fw Date columns are provided to help sort the configuration data by the date changes occurred. You can filter out the display of Sw, Hw, or Fw events by unchecking the "Show" events at the top of the list.

* The number of stored configurations is controlled by the Configuration Management preferences.

Using Configuration Labels

You can apply labels to a device configuration to help identify known good configurations or other special configurations in the Configurations and Configuration History displays.

To apply a configuration label, select the device configuration in the Configurations or Configuration History display, then click the Label icon in the toolbar. The "Apply a Label" dialog will be displayed.

Figure 8-5. Apply Label to Device Configuration dialog

Note that when accessed from the Configuration History, the device name panel is not shown. Also, if multiple devices are selected in the Configurations listing, each of the devices will be listed in the "Apply a Label" dialog.

Enter a Label for the device (software) configuration, then click OK. The device configuration record will be updated with the new Label.

If you are not sure if the label is unique–that it has not been used before for the selected device, check (click) the Automatically move label option. This will move the label to the selected configuration, from a configuration on which it was previously used.

You can apply multiple labels to any given configuration, but each label must be unique. Once a Label is applied, the Label cannot be edited or removed from that configuration.

Comparing Device Configurations

The Configuration Manager allows you to compare configurations between devices, or two separate configurations on the same device. You can then use data from one configuration to edit or restore a device configuration on one or more devices.

To compare device configurations between two separate devices, in the Devices List or the Configurations tab, select two devices in the list, then click the Compare icon in the toolbar. In the confirmation pop-up dialog, click Compare! to continue with the comparison.

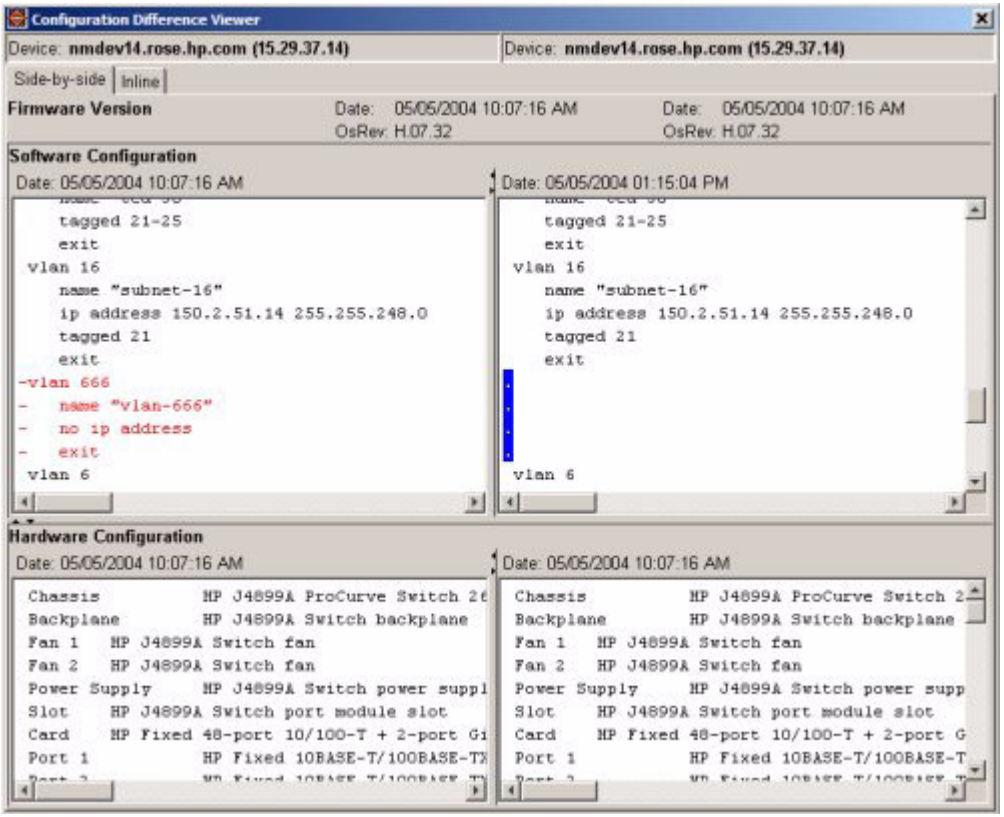


Figure 8-6. Configurations Difference Viewer, default display

The default display is Side-by-side, that is with one device configuration in the right side and the other on the left. Differences in the software configuration are highlighted with different colored text.

If you want to view only the differences between the two configurations, click the Inline tab.

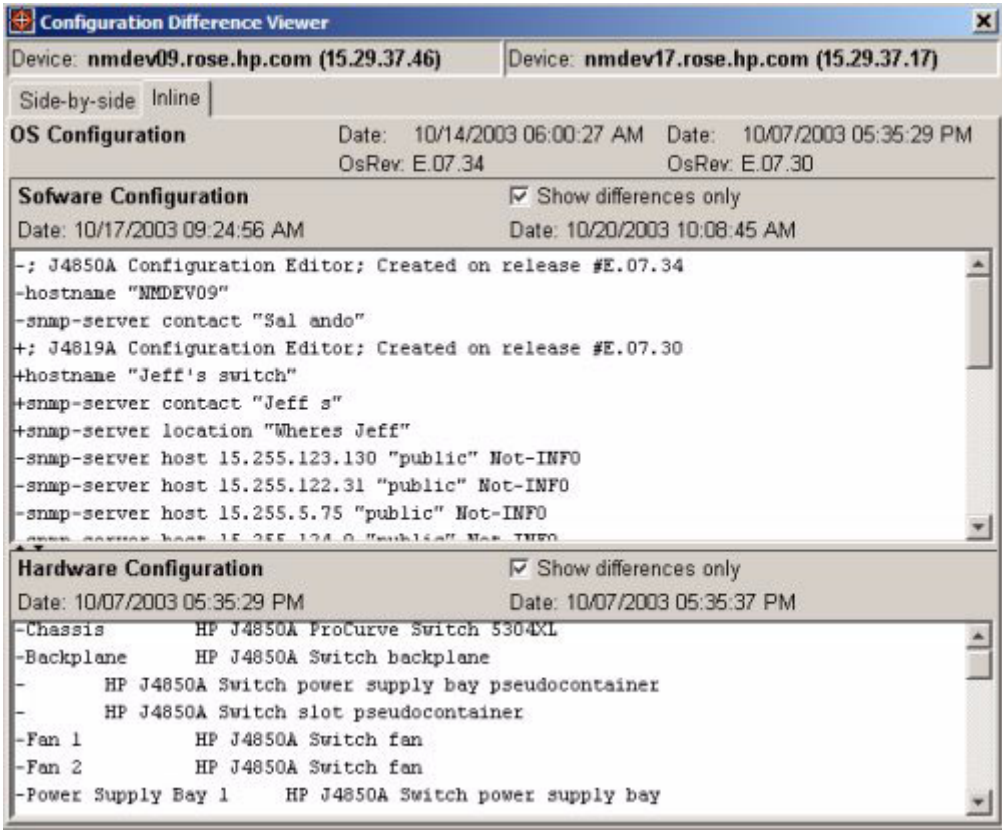


Figure 8-7. Configuration Difference Viewer, Inline display

Click to check the Show differences only option. The inline display will list the first device type, software release, and device name. Then the second device is listed, with the differences in configuration from the first device listed. No other colors or indicators are used to highlight differences between the two configurations.

Updating Device Configurations

After reviewing your network device configurations, you can use the Deploy Wizard to edit the software configuration and deploy it to a device (commit to flash). The Deploy Wizard will perform a total replacement of the software configuration on the target device and then reboot the device and capture the new configuration information. Deployment is useful when you capture a known good configuration and want to restore that configuration in its entirety, or apply the configuration to other devices.

Note: Use the Device Manager for simple tasks like changing the host name, community names, and authorized managers. Use the CLI Wizard, Telnet, or Web Agent for more complex configuration changes.

Using the Deploy Wizard

To deploy a known good configuration to a device, go to the Configuration History window for the device and select (highlight) the configuration to be deployed, then click the Deploy Wizard icon in the toolbar.

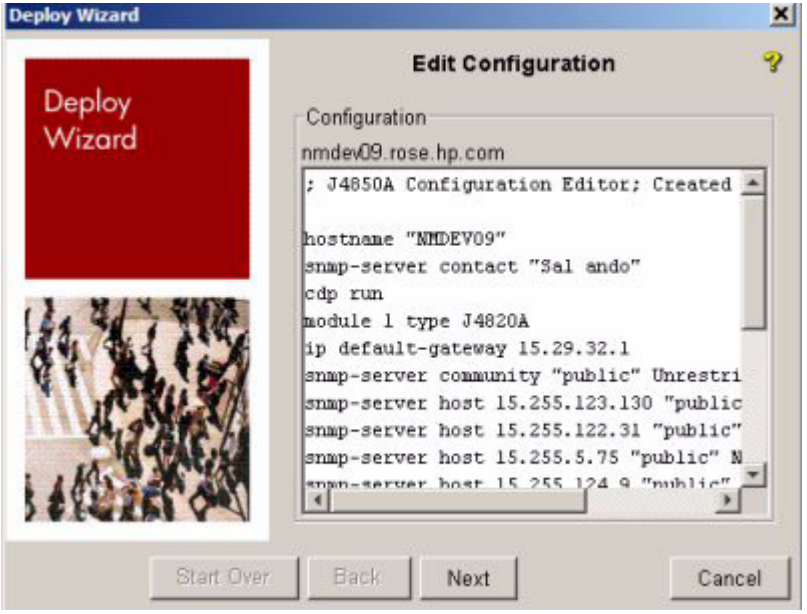


Figure 8-8. Deploy WIzard, Edit Configuration dialog

NOTE:

For most HP ProCurve devices the CLI commands for the configuration are displayed. For the 8000, 4000, 2400, and 1600 series devices, the configuration is shown and edited in record format.

Assuming you have selected a known good configuration, no edits should be needed. However, you can click in the configuration display and edit the configuration as needed. Note that there is no parsing or interpretation on commands entered in the Deploy Wizard. For details on CLI commands used for device configuration, refer to the Management and Configuration Guide for the device.

Click Next to continue to Schedule Deployment.

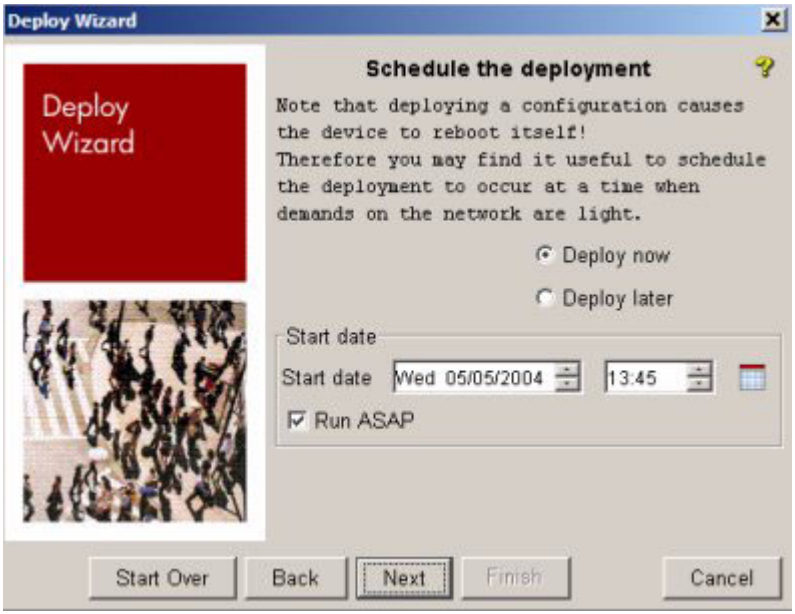


Figure 8-9. Deploy WIzard, Schedule deployment dialog.

- Select Deploy now if you need to deploy the configuration immediately to correct a problem in the device. The configuration will deploy as soon as you click the Next button.
- Select Deploy later to deploy the configuration at the date and time that you specify in the Start date fields.

If you selected the Deploy later option, click Finish to save the configuration deployment schedule and exit the wizard.

If you selected the Deploy now option, when you click Next the Deploy Wizard will display a monitor of the deployment status. Possible results are:

- Successful - The configuration deployed successfully.
- Deployment Failed - The configuration was not deployed due to a bad connection, nonexistent or invalid file, or invalid permissions.
- Configuration files identical - No changes were made because the configuration file on the device is identical to the configuration deployed.

Click Close to exit the Deploy Wizard.

Tip: To apply a known good configuration from one network device to another, you can copy portions of the software configuration information from the Configurations details or Comparison display, then paste the copied configuration in the "Deploy Wizard:Edit" dialog or "CLI Wizard:Commands" dialog.

Configuring Devices with CLI

The CLI Wizard feature in the Configuration Manager lets you issue a configuration command to multiple devices at the same time. In this way you use a "batch process" to update the configuration on all devices at once, instead of having to update each device separately.

To issue a command to multiple devices using the CLI Wizard,

1. Select the devices in the Devices List or Configurations list display.
2. Click the CLI Wizard icon in the toolbar. This will launch the CLI Wizard.

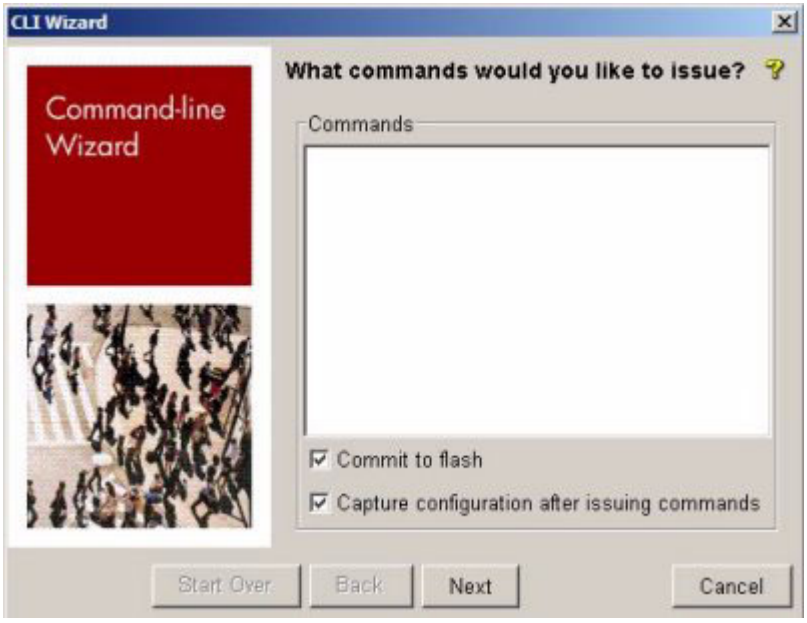


Figure 8-10. CLI Wizard, Commands dialog

3. Click in the text box and type in the configuration command(s) you want to apply.

   You can enter any mixture of commands or "show" commands. The commands will be executed in the order entered. Care should be taken when issuing commands that change an IP address or commands that will cause a device to reboot.

4. The Commit to flash option is essentially a "write memory" command that will commit commands to the startup configuration.

The Capture configuration... option tell Configuration Manager to automatically scan the device to capture the configuration after the commands are issued.

Click the check box to deselect these options. A check mark indicates the options are enabled.

5. Click Next to continue.:

Figure 8-11. CLI Wizard, Select when to execute dialog

6. Select when you want to execute the CLI commands:
   - Select Send commands now if you want to execute the commands immediately to repair a problem or improve performance.
   - Select Send commands later to send commands at a time when the impact to network performance will not be a problem.
7. Click Next to continue.
   a. If you selected the Send commands now option, the CLI Wizard will display a monitor of the command status.

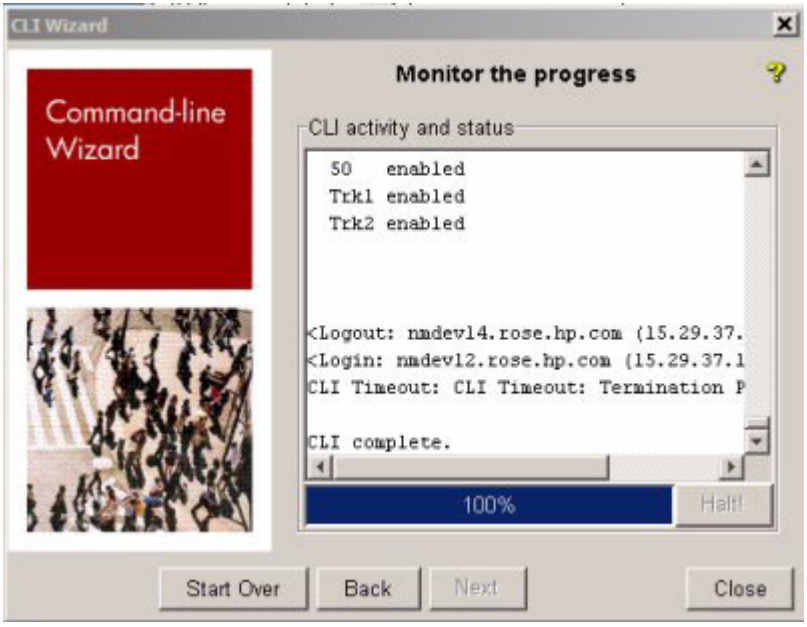


Figure 8-12. CLI Wizard, Monitor dialog

In the Monitor dialog, click Halt to stop the CLI command action. Otherwise, the monitor will display the results of each command.

NOTE: If you issue commands to multiple devices using the CLI Wizard, it issues the commands to five devices at a time, in parallel, until all devices are configured.

b. If you selected the Send commands later option, when you click Next a scheduling dialog is displayed.

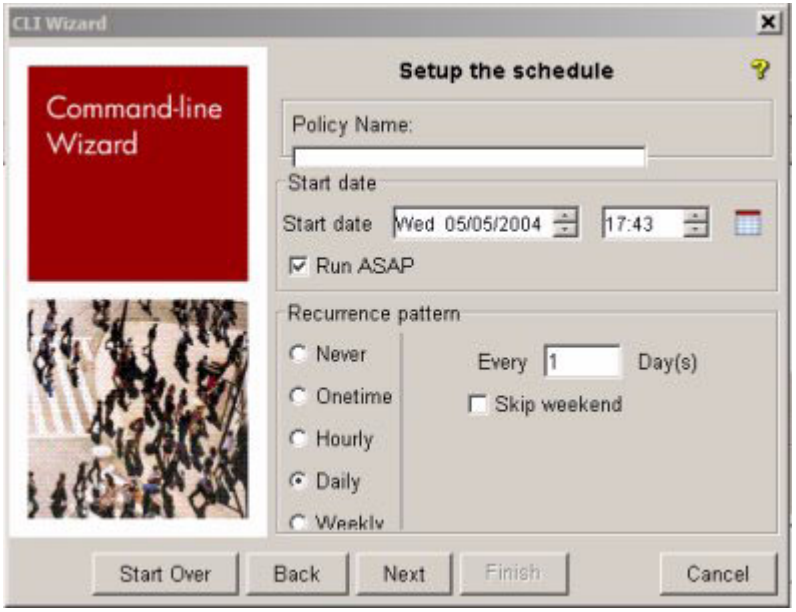


Figure 8-13. CLI Wizard, Schedule setup dialog

8. Enter a name under which the CLI commands will be stored, then enter the start date and time, and the recurrence pattern if you want to repeat the commands at scheduled intervals, similar to a CLI policy. (Chapter 10)

Never	No further action is required (Policy definition is saved, but will not be enforced).
One time	No further action is required (the currently scheduled time is used with no recurrences).
Hourly	Type the number of hours and minutes to wait between executing commands. If you do not want the commands executed on Saturdays and Sundays, check the Skip weekend checkbox.
Daily	Type the number of days to wait between enforcements. If you do not want the commands enforced on Saturdays and Sundays, check the Skip weekend checkbox.

9. Click Next to continue.

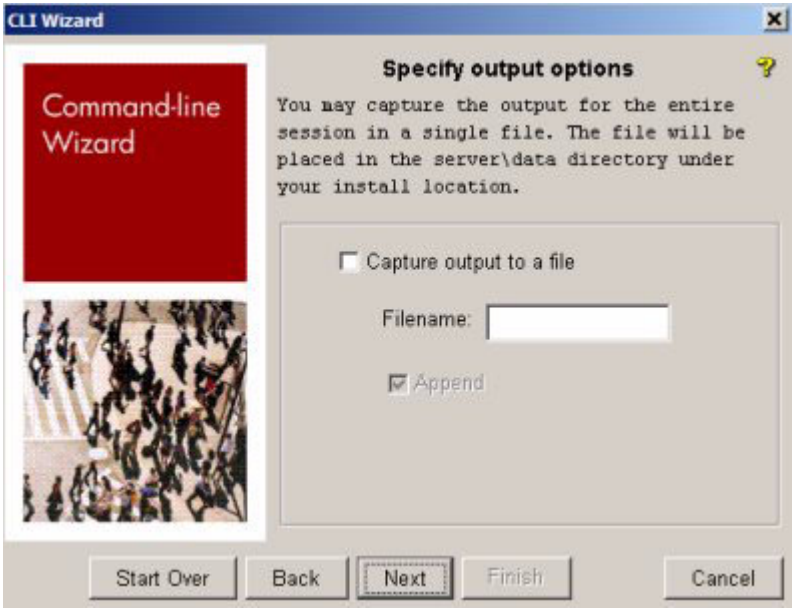


Figure 8-14. CLI Wizard, Output Options dialog

10. Select the Session Output options:
    a. If you do not want to capture the output for the session, click Next to close the "Specify Output Options" window.
    b. Click the Capture output to a file checkbox to capture the output for the session.
    c. Type in the file name in which to store the output.
    d. Click the Append checkbox to append the next session output to previous output if the file already exists.

       To overwrite an existing file, ensure that the Append checkbox is not checked.
    e. Click Next. The Show Selected devices dialog is displayed, with the list of devices to which the CLI commands will be applied.

Figure 8-15. CLI Wizard, Show Selected Devices dialog

11. Click Finish to exit the CLI Wizard, or Start Over to return to the Commands dialog and issue additional commands.

Performing Configuration Scans

When the PCM+ Server is installed, it uses a default policy that automatically scans devices on the network to collect device status and configuration information once each day. You can also perform a manual scan at any time.

Manual Configuration Scanning

To manually scan a device or group of devices, select the device or devices in the Devices Lists display, then click the Scan button in the toolbar. Alternately, you can right-click on the device in either the navigation tree, or the network map, then select the Scan option from the menu. Either action will launch the Scan Wizard.

Figure 8-16. Configuration Manager: Scan Wizard, Comment dialog.

You can enter a comment that will be stored in the database along with the configuration record, or just proceed to the next dialog.

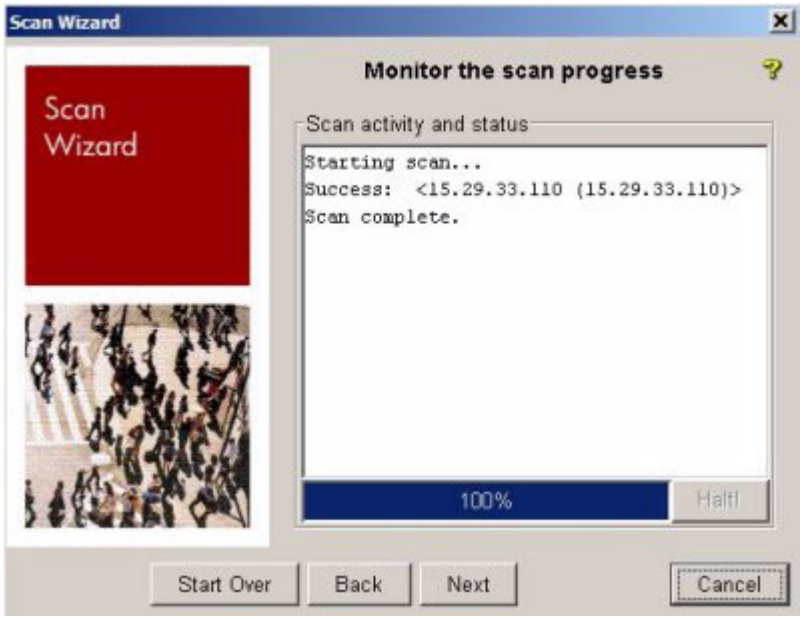


Figure 8-17. Configuration Manager: Scan Wizard, Monitor dialog.

If the device is not supported by the Configuration Manager, the scan process returns a failure notice in the Monitor dialog. The scan process will also fail if the correct Write Community Name has not been configured for the device. Otherwise, the scan proceeds and the "View results" dialog is displayed.

If you selected multiple devices to scan, you can click the Halt! button to stop the scan process after it starts. The scan will complete on the device currently being scanned, then the scan process is stopped before continuing to the next device in the list. IN the case of a single device being scanned, once the scan is started, clicking Halt! will have no real effect.

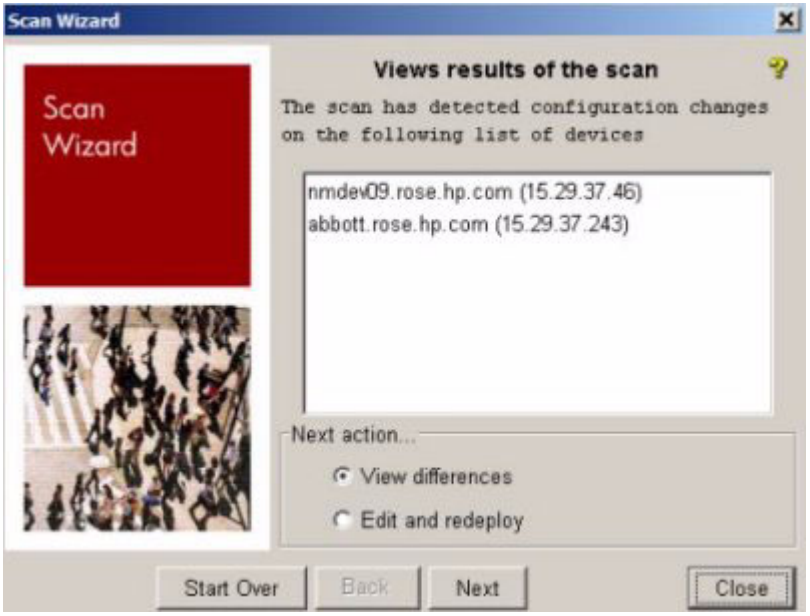


Figure 8-18. Configuration Scan Wizard, View results dialog.

- To view differences found between scanned configurations, select the View differences option, then click Next. The View differences dialog will be displayed.

NOTE: If this is the first time the device has been scanned, the "View differences" options will not work, since the system is unable to detect changes until more than one configuration has been scanned.

- To edit the changed configuration, select the device in the "View results of scan" listing, select the Edit and redeploy option, then click Next. The Deploy Wizard: Edit dialog is displayed (see figure 8-8).

  Refer to the instructions for using the Deploy Wizard to update configurations, starting on page 8-10.

If there are no changes detected, the scan results box is empty.

Figure 8-19. Configuration Scan Wizard, View differences dialog

- In the "View differences" dialog, select the device, then click View... The "Configuration Difference Viewer" is launched showing the current and previous configuration scan information (see figure 8-6)

When you have completed the manual scan and configuration review process, click Close to exit the Scan Wizard.

Scheduling Configuration Scans

You can use configuration policies to set Configuration Management parameters and configure Scheduled scans to scan device configurations at regular intervals. For details refer to “Using Configuration Policies” on page 10-1.

Configuration Management Preferences

To set the Configuration Manager preferences, click the Preferences icon in the main toolbar, then select (click) the Configuration Management option in the Global menu.

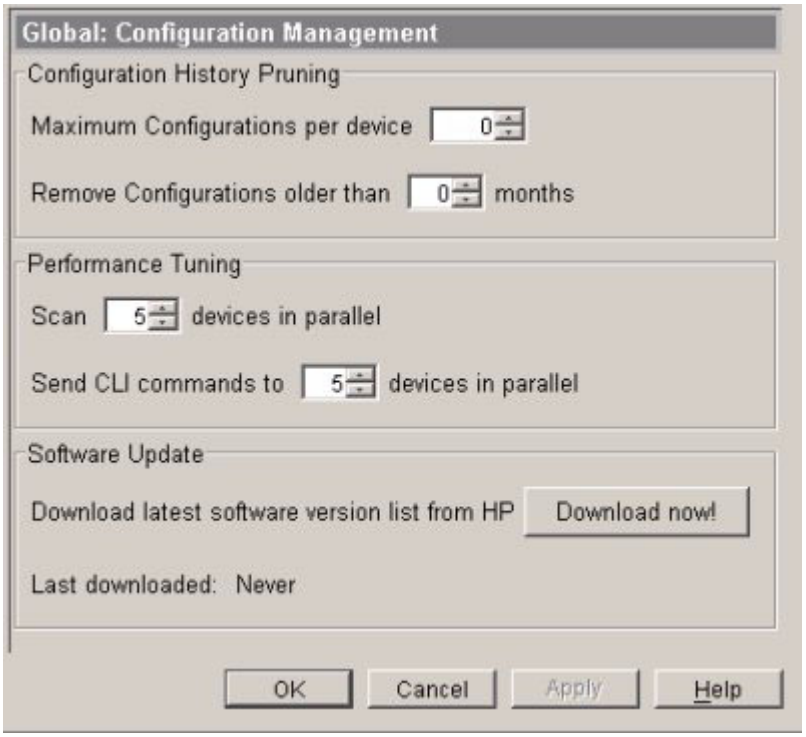


Figure 8-20. Global Preferences:Configuration Management settings

You can type in changes to the Configuration History Pruning and Performance Tuning parameters, or use the buttons to increase or decrease the parameters.

The default entry for Maximum Confiugrrations is 0, which allows an unlimited number of configuration. Similarly, the Remove Configurations default of 0 indicates unlimited, that is, no configurations will be removed.

The Software Update option (Download now!) will go out to the HP ProCurve support web site and download a listing of the latest software versions.

Setting Preferred Switch Software Versions

The Switch Software window lets you select the software configuration version you want to use for each device type. In a preferred version is not identified, the most recent switch software version is used for software updates.

To set the preferred software configuration version:

1. Navigate to the Switch Software window.
   [Preferences->Configuration Management->Switch Software]

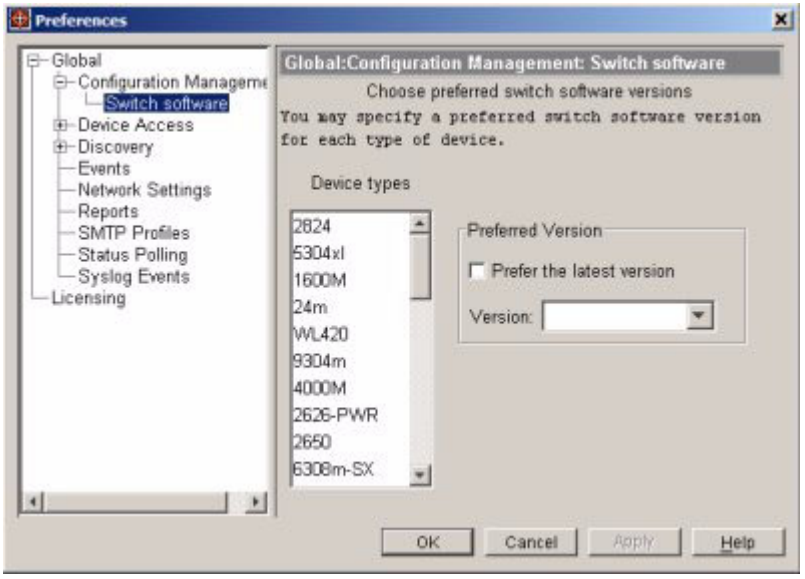


Figure 8-21. Global Preferences: Switch Software settings window

2. Scroll down the Device Types list and select the device type you want to set.
3. To use the most recent software configuration to update devices, check the Prefer the latest version checkbox.

   To use a specific version, use the up and down arrow keys to select the desired version from the Version field.
4. Click OK to save the settings and close the Switch Software window.

Network Settings

PCM+ needs external web access to retrieve the latest switch software files for HP ProCurve network devices from the HP ProCurve web site. If the HTTP proxy was not configured at installation, or if the proxy server has changed, use the Network Settings to set configure the Proxy settings.

To configure the Network Proxy settings:

1. Select Preferences->Network Settings.

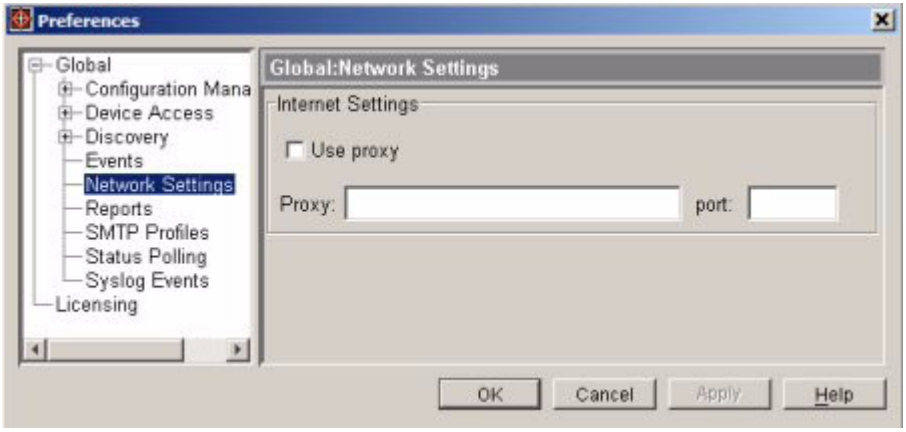


Figure 8-22. Global Preferences: Network Settings window

2. Click the Use proxy check box, if it is not already selected.
3. In the Proxy field, type the DNS name or IP address of the proxy server for the subnet.
4. In the Port field, type the port number used to access the proxy.
5. Click OK to save the network settings and close the window.

Updating Switch Software

HP provides periodic software updates for HP ProCurve switches via the HP ProCurve Support Web site. You can use the Software update feature in PCM+ to automatically download and apply updates to devices at scheduled times.

Downloading the Software Version List

When you review the Configurations listing, the "Latest" column in the display indicates whether the device is running the most recent switch software version. This is done by comparing the current software version found in the MIB during the configuration scan to the current software listing.

To download the latest listing of HP ProCurve Switch Software versions, select the Configuration Management option in the Preferences menu (see figure 8-20 on page 8-23). Click the Download now! button in the Software Update section of the window. This will download a listing of the current switch software revisions from the HP ProCurve Web site to the PCM server. (server/data/download/procurve_firmware.prp). You can also sign up for the driver update notification at: http://h30046.www3.hp.com/driverAlertProfile.php?referer=/subprofile_summary.php.

Scheduling Automatic Updates

To schedule devices for automatic software updates, or to edit an existing software update schedule:

1. Select the Interconnect Devices node or Device Group node in the navigation tree
2. Select the device or devices in the Devices List or Configurations tab display.
3. 

Click the Software Update icon in the toolbar to launch the Software Update Wizard.

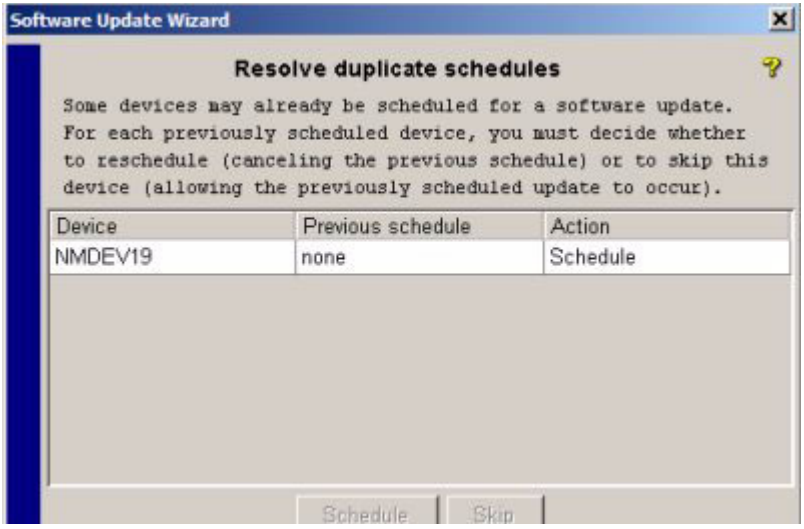


Figure 8-23. Software Update Wizard, schedule dialog

4. Click in the dialog to enable the Schedule and Skip buttons, then set the Action to Schedule or Skip (exclude) for each device.

   If the devices were not previously scheduled, the Action defaults to Schedule and you can continue with no other action set up.

   If you set the Action to Skip for all devices in the list, there is no other setup required. Click Cancel to exit the Wizard.

5. Click Next to display the Scan devices dialog.

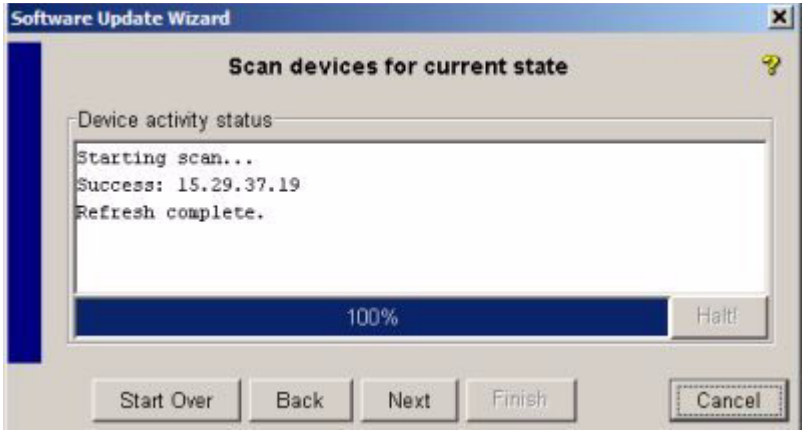


Figure 8-24. Software Update Wizard, Scan devices dialog

The wizard will scan to get the current software state for each device.

6. When the scan (Refresh) is complete, click Next to display the Select Version dialog.

   PCM will display a warning dialog similar to the following figure.

   Click OK to close the dialog and continue.

Figure 8-25. Software Update Wizard, Select version dialog

The Primary column lists the primary software image (primary flash) found on the device. The Secondary column lists the secondary software image (secondary flash) found on the device, if any. An asterisk (*) next to the software version indicates the software image that is currently running, or "boot flash". In some cases you may use the Secondary image

until you have determined compatibility between newer software versions and your existing device configuration. Note that secondary images are only available in dual image devices.

7. Select which software image you want to update on the device, Primary or Secondary.
8. Click the Select Version box to enable the software version pull-down menu, then select the version you want to upload to the device. The pull-down menu lists all software versions currently available for the device.

   To update all devices to the newest software available, click Set all to latest version.
9. Click Next to display the Setup dialog.

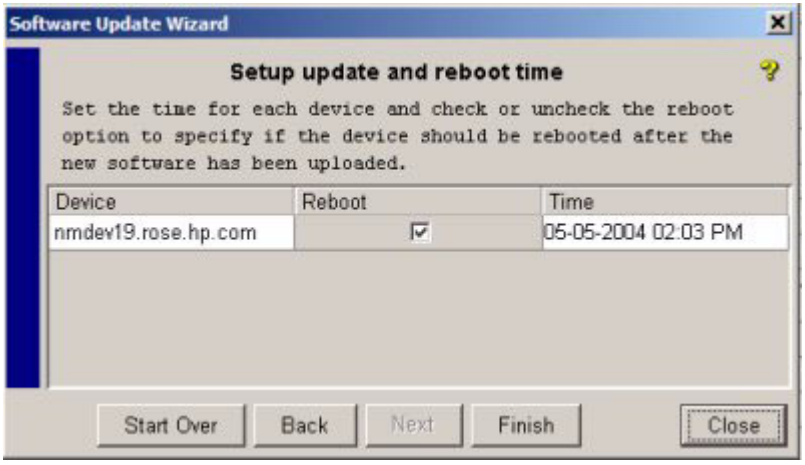


Figure 8-26. Software Update Wizard, Setup update dialog

10. The software update Setup will have the Reboot option selected (checked) by default. This indicates that the system should be automatically rebooted after the software is updated. If you do not want the system to be rebooted, de-select the Reboot option.
11. Set the Time that you want the software update to be performed. You can type in the date, or use the buttons to increase or decrease the entries for date and time.

Caution: If you enter a time that is earlier than the current date and time, and there is a more recent software update, PCM will attempt to perform the update and reboot the switch immediately.

The system will be rebooted on the currently running software. If you selected to update the Secondary software image, and the Primary software image is the currently running version on the device, the device will be rebooted using the Primary image, not the updated software version. To reboot the device using the updated software version, you will need to do a manual reboot with the Secondary software image.

12. Click Finish to save the Software Update schedule and exit the Software Update Wizard.

Reviewing Software Update Status

To review scheduled switch software updates, select a Device Group node in the navigation tree, then click the Software Update Status icon in the main PCM toolbar.

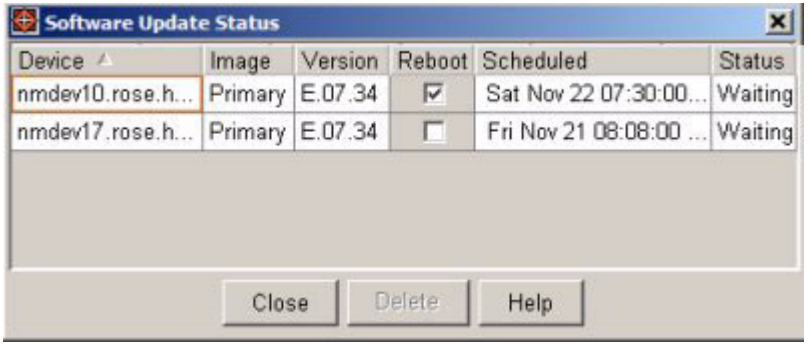


Figure 8-27. Switch Software Update Status dialog

The Software Update Status dialog displays the devices currently set up in the software update schedule with the following information:

- **Device** - Name or IP address of the device to be updated.
- **Image** - The software image to be updated, primary or secondary.
- **Version** - The version number of the software update
- **Reboot** - A check mark indicates that the device will reboot automatically after the software is updated.
- **Scheduled** - Date and time the software update is scheduled to occur.
- **Status** - Current status of the software update. Possible status types are: Waiting, Update Completed, Error (update failed).

Deleting Scheduled Software Updates

To delete a device from a scheduled software update, select the device in the Software Update Status dialog, then click Delete. Click OK in the confirmation pop-up to complete the process. The device will be removed from the software update schedule and the Software Update Status dialog will be updated.

To delete an entire Software update schedule, use the Software Update Status dialog to delete each of the devices included in the schedule.

Use the Software Update Wizard if you want to exclude (skip) a device from a scheduled software update without deleting it from the schedule.

This page is intentionally unused.

Using VLANs

Chapter Contents

About VLANs

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.

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

At default settings, all ports on HP ProCurve 2500, 2800, 4100gl, and 5300xl series switches are members of the default VLAN, with a VLAN ID of 1 and VLAN Name DEFAULT_VLAN. This means that, until you have defined additional VLANs, all of the hosts connected to these switches are in the same VLAN.

The default VLAN is also the primary VLAN. The primary VLAN is the VLAN the switch uses to run and manage DHCP or Bootp, and stacking features. You can designate another VLAN as primary; however it must be a static VLAN, it cannot be a dynamic (GVRP learned) VLAN.

You can use the PCM+ VLAN Manager to partition switches into multiple virtual broadcast domains by adding one or more additional VLANs and configuring ports for the new VLANs. You can change the name of the default VLAN, but you cannot change the default VLAN’s ID (which is always “1”). Although you can remove all ports from the default VLAN, this VLAN is always present; that is, you cannot delete it from the switch.

For a more detailed description of VLANs and GVRP, please refer to the "Management and Configuration Guide" for your switch.

Viewing VLAN Groups (Maps)

To view a listing of currently configured VLANs in your network, expand the Network Map node in the navigation tree, then click the VLANS node.

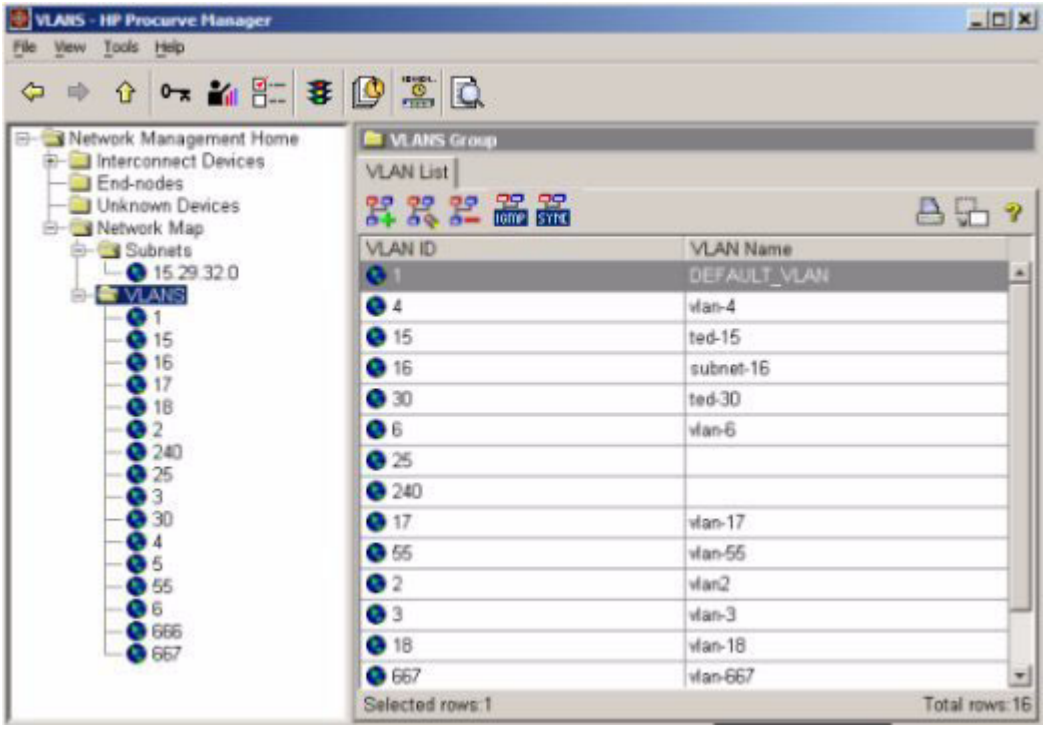


Figure 9-1. VLAN List

You can click on the VLAN in either the navigation tree or the VLAN list to view the VLAN Map.

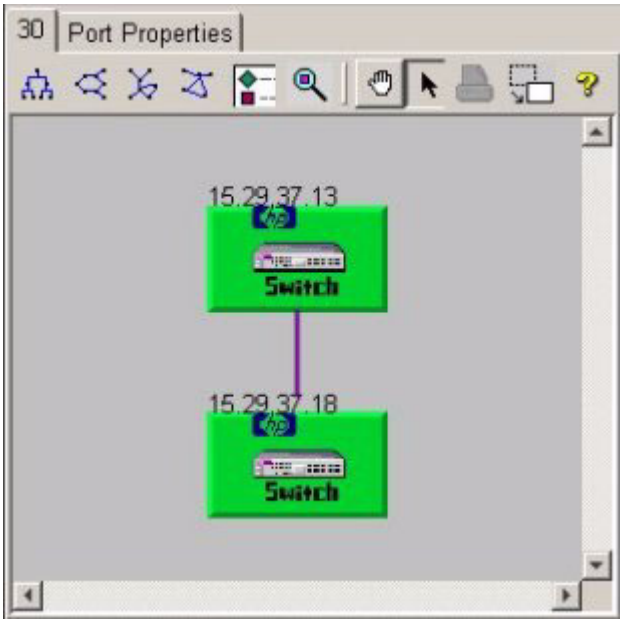


Figure 9-2. VLAN Map display

The VLAN ID (VID) is shown on the tab for the display, and the Port Properties tab is enabled. Otherwise, the map functionality is the same as described in Chapter 4, “Using Network Maps”.

To review the port properties for the VLAN, click the Port Properties tab. This is a view only display, you cannot alter the port properties in this screen. Refer to the discussion of VLAN Port configuration on page 9-8, or “Modifying Port Assignments” on page 9-21 for more information.

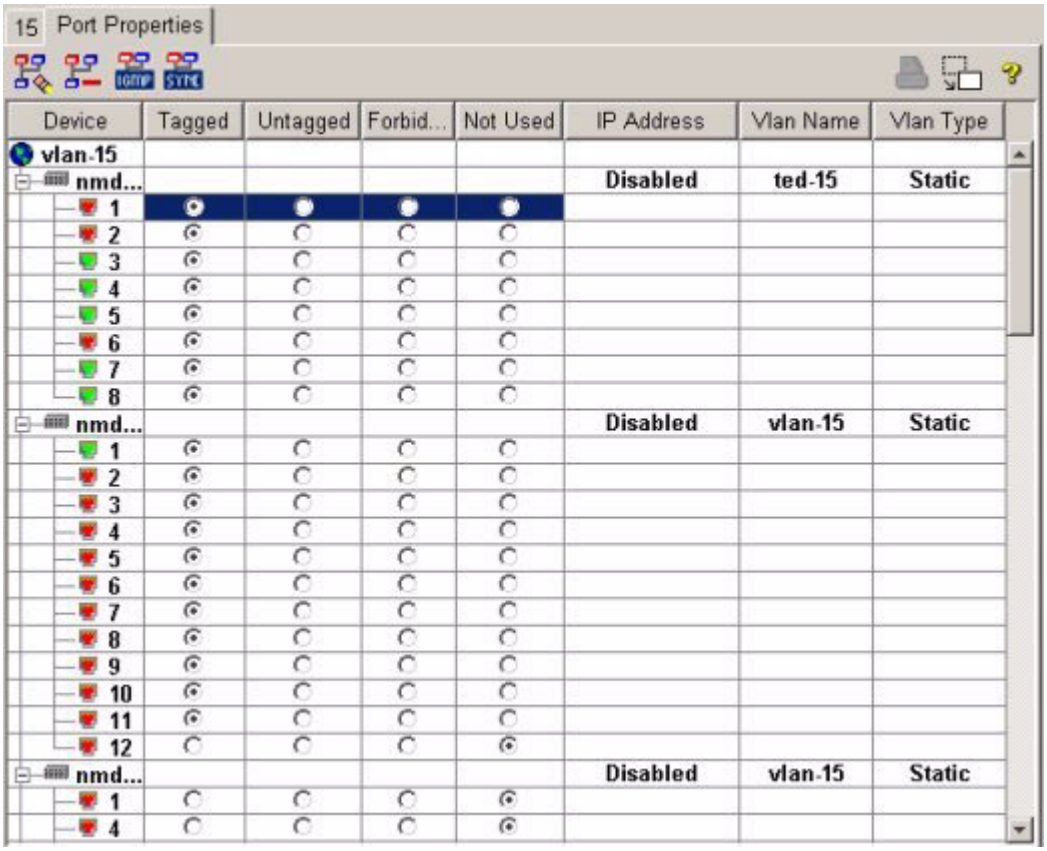


Figure 9-3. VLAN Port Properties display.

The VLAN Port Properties display lists

- The device and ports
- The port properties, one of:
  - Tagged: Port can be included in multiple VLANs.
  - Untagged: Port can be included in only one VLAN.
  - Forbidden: Port cannot be included in this VLAN.
  - Not Used: The port is not included in this VLAN.
- IP Address if applicable
- VLAN Name
- VLAN Type (static or dynamic)

Creating a VLAN

To create a new VLAN, click the Create button in the VLANs List toolbar, or right click the VLAN node in the navigation tree and select Create VLAN from the menu.

This will launch the Create VLAN Wizard which will guide you through the process of creating a VLAN. The following examples of the Create VLAN Wizard dialogues explain the data needed to create a VLAN.

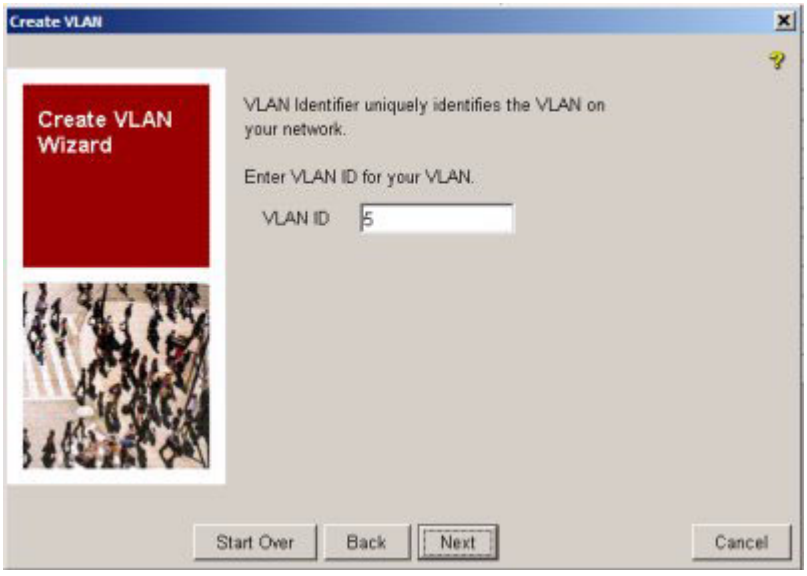


Figure 9-4. Set VLAN ID dialogue

Enter VLAN ID. This is a numeric value between 2 and 4094. The number 1 is reserved for the default VLAN.

Click Next to continue with selecting the devices to be included in the VLAN.

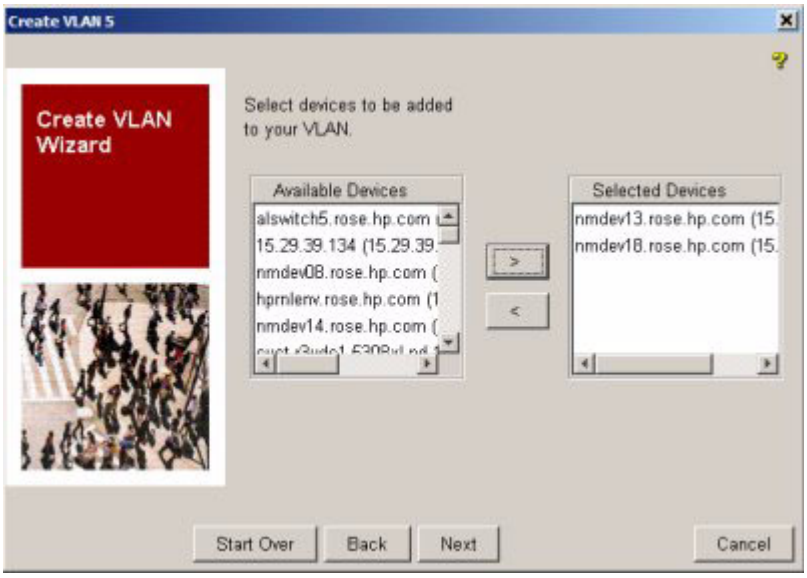


Figure 9-5. Select VLAN devices dialogue

Select the switches to be included in the VLAN from the list of available devices. Use the buttons to move devices to the Selected Devices list, or back to the Available Devices list.

In the next dialogue, you will configure how the IP Address information for the VLAN will be determined, and configure the ports for each device to be included in the VLAN.

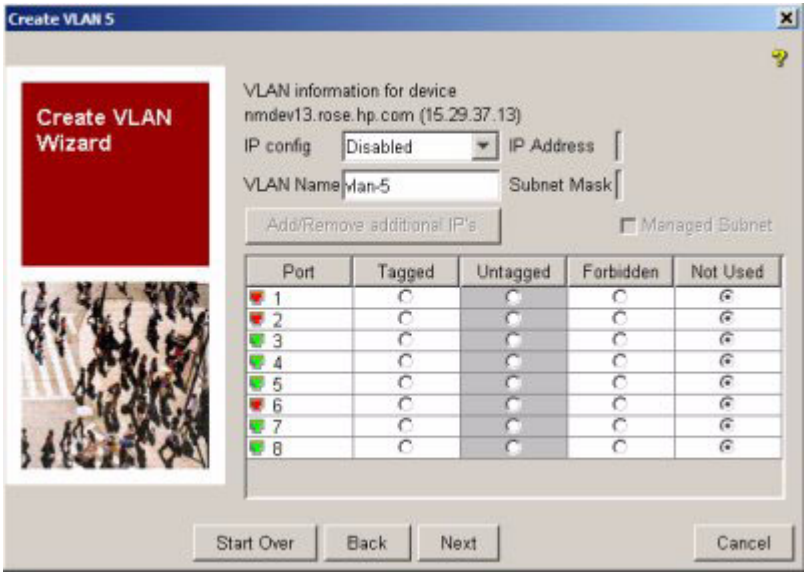


Figure 9-6. VLAN Port configuration dialogue

Use the drop down menu to select the way that you want the IP addresses determined for the VLAN:

- **Manual**: Set the IP address at the console. When selected, the IP Address and Subnet Mask fields will be enabled so you can type in the IP Configuration information.
- **Disabled**: IP is disabled and there is no access to management or telnet. NOT RECOMMENDED
- **DHCP/Bootp**: The Bootp (or DHCP) protocol automatically sets the IP Address. This is used for dynamic VLANs with devices that support GVRP (IEEE 802.1Q standard)

Use the radio buttons to select the VLAN option for each port. If you select the option at the top level (A, B, etc.) for a group of ports, it will be applied to all ports in the group.

The VLAN port options are:

- Tagged: Port can be included in multiple VLANs.
- Untagged: Port can be included in only one VLAN.
- Forbidden: Port cannot be included in this VLAN.
- Not Used: The port is not included in this VLAN.

If the device does not support 802.1Q (GVRP), or GVRP on the device is Disabled, the Forbidden button will be disabled.

For 9300 series switches, if a port has been classified as tagged in another VLAN, the Untagged option is disabled, and vice versa (once classified as untagged, it cannot be tagged in another VLAN).

In the next screen you can review the VLAN port configurations.

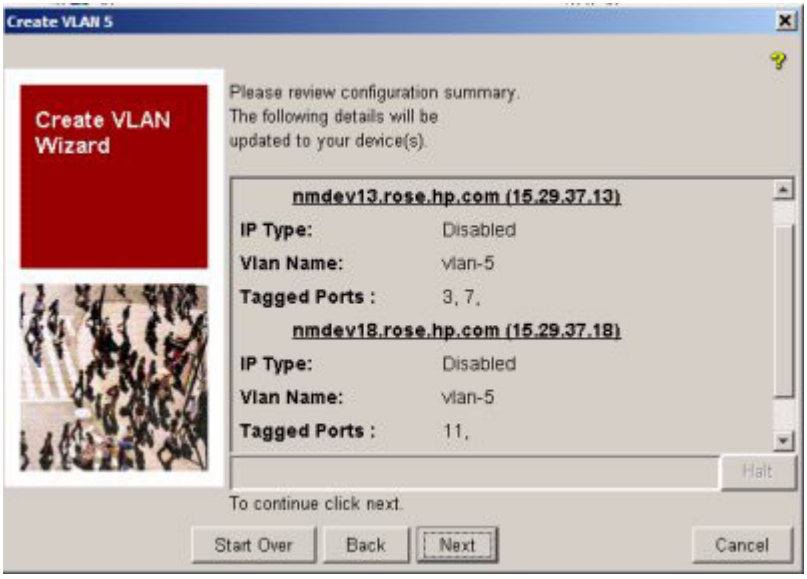


Figure 9-7. VLAN Configuration Review dialogue

If you are not satisfied with the configuration, click Back to return to the configuration screen, or Start Over to return to the Set VLAN ID dialogue.

To complete the Create VLAN process, click Next. Devices shown in the list will be rebooted when the VLAN is configured. To halt the process before it completes, click Halt.

Once the VLAN configuration is complete, click Close in the final Create VLAN dialogue to exit the Create VLAN wizard. The VLAN list should be updated with the new VLAN ID.

Modifying VLANs

To modify a VLAN's configuration, click the VLAN node in the navigation tree to display the list of VLANS. Select the VLAN ID, then click Modify VLAN icon in the toolbar.

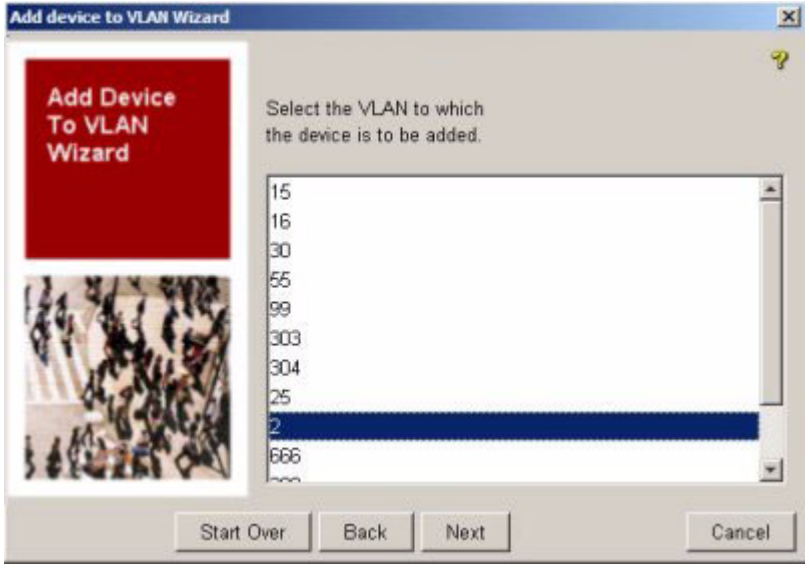
This will launch the Modify VLAN Wizard, which works similar to the Create VLAN wizard. You will be able to change the IP Address settings and Port settings for the devices already included in the VLAN.

When the "Successfully completed" message appears, click Close to exit the Modify VLAN Wizard.

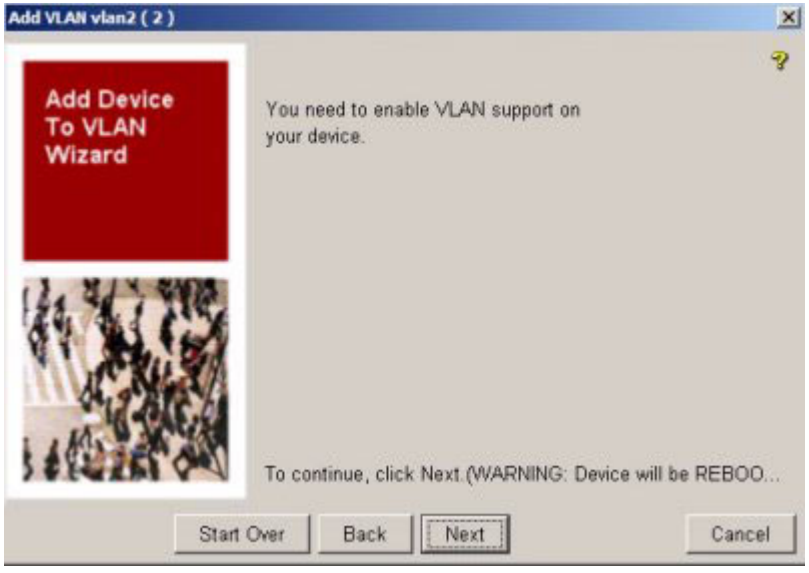
Adding a Device to a VLAN

To add another device to a VLAN that you have already created, select the device in the Devices List or in the navigation tree, then double-click to display the Device Properties window. In the Device Properties window, click the Add to VLAN button in the toolbar. This launches the Add VLAN Device Wizard.

In the next dialogue, you will select the VLAN to which you want to add the device.



If the device is not configured for VLAN support, you will get the following dialogue prior to being allowed to add the device to a VLAN.



Once you have selected the VLAN, you will configure the ports for the VLAN, then proceed through verifying and applying the configuration as described under “Creating a VLAN” on page 9-6.

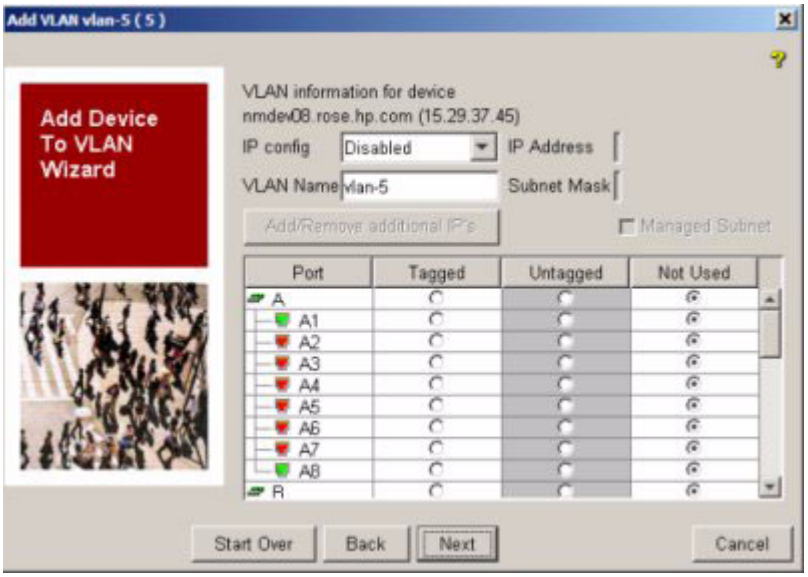


Figure 9-8. VLAN Port Configuration dialog

Synchronizing the VLAN Name

If you add a new device with the wrong VLAN Name, or modify the VLAN name and want to make sure that it appears for all devices (ports) in the VLAN, you can use the "Synchronize" feature to apply the VLAN name to all devices configured in the VLAN.

To synchronize the VLAN name on all devices in a VLAN, navigate to the VLAN’s Port Properties tab (Network Maps->VLANs->VLAN ID), and click the Synchronize icon in the toolbar.

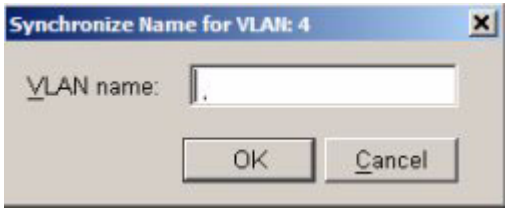


Figure 9-9. Synchronize VLAN Name dialog

Enter the name to be used, then click OK.

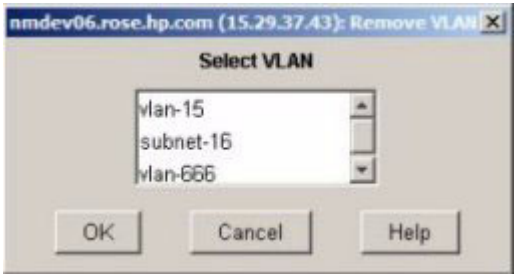
PCM will check the VLAN name to ensure that it is not a duplicate. If it is already used for another VLAN, you will get an error message. Otherwise, the VLAN name will be updated on all devices in the VLAN and the new name will appear in the Port Properties display.

Removing a Device from a VLAN

To remove a device from a VLAN,

- Select the device in the Devices List or the VLAN map, then right click and select Remove from VLAN on the menu or,

- Double-click on the device in the navigation tree or Devices List to display the Device Properties, then click the Remove from VLAN button in the toolbar. The Select VLAN dialogue will be displayed.



Select the VLAN(s) from which the device is to be removed, then click OK. You will get a confirmation dialogue, click yes to complete the process.

To complete the process and have the changes appear correctly in the VLANs Map display, you may need to do a Manual Discovery, or Re-discover on the device.

Making VLANs Static

You can configure a dynamic VLAN (using DHCP/Bootp), then decide at a later time convert it to a static VLAN.

To convert from a VLAN from dynamic to static:

- Expand the navigation tree to select the VLAN,
- Click the VLAN node to display the map.
- Right click on a device in the VLAN map,
- Select the Make VLAN Static option from the menu.

A dynamic VLAN does not have an IP address, it moves traffic on the basis of port membership in VLANs. However, after you convert a dynamic VLAN to a static VLAN, it is then necessary to assign ports to the VLAN in the same way you would for a manually configured VLAN.

Making a VLAN Primary

Because certain features and management functions run on only one VLAN in the switch, and because DHCP and Bootp can run per-VLAN, there is a need for a dedicated VLAN to manage these features and ensure that multiple instances of DHCP or Bootp on different VLANs do not result in conflicting configuration values for the switch. The *primary* VLAN is the VLAN the switch uses to run and manage these features and data. In the factory-default configuration, the switch uses the default VLAN (VID 1) as the primary VLAN. However, to provide more control in your network, you can designate another VLAN as primary.

Designating a non-default VLAN as primary means that:

- The stacking feature runs on the switch's designated primary VLAN instead of the default VLAN
- The switch reads DHCP responses on the primary VLAN instead of on the default VLAN.
- The default VLAN continues to operate as a standard VLAN (except, as noted previously, you cannot delete it or change its VID).
- Any ports not specifically assigned to another VLAN will remain assigned to the Default VLAN, regardless of whether it is the primary VLAN.

Candidates for primary VLAN include any static VLAN currently configured on the switch. (A dynamic—GVRP-learned—VLAN that has not been converted to a static VLAN cannot be the primary VLAN.)

To designate a VLAN as Primary:

- Expand the navigation tree to select the VLAN,
- Click the VLAN node to display the map.
- Right click on a device in the VLAN map,
- Select the Make VLAN Primary option from the menu.

Note that the Make VLAN Primary option is disabled if the VLAN is dynamic.

If you configure a non-default VLAN as the primary VLAN, you cannot delete that VLAN unless you first select a different VLAN to act as primary.

Deleting a VLAN

To delete a VLAN, right click the VLAN node in the navigation tree, then select the Delete VLAN option from the menu, or

Select the VLAN in the VLAN List, then click the Delete button in the VLAN List toolbar.

Prior to deleting the VLAN, make sure that all ports are assigned to a different VLAN. If the ports in the VLAN are all "Tagged" this should not be a problem as they should still be included in the Default VLAN (VID 1). If the Ports are "Untagged" the VLAN manager will re-assign the ports to the Default VLAN.

You cannot delete the Primary VLAN, and you cannot delete the Default VLAN (VID 1).

Modifying VLAN Support on a Device

To modify the VLAN support on a device, double-click on the device in the Devices List or navigation tree to display the Device Properties window, then click the Modify VLAN Support button in the toolbar.

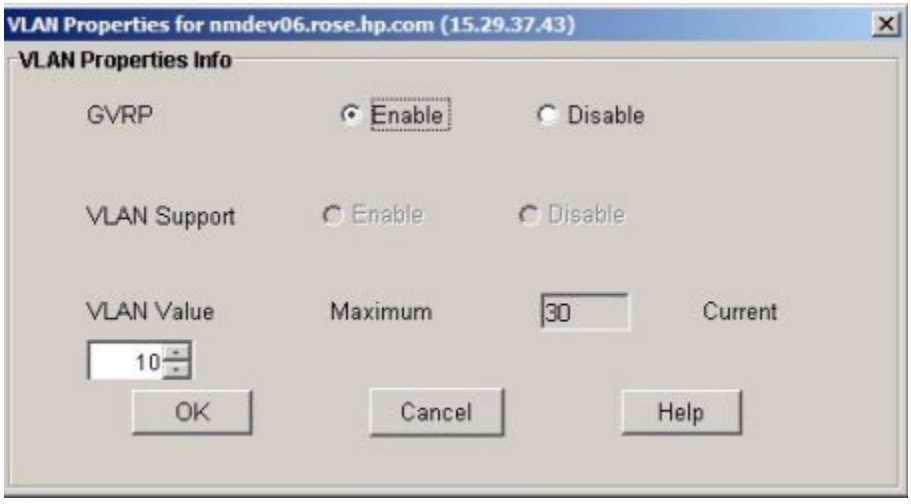


Figure 9-10. VLAN Properties (Support for VLAN on device)

If the device is GVRP capable, you can select to enable or disable support for GVRP.

For devices that are not GVRP capable (such as 1600 and 4000m series) you can select to enable or disable VLAN support.

The VLAN Value indicates the maximum number of VLANs to which ports on the switch can be assigned. The Current field indicated the number of VLANs currently configured per port. You can increase or decrease the current number of allowed VLANs.

NOTE

Enabling VLAN support can cause the selected device to reboot.

VLAN Support on Wireless Devices

Options specific to configuring VLAN support on HP ProCurve Wireless devices are described below.

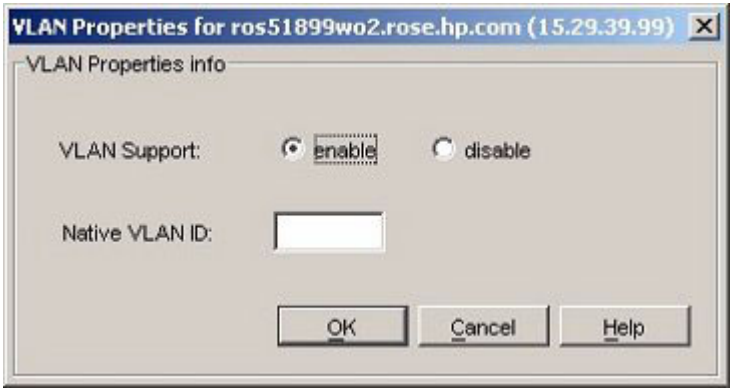


Figure 9-11. VLAN Properties for 420wl

1. Click the Enable button to enable VLAN support.
2. In the Native VLAN ID field, type the VLAN ID of the native VLAN for the device.
3. Press OK to apply these changes to the device.
   Click Cancel to close the window without saving your changes.

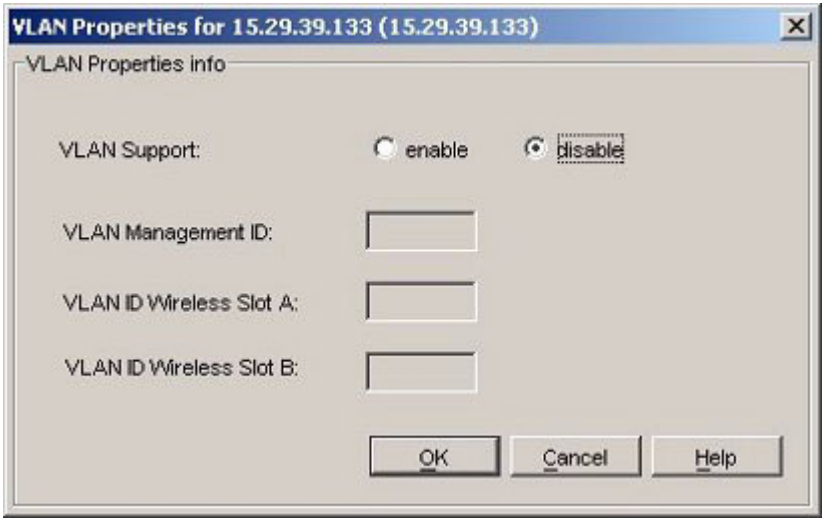


Figure 9-12. VLAN Properties for 520wl

1. To enable VLAN support, click the Enable button in the VLAN support field.
2. In the VLAN Management ID field, type the ID of the VLAN you want to set as the management VLAN. The management VLAN is used by PCM to manage the network.
3. In the VLAN ID Wireless Slot A and Slot B fields, type the VLAN ID of the VLAN you want to associate with each slot on the device.
4. Press OK to apply these changes to the device.
   Click Cancel to close the window without saving your changes.

NOTE: Enabling VLAN support can cause the selected device to reboot.

VLAN Support for 520wl With Version 2.4.5 or Newer Software

If you have installed version 2.4.5 of the 520wl switch software, the VLAN properties dialog will appear as follows:

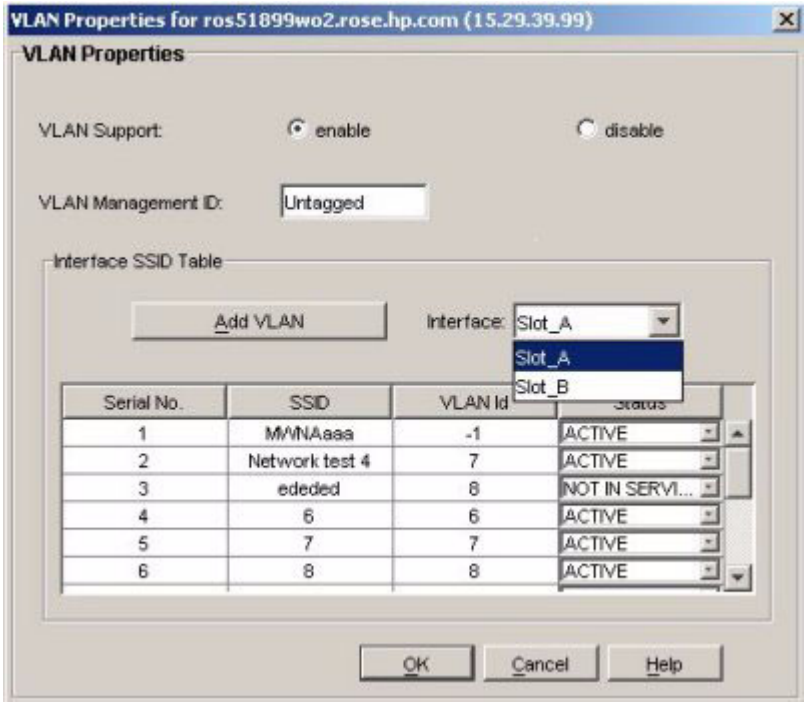


Figure 9-13. VLAN Properties for 520wl, running version 2.4.5 software

1. In the VLAN Management ID field, type the ID of the VLAN you want to set as the management VLAN. You can enter a number from -1 to 4094, or type in "Untagged" (-1 is equivalent to Untagged).
2. You can edit the SSID (network) name. Just click in the SSID field of the table for the interface you want to edit.
3. To edit the VLAN ID, click in the VLAN Id field to select it then enter the number you want to assign.
4. Click in the Status field, then select the Status from the pull-down menu. The options are Active, Delete or Not in Service.

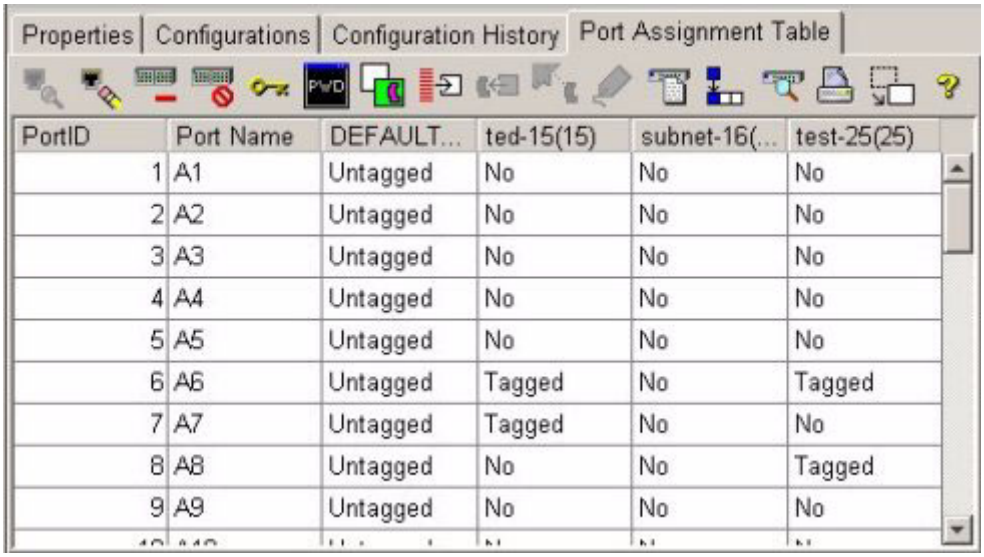
   If you select the Delete option, the VLAN will be removed.
5. Click the Add VLAN button to add a SSID/VLAN pair to an interface.

   a. Enter the VLAN ID, either Untagged, or a number from 1-4094.
   b. Enter the SSID (network name) for the VLAN.
   c. Select the Status from the pull-down menu. "Active" or "Not In Service."
   d. Click OK to save the new VLAN configuration and close the dialog.

If the interface (network card) does not support multiple SSIDs, only the SSID and VLAN Id fields are editable, the Status will always be Activ, and the Add VLAN button will be disabled.

Port Assignments on a Device

To review the current port assignments for the Device, click the Port Assignments Table tab in the Device Properties window.



PortID	Port Name	DEFAULT...	ted-15(15)	subnet-16(...	test-25(25)
1	A1	Untagged	No	No	No
2	A2	Untagged	No	No	No
3	A3	Untagged	No	No	No
4	A4	Untagged	No	No	No
5	A5	Untagged	No	No	No
6	A6	Untagged	Tagged	No	Tagged
7	A7	Untagged	Tagged	No	No
8	A8	Untagged	No	No	Tagged
9	A9	Untagged	No	No	No

Figure 9-14. Device Properties: Port Assignments table

The table lists each of the VLANs to which a port is assigned and current configuration of the port VLAN support (tagged, untagged, etc.)

Modifying Port Assignments

Click the Modify Port Assignments icon in the toolbar to change the VLAN port assignments. This will launch the Modify Port Assignments window.

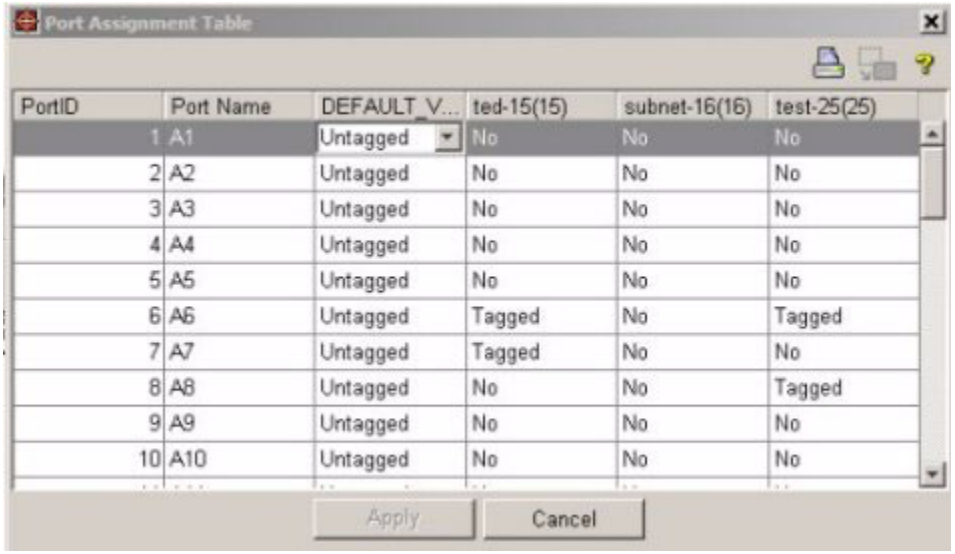


Figure 9-15. Modify Port Assignments window

To modify port assignments, click on the VLAN Port properties cell in the table. This will enable a pull-down menu you can use to select the Property you want to have for the port in that VLAN. The VLAN port options are:

- Tagged: Port can be included in multiple VLANs.
- Untagged: Port can be included in only one VLAN.
- Forbidden: Port cannot be included in this VLAN.
- No: The port is not included in this VLAN.

Change the port properties as needed, then click Apply to save the changes and close the Modify Port Assignment Table.

Modifying GVRP Port Properties

To modify VLAN support by individual port on a device that supports GVRP, click the Modify GVRP Port Properties button in the Port Assignment Table toolbar.

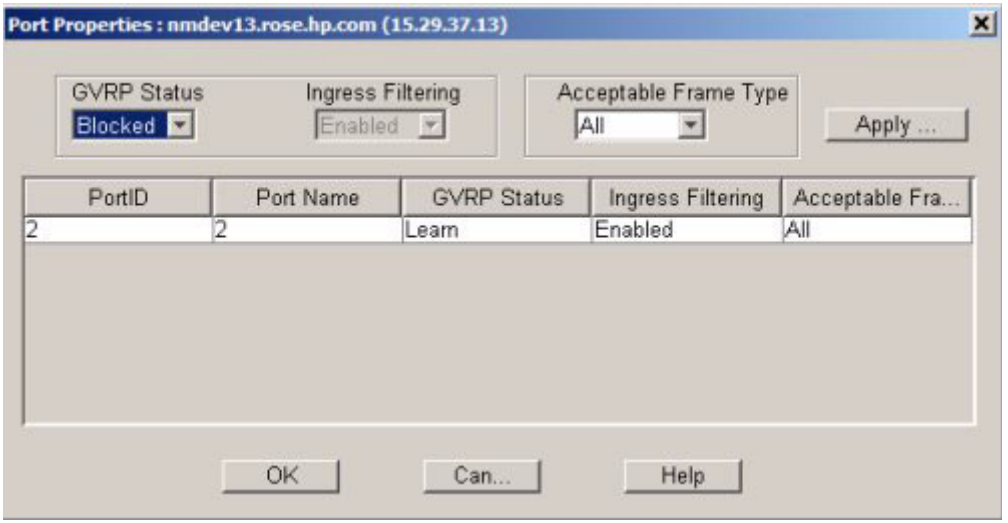


Figure 9-16. Device Properties: Port Properties dialogue.

Select the GVRP status for the port: Blocked, Learn, or Disabled.

Select the Acceptable Frame Type: All or Tagged.

Click Apply to update the Port Properties display, then click OK to close the dialogue.

Using IGMP to Manage Multicast Traffic

This section describes how to configure IGMP controls using PCM+, to reduce unnecessary bandwidth usage on a per-port basis in your VLANs.

In a network where IP multicast traffic is transmitted for various multimedia applications, you can reduce unnecessary bandwidth usage on a per-port basis by configuring IGMP (Internet Group Management Protocol controls). In the factory default state (IGMP disabled), the switch simply floods all IP multicast traffic it receives on a given VLAN through all ports on that VLAN (except the port on which it received the traffic). This can result in significant and unnecessary bandwidth usage in networks where IP multicast traffic is a factor.

Enabling IGMP (on switches that support it) allows the ports to detect IGMP queries and report packets, and manage IP multicast traffic through the switch. Using IGMP, switches can be configured to direct the multicast traffic to only the ports where needed. If multiple VLANs are configured, you can configure IGMP on a per-VLAN basis.

For a more detailed description of using IGMP on HP ProCurve devices, refer to the "Management and Configuration Guide" for your switch.

Enabling IGMP on VLANs

IGMP configuration on the switch operates at the VLAN context level. If you are not using VLANs, then configure IGMP in VLAN 1 (the default VLAN) context.

To enable IGMP settings on a VLAN, select the VLAN node in the navigation tree and display the Port Properties tab.

1. Click the IGMP icon in the toolbar to launch the IGMP Settings Wizard. (You can also select the IGMP Settings option from the right-click menu.)
2. Click Next in the "Welcome" dialog to continue.

Figure 9-17. IGMP Device Selection dialog.

3. Select the device(s) on which you want to change the IGMP settings, then click Next.

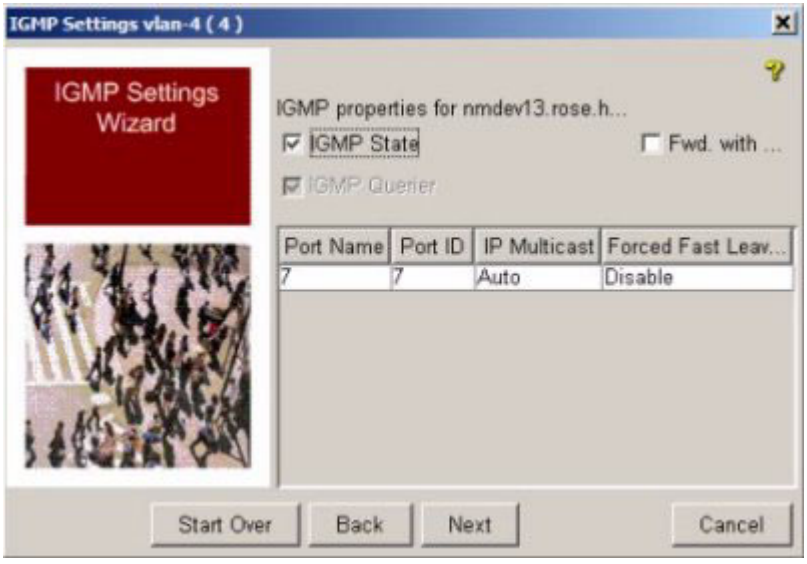


Figure 9-18. IGMP Properties dialog

4. Use IGMP Settings dialog to enable or disable multicast operations. The wizard lists the following information about ports on the selected device:
   - Port Name: The name used to identify the port
   - Port ID: The port number
   - IP Multicast: Auto/Blocked/Forward**:** Indicates the individual ports are configured to one of the following states:
   - **Auto** (the default): Causes the switch to interpret IGMP packets and to filter IP multicast traffic based on the IGMP packet information for ports belonging to a multicast group. This means that IGMP traffic will be forwarded on a specific port only if an IGMP host or multicast router is connected to the port.
   - **Blocked:** Causes the switch to drop all IGMP transmissions received from a specific port and to block all outgoing IP Multicast packets for that port. This has the effect of preventing IGMP traffic from moving through specific ports.
   - **Forward:** Causes the switch to forward all IGMP and IP multicast transmissions through the port.
   - Forced Fast Leave: indicates whether "Forced Fast Leave" is enabled or disabled. Where a port is connected to multiple end nodes, this feature improves blocking of unnecessary IGMP traffic to the port. (Refer to the discussion of "Automatic Fast-Leave IGMP" in the "Management and Configuration Guide" for your switch for details on using this option).

5. To configure IGMP settings for the device:
   a. To enable IGMP on the device, click the IGMP State checkbox.
   b. To disable the IGMP Querier on the selected device, click the IGMP Querier Mode checkbox. (The default is "enabled")

      The IGMP Querier eliminates the need for a multicast router. HP recommends that you leave the IGMP Querier enabled even if a multicast router is performing the querier function in your multicast group.

      NOTE: IGMP Querier can only be enabled if an IP address is configured for the VLAN.
   c. To give IGMP traffic a higher priority than other traffic, check the IGMP Forward with High Priority checkbox. When this feature is disabled, the switch or VLAN processes IP multicast traffic and all other traffic in the order received.

      NOTE: The Forward with high priority setting is not available when configuring IGMP settings for 9315, 9308, 9304, 6208, and 6308 switches.

d. Click Next.

e. Click in the IP Multicast column to change the setting an individual port. When you click in the field a drop-down menu is enabled from which you can select Auto, Forward, or Blocked

f. Click in the Forced Fast Leave column to select Enabled or Disabled for individual ports.

Repeat the IGMP configuration described above for each of the VLAN devices you selected.

After the final device is configured, the IGMP Settings Summary dialog will be displayed.

Figure 9-19. IGMP Settings Summary dialog

6. Review the IGMP configurations

   To change the settings, click Back or Start Over, and modify the settings as needed.

7. If the settings are correct, click Next to download the new settings.

   Click Halt to stop the download if needed.

8. Check the results to ensure that the settings were downloaded successfully, then click Close to exit the IGMP Wizard.

IGMP Settings for Routing Switches

For the HP ProCurve Routing Switches, series 93xx, 62xx, and 63xx, the IGMP settings are configured somewhat differently than for other supported-Switches.

Figure 9-20. IGMP Setting for Routing Switches

To configure IGMP on routing switches:

1. Click the Enable radio button.
2. Set the IGMP Querier Interval (the frequency the device will query for group membership). The value can be from 1 to 3600 seconds.
3. Set the IGMP Group Membership Time (the value after which the group membership becomes inactive). The value can range from 1 to 7200 seconds.
4. Click OK to save the settings and close the window.

Modifying IGMP Settings

To modify the IGMP Settings on a VLAN, use the IGMP Settings wizard as described for "Enabling IGMP on VLANs" beginning on page 9-23.

You can also modify IGMP setting for an individual device in a VLAN.

1. Select the device node in the navigation tree to display the device "Properties" tab.
2. Click the IGMP icon in the toolbar to launch the IGMP Settings Wizard.
3. Edit the IGMP settings as described for enabling IGMP, starting on page 9-23.

This page is intentionally unused.

10

Using Configuration Policies

Contents

How Configuration Policies Work

As the term suggests, *configuration policy* refers to configuration settings you can enforce across a range of devices on the network. The PCM+ Policy Manager component can be used to define and enforce Community Names, Trap Receivers, Authorized Managers, and Spanning Tree Protocol settings consistently on any "Group" of devices that you define. You can use policies to ensure that the devices targeted by the policy contain the desired settings.

To use configuration policies, you need to:

- Create a device "Group," that is, define the devices to be targeted by the policy.
- Define a Policy, that is, set the parameter to be enforced and specify the target Group to which it will be applied.

Once the Group and Policy are created, you can enforce (apply) the policy directly and/or schedule the Policy for automatic enforcement at a specific time or recurring times.

Also, the policy manager can be used to generate an application event to alert you that device settings need to be changed whenever settings do not match the policy's definition. This is especially useful in detecting possible security or process problems.

For example, an event can be generated when:

- The community name, authorized manager, or trap receiver state of a targeted device is out of compliance with the state defined in the policy.
- An error occurs when attempting to communicate with the targeted device.

Configuring Custom Groups

To create a custom group, expand the Interconnect Devices node in the navigation tree, then click on the Custom Groups node to display the Custom Groups window.

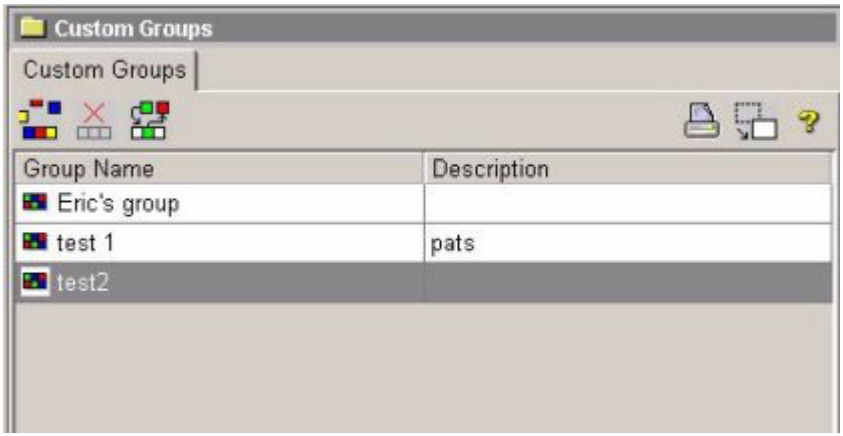
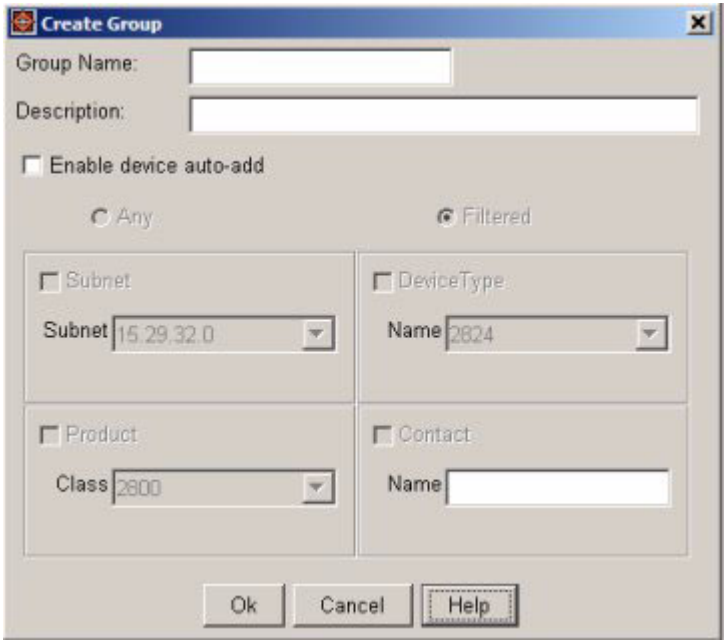


Figure 10-1. Custom Groups window

While custom groups are required for working with Policies, you can also create device groups for other reasons, such as to simplify management tasks, or for monitoring purposes. Regardless of your reason for creating the device group, the procedures for creating Groups are the same.

Creating Groups

Click the "Create a new Group" icon in the toolbar to launch the Create Group dialogue box.



1. Type in the name used to identify the Group. A group name can contain alphanumeric characters, spaces, and special characters.
2. Enter a description for the group in the Description field.
3. Click "Enable device auto-add" to set PCM to add newly discovered devices that meet the group (filter) criteria.

   When using the "auto-add" feature, you must set the "add" criteria.

   - Any: Adds all newly discovered devices to the group.
   - Filtered: Add only devices meeting the specified filter criteria, which can be any one or combination of the following:
     i. Subnet: Enter the subnet address. Only new devices with IP addresses that are members of the specified subnet will be automatically added to the group.
     ii. Device Product: Select the HP ProCurve switch series (2800, 5300xl, etc) from the pull-down menu. Only new devices belonging to that product class will be automatically added to the group.
     iii. Device Type: Select the specific switch name (model) from the pull-down menu. Only new devices of the specified model are automatically added to the group.
     iv. Contact: Enter a contact name. New devices with this contact name configured will be added automatically to the group.

4. Click **OK** to save the new Group and close the Create Group window.

The Custom Groups lists will be updated with the new Group information.

Adding Devices to a Group

To add devices to a group, select the device in the Devices List, then click the Add Device to Group icon in the Device List toolbar.
You can use [Shift + click] or [Ctrl + click] to select multiple devices at once.

This launches the Add Devices to a Group dialogue.

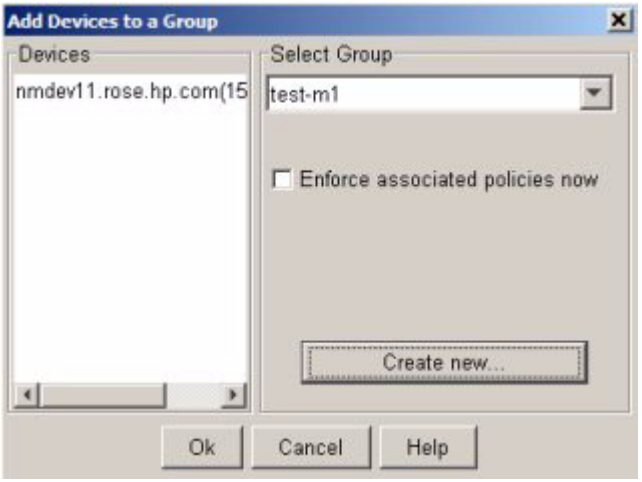


Figure 10-2. Add Devices to a Group dialogue.

1. Use the Select Group pull down menu to assign the group, or you can click Create new... to create a new group.
2. Click the "Enforce associated policies now" ckeckbox if you want any policies configured for the group to be applied as soon as the device is added to the group
3. Click Ok to close the dialogue and return to the main PCM (Devices List) window.

"Easy Add" Method for Creating a Group

You can create a group and add the devices at the same time.

1. In the Devices List window, select all of the devices you want to include in the group, then click the Add Devices to Group icon in the toolbar.

2. In the Add Device to Group dialogue, click Create new... to display the Create Group dialogue. Enter the Group Name and Description, click Ok to return to the Add Devices dialogue, then click Ok in the Add Devices dialogue.
   The Custom Groups list is updated with the new Group information.

Reviewing Group Information

To review the devices included in the Group, expand the Custom Groups node in the navigation tree, then select the Group name to display the device list for the group.

Easy Update of Group Membership

Use the Group Membership Wizard to take advantage of the device auto-add feature and quickly add new devices or remove devices from the group.

1. Select the Group you want to update from the Custom Groups window, or under the Groups node in the navigation tree.

2. Click the Group Membership icon in the toolbar to launch the Group Membership Wizard.

3. Review the group information. If you want to change the group name, click Modify group... to launch the Modify Group dialogue end edit the name or filters.

   Click Next to proceed with the automatic update.

4. Click to select the automatic update options you want to apply when adding members to the group.
   - Remove devices not matching filters will cause the wizard to remove devices that are currently members of the group but that no longer meet the criteria of the filter. If unchecked, no members will be removed.
   - Apply associated policies to new members will cause any policies associated with this group will be executed against the new devices that are found and added to the group.
5. Click Find to complete the process. The wizard will display the devices that are found and added, and any devices that are removed.

6. Click Close to exit the wizard

Modifying Groups

To modify a Group:

1. Select the Custom Groups node in the navigation tree to display the Groups table.
2. Select the Group name in the group list.
3.  Click the Modify Group icon in the device list toolbar.

   The Modify Group Name dialogue is displayed, (similar to Create Group) allowing you to edit the Group Name and Description text.
4. Click Ok to save your changes and update the Group information.

An alternate method for launching the Modify Group dialog is:

1. Expand the Custom Groups node in the navigation tree to display the custom group names,
2. Right-click on the group name and select "Modify" from the menu.

The process to add devices to an existing group is the same as described previously, see “Adding Devices to a Group” on page 10-5.

Removing Devices and Groups

To remove a device from a Group:

1. Expand the Custom Groups node in the navigation tree to display the group names.
2. Click the Group name in the tree to display the Devices list for the group.
3.  Select the device in the Device List, then click the "Remove from Group" icon in the toolbar.
4. Click Yes in the confirmation dialogue to complete the process and update the Group devices list.

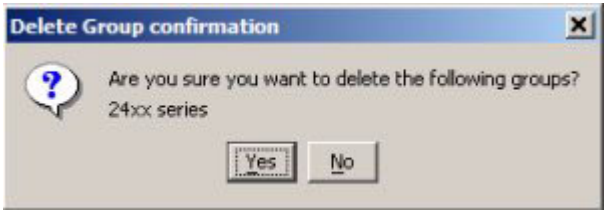
To remove a device from multiple groups at the same time, select the device in the navigation tree or Devices list, then use the right click menu and select the "Remove from group" option. This launches the "Remove from Groups" dialogue.

The Remove button is enabled when you select a group or groups in the list. When you click Remove, the dialogue is closed, and the device list for the selected groups are updated.

Deleting A Group

To delete a Group:

1. Select the Custom Groups node in the navigation tree to display the Groups table.
2. Select the Group name in the groups table.
3. Click the Delete Group icon in the toolbar. A confirmation dialogue will be displayed.



4. Click Yes to update the Custom Group information.

   Another dialogue indicating the group has been deleted will be displayed. Click OK to close the dialog and return to the PCM window.

An alternate method for deleting a group is:

1. Expand the Custom Groups node in the navigation tree to display the custom group names,
2. Right-click on the group name and select "Delete" from the menu.

Configuring Policies

Defining a policy and targeting a group of devices ensures that specified settings are consistently enforced on the targeted group of devices. You can define and enforce several types of policies on any group of devices.

Click the Policies tab in the Network Management Home window to display the Policies list, which contains the following information about every policy:

Name: The name assigned to the policy

Type: The type of policy (see Policy Types below.)

Enabled: True indicates the policy will be enforced (applied) at scheduled intervals. False indicates the policy is disabled and will not be enforced.

Enforcing Now: True indicated the policy is being enforced at present time. False indicates the policy is not currently enforced.

Last Enforcement: Date and time when the policy was last enforced, either manually or at a scheduled interval.

Details: String provided by the policy when it was last enforced (e.g., Enforcement succeeded)

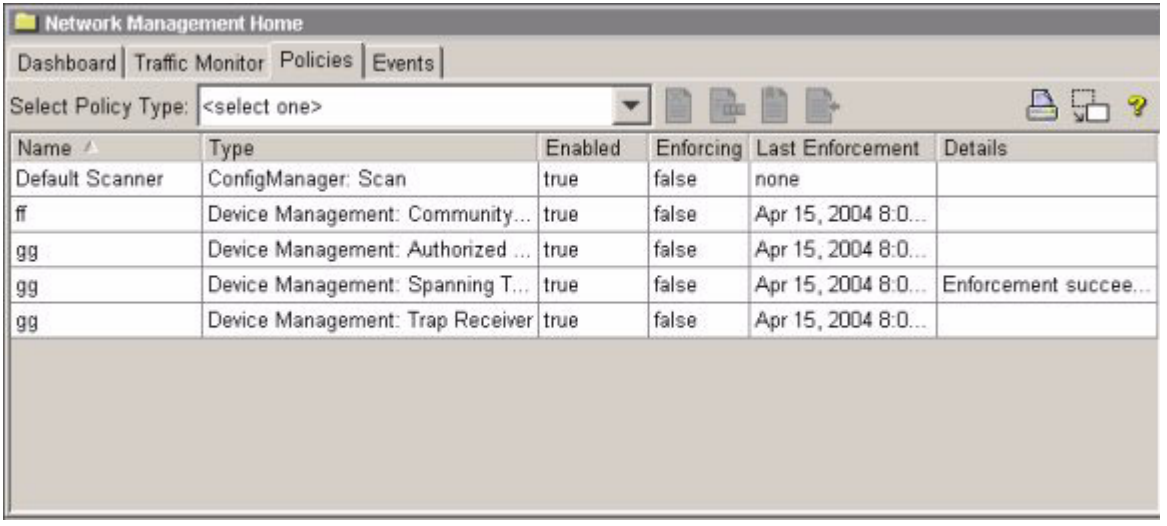


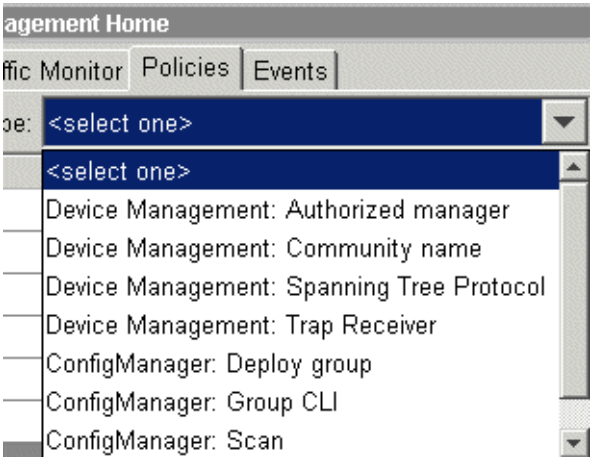
Figure 10-3. Policies window

Creating a Policy

Device Management policies can be used to configure and maintain the SNMP management settings for a group of devices on the network. The parameters you configure in the policy are the same as you configure individually using the PCM Device Manager feature (see Chapter 6, "Managing Network Devices"). Config Manager policies are used for maintaining configurations for a group of swtches. The parameters you use in the policies are the same as described for individual device configuration in Chapter 8, "Managing Device Configurations."

Process Overview

To create a new policy, select the Policy Type from the pull-down menu to launch the "Policy Wizard."



The basic process for creating a policy is:

1. Configure the Policy Properties: define the Policy name and desciption.
2. Select the Targets: select the Groups to which the Policy will be applied.
3. Set the Enforcement schedule for the Policy.
4. Configure the parameters to be included in the Policy. The display for policy parameters will vary based on the selected policy type.

For each Policy parameter, set the Previous device settings (select the radio button at the bottom of the window) to configure the action taken on the device by the Policy enforcement.

- Leave indicates the Policy will allow previous settings on a device to remain in place.
- Clear indicates the Policy will replace the previous settings on a device.

The next section describes the first three steps, common to all policy types, then the specific details for configuring the different parameters for each policy type will be described.

Setting Policy Properties

To set the Policy Properties:

1. Select the Policy type to launch the Policy wizard.

Figure 10-4. Set Policy Properties dialog

2. Enter a Name for the Policy. The data field allows up to 42 alpha-numeric characters. Special characters and spaces are not allowed.
3. Type in a brief description of the policy.
4. Click Next.

Configuring Policy Targets

After defining the Policy name, the next step is to define the target groups, that is the device groups to which the Policy will be applied.

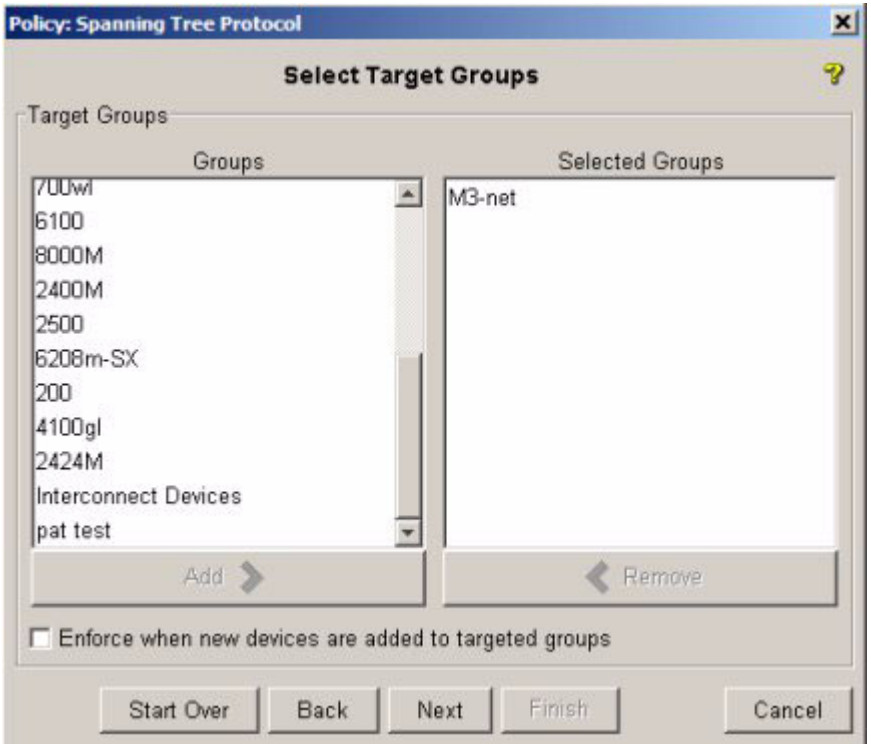


Figure 10-5. Select Target Groups policy dialog

5. Click on a group name in the Groups list, then click Add >.

   The group will be moved to the Selected Groups list.

6. To remove a targeted group for a policy, select the Group name in the Selected Groups list, then click < Remove to move the Group back to the Groups list on the left.

7. To automatically enforce the policy when a device is discovered and added to a targeted group, click the Enforce when new devices are added checkbox.

   Note that the automatic enforcement option is not available for all policy types.

8. Click Next.

Scheduling Policy Enforcement

The next step in configuring policies is setting up an Enforcement Schedule.

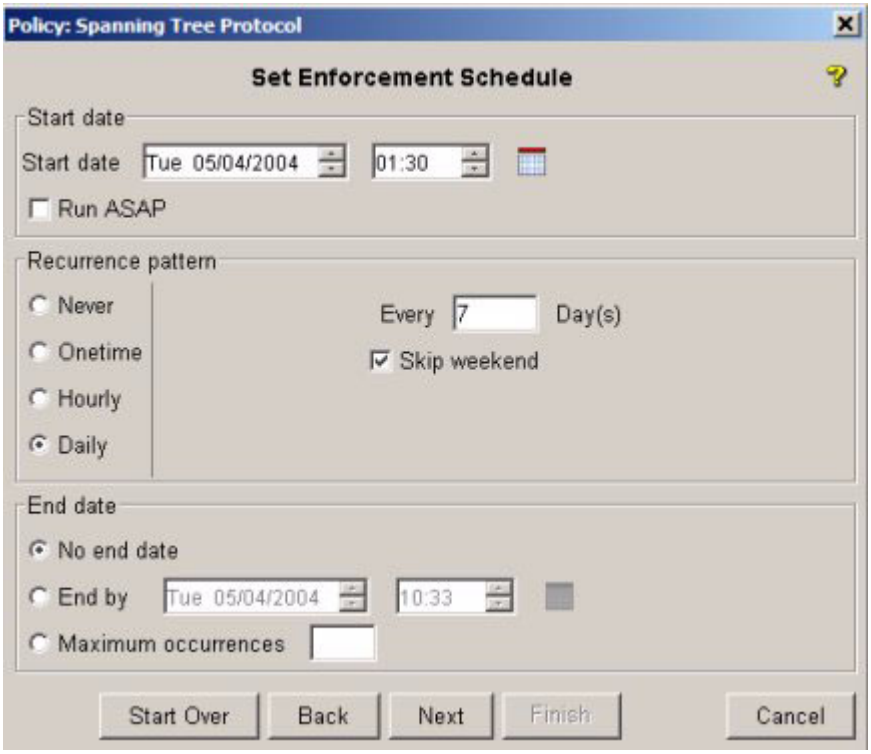


Figure 10-6. Set Policy Enforcement Schedule dialog

NOTE: Only those scheduling attributes relevant to the type of policy being created will be available.

9. Set the Start Date for enforcement of the policy. The default is the date and time the policy is created.

   You can type in a new date and time, or use the arrows to increase or decrease the date and time entries. Note that the time clock uses 24 hour format; thus a time of 22:00 is used to indicate a start time of 10:00 pm.

   Check (click) the Run ASAP checkbox to enforce a policy as soon as possible after the start date. This is especially useful when a policy is re-enabled (after being disabled) . The policy will be enforced immediately if it missed a scheduled enforcement time while disabled.

10. Define the schedule enforcement interval using the Recurrence pattern options:

Table 10-1. Recurrence Pattern Options

If you select...	Do...
Never	No further action is required (Policy definition is saved, but will not be enforced).
One time	No further action is required (the currently scheduled time is used with no recurrences).
Hourly	Type the number of hours and minutes to wait between enforcements. If you do not want the policy enforced on Saturdays and Sundays, check the Skip weekend checkbox.
Daily	Type the number of days to wait between enforcements. If you do not want the policy enforced on Saturdays and Sundays, check the Skip weekend checkbox.
Weekly	Check the boxes for the days of the week you want to enforce the policy.
Monthly	Click the Last day of the month button to enforce the schedule on the last day of the month. OR Click the Day button and use the up or down arrows to select the day of the month.

11. Click the radio button to select No end date, End by, or Maximum occurrences to identify when the schedule should end.
    - If you select No end date, the schedule will run at the selected intervals until the policy is changed or deleted.
    - If you selected End by, click the up and down arrows in the End by field until the desired end date and time are shown.
    - If you selected Maximum occurrences, type the number of times the policy should be enforced before it is disabled automatically.
12. Click Next to continue with the policy configuration.

Configuring Specific Policy Types

From this point forward, the dialogs presented by the Policy Wizard will vary based on the Policy type you selected. The specific configuration parameters for each Policy type are described below in the order in which they appear in the "Select Policies Type" list.

Authorized Manager Policy

For the Device Management:Authorized Manager policy, after setting the properties, target, and enforcement schedule, Policy Wizard will launch the Authorized Manager Configuration dialog, which operates similarly to the Authorized Managers tab in the Device Manager (refer to page 6-10).

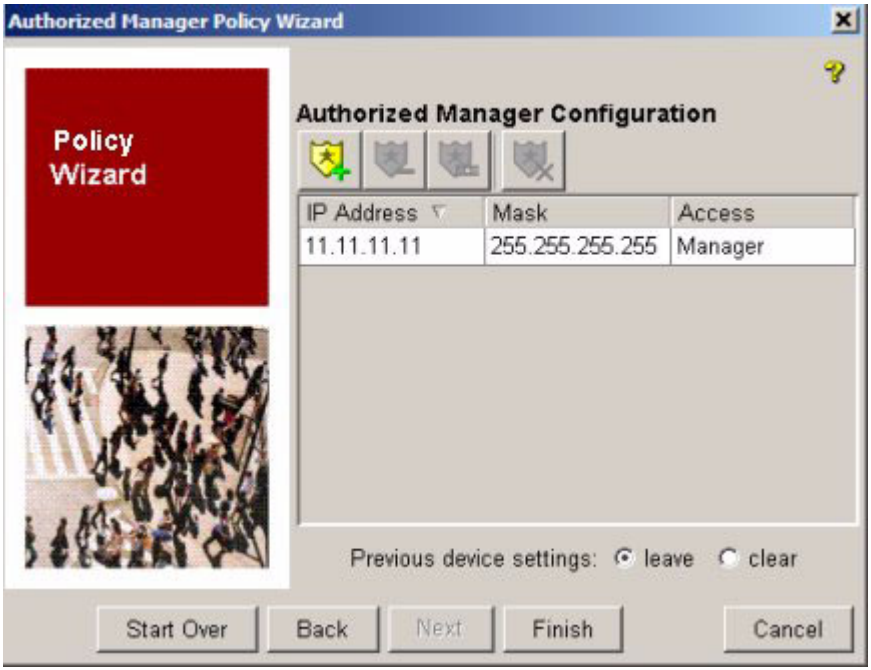
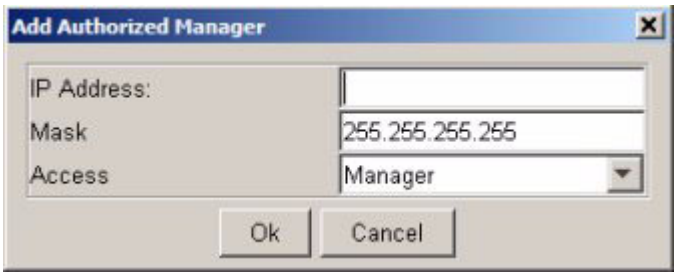


Figure 10-7. Device Management:Authorized Manager wizard

1. To add an Authorized Manager, click the Add button in the toolbar. This will display the Add Authorized Managers dialogue.



2. Enter the IP Address of the management station. The station must have the HP ProCurve Manager application installed.
3. Enter the IP Mask address.
   - The default IP Mask is 255.255.255.255, which 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.)
   - 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.
4. Select the Access level for the station.
   - Manager: Enables full access (read and write) to device configuration functions.
   - Operator: Enables read only functionality to device configurations.
5. Click Ok to complete the process and close the dialog.

   PCM will validate the IP address. If it is invalid you will get an error message, and the Add Authorized Managers dialog remains open so you can edit the IP address and retry.
6. Select the Previous device settings option in the Policy Wizard:
   - Leave saves the previouse device settings when the policy is enforced
   - Clear removes previous device settings when the policy is enforced.
7. Click Finish in the Policy Wizard dialog to save the Authorized Managers policy and exit the Wizard.

Modifying Authorized Managers

To modify an Authorized Manager, click the Modify icon on the toolbar. This will open the Modify Authorized Manager dialogue, which has the same inputs as the Add Authorized Managers dialogue. Edit the existing entries, then click Ok.

Deleting Authorized Managers

To delete an Authorized Manager, select the entry in the Authorized Managers list, then click the Delete icon in the toolbar.

You can also use the Delete All icon to delete all the authorized manager entries, without first having to select the entries.

Community Names Policy

For the Device Management:Community name policy, after setting the properties, target, and enforcement schedule, Policy Wizard will launch the Community Name Configuration dialog, which operates similarly to the Community Names tab in the Device Manager (refer to page 6-6).

Figure 10-8. Device Management:Community Name wizard

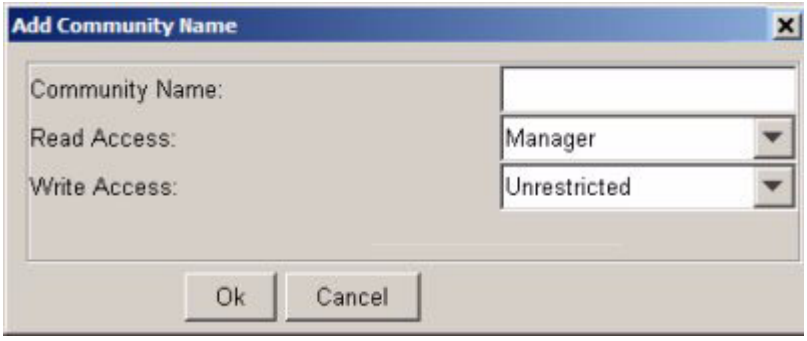
The Community Names Configuration dialog lists the community names configured for the Policy and the following information about each community name:

- Manager- A check mark identifies this as the community name used by the HP ProCurve Manager to communicate with the device.
- Community Name - the SNMP community name.
- Read Access- Permissions that govern the community name's ability to read from devices.
- Write Access - Permissions that govern the community name's ability to write to devices.

The Previous device settings options indicate the action taken on the device by the Policy enforcement.

- Leave indicates the Policy will allow previous Community Name settings on a device to remain.
- Clear indicates the Policy will clear (replace) the Community name settings on the device.

1. To add a Community Name, click the Add icon in the toolbar. This will display the Add Community Name dialogue.



2. Type in the SNMP Community Name to be added, up to 16 characters. The characters "<" and ">" cannot be used.
3. Select the Read Access permission from the menu: Manager provides full read and write permissions, Operator has read-only permissions.
4. Select the Write Access permission from the menu, either Unrestricted or Restricted.
5. Click OK.

If the community name is invalid, you will get an error message. Otherwise, the Add dialogue is closed and the Community Names list is updated with the new entry.

6. Select the Previous device settings option in the Policy Wizard:
   - Leave saves the previouse device settings when the policy is enforced
   - Clear removes previous device settings when the policy is enforced.
7. Click Finish in the Policy Wizard dialog to save the Community Names policy and exit the Wizard.

Note:

If no other community name policies have been defined, the system will set the new community name to be the "Management" community. Thus, if you create a community with Read access = Operator, you will need to create a second community name policy with Read Access = Manager, and then set it as the management community. See “Modifying Management Community Access” on the next page for details.

Modifying Community Names

To modify a Community Name, select a community name in the list then click the Modify icon in the toolbar. This will display the Modify Community Names dialogue, similar to the Add Community Names dialogue shown above.

Edit the community name entries as described in the Add process. When you click OK, a validity check on the community name will be performed. If it is valid, the Community Names list will be updated with the new entry.

Deleting Community Names

To delete a Community Name, select the name in the Community Names list then click the Delete icon in the toolbar. A confirmation dialogue will be displayed.

Click OK to complete the delete process.

Using the Policy Manager, you can delete the Management community name. If you do, the Community name that is at the top of the list will automatically be selected as the default Management Community.

Modifying Management Community Access

When using Policy Manager, the first Community name added is set to the Management community. This is used by PCM for auto-discovery, traffic monitoring, SNMP trap generation and threshold setting. If security for network management is a concern, it is recommended that you change the write access for the "public" community to "restricted."

To change the Management Community, select the Community name in the list, then click the "Set as Management Community" icon in the toolbar.

The "Management" indicator (check mark) will now appear next to the new entry.

Spanning Tree Protocol Policy

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.

For the Device Management:STP policy, after setting the properties, target, and enforcement schedule, Policy Wizard will launch the Set STP State dialog.

1. Click the radio button to specify the Spanning Tree Protocol setting for devices in the target group.
   - Enable STP - enables Spanning Tree Protocol on the device.
   - Disable STP - disables Spanning Tree Protocol on the device.
2. Click Next

3. Click Finish to save the policy and close the wizard.

Modifying an STP Policy

The only modification to STP policies is to enable or disable STP on the target device group.

To modify the STP policy, select it in the Policies [tab] list, then click the Modify icon in the toolbar to launch the STP policy wizard and edit as needed.

Deleting an STP Policy

To delete an STP policy, select it in the Policies [tab] list, then click the Delete icon in the toolbar. Click Yes in the confirmation dialog to complete the process.

The Policy will be removed from the list in the Policies tab display.

Trap Receivers Policy

For the Device Management:Trap Receivers policy, after setting the properties, target, and enforcement schedule, Policy Wizard will launch the Trap Receivers Configuration dialog, which operates similarly to the Trap Receivers tab in the Device Manager (refer to page 6-3).

Figure 10-9. Device Management:Trap Receiver wizard

The PCM management station is set as a default trap receiver for the other devices on the network. You can specify other stations as additional trap receivers or the change the default trap receiver with a Trap Receivers policy.

1. Click the Add Trap Receiver icon in the toolbar to display the Add Trap Receiver dialogue.

2. Enter the IP Address of the device to receive traps.
3. Use the Event log filter drop-down menu to select the types of events the Trap Receiver will accept.
4. Click OK.

A validity check is performed on the IP address to ensure it is a valid IP address, and that it is not a multicast address, loopback address, or the subnet broadcast address of the device.

If it is a valid IP address the Trap Receivers list is updated with the new entry and the Add Trap Receivers dialog is closed.

If the IP address is not valid, an "Invalid IP address" message is displayed and the Add Trap Receiver dialog remains open so you can fix the IP Address and retry.

5. Select the Previous device settings option in the Policy Wizard:
   - Leave saves the previouse device settings when the policy is enforced
   - Clear removes previous device settings when the policy is enforced.
6. Click Finish in the Policy Wizard dialog to save the Trap Receivers policy and exit the Wizard.

NOTE:

When PCM (server) starts up, it binds to port number 162 and that is the port that all incoming traps arrive on. If a previous process is already bound to that port, PCM will not be able to receive traps because the port is in use. Make sure no process is bound to port 162. Examples of applications that bind to port 162 are the Windows SNMP Trap Receiver Service*, TopTools, HP OpenView, MG-Soft MIB Browser Trap Ringer, etc.

In the event that a process was bound to port 162 when ProCurve Manager was started simply terminate the process and restart the ProCurve Manger (server). To restart the PCM server (in Windows):

a. Go to Control Panel->Administrative Tools-> Services.
b. Double click on the HP ProCurve Network Manager Server, click the Stop button, and then click the Start button.

Modifying Trap Receivers

To modify a Trap Receiver, select it from the list, then click the Modify Trap Receiver icon in the toolbar to display the Trap Receiver pop-up dialog.

1. Edit the IP address
2. Edit Event log filters as needed.
3. Click OK to save the changes and update the Trap Receivers list.

Deleting Trap Receivers

To delete a Trap Receiver, select the entry from the list, then click the Delete Trap Receiver icon in the toolbar.

You can use "Shift + click" or "Ctrl + click" to select multiple trap receivers to delete at once.

Click Yes in the confirmation dialog to complete the process.

You can delete all trap receivers at the same time by clicking the Delete All icon in the toolbar.

Click Yes in the confirmation dialog to complete the process.

Deploy Group Policy

The Deploy Group Policy Wizard is used to create a schedule for rolling back to a previously labelled configuration on one or more device groups. For example, deployment is useful when you capture a known good configuration and want to restore that configuration in its entirety or apply it to other devices. For information on creating labelled configurations, refer to “Using Configuration Labels” on page 8-7.

Remember that deployment of a configuration to an HP ProCurve device requires rebooting the device.

Note:

Use the Device Manager for simple tasks like changing the host name, contact, location, community names, and authorized managers. Use the CLI Wizard, Telnet, or Web Agent for more complex changes to a configuration.

To add a Deploy Group Policy:

1. Select ConfigManager:Deploy Group from the Select Policy Type drop-down list on the Policy tab to start the Policy Wizard.

You can also launch the Deploy Group Wizard by clicking the Deploy button on the Configuration History window or other group-related window.

2. In the Set Properties window of the Deploy Group Policy Wizard, type the name that will be used to identify the policy.

   Type a brief description of the policy in the Description field. This description might contain the purpose of the policy or any other information pertinent to the policy.

   In the Rollback Label box at the bottom of the window, click the drop-down arrow and select the configuration you want to deploy. The configuration must be a labelled configuration.

3. Click Next.

4. Select the Policy Schedule options (refer to page 10-14), then click Next.

5. Select the Session Output options:
   a. If you do not want to capture the output for the session, click Next to close the Specify Output Options window.
   b. Click the Capture output to a file checkbox to capture the output for the session.
   c. Type in the file name in which to store the output.
   d. Click the Append checkbox to append the next session output to previous output if the file already exists.

      To overwrite an existing file, ensure that the Append checkbox is not checked.
   e. Click Next.

6. Select the Target Groups (refer to page 10-13), then click Next.

7. Click Finish.

Group CLI Policy

The Group CLI Policy Wizard can be used to execute CLI (Command LIne Interface) commands, or a command 'script' on selected device groups at set intervals.

1. Select ConfigManager:Group CLI from the Select Policy type drop-down list on the Policies tab to launch the Policy Wizard.

   The Group CLI policy wizard functions similarly to the Command Line Wizard, described on page 8-13 of the "Managing Device Configurations" chapter.

   When you have entered the commands you want for the Policy, click Next.

2. Select the Policy Schedule options (refer to page 10-14), then click Next.
3. Select the Session Output options:
   a. If you do not want to capture the output for the session, click Next to close the Specify Output Options window.
   b. Click the Capture output to a file checkbox to capture the output for the session.
   c. Type in the file name in which to store the output.
   The specified file will be placed under the "server\data" directory.
   d. Click the Append checkbox to append the next session output to previous output if the file already exists.

      To overwrite an existing file, ensure that the Append checkbox is not checked.
   e. Click Next.
4. Select the Target Groups (refer to page 10-13), then click Next.
5. Click Finish.

Group Scan Policy

The Scan Policy wizard is used to create a schedule for scanning device configurations on one or more device groups.

To add a scan policy:

1. Select ConfigManager Scan from the Select Policy type drop-down list on the Policies tab to start the Policy wizard.
2. In the Policy Properties window, type in a name to identify the scan policy.

   If desired, type a brief description for the policy in the Description field.

3. Click Next.
4. Select the Policy Schedule options (refer to page 10-14), then click Next.
5. Select the Target Groups (refer to page 10-13), then click Next.
6. Click Finish.

Software Update Policy

Use a Software Update Policy to schedule downloading the index of switch software versions available for devices in the target group. A frequently recurring policy ensures the latest Switch software versions are available for updates.

To add a Software Update policy:

1. Select Software Update:Download Software Index from the Select Policy type drop-down list on the Policies tab to start the Policy wizard.
2. In the Name field of the Select a Name window, type the name you want to use to identify the policy.

   Type a brief description of the policy in the Description field.
3. Click Next.
4. Select the Policy Schedule options (refer to page 10-14), then click Next.
5. Select the Target Groups (refer to page 10-13), then click Next.
6. Click Finish.

Enforcing Policies

You can use the scheduling options when creating or modifying a policy to set recurring enforcement of the policy at specified date and time intervals, or you can enforce the policy manually at any time.

To enforce a policy manually:

1. Click the Policies tab in the PCM home display.
2. Click (select) the policy you want to enforce from the Policies list.
3. Click the "Enforce" icon in the toolbar to execute the policy on devices in the target group.
4. Click Yes in the confirmation dialog to enforce the policy now.

   The Last Enforcement field for the policy will be updated with the current date, indicating enforcement of the policy.

To disable or enable the scheduled enforcement of a policy:

1. Click (select) the policy you want to enforce from the Policies list.
2. Click on the "Enable/Disable" enforcement icon in the toolbar. This icon acts as a toggle that can be used to enable or disable scheduled enforcement at any time.
3. Click Yes in the confirmation dialog to enable or disable enforcement.

   The Enabled field for the policy will change from true to false, or vice versa.

Modifying Policies

To modify a policy:

1. Click the Policies tab in the PCM home display.
2. Click (select) the policy you want to modify from the Policies list.
3. Click the "Modify" icon in the toolbar to launch the Policy wizard.

The Policy wizards work in the same manner as described for creating new policies, simply edit the Policy parameters in the wizard dialogs as needed.

Deleting Policies

To delete a policy:

1. Click the Policies tab in the PCM home display.
2. Click (select) the policy you want to delete from the list.
3. Click the delete icon in the Policies toolbar.
4. Click Yes in the confirmation dialog to delete the policy.

   The policy will be removed from the Policies listing.

This page is intentionally unused.

Index

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

Edition 2
June 2004

Manual Part Number
5990-6046