PREGÃO 118/2003
Pasta 02

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0001
3740
Doc:

You can configure NNM to automatically page or email a specific person whenever an alarm is received about a specific device. You can also configure a pop-up window to appear over the NNM map if a certain event occurs or launch any customized action that you wish.

- Facilitate team communication to eliminate duplicate efforts.

  Your support team can use NNM's Alarm Browser as a prioritized to-do list. Each team member can select issues to work on and change the alarm's status to *Acknowledged*. Everyone on the team will see immediately that the alarm is being addressed.

- Distribute responsibility.

  You can set up custom categories for incoming alarms and configure specific devices to post their alarms to your custom categories. For example, configure the alarms generated by devices in each department to post their alarms to a category identifying the department. Your team members can access the alarm list that applies to them, without needing to sort through alarms for all departments.

Work Sheet for Planning

Group/user: _____

Role/purpose: _____

Organization/Location: _____

Hours/shift: _____

Email address: _____

Phone number: _____

What do they need to know?

How often do they need this information?

Why do they need to know?

Which devices do they need to monitor?

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0002
3740
Doc:

— Every few days?

- Devices that do not require active monitoring.

  Not important enough to warrant generating network traffic (for example individual PCs). Therefore, you can disable NNM's polling of these devices by setting them to *unmanaged* or you can configure polling to run very infrequently.

  Although you configure certain devices or groups of devices to be *unmanaged* by NNM, the device's SNMP agent can be configured to forward traps to the management station if anything goes wrong. These traps will appear as alarms in NNM's Alarm Browser once you configure them to do so by using NNM's event configuration feature.

  NNM can be configured either to include the unimportant devices on your maps or to exclude them from the map.

Work Sheet for Devices

Identify which devices on your network fit into the following groups. Your list will come in handy when you are troubleshooting NNM's initial discovery, when you are customizing NNM's polling configuration, and when you are creating customized maps for your team.

- Mission-critical devices.

  Must be frequently monitored on a proactive basis to ensure continuous service.

- Important (but not critical) devices.

  These devices can be monitored less frequently than mission-critical devices. For example: you may want NNM to monitor some devices every 30 minutes, or every 12 hours, or every 7 days. Decide upon meaningful monitoring frequencies for different groups of your network devices

- Devices that do not require network management.

  These devices do not require active monitoring (their SNMP agents can be configured to forward traps to the management station if anything goes wrong).

TIP

Network devices that did not show up on anyone's worksheet from the previous section in this chapter probably do not need to be actively managed by NNM.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0003
Fls. Nº
3740
Doc:

Starting with a Well-Configured Network

As explained in Chapter 2, "How Does NNM Work?," on page 49, NNM communicates with the devices on your network through standard network protocols. For NNM to gather accurate information, your network needs to be in a well-configured state so that each device can be successfully accessed.

The following aspects of a well-configured network do not need to be in perfect shape on your network before you install NNM. However, the closer you are to having a well-configured network, the quicker and easier it will be to configure NNM. Relevant issues include:

- Consistent IP addressing scheme
- Consistent subnet masks configured
- DHCP address ranges identified
- Consistent name resolution scheme (such as DNS or NIS)
- SNMP agents configured on each device:
  - — Know the agent's GET- and SET-community names
  - — Update the trap-forwarding (trap destination) list to include the NNM management station
  - — Know which MIB is being used and obtain a copy of it to load into the NNM management station's MIB database later on

Consistent IP Addressing Scheme

A list of your *network-level* IP addresses would be handy to have during the initial discovery process so that you can quickly verify that NNM has successfully discovered everything you need. This list could also be used to create a seed file to speed the discovery process.

Remember that all devices that you wish to manage must have a valid IP address. For hubs and other network devices that normally do not have IP addresses and enabled SNMP agents, it is often possible to manually establish them. Determine if the device can support SNMP, then physically visit each device or access it through a terminal and take the necessary steps to assign an IP address and enable the SNMP agent. Contact the device's vendor if you need more information.

Subnet Masks Consistently Configured

If the subnet masks on the management station or configured on your network devices are incorrect, discovery may be different from what you expected. If the subnet mask is too restrictive, you won't discover your whole management domain. If the subnet mask is not restrictive enough, you discover more than you bargained for.

Non-contiguous subnet masks (for example, 255.255.0.255) are not supported by NNM. Also, in hierarchical subnets, two subnets having the same IP subnet address but different subnet masks are not supported. See the white paper about subnet masks ("White Papers" on page 75) for more information.

TIP

NNM does not detect proxy ARP (an alternative to defining extensive routing tables). If NNM is running in an environment using proxy ARP, alarms about misconfigured subnet masks are generated. In this case, these alarms can be ignored.

DHCP Address Ranges Identified

HP strongly suggests that you assign a range of IP addresses to be randomly assigned to mobile computers when they access your network. NNM can handle this range of addresses in a way that does not cause problems as users hook up to and disconnect from the network.

Consistent Name Resolution Scheme

NNM depends upon your network name resolution scheme being in good working order (DNS, NIS, NIS+, NetBios, local hosts files). NNM cannot conduct successful discovery if it is receiving inaccurate information. NNM will exhibit performance problems and erratic behavior when your name resolution scheme is not working. If you have name resolution in place prior to NNM's initial discovery process, hostnames are used for map symbol labels, rather than IP addresses. Hostnames generally make the NNM maps and alarm messages more meaningful to your team.

If you are using DNS, it is recommended that the management station be a caching or secondary name server. Ensure that the management station secondary name server is not serving any other clients.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0004
3740
Doc:

NOTE Point your web browser to `http://www.docs.hp.com` and search for a document titled *Installing and Administering Internet Services* (part number B2355-90147). This document contains information about configuring a caching-only name server.

Quick Check of Your Name Resolution Scheme

To test the health of the name resolution implementation before installing NNM, try the following procedure.

1. Find the `gethost.exe` tool (provided on the NNM installation CD) and copy it to the hard drive of the machine where you will install NNM.

   Windows: *`CD-ROM drive`*`:\support\gethost.exe`

   UNIX: Mount the CD drive,
   `/cdrom/OVDEPOT/OVNNMgr/OVNNM-RUN/opt/OV/support/gethost`

2. Choose an IP address that is not in use on your network.

3. Navigate to the directory where you copied `gethost`. At the command prompt type either:

`gethost -a -i bogusIPaddress`

`gethost -i realHostName`

4. If you receive an immediate answer, your name resolution scheme is in good shape. If your system hangs while trying to formulate an answer, clean up your network name resolution before installing NNM.

NOTE To test the health of the name resolution implementation after installing NNM, see "Opening NNM takes a long time" on page 133.

SNMP Agents and Their MIBs Configured

The SNMP agent on each network device responds to GET and SET requests from NNM and continuously monitors the device upon which it resides. The agent generates and sends SNMP traps to NNM whenever an error condition arises that is defined in the agent's MIB file.

Configure each SNMP agent's community names and trap destination list specifically for your particular network. Obtain a copy of the agent's MIB file so that you can configure NNM to take full advantage of all the management capabilities provided by the agent.

If an SNMP agent is not currently installed on a network device that you need to monitor, contact the vendor of the device.

GET- and SET-Community Naming Scheme

Community names are a lightweight security technique employed by SNMP agent software. If the network management software wants to communicate with the SNMP agent software, both must use the same community name during GET and SET requests and talk over the same port. By default, community names are often set to PUBLIC and the port is set to 161. NNM assumes that these defaults are in use unless you inform it otherwise. Many network administrators change the GET-community name so that hackers cannot obtain sensitive information about their devices. It is even more common for network administrators to change the SET-community name, since knowing this community name enables others to make system configuration changes to the device itself, either inadvertently or maliciously.

In order to work, NNM depends upon successful communication with the SNMP agents installed on your network devices. If the community names have been changed from PUBLIC or the port changed from 161, you need to inform NNM of the new ones. (NNM cannot obtain these automatically because that would defeat the security feature.) NNM tests community names in the file `netmon.cmstr`. See "GET- and SET-Community Name and SNMP Port Issues" on page 145.

Trap Destination List Updated to Include the NNM Management Station

The SNMP agent software continuously monitors its device for error conditions defined in the installed MIB. When an error condition is detected, a trap message is automatically forwarded to all devices listed in the agent's trap-forwarding list. When configuring the SNMP agent on

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0005
3740
Doc:

each network device, configure the agent's trap forwarding list (or trap destination list) to include the NNM management station's host name or IP address. NNM will then receive traps from the device and keep you informed. Refer to the agent's documentation for information about how to do this. See "Ensuring that NNM Receives Traps from Your Network Devices" on page 325.

TIP *HP-UX systems only:* For hosts with HP OpenView SNMP agents, NNM automatically updates the trap forwarding list when the device is discovered, provided that the correct SNMP SET-community name is configured within NNM. See "GET- and SET-Community Name and SNMP Port Issues" on page 145.

Obtain a Copy of the SNMP Agent's MIB File

Often vendors provide custom MIB files that define specific objects for monitoring the particular device. Be sure to request a copy of the custom MIB so that you can install it into NNM's MIB database later on.

NOTE List of all of the MIBs in use on your network devices. These same MIBs will need to be installed on the NNM management station. See "Loading MIBs in the MIB Database" on page 413. After you install the MIB you can configure NNM to handle each trap as you wish. See "Event Configuration Overview" on page 422.

To obtain the most recent version of a MIB file, check NNM's installation CD, contact the vendor who wrote the MIB file, or search the website `ftp://ftp.isi.edu/mib/` for quick access to the MIB file. Make sure the MIB file that you load onto the management station's MIB database is the same version being used by the SNMP agent on your network device.

DMI Service Providers and Their MIFs Configured

If your management station uses a Windows operating system, NNM **automatically subscribes** to receive DMI events from all managed systems running DMI version 2.0.

Keep track of any vendor-specific MIF files being used on these devices. Your list will come in handy later in NNM's configuration process. If your DMI service provider software is using a vendor-specific MIF instead of or in addition to the DMTF's standard MIF, during NNM's configuration process you must configure NNM to understand the custom MIF events.

For information about configuring DMI MIFs, see "DMI Events (Indications)" on page 327, "DMI Browser" on page 417, and "Loading DMI-to-SNMP Event Mappings" on page 419.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0006
3740
Doc:

5 Initial Network Discovery: Options and Troubleshooting

RQS nº 03/2005 - CN - CPMI - CORREIOS
0007
Fls. Nº
3740
Doc:

The first step toward configuring Network Node Manager (NNM) is to install the software and allow initial discovery to run.

NNM automatically discovers each device on your network and its connective relationship to other devices. NNM's object and topology databases store the discovered information and NNM uses this information to draw the default map and set up the event tracking system. After initial discovery has run to completion, you use the map to identify and fix problems on your network.

Often, network administrators with routed environments simply start NNM and allow it to run initial discovery with the default settings. By default, your management domain consists of the network indicated by your *management station's IP address and subnet mask*. NNM discovers everything to the edges of that network and **manages** (monitors) the devices discovered up to the number in your license agreement limit.

If you need to manage multiple networks, you can *add* them to the management domain by:

- Manually selecting symbols on the map and setting them to *managed* (see "Interactively Expand/Limit Your Management Domain" on page 117).
- Automatically setting devices on multiple networks to *managed* by creating and using a seed file, using the `loadhosts` program, and/or increasing the IPX-Hop Count (see "Automatically Expand Your Management Domain" on page 119).

In very large enterprises and bridged environments, the initial discovery process may detect such a large number of devices that managing them all would exceed your organization's and your management station's resources. In this case, you may want to *limit* the number of devices included in the initial discovery process. You can limit initial discovery so that it only includes your organization's mission-critical devices by:

- Manually selecting unimportant symbols on the map and setting them to *unmanaged* (see "Interactively Expand/Limit Your Management Domain" on page 117).
- Creating and using a `netmon.noDiscover` file that specifies which devices to *exclude* from the discovery process, using the `loadhost` program to discover only the devices on your list, creating and using a *discovery filter* that controls which devices or types of devices to

1855

include in the discovery process, using the `oid_to_type` file to unmanage groups of devices, and/or decreasing the IPX Hop Count (see "Automatically Limit Your Management Domain" on page 124).

If your network is quite large, but you don't want to eliminate devices from the management domain, you can visually break the map into smaller units or create multiple maps that draw information from the same databases. You can use the hide feature or map filter to show different aspects of your network on each map. See Chapter 8, "Map Customization," on page 211.

It is also possible to use multiple management stations in a hierarchical arrangement that divides up the management responsibility yet shares critical information. See *A Guide to Scalability and Distribution* for more information.

You start benefiting from NNM immediately. This initial map discovery process may reveal configuration problems on your network, such as SNMP agents that are not communicating properly, incorrect subnet masks or DNS settings, mismatched community names, and unexpected connections to network segments that you do not own. The map is a visual representation of the communications channels established between NNM and the devices in your network. The accuracy of these links determines whether or not NNM can provide valuable information to help you manage your network. Be sure to follow the directions for verifying the accuracy of your maps (see page 109) and to fix any problems before continuing with further customizations to NNM (page 131).

TIP

Your company may have purchased multiple HP OpenView products. If you are using other HP OpenView applications in addition to NNM, you may notice that the menu choices and options provided within the software vary from what is presented in this book. This is because the other HP OpenView applications integrate closely with NNM to take advantage of the features that NNM already provides. Other HP OpenView programs build upon the foundation provided by NNM.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0008
3740
Doc:

Install Network Node Manager (if you have not already done so)

See the *Quick Start Installation Guide* included with the NNM Installation CD for instructions about how to install Network Node Manager. Make sure that your management station meets the minimum requirements before you start.

NOTE

In this manual, `C` and `$LANG` in directory listings are variables for the language currently in use. `C` contains the English version.

Installing IPX Transport Software (Windows only)

For management stations running a Windows operating system:

IPX discovery is an optional component of Windows operating systems. If you want to discover and monitor IPX nodes, be sure to install the NWLink IPX/SPX Compatible Transport network software stack before or during the NNM installation process. These drivers are included with the Windows operating system installation software, but are not installed by default. See the *Quick Start Installation Guide* included with NNM's installation CD for more information.

Establishing Universal Pathnames (UNIX only)

For management stations running a UNIX operating system:

This book uses directory pathnames that are independent of the underlying file structure of the operating system you are using (see your data sheet to learn specifically which operating systems and versions this release supports). For each Network Node Manager directory, a single pathname is used rather than multiple pathnames that vary by system. For example, the pathname for the NNM log file is stated as `$OV_LOG` rather than `/var/opt/OV/share/log` for HP-UX 10.X, 11.X and Solaris 2.X systems.

Take the following steps to set up each user's environment. Setting the universal pathnames and paths as shown is temporary; you will need to do this every time you start a terminal window. Or you can permanently set each user's path by modifying the path in the appropriate files shown below:

If running sh or ksh: Modify the path in the `.profile` file.

If running csh: Modify the path in the `.login` file.

If running VUE: Modify the path in the `.vueprofile` file.

1. If you want to use the universal pathnames that have been incorporated into NNM, you need to *source* the file into your current environment. Use one of the following commands, depending on which shell you are running. If you are not sure which shell you are running, execute:

   ```
   echo $SHELL
   ```

NOTE Be sure to include a space between the `.` and the `/` in the `sh` or `ksh` commands.

If running sh or ksh:

HP-UX 10.X, HP-UX 11.X,
Solaris 2.X `. /opt/OV/bin/ov.envvars.sh`

If running csh:

HP-UX 10.X, HP-UX 11.X,
Solaris 2.X `source /opt/OV/bin/ov.envvars.csh`

See the *ov.envvars* manpage for additional information about this script and information about the universal pathname equivalents.

2. Set the path to include `$OV_BIN` and `$OV_MAN`. Execute the following commands:

   If running sh or ksh:

   ```
   PATH=$PATH:$OV_BIN
   MANPATH=${MANPATH:-/usr/man:/usr/share/man}:$OV_MAN
   export PATH
   export MANPATH
   ```

   If running csh:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0009
Fls. Nº
3740
Doc:

```
set path=($path $OV_BIN)
if (${?MANPATH} == 0)setenv MANPATH "/usr/man:/usr
/share/man"
setenv MANPATH "${MANPATH}:${OV_MAN}"
```

NOTE All NNM documentation referring specifically to a UNIX operating system assumes that you have activated the universal-pathname environment variables.

For example, a written procedure might include the following step:

```
cd $OV_BACKGROUNDS
```

This command takes you to the local directory containing submap backgrounds, and it works regardless of which version of the UNIX file system is involved. Note that if you need to know the actual pathname, you can always enter a command like the following:

```
echo $APP_DEFS
```

The response to this command will be the actual local pathname:

- *HP-UX*: `/usr/lib/X11/app-defaults`
- *Solaris 2. X:* `/usr/openwin/lib/app-defaults`

Discover the Network... Let NNM Do It

Let NNM do the work discovering your network for you. NNM sets up several databases, creates the default map, and establishes communication links for tracking events on your network.

Overview

First NNM's services (background processes) are started. Expect intense polling traffic at first as the network monitoring service, `netmon`, works as quickly as possible to discover each device on your network. An `ICMP ping` is issued for each device identified in any found ARP table and an `snmpwalk` command is issued to gather information about each discovered device. If a serial WAN link is discovered, NNM checks the router's routing table for clues about how to continue with discovery. The frequency of polling for new nodes automatically decreases as fewer new objects are discovered per polling cycle.

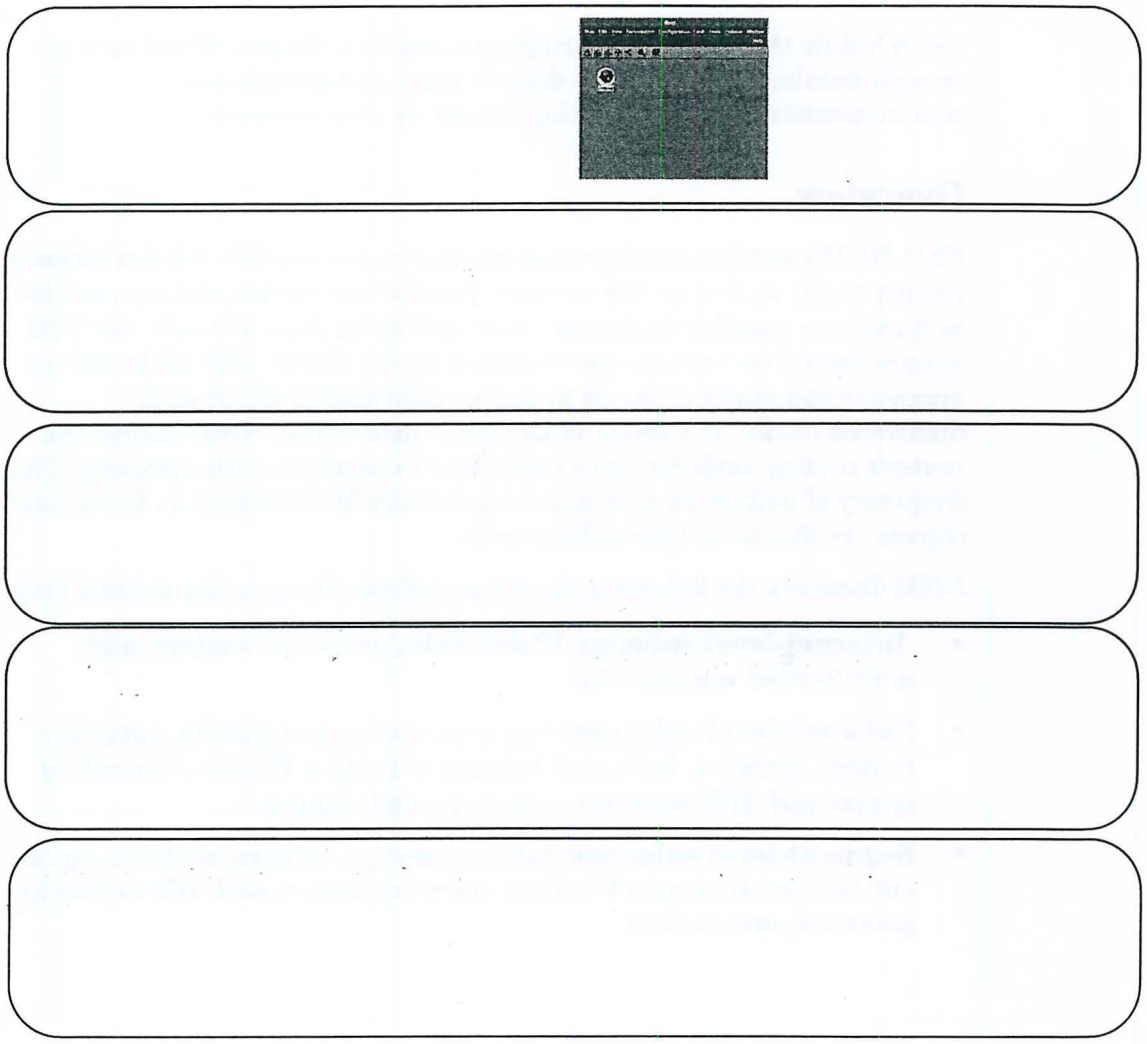
NNM discovers the following objects and places them on the default map:

- **Internet-level submap:** IP networks, gateways, routers, and multi-homed workstations
- **Network-level submaps:** bus, star, and ring segments; gateways, routers, switches, hubs, and bridges; *if using a Windows operating system add:* IPX networks, gateways, and routers
- **Segment-level submaps:** hosts, gateways, routers, switches, hubs, and bridges; *if using a Windows operating system add:* IPX networks, gateways, and routers

RQS nº 03/2005 - C
CPMI - CORREIOS
Fls. Nº 0010
3740
Doc:

- **Node-level submaps:** network interface cards

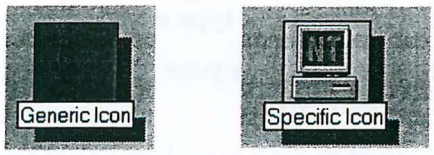
Figure 5-1 A Typical Hierarchy of Persistent Submaps



NNM uses the information about each device gathered by `netmon` to determine the most accurate and descriptive symbol to use on the map. If NNM cannot match the `sysObjectID` to a specific symbol type, the node will be represented as a generic symbol on the map (a shape without a specific descriptive icon inside of the shape). For example, some IP nodes

that are not computers (connectors such as bridges and repeaters) may initially appear on the map as hosts. See "Troubleshooting Discovery" on page 131 for more information.

Figure 5-2 **Generic Computer Icon versus Specific Descriptive Icon**



NOTE

NNM determines which symbol to use for each device by referencing the information contained in two configuration files:

- *Windows:*

  ```
  install_dir\conf\oid_to_sym
  install_dir\conf\oid_to_type
  ```

- *UNIX:*

  ```
  $OV_CONF/oid_to_sym
  $OV_CONF/oid_to_type
  ```

Although the entries in these files are already extensive, you may encounter a situation where you want to make additions or changes to these files. For example, if you see a generic icon on the map and wish to assign a specific icon or if you want to create your own new icons. See the instructions at the beginning of each of these ASCII files. See also the *oid_to_type* and *oid_to_sym* reference pages in NNM's online help (or the UNIX manpages) and Appendix D, "Changing All the Symbols for a Particular Device," on page 661 and Appendix E, "Changing an Object's Vendor and SNMP Agent," on page 675 for more information.

Start the NNM Services (background processes)

NNM starts collecting the information needed to draw the default map as soon as you start the NNM services. The services continually monitor the network and track activity. You need to start them the first time you use NNM; thereafter, they run continually whether or not you have the NNM user interface open. To learn more about these services, see Appendix A, "NNM Services and Files," on page 539.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0011
Doc: 3740

To start the services (background processes):

- *Windows:*
  Select `Start:Programs:HP OpenView: Network Node Manager Admin->NNM Services - Start`.
- *UNIX:*
  As root, at the command prompt, type **ovstart**

  The `$OV_BIN` directory must be in your `PATH`. If not, you must type **$OV_BIN/ovstart** to start NNM.

  See the *ov.envvar* manpage for a complete list of the universal pathnames and their equivalents, and information about a script for setting up environmental variables that will create the pathnames on your system.

Make Sure NNM's Services Are Successfully Running

To generate a status list of the services that make NNM work:

- *Windows:*

  Select `Start:Programs:HP OpenView:Network Node Manager Admin->NNM Services - Status`
- *UNIX:* At the command line prompt, type **ovstatus -c**.

TIP Type **ovstatus -c** for concise, one-line-per-process information.

If any of the services are not successfully running, see Appendix A, "NNM Services and Files," on page 539 for information about troubleshooting services before continuing.

Open NNM

Opening NNM takes a few minutes as the maps are synchronized with the databases. To start NNM's user interface (foreground processes):

- *Windows:*
  Select `Start:Programs:HP OpenView:Network Node Manager`.
  NNM automatically starts all installed and registered applications.

- *UNIX:* At the command prompt, type **ovw**. NNM automatically starts all installed and registered applications.

Configure an Inventory Report

Use the web Reporting interface to configure an inventory report. An inventory report lists the network nodes that are contained in the topology database, organized by subnet. You can use this report to help verify the accuracy of the initial discovery of your network. Refer to the online help for more information on configuring an inventory report.

Let NNM Run Over Night to Populate the Maps

The initial discovery process takes time. We recommend that you let NNM run over night to gather the majority of network information available. As NNM maps your network, it constantly rearranges icons. Therefore, it is best to wait until initial discovery has finished before exploring the default map.

NNM gathers information to the limits of the network indicated by the management station's IP address and subnet mask. NNM then checks the ARP table on each discovered device and expands the map by adding devices listed in each ARP table to the map. NNM also detects serial WAN links (for which ARP caches have no entries) and then checks the resident routing table instead. Devices listed in the routing table are then discovered and the process continues. NNM follows this process each time communication is established with a device, so your maps will continue to grow over time. (See Chapter 2, "How Does NNM Work?," on page 49 for a more detailed explanation about how NNM discovers network information.)

NOTE While NNM discovers and maps your network information, explore the *Get Acquainted with HP OpenView Network Node Manager: Training for NNM Operators* CD provided with NNM so that you will understand what you are seeing after the discovery process is complete.

After NNM completes initial discovery, verify the accuracy of the map (see page 109), making sure that any devices that you have identified as mission-critical in Chapter 4, "Planning Your NNM Configuration," on page 79 appear on the map. Then fix any problems by:

RQS nº 03/2005 - C...
CPMI - CORREIOS
Fls. Nº 0012
3740
Doc:

- Interactively expanding or limiting your management domain (see page 117).
- Automatically expanding your management domain (see page 119).
- Automatically limiting your management domain (see page 124).
- Troubleshooting the initial map to ensure your network is configured properly (see page 131).
- Delete NNM's object and topology databases and restart discovery, if necessary (see page 161).

When you are satisfied with the accuracy and completeness of the initial map, go to Chapter 6, "Preserve Your Sanity: Backup and Polling Configuration," on page 163 to learn how to back up your work and to customize the polling configurations.

1846

Verify the Accuracy of the Initial Discovery

Now that NNM has had time to map all the network connections discovered, take the time to make sure you recognize what was found. Refer to the checklists that you developed in Chapter 4, "Planning Your NNM Configuration," on page 79 to verify that all mission-critical devices are present.

Usually there are a few surprises on your map. NNM allows you to easily identify such things as connectivity problems and security risks. Take the time to fix any problems that you discover (see "Troubleshooting Discovery" on page 131).

This section includes information about NNM's tools that make verifying the information on your maps easier:

- Inventory report

  View or print the inventory report.

- Object properties information

  View a detailed description of the underlying object properties for the selected internet, network, segment, node, or interface symbol.

- Find object feature

  Locate map elements quickly using the `Edit:Find` menu item.

TIP

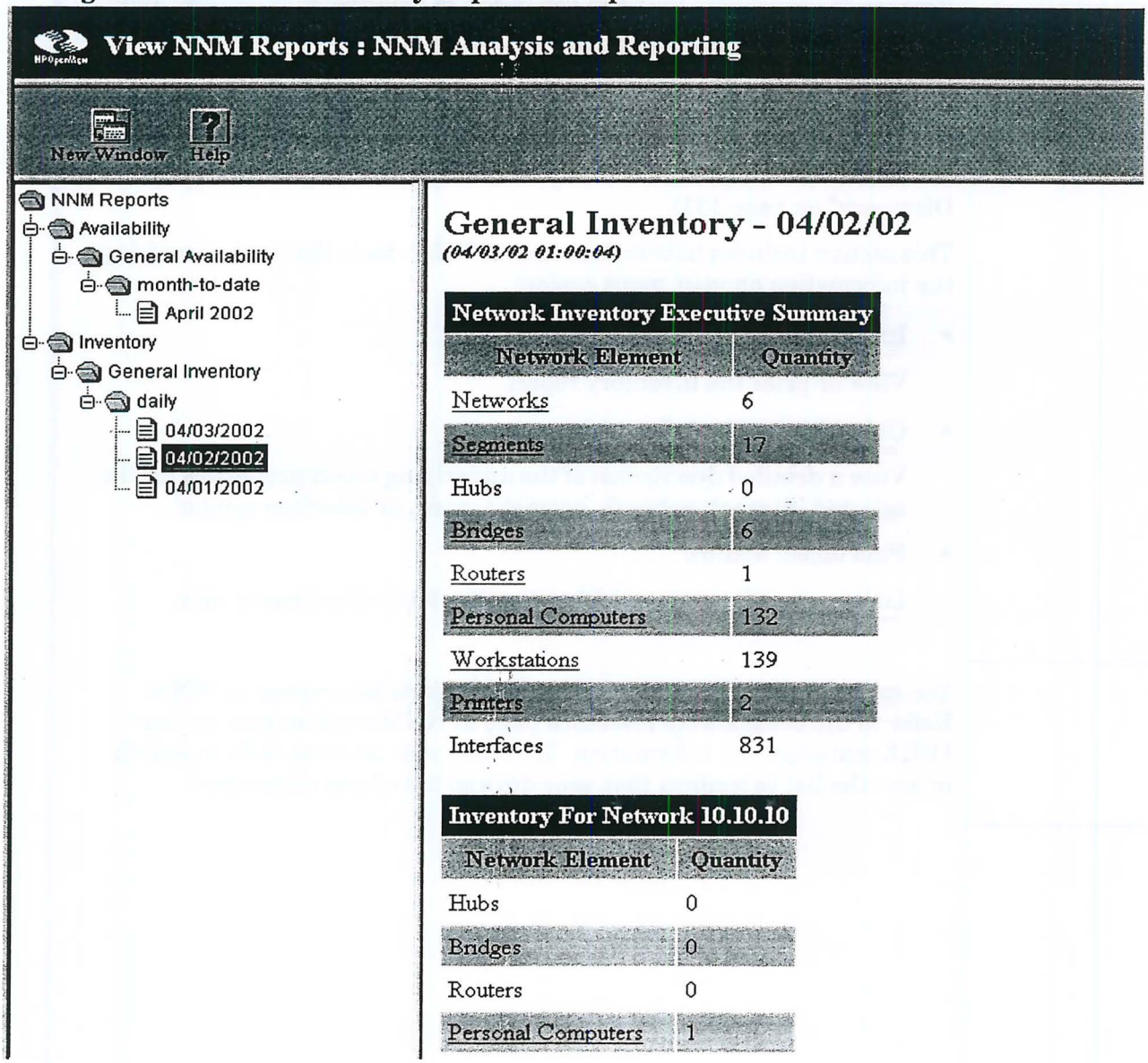
You can generate an ASCII file that lists objects discovered by NNM. Refer to the *ovtopodump* reference page in NNM's online help (or the UNIX manpage) for information. Then use your favorite tools to search or sort the list to confirm that your devices have been discovered.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0013
3740
Doc:

Printing the Inventory Report

Use the inventory report to see a detailed list of what was discovered on your network. The inventory report lists the network nodes that are contained in the topology database, organized by subnet. An example of an inventory report follows.

Figure 5-3 Inventory Report Example



From the Network Inventory Executive Summary, you can click on entries in the Network Element column to see more details.

See the NNM online help for more information on the web Reporting interface.

Viewing the Properties of Your Network Configuration

You can gain quick access to the `IP Map` service's information that describes your network and system configurations. The information in the dialog boxes for object properties can help you determine if everything is present and accounted for on the initial map.

Viewing Object Descriptions

You can view the object properties for any network element that NNM manages, such as an internet, network, segment, node, or interface. The object database maintains this information. Object properties are always as current as NNM's last polling cycle.

Description of an Internet Object Simply select the Internet symbol on the root submap and right-click with the mouse. Select `Object Properties` and select `IP Map`. See NNM's online help for more information and specific directions. NNM provides the following information:

- number of networks on the internet
- number of segments on the internet
- number of nodes contained within the internet
- number of interfaces contained within the internet
- number of gateways/routers on the internet
- any status or error messages may appear in the `Messages` field

Description of a Network Object Simply select any network symbol on the map and right-click with the mouse. Select `Object Properties` and select `IP Map`. See NNM's online help for more information and specific directions. NNM provides the following information:

- the network name as it appears on the map
- network address

IRQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0014
3740
Doc:

- subnet mask associated with the network number
- status of the network
- number of segments on the network
- number of nodes contained within the network
- any status or error messages may appear in the `Messages` field

Description of a Segment Object Simply select any segment symbol on the map and right-click with the mouse. Select `Object Properties` and select `IP Map`. See NNM's online help for more information and specific directions. NNM provides the following information:

- status of the segment
- number of nodes on the segment
- any status or error messages may appear in the `Messages` field

Description of a Node Object Simply select any node symbol on the map and right-click with the mouse. Select `Object Properties` and select `IP Map`. See NNM's online help for more information and specific directions. NNM provides the following information:

- hostname that was assigned when the node was initially discovered
- status of the node
- information about and status of each interface installed on the node
- system description as returned by the SNMP agent (*)
- system location and system contact as returned by the SNMP agent (*)
- system object ID of the node (*)
- any status or error messages may appear in the `Messages` field

* The node must support SNMP to return this information.

Description of an Interface Object Simply select any interface symbol on the map and right-click with the mouse. Select `Object Properties` and select `IP Map`. See NNM's online help for more information and specific directions. NNM provides the following information:

- address of the interface

- subnet mask (IP only)
- link-level address (physical address)
- interface type
- status
- any status or error messages may appear in the `Messages` field

Finding Specific Devices on the Map

The `Edit:Find` menu item enables you to search for objects that contain a common characteristic. You can:

- Find objects in either the open map or an open snapshot based on the value of a specific attribute.
- Create a selection list of objects with particular characteristics, such as all routers.
- Open the submap of each found object.

You can find objects based upon these object and symbol characteristics (see page 205 for more information):

- Selection Name

  You can find objects based on a selection name or part of a selection name.

- Attribute

  You can search for objects based on the values of chosen attributes, such as `isRouter`.

- Comments

  You can search for all objects that have a specific comment or portion of a comment. You may establish conventions for embedded keywords and use these in the `Find By Comment` operation. In this manner, you can find objects based on a key that is not a supported attribute.

- Symbol Status

  You can find objects that are represented by a symbol with the given status. Each found symbol is listed separately.

- Symbol Type

RQS nº 03/2005 - CN - CPMI - CORREIOS
0015
Fls. Nº
3740
Doc:

You can find all objects that have a symbol of a given type (class and subclass).

- Label

  You can search on the label string (comments added by you).

Entering Strings in Find Operations

When you select `Edit:Find`, input in the form of a string value is sometimes required. For several operations, you have a choice between two types of searches: exact match and pattern matching.

Exact Match — Exact match finds only those objects whose attribute value exactly matches the string entered. To switch to the exact match search, click on the `Exact Match` radio button. You must enter the complete string in this mode.

Pattern Matching — When pattern matching is used, you may enter a simple substring or a regular expression. The following section, "Regular Expressions," discusses some of the special characters you can use in regular expressions.

A valid regular expression may consist completely of printable characters. However, in a regular expression, certain symbols have special meaning; see the following table. (*HP-UX only:* more regular expressions are available, see the *regexp* manpage.)

Table 5-1 Regular Expressions for Pattern Matching

Special Character	Meaning	Examples

. (period)	Matches any single printable or nonprintable character except <newline> (unless it is used inside brackets).	`node.in` matches:
		`node3interface`
		`nodeXinterface`

1840

Table 5-1 Regular Expressions for Pattern Matching (Continued)

Special Character	Meaning	Examples

* (asterisk)	Means zero or more occurrences of the preceding character.	`node*` matches:
		`nod`
		`node`
		`nodeTwo`
		`nodee`

^ (Caret)	If the caret is the first symbol, then the following string must be the first part of any matching string.	`^Box` matches the string:
		`Box elder`
		but does not match the string:
		`Big Box`

$(dollar)	If dollar is the last symbol, then the preceding string must be the last part of any matching string.	`long$` matches the string:
		`belong`
		but does not match the string:
		`longer`

Results of the Find Operation

NNM reports all found objects to you in the dialog box. The `Message` area reports the results of the search. It will display:

- the number of objects found
- errors
- further instructions

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0016
3740
Doc:

Symbols of found objects are listed by selection name in the `Located and Highlighted` area. If a found object is represented by multiple symbols, each symbol is displayed on a separate line.

Table 5-2 Results of the Find Operation

Parameter	Meaning
`Selection Name`	The selection name of the object.
`Submap Name`	The name of the submap that displays a symbol of a found object.
`Symbol Label`	The symbol label as it appears on the submap.

The following three example entries display one found object and three symbols that represent the object in three different submaps:

```
NodeBob:lanCard:IP address [connection to segment]

NodeBob [connection to segment]

NodeBob [hostname]
```

The symbols of found objects are highlighted on submaps.

Interactively Expand/Limit Your Management Domain

The NNM default map includes any devices that have already been discovered. You control which of these devices are **managed** (monitored by NNM's services) and which of these devices are **unmanaged** (placed on the map as a light-tan icon, but not monitored by NNM services). NNM does not actively monitor unmanaged devices through polling. However, you can still configure each unmanaged device's SNMP agent or DMI service provider to forward traps to the NNM management station's event tracking system (see "Ensuring that NNM Receives Traps from Your Network Devices" on page 325).

Normally, you customize the size of your management domain by interactively *managing* devices from other networks to expand it and/or *unmanaging* non-critical devices to limit network management traffic and the size of your map.

TIP If this approach seems too time consuming based upon the size of your management domain, see page 119 and page 124.

Adding Networks to Your Management Domain

To add a network to your management domain, find the IP address and hostname of at least one high-traffic device within the network that you wish to add. Gateways, routers, or multi-homed servers make the best choice. Then:

- On the Internet-level submap, select the `Edit:Add Objects` menu item.
- Select the *Connector* Symbol Class icon, then drag the *Gateway* Symbol Subclass icon onto your Internet-level submap. Choose this gateway connector regardless of the type of device you are using to start the discovery. The `Add Object Palette` appears.
- Double-click on `IP Map` to open the `Set Attributes` dialog box.

RQS nº 03/2005 - CI
CPMI - CORREIC
Fls. Nº 0017
3740
Doc:

- Type in the IP address and hostname of an SNMP enabled device within the network that you wish to add to your management domain, then click on the Verify button.

  Once NNM runs the configuration check, NNM will correct the symbol choice and (if necessary) placement for you. The device is configured to be managed by NNM.

Managing an Unmanaged Network Device

To change the status of a network device from unmanaged to managed (see NNM's online help for more information):

1. From any submap, use NNM's `Edit:Find` menu item to locate the device's symbol on the map.
2. Select the device's symbol and select `Edit:Manage Objects`.
3. Select a router that is connected to the new network symbol and use the `Fault:Network Connectivity->Poll Node` menu item.

   NNM conducts discovery on that device's assigned network or networks and the nodes within any neighboring networks. NNM updates the map, databases, and event monitoring to include these devices.

Unmanaging a Managed Network Device

If you *unmanage* a network symbol or segment symbol during active discovery, a few node symbols on that network or segment may not be reset to unmanaged. To avoid this problem while *unmanaging* the network symbol or segment symbol, do one of the following:

- Wait until NNM finishes active discovery before unmanaging an object.
- Turn *new-node discovery* polling off. From any submap, select the `Options:Network Polling Configuration`. Disable the `New Node Discovery` option. Don't forget to turn polling back on again when you are finished modifying the map.

Automatically Expand Your Management Domain

Normally, netmon generates the discovery process outward from the management station and includes only the management station's IP network in the management domain. If your NNM maps are too limited and do not show *all* the networks for which you are responsible, and adding the missing networks one by one (page 117) would be too time-consuming, you have several choices to consider for customizing the discovery process:

- Seed File(page 120)

  If your management domain contains multiple networks (especially networks that are not adjacent to each other), consider using a seed file. A **seed file** instructs netmon to generate the map starting from multiple IP addresses instead of or in addition to the management station's IP address. This saves you time by eliminating the manual process of expanding the management domain.

- loadhosts Program (page 122)

  If your management domain contains few SNMP devices, you can speed up netmon's discovery process by creating an ASCII file listing devices that need to be added to the topology database and map. The loadhosts program reads this file and adds the devices listed in this file directly to your topology database, bypassing the netmon discovery process. Upon being added to the topology database, netmon begins polling the devices as newly discovered devices and expands your management domain from these new nodes.

TIP If you already keep a local hosts file that lists important SNMP-enabled nodes on your network, you can use that file.

- IPX Hop Count (Windows only, page 123)

  If you installed the Windows drivers for the IPX stack, during discovery gateways and servers acting as routers return a **hop count** (how many hops are allowed through gateways and routers to

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0018
Doc: 3740

get to the network) for each network of which the router is aware. You can expand the extent of discovery by setting the maximum hop count to a higher number.

TIP Remember that each additional managed network device increases the network management traffic being generated. Refer to the critical-device list that you established in Chapter 4, "Planning Your NNM Configuration," on page 79 for guidance about keeping the management polling traffic to a reasonable minimum. Unmanage devices that are not mission-critical.

Create a Seed File Specifying Multiple IP Networks to Manage

A seed file is an ASCII file containing a list of network-level IP addresses or host names (not IPX addresses). The contents of the seed file define your map's initial management region. Gateways make the best seeds because they maintain the largest ARP tables. If you add the major gateways, `netmon` will discover the rest of the nodes on the network, so you do not have to include all nodes in the seed file. All networks attached to the devices listed in your seed file will be discovered and set to *managed*. Networks implied by each node's IP address are discovered and added automatically to the map.

1. Create an ASCII file. The name and location of this ASCII seed file is up to you. In this file, list any hostnames or IP addresses that NNM should use to begin discovery. Each hostname or IP address must be on its own line, and each listed device must support SNMP. Specifically, `netmon` must be able to determine the subnet mask for each interface in a specified node. Otherwise, the seed file entry will be ignored.

   You can include notes to yourself in the seed file by using *comments* (preceded by a # sign) after the hostname or IP address on a line.

   Example seed file:

```
node1.division.company.com
router4.division.company.com  #Gateways are best
192.0.2.44
192.0.2.45
```

TIP Bridges and hubs may or may not maintain ARP tables. The ARP tables are the key to expanding NNM's discovery.

2. Make a backup copy of the netmon's local registration file:
   - *Windows:* `install_dir\lrf\netmon.lrf`
   - *UNIX:* `$OV_LRF/netmon.lrf`
3. Load the `netmon.lrf` file into your text editor. The `netmon.lrf` file consists of the following.

```
netmon:netmon:
OVs_YES_START:ovtopmd,pmd,ovwdb:-P:OVs_WELL_BEHAVED: 15:
```

4. Insert the seed file option (`-s filepath`) after the `-P`.

   For example, adding the seed file, `nodelist`, to use as input to netmon on a management station running the Windows operating system would change the file to look like:

   Windows (Note the required \ character after the drive letter and the \ character in the path statement.):

```
netmon:netmon:
OVs_YES_START:ovtopmd,pmd,ovwdb:-P -s
"C\:\install_dir\conf\nodelist":OVs_WELL_BEHAVED:15:
```

   UNIX:

```
netmon:netmon:
OVs_YES_START:ovtopmd,pmd,ovwdb:-P -s
/etc/opt/OV/share/conf/nodelist:OVs_WELL_BEHAVED:15:
```

5. Save the edited `netmon.lrf` file in the following location:
   - *Windows:* `install_dir\lrf\netmon.lrf`
   - *UNIX:* `$OV_LRF/netmon.lrf`
6. Stop the netmon service. At the command prompt, type:
   `ovstop netmon`
7. To update NNM's configuration file, `ovsuf`, at a command prompt, type:

   Windows: **`ovaddobj install_dir\lrf\netmon.lrf`**

   UNIX: **`ovaddobj $OV_LRF/netmon.lrf`**

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0019
Doc 3740

`ovaddobj` updates `netmon`'s information in the `ovsuf` configuration file (which instructs the start-up process what to start).

8. Restart the `netmon` service. At the command prompt, type:

   `ovstart netmon`

NNM starts discovering from all locations identified in your seed file. Give NNM time to complete the process. Then you can manually make additions/changes to the map after the effects of the seed file are in place (see page 117).

Use loadhosts

`loadhosts` is a program provided with NNM that allows you to place a list of IP addresses directly into the topology database. This is useful when:

- There are few SNMP nodes on your network. Using `loadhosts` speeds up the discovery process.
- You already maintain a list of the important SNMP nodes on your network.

  Windows:
  `\WinNT\system32\drivers\etc\hosts` file or
  `\WinNT\system32\drivers\etc\Lmhosts` file

  UNIX: `/etc/hosts` file

  Using `loadhosts` ensures that your critical devices are immediately included in NNM's databases and on the map.
- If it is critical to keep network management traffic to an absolute minimum (see page 127).

See the *loadhosts* reference page in NNM's online help (or the UNIX manpage) for more information.

1. Create an ASCII file listing each IP address or hostname on a separate line.
2. At the command prompt, type:

`loadhosts -m` ***`subnet-mask filename`***

The following example loads the `\etc\hosts` file on a management station running a Windows operating system, with the subnet mask set:

```
loadhosts -m 255.255.248.0 \WinNT\system32\drivers\etc\hosts
```

The netmon service receives events about the new additions to the topology database and runs the discovery and configuration poll on those newly added nodes.

Expand the IPX Hop Count (Windows only)

If you installed the Windows drivers for the IPX stack, gateways and servers acting as routers return a hop count during discovery (how many hops through gateways and routers to get to the network) for each network of which the router is aware. You can control the extent of IPX discovery allowed by NNM.

To increase the maximum hop count for discovery, open any submap and select the `Options:Network Polling Configuration IP/IPX` menu item. On the `IPX Discovery` tab, specify the hop count of your choice. This change takes effect the next time IPX discovery runs.

To discover *all* IPX networks, set the value up to 16—the maximum allowed by IPX. However, see note below.

NOTE Setting the maximum hops to 16 can cause a large number of nodes to be discovered rapidly, causing both short-term and long-term system performance problems due to polling traffic. Unless you are sure your system is appropriately configured to handle the number of IPX nodes in your environment, Hewlett-Packard recommends that you expand your management domain slowly.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0020
3740
Doc:

Automatically Limit Your Management Domain

If your network maps are too complex to be useful, you have several choices to consider for customizing the discovery process.

If all the devices that are shown on your map must remain in your management domain, you can use **container** icons (see page 248) and create custom submaps to break up the visual information into smaller chunks and customize your map in a number of ways. (See Chapter 8, "Map Customization," on page 211 for information about customizing the map itself rather than customizing the discovery process.)

If you do not need to retain all the devices that are shown on your map, NNM has options that you can use individually or in combination:

- `netmon.noDiscover` File (page 125)

  You create this file listing IP addresses or ranges of IP addresses for NNM to *exclude* from the discovery process; therefore, excluding them from NNM's databases and maps. During initial discovery when NNM discovers a device, the device's IP address is checked against the `netmon.noDiscover` file. If the IP address is matched in the `netmon.noDiscover` file, the device is dropped and not polled for any more information. The device may be discovered again during subsequent new-node-discovery polls; however, it will once again be discarded. This is the easiest method for limiting discovery and also reduces network management traffic more than using a discovery filter (explained below).

- `loadhosts` Program (page 127)

  If you need to keep network management traffic to an absolute minimum, you can turn off `netmon`'s discovery polling cycle and then use the `loadhosts` program to add your network's critical devices directly to your topology database. Only the devices that you specify in the ASCII file of IP addresses/hostnames are included in your management domain.

TIP If you already keep a local hosts file that lists important SNMP-enabled nodes on your network, you can use that file.

- Discovery Filter (page 128)

  You can write Boolean logic into the NNM filter file to specify which devices will or will not pass initial discovery and be added into NNM's object and topology databases. A discovery filter is much more work for the `netmon` service than the `netmon.noDiscover` file because *each device is polled for all MIB attributes* before it is checked against the discovery filter (this is because a discovery filter can be applied to many attributes of a device). If the device does not pass the discovery filter, all information is discarded. The device may be discovered and polled again during subsequent new node discovery polls; however, the information gathered will once again be discarded.

- `oid_to_type` File (page 129)

  You can open and modify the `oid_to_type` file so that specific *types* of devices are automatically configured as *unmanaged* during initial discovery. The devices show up on your map and are included in the NNM databases, but won't be included in the network management polling traffic generated by NNM.

- IPX Hop Count (Windows only, page 130)

  If you installed the Windows drivers for the IPX stack, during discovery gateways and servers acting as routers return a hop count (how many hops are allowed through gateways and routers to get to the network) for each network of which the router is aware. You can restrict the extent of discovery by lowering the maximum hop count.

Create a netmon.noDiscover File to Exclude Devices

The `netmon.noDiscover` file works at the very beginning of the discovery process. Entries in the `netmon.noDiscover` file are the "don't discover" list. No polling (SNMP or ICMP) is done on devices listed in the `netmon.noDiscover` file. Devices listed in your `netmon.noDiscover` file are not included in NNM's databases or displayed on NNM's maps.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0021
3740
Doc:

If you are using HSRP, you can add the virtual IP address of your HSRP-configured routers to the `$OV_CONF/netmon.noDiscover` file. This stops NNM from deleting and rediscovering the virtual IP address in a regular pattern, which can cause participating routers to be deleted from and re-added to your map. Use the following procedure:

1. Add the virtual IP address of your HSRP-configured routers to the `$OV_CONF/netmon.noDiscover` file.
2. If NNM has already discovered the virtual IP address of your HSRP-configured routers, execute `ovtopofix -r a.b.c.d` where *a.b.c.d* is the virtual IP address of your HSRP-configured routers.
3. Run `ovtopodump -lR` to make sure the virtual IP address is gone. See the `ovtopodump`, `ovtopofix`, and `netmon.noDiscover` reference page (or the UNIX manpage) for more information.

For more detailed information, see the *netmon.noDiscover* reference page in NNM's online help (or the UNIX manpage).

Use the following procedure to create entries in the `netmon.noDiscover` file.

1. Create an ASCII file. Name and place it as follows:
   - *Windows:* *install_dir*`\conf\netmon.noDiscover`
   - *UNIX:* `$OV_CONF/netmon.noDiscover`
2. List specific IP addresses or IP wildcards, one per line. Example `netmon.noDiscover` file entries are:

   ```
   10.2.112.86 # one node

   10.2.*.* # all nodes from 10.2.0.0 to 10.2.255.255

   10.2.1-255.0-49 # first 50 nodes in 10.2.1-255 range

   *.*.*.* # all nodes - nothing will be discovered

   10.2.4-5.* # all nodes in either 10.2.4.* or 10.2.5.*
   ```

3. After you have created or modified the `netmon.noDiscover` file, force `netmon` to acknowledge the change by doing one of the following:
   - To only affect future discovery, stop and restart the `netmon` service.
   - To force changes on the map as well as future discovery:

— Stop and restart the `netmon` service.

Use the `Edit:Find` feature with the same criteria that you used in your `netmon.noDiscover` file to select all the map objects to be excluded from the future discovery. Then delete them from your map. They will not be rediscovered.

-OR-

— Wipe out the databases and start again by following the directions in "Stop Everything and Start Discovery Over Again" on page 161.

TIP If you change your mind later and *remove* IP addresses from the `netmon.noDiscover` file, simply stop and restart the `netmon` service to force NNM to acknowledge the change. The nodes will be rediscovered at the next polling cycle.

Use loadhosts

`loadhosts` is a program provided with NNM that allows you to place a list of IP addresses directly into the topology database. This is useful when:

- There are few SNMP nodes on your network. Using `loadhosts` speeds up the discovery process (see page 122).
- You already maintain a list of the important SNMP nodes on your network:

  Windows:
  `\WinNT\system32\drivers\etc\hosts` file or
  `\WinNT\system32\drivers\etc\Lmhosts` file

  UNIX: `/etc/hosts` file

  Using loadhosts ensures that your critical devices are immediately included in NNM's databases and on the map.
- It is critical to keep network management traffic to an absolute minimum. Turn off the new-node discovery polling process, then use the `loadhosts` program to accomplish discovery of the critical devices you wish to monitor. As long as new-node discovery is turned off, these are the only devices that will appear on your maps.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0022
3740
Doc:

See "Controlling the Amount of Traffic Generated by NNM" on page 178 for more information about NNM's polling cycle choices.

See the *loadhosts* reference page in NNM's online help (or the UNIX manpage) for more information.

1. Create an ASCII file listing each IP address or hostname on a separate line.
2. Turn off NNM's new-node discovery polling feature.

   From any submap, select the `Options:Network Polling Configuration` menu item and disable the New-Node Discovery feature.

   See NNM's online help from this dialog box for more information.
3. If you want to start initial discovery over again, see "Stop Everything and Start Discovery Over Again" on page 161.
4. At the command prompt, type:

`loadhosts -M subnet-mask filename`

The following example loads the `\etc\hosts` file on a management station running the Windows operating system, with the subnet mask set:

```
loadhosts -m 255.255.248.0 \WinNT\system32\drivers\etc\hosts
```

The `netmon` service receives events about the new additions to the topology database and runs the discovery and configuration poll on those newly added nodes.

Create a Discovery Filter Identifying Which Devices to Include

All filters consist of sets of Boolean logic that you enter into the NNM filters file:

- *Windows:* `install_dir\conf\c\filters`
- *UNIX:* `$OV_CONF/$LANG/filters`

After creating and testing your *discovery* filter, open the `Options:Network Polling Configuration` dialog box and enter the name of your filter in the `Use filter` field. Your filter will be used during all future discovery processes.

To update the object database and enforce the filter rules upon past discoveries, you must use the `ovtopofix` command to force `netmon` to acknowledge your new filter and clean out the existing information in NNM's databases so that your discovery filter changes are reflected on your maps.

See *A Guide to Scalability and Distribution* for information about writing, testing, and implementing the discovery filter. See also the *OVfilterIntro*, *netmon*, *ovfiltercheck*, and *ovfiltertest* reference pages in NNM's online help (or the UNIX manpages) for more information.

TIP

While learning how to use the Boolean language, you may wish to explore the information about *map* filters first (rather than discovery filters). NNM interactively reflects changes to the map filter on the existing maps (rather than requiring that you run the `ovtopofix` command first). Therefore, you can try different Boolean strategies and see their effect on the map right away. See *A Guide to Scalability and Distribution* for more information.

Modify the oid_to_type File to Unmanage Devices by Type

You can instruct NNM to automatically set specific types of devices to *unmanaged* during discovery, such as all end-user PCs or all printers. If you want to use this feature *after* you have already finished initial discovery, make the changes to the `oid_to_type` file and see "Stop Everything and Start Discovery Over Again" on page 161.

The `oid_to_type` file (included with NNM) lists a large number of known `sysObjectIDs`. You can use the `U` parameter to automatically set specific types of devices to unmanaged during initial discovery. This flag only affects initial discovery status. You can change any device from unmanaged to managed at a future time.

You do not need to stop NNM when editing this file. To notify `netmon` of the changes when you are done:

- To only affect devices discovered in the future, at the command line type **`xnmpolling -event`**

1826
IRQS nº 08/2005 - CN - CPMI - CORREIOS
Fls. Nº 0023
3740
Doc:

- To go back and start initial discovery again so that this change affects all devices on your network, see "Stop Everything and Start Discovery Over Again" on page 161.

See the directions at the beginning of the editable ASCII `oid_to_type` file. See also the *oid_to_type* references pages in NNM's online help (or the UNIX manpages) for more information.

The following example entries would set devices containing either of two specific Windows versions to unmanaged, would set to unmanaged any IPX device that is not specifically identified elsewhere in the `oid_to_type` file, and would set to unmanaged any non-SNMP/IPX/IP device not specifically identified elsewhere in the `oid_to_type` file:

```
1.3.6.1.4.1.311.1.1.3.1::Windows NT:U # Windows NT
1.3.6.1.4.1.311.1.1.3.1.1::Windows NT:U # Windows NT
DEFAULT:::U
DEFAULT_IP:::
DEFAULT_IPX:::U
DEFAULT_SNMP:::
```

The `oid_to_type` file acknowledges specific `sysObjectIDs`, then wildcard `sysObjectIDs`, and then the `DEFAULT` settings.

Limit the IPX Hop Count (Windows only)

If you installed the Windows drivers for the IPX stack, gateways and servers acting as routers return a hop count during discovery (how many hops through gateways and routers to get to the network) for each network of which the router is aware. You can control the extent of IPX discovery allowed by NNM.

To reduce the maximum hop count for discovery, open any submap and select the `Options:Network Polling Configuration IP/IPX` menu item. On the `IPX Discovery` tab, specify the hop count of your choice.

The extra devices that were discovered based upon the old hop-count number must be manually deleted from your map. Once deleted, the discovery process will not add them again.

Troubleshooting Discovery

This section contains information about resolving common challenges encountered during NNM's discovery of your network:

- IP discovery problems and solutions (page 131)
- IPX discovery problems and solutions (page 153)

Often times, the trouble is caused because of breakdowns in your well-configured network plan (see "Starting with a Well-Configured Network" on page 90): GET and SET community names other than *public*, DNS name resolution inconsistencies, duplicate IP addresses, incorrect subnet masks, or incorrectly configured SNMP agents or DMI service providers on specific devices. NNM's map and event tracking system can make it much easier for you to identify offending devices and isolate what exactly is wrong, so you can fix the problem.

Remember to take advantage of the online discussion group, OV Forum, provided for NNM customers to communicate with each other (see "OpenView Forum" on page 77). You will find a wealth of information there.

IP Discovery and Layout

The IP troubleshooting information is broken into several groups:

- "Network Issues" on page 133
  - "Opening NNM takes a long time" on page 133
  - "NNM's initial discovery found zero nodes" on page 133
  - "All or most of the map is wrong" on page 135
  - "Whole IP networks are missing from my map" on page 135
  - "Strange networks appeared on my map" on page 136
- "Router Issues" on page 136
  - "My default router shows up on the map as a host" on page 136
  - "Some of my routers are missing" on page 136

1824
REQ nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0024
3740
Doc:

— "One router shows up twice on my map as if it were two devices" on page 137
— "Logical interfaces (secondary IP addresses) are missing from my router's interface card submap" on page 137
— "NNM's discovery process negatively impacts my router's performance" on page 138
— "My routers are set to managed but the map doesn't expand" on page 138

- "Problems With Specific Devices" on page 138
  — "IP addresses are used to identify devices, rather than their hostnames" on page 138.
  — "The map includes devices and routing links that I have never heard of before" on page 139
  — "A few devices are depicted inaccurately on the map" on page 139
  — "An SNMP device shows up on the map as a non-SNMP node" on page 139
  — "A host shows up on the map as a router" on page 140
  — "Some of my devices are missing from the map" on page 140
  — "Devices are labeled with the IP address, when I have a name resolution system in place. What happened to the hostname" on page 141
  — "Multi-homed hosts show up as separate devices" on page 141
  — "How does NNM decide which one of multiple hostnames to use for a device" on page 142
  — "Devices have generic icons rather than manufacturer-specific icons" on page 142
  — "The name of a system running Windows is incorrect on the map" on page 143
  — "Addresses from two distinct nodes within a system running Windows are merged into a single node" on page 143
  — "DNS hostname is incorrect on map symbols for a system running Windows" on page 143
- "General IP Suggestions" on page 144

— "Check NNM's Alarm Browser: Configuration Alarms" on page 144

— "Duplicate IP Address Errors" on page 144

— "Routing Table Configuration" on page 144

— "GET- and SET-Community Name and SNMP Port Issues" on page 145

— "Subnet Mask Issues" on page 149

— "Running netmon with the Jumpstart (-J) option" on page 152

Network Issues

Opening NNM takes a long time

This is probably caused by an incorrectly configured name resolution scheme. To verify that this is the problem, do the following:

1. Find the `checkDNS.ovpl` tool.

   Windows: (located on the NNM installation CD)
   `\support\checkDNS.ovpl`

   You must copy `checkDNS.ovpl` and `gethost` into the following directory on the NNM management station:

   `install_dir``\support\*`

   UNIX: `/opt/OV/support/checkDNS.ovpl`

2. Navigate to the directory containing `checkDNS.ovpl` on the NNM management station. At the command prompt type:

   `checkDNS.ovpl -v`

3. Every device listed in the NNM topology database is issued an appropriate `gethostbyaddr` or `gethostbyname` system call. Addresses or hostnames that are too slow in responding are identified in the output on the screen. Clean up the name resolution for addresses or hostnames identified as being too slow.

NNM's initial discovery found zero nodes

- First, verify that NNM's `netmon` service is running:

  — *Windows:* Select `Start:Programs:HP OpenView: Network Node Manager Admin->NNM Services - Status.`

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0025
3740
Doc:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0026
3740
Doc:

— *UNIX:* At the command line prompt, type **ovstatus -c**.

If any of the services are not successfully running, see "Troubleshooting NNM Itself" on page 577 for information about troubleshooting services before continuing.

- Make sure that your network devices are running and responding to pings and SNMP requests. From the command line, issue the `ping` commands and the SNMP requests (`snmpget` and `snmpwalk`), or from any submap use the `Fault:Network Connectivity` menu choices.

  Make sure that SNMP agents are installed and running on each agent system, particularly on gateways. The problem may be that there are no SNMP agents installed.

  Your SNMP GET- and SET-Community names may not be matching up with the settings on the management station. See "GET- and SET-Community Name and SNMP Port Issues" on page 145 for more information.

- If you have very few SNMP nodes on your network, run `loadhosts` to force `netmon` to find them. See "Use loadhosts" on page 122.

  Or run `netmon` with the jumpstart (`-J`) option. See "Running netmon with the Jumpstart (-J) option" on page 152 for more information.

- Make sure that the appropriate SNMP agent is installed and running on the management station:

  — *Windows:* `SNMP EMANATE Master Agent Service`. The service must be running on the management station for discovery to function correctly. You can verify status in the `Windows NT Services` applet in the Control Panel.

  — *UNIX:* `snmpdm`. An `snmpdm` agent must be running on the management station for discovery to function correctly.

- If you specified a seed file, verify that the seed file exists and that you are using the seed file's correct name in `netmon`'s LRF file. Also, verify that you included all the nodes that you want to use as seeds in the seed file and that all the nodes listed in the seed file support SNMP. Do not use bridges and hubs as seeds, since they do not maintain ARP tables.

- From any submap, select the `Fault:Network Connectivity:Ping` menu item to contact your default router and the closest SNMP-supporting router to start gathering ARP table information.

- Make sure your default route is configured correctly. This information determines how IP packets are routed on nodes. To find the default route, do one of the following:
  - Select your management station's symbol on the NNM map and select the `Configuration:Network Configuration:IP Routing Table` menu item.

TIP You may want to establish a policy for using a standard default route so that only one router needs to maintain the routing table.

  - From the command prompt, issue the following command:
    - *Windows:* `ipconfig /all`
    - *UNIX:* `netstat -r`

All or most of the map is wrong

If all or most of the map database is inaccurate, do the following.

On your NNM map, select the questionable router symbols on the map, then use the `Edit:Object Properties` and select `IP Map` to see the current subnet mask configuration.

If a router's subnet masks are incorrectly configured, correct the configuration (see "Subnet Mask Issues" on page 149) and restart discovery (see "Stop Everything and Start Discovery Over Again" on page 161).

Whole IP networks are missing from my map

NNM isn't yet managing any devices within the missing IP network:

- Routers with addresses in the missing IP networks may not be accessible via SNMP. See "GET- and SET-Community Name and SNMP Port Issues" on page 145.
- See "Interactively Expand/Limit Your Management Domain" on page 117.
- If you have several additional networks that you need to add, consider creating a seed file to set devices within those networks to *managed* all at once. See "Create a Seed File Specifying Multiple IP Networks to Manage" on page 120 for more information.

ECT 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0027
3740
Doc:

Strange networks appeared on my map

The most common cause of this problem is incorrect subnet masks. See "Subnet Mask Issues" on page 149 for more information.

To check the network device's current subnet mask configuration, select the device's symbol on the map and use the map's `Edit:Object Properties` and select `IP Map`.

Router Issues

My default router shows up on the map as a host

If the default router shows up as a host on the map, verify the following:

- The most common reason that `netmon` incorrectly identifies a router as a host is that your SNMP GET- and SET-Community names may not be matching up with the settings on the management station. See "GET- and SET-Community Name and SNMP Port Issues" on page 145 for more information.
- Make sure that IP Forwarding on the router is set to "forwarding" *and* that the router has more than one interface card. From any submap, select the router's symbol and select the `Tools:SNMP MIB Browser` menu item and browse the following information:
  - IP Forwarding configuration (`.1.3.6.1.2.1.4.1`)

    `.iso.org.dod.internet.mgmt.mib-2.ip.ipForwarding`
  - Number of interfaces (`.1.3.6.1.2.1.2.1`)

    `.iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber`

  IP Forwarding is a vendor/device-specific configuration. See your device's documentation for more information.

Some of my routers are missing

If routers are not showing up on your network, check to see if the routers are "backup" routers; that is, routers used in an emergency when another router goes down. `netmon` may not discover backup routers, because `netmon` looks only for nodes on the network that are actually used. Therefore, a backup router will be discovered either as a host or it may not be discovered at all. To solve this problem, follow these steps:

1. Manually add the router to the map. See "Interactively Expand/Limit Your Management Domain" on page 117 for information about manually adding the router.
2. Use the `Fault:Network Connectivity:Ping` to determine the initial status condition of the router and turn its map symbol green (managed).
3. Use the `Fault:Network Connectivity:Poll Node` to get the information that `netmon` needs to connect the router in the proper place on the map.

One router shows up twice on my map as if it were two devices

See "Multi-homed hosts show up as separate devices" on page 141.

Logical interfaces (secondary IP addresses) are missing from my router's interface card submap

Secondary addresses are logical interfaces that are configured in addition to the physical interfaces on a router. Unfortunately, for some agents, these additional interfaces are not included in the IP address table returned through SNMP. Therefore, NNM is unaware that these interfaces exist.

When an IP address is found in an ARP Cache and it resolves to the same official name as a router, the IP address is added as an additional interface. When the router's node submap is displayed, the primary interfaces (the ones returned through SNMP) have labels that contain the first word of the interface description. The secondary addresses (the ones discovered in an ARP Cache) have only their IP addresses as their labels.

NNM can discover secondary addresses only if:

- The secondary address resolves to the same official name as the router.
- The secondary address is connected to an existing subnet.

If NNM fails to discover all the configured secondary addresses, they can be manually added as interface symbols to the router's node submap. If the interface is connected to a new subnet, that subnet must also be manually added. NNM will not automatically add the subnet symbol. See the *netmon* reference page in NNM's online help (or the UNIX manpage) for information about the `-S` parameter.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0028
3740
Doc:

The secondary addresses can be placed in a seed file that will be used by the netmon service for discovery (see "Create a Seed File Specifying Multiple IP Networks to Manage" on page 120). In this case, the secondary address interface symbols and the corresponding networks will be added to the map automatically.

NNM's discovery process negatively impacts my router's performance

This can happen when NNM is requesting ARP cache tables or routing tables from the router. You can use the `netmon -R` parameter to stop NNM from polling any routing tables. This cuts down on polling traffic since routing tables can be quite extensive. However, using this option means that NNM cannot discover remote routers over serial WAN links without the help of either a seed file (page 120) or loadhosts (page 122). See the *netmon* reference page in NNM's online help (or the UNIX manpage) for more information about `netmon -R`.

My routers are set to managed but the map doesn't expand

One of the following may be the problem:

- Open the Interface submap for each router by double-clicking on the router symbol and verify that all interface cards are discovered. If any are missing add them manually.
- The missing network may simply be a quiet network; without network traffic, the ARP tables won't be populated to aid NNM in the discovery process. See "Running netmon with the Jumpstart (-J) option" on page 152.
- Your router may have static routes over serial interfaces. NNM can't discover the information it needs to expand discovery because static routes may not have an entry in the routing table with a next hop address. To bypass this issue:
  - — *Windows:* Manually add the corresponding interface card.
  - — *UNIX:* Ping the corresponding interface card.

Problems With Specific Devices

IP addresses are used to identify devices, rather than their hostnames

See "Opening NNM takes a long time" on page 133. See "Consistent Name Resolution Scheme" on page 91 for more information.

The map includes devices and routing links that I have never heard of before

This is probably caused by incorrectly configured subnet masks. See "Subnet Mask Issues" on page 149 for information about fixing problems with subnet masks.

A few devices are depicted inaccurately on the map

If isolated information in the map database is inaccurate, check the following:

- From any submap, select the inaccurate symbol, right-click with the mouse, and select `Object Properties, IP Map`. Write down the `System Object ID` number. Verify that the device supports SNMP (`isSNMPSupported=true`). Then, open the `oid_to_type` and `oid_to_sym` files to make sure there is an appropriate entry for that `sysObjectID` number. Also, check the registration files included in the *`install_dir`*`\symbols\` (`$OV_SYMBOLS/$LANG`) directory. Make any additions or corrections. Then, select the node's symbol on any submap, select `Fault:Network Connectivity->Capability Poll`. It may take some time before the map symbol updates. See Appendix D, "Changing All the Symbols for a Particular Device," on page 661 for more information.
- If changes to the underlying object's configuration have recently been made, select the device's symbol on any submap, then select the `Fault:Network Connectivity:Poll Node` menu item. This forces an immediate configuration check and updates NNM's databases to reflect your changes. You can also simply wait until the next polling cycle.

An SNMP device shows up on the map as a non-SNMP node

If NNM incorrectly identifies an SNMP node as a non-SNMP node, therefore displaying it as an unmanaged symbol:

- The problem may be that all of `netmon's` SNMP requests to a node failed. During SNMP requests, `netmon` asks for system information, interface table, IP address table, routing table, ARP cache, and possibly Bridge or Repeater MIB tables.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0029
Fls. Nº
Doc: 3740

If the node does not reply with a `sysObjectID`, `netmon` assumes that the node does not support SNMP. If, however, a configuration check succeeds, `netmon` assumes the node *does* support SNMP. Note that SNMP requests can fail if the transport is very busy. SNMP runs over UDP.

- The most common cause of this problem is that your SNMP GET- and SET-Community names may not be matching up with the settings on the management station. See "GET- and SET-Community Name and SNMP Port Issues" on page 145 for more information.
- Another common reason for failures is that the SNMP agent returns incorrect information. See "GET- and SET-Community Name and SNMP Port Issues" on page 145 for more information.

A host shows up on the map as a router

If you have a host that shows up as a router, it may be because the host has *multiple interfaces* and *IP forwarding,* therefore meeting the criteria of a router. To check the current configuration on the host:

1. From any submap, select the host's symbol and select the `Tools:SNMP MIB Browser` menu item and browse the following information:
   - IP Forwarding configuration (`.1.3.6.1.2.1.4.1`)

     `.iso.org.dod.internet.mgmt.mib-2.ip.ipForwarding`
   - Number of interfaces (`.1.3.6.1.2.1.2.1`)

     `.iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber`
2. From any submap, select the host's symbol and determine the device's System Object ID (`sysObjectID`) by using `Edit:Object Properties` and selecting `IP Map`. Use the `Edit:Find->Object By Attribute` menu item.

   Find all devices with the same `sysObjectID`.

   If all instances of this device are showing the same misbehavior on the map, see the *oid_to_type* reference page in NNM's online help (or the UNIX manpage) for information about the `M` parameter in the `oid_to_type` file that designates a device as a *multi-homed host* (not a gateway).

Some of my devices are missing from the map

There may be a problem with ICMP communication (`ping`):

- Select the `Fault:Network Connectivity:Ping` menu item and enter the missing IP address. If you can communicate directly with the device in this manner, it will automatically be added to the map.
- See "Interactively Expand/Limit Your Management Domain" on page 117.
- Check the device itself to ensure that it is not powered down.

The device may be in a network which is not yet *managed* by NNM:

- See "Interactively Expand/Limit Your Management Domain" on page 117.
- If you have several additional networks you need to add, consider creating a seed file to set multiple networks to *managed* all at once. See "Create a Seed File Specifying Multiple IP Networks to Manage" on page 120 for more information.

If initial discovery doesn't find many SNMP objects or if your SNMP community names are in disarray, the `netmon` jumpstart command (`-J` option) can force detected SNMP agents to generate ICMP broadcasts to populate their ARP tables, thus aiding the discovery process. See "Running netmon with the Jumpstart (-J) option" on page 152 for more information.

Devices are labeled with the IP address, when I have a name resolution system in place. What happened to the hostname

Check the DNS, NIS, or other name resolution configuration.

Use the `nslookup` tool that is included in the Windows or UNIX operating system. This utility can easily verify which part of the name-resolution configuration is incorrect. The reverse map must also work (`nslookup` must be able to resolve an IP address to a hostname, as well as resolve a hostname to an IP address). See your operating system's documentation for more information.

TIP Make sure that the case (use of uppercase and lowercase letters) is consistent in your hostnames.

Multi-homed hosts show up as separate devices

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0030
3740
Doc:

- The most common reason that `netmon` incorrectly identifies a multi-homed host as separate devices is that your SNMP GET- and SET-Community names may not be matching up with the settings on the management station. See "GET- and SET-Community Name and SNMP Port Issues" on page 145 for more information.
- Check the DNS, NIS, or other name resolution configuration.

  See also "Devices are labeled with the IP address, when I have a name resolution system in place. What happened to the hostname" on page 141 and "The name of a system running Windows is incorrect on the map" on page 143 for more information about name resolution.
- See the *oid_to_type* reference page in NNM's online help (or the UNIX manpage) and explore the `M` parameter setting for multi-homes hosts.

How does NNM decide which one of multiple hostnames to use for a device

NNM uses the hostname associated with the lowest numbered IP address which resolves to a name.

Devices have generic icons rather than manufacturer-specific icons

- The most common reason that devices display on the map with generic icons is that your SNMP GET- and SET-Community names may not be matching up with the settings on the management station. See "GET- and SET-Community Name and SNMP Port Issues" on page 145 for more information.
- From any submap, select the inaccurate symbol, right-click with the mouse, and select `Object Properties, IP Map`. Verify that the device supports SNMP (`isSNMPSupported=true`). Write down the `System Object ID` number. Then, open the `oid_to_type` and `oid_to_sym` files to make sure there is an appropriate entry for that `sysObjectID` number. Also, check the registration files included in the *`install_dir`*`\symbols\` (`$OV_SYMBOLS/$LANG`) directory. Make any additions or corrections. Then, select the node's symbol on any submap, select `Fault:Network Connectivity->Capability Poll`. It may take some time before the map symbol updates. See Appendix D, "Changing All the Symbols for a Particular Device," on page 661 for more information.

The name of a system running Windows is incorrect on the map

If an IP address to IP hostname lookup fails, the system attempts to resolve the address via NETBIOS. If the system with the IP address does not have a NETBIOS name that can be resolved back to the IP address in question, the symptoms described above can occur, as well as other communication problems with the target system.

To verify and correct the NETBIOS name on the target system, do the following:

1. On the remote system, access the Windows `Control Panel`.
2. Double-click on the `Network` icon; a dialog box will appear.
3. Correct the configured computer name.

NOTE Changing the name of the target system may affect other network connections for the system.

See also "Devices are labeled with the IP address, when I have a name resolution system in place. What happened to the hostname" on page 141 for more information about name resolution.

Addresses from two distinct nodes within a system running Windows are merged into a single node

See "The name of a system running Windows is incorrect on the map" on page 143 for information about resolving this.

DNS hostname is incorrect on map symbols for a system running Windows

See "The name of a system running Windows is incorrect on the map" on page 143 for information about resolving this.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0031
3740
Doc:

General IP Suggestions

Check NNM's Alarm Browser: Configuration Alarms

NNM's Alarm Browser sorts network alarms into useful categories for you. With your map open, notice the `Alarm Categories` window off to the side of your map. Click on the `Configuration Alarms` button to display the list of problems that NNM has discovered. Fix any problems before continuing. You will find information such as:

- Inconsistent subnet masks discovered on specific nodes (see "Subnet Mask Issues" on page 149).
- Duplicate IP addresses discovered on specific nodes.

Duplicate IP Address Errors

Duplicate IP addresses may cause the following NNM behavior:

- In an effort to keep the map current, NNM may continuously move the device symbol from one submap to a second submap and back again as it discovers the first device using the IP address and then discovers the second device using the same IP address.
- NNM's Alarm Browser may show multiple `Mismatched link-level address` alarms indicating that ARP tables on your network devices are continuously working to update based upon messages received from the two devices using the same IP address.

If within the alarm message NNM identifies the host name of the two devices, correct the problem on one of the two offending devices.

If within the alarm message NNM identifies the MAC address or link-level address of the two devices, use NNM's `Edit:Find->Object by attribute` feature to identify the two offending devices.

Routing Table Configuration

Make sure your network device's routing tables are configured properly. To check the routing table configuration on an SNMP-enabled device, select the device's symbol on any submap, then select `Configuration:Network Configuration->IP Routing Table`.

TIP NNM does not detect proxy ARP (an alternative to defining extensive routing tables). If you receive alarms about misconfigured subnet masks, proxy ARP may be the problem. If you wish to prevent these alarms from posting, highlight one of the alarms in the Alarm Browser and select `Action:Configure Event`. Then modify the event's configuration so that the alarm category is set to `Don't log or display`.

GET- and SET-Community Name and SNMP Port Issues

Community names are a security technique employed by SNMP agent software. If the network management software wants to communicate with the SNMP agent software, both the management station and the SNMP agent must know the current GET-community name and talk over the same port. By default, community names are often set to *public* and the port is set to 161. NNM assumes that these defaults are in use unless you inform it otherwise. Many network administrators change the GET-Community name so that hackers cannot obtain sensitive information about their devices. It is even more common for network administrators to change the SET-Community name, since knowing this community name enables others to make system configuration changes to the device itself.

In order to work, NNM depends upon successful communication with the SNMP agents installed on your network devices. If the GET-community names have been changed from *public* or the port changed from 161, you need to inform NNM of the new ones. (NNM cannot obtain these automatically because that would defeat the security feature.)

NOTE If you do not have access to the GET-Community names, for critical devices in your network, see "If Community Names are Unavailable" on page 148.

To inform NNM of the community naming scheme and ports in use on your network:

1. Open any submap and select the `Options:SNMP Configuration` menu item.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0032
3740
Doc:

2. Enter the specific information about your community naming scheme for IP and IPX devices in this dialog box. For your convenience, you can use wildcard entries when indicating IP addresses. If no SET-Community name is defined, NNM uses the GET-Community name for SNMP SetRequests.

   In this same dialog box, you can indicate any SNMP proxies that you have set up for non-SNMP devices and indicate any nonstandard remote-port configurations that are in use by SNMP agent software on your network (default is port 161). Generally, a remote port is only specified for specialized proxy agents that do not listen to the standard SNMP port.

   Check NNM's online help from this dialog box for more information and directions.

For technical information, see the *ovsnmp.conf* reference page in NNM's online help (or the UNIX manpage).

You can also change these values using a command line interface. For more information, see the *xnmsnmpconf* reference page in NNM's online help (or the UNIX manpage). If you need to know the specific configuration settings for a particular device, use:

```
xnmsnmpconf -resolve device_name
```

For information about configuring SNMP for collection stations and management stations, refer to *A Guide to Scalability and Distribution*.

To determine which GET- and SET-Community name is currently configured in the SNMP agent on each device in your network, refer to the documentation that came with each SNMP agent software package.

If you change the community names on the agent, you also *must* configure the community names for that agent on the management station.

If the settings on both your management station and your SNMP device's agent software are correct and it still does not work, try the following and then contact the vendor of the SNMP agent software.

To verify that the problem resides in the device's SNMP agent, do one of the following. Then see if the information returned to you by the device's SNMP agent makes sense. Make sure common entries in these two tables match:

- On any submap, select the device's symbol and select the `Tools:SNMP MIB Browser` menu item. Then browse the following MIB tables:
  - interface table `.1.3.6.1.2.1.2.2` (`.iso.org.dod.internet.mgmt.mib-2.interfaces`)
  - IP address table `.1.3.6.1.2.1.4.20.1` (`.iso.org.dod.internet.mgmt.mib-2.ip.ipAddrTable`)
- From the command prompt using `snmpget` or `snmpwalk`, type:

```
snmpwalk nodename (or IP address) .1.3.6.1.2.1.2.2
snmpwalk nodename (or IP address) .1.3.6.1.2.1.4.20.1
```

Contact the vendor who supplied the SNMP agent software if the information returned to your request doesn't make sense.

Symptoms of incorrect community names include

- The default router is not discovered.
- Hosts appear to not support SNMP.
- `netmon` incorrectly identifies a router as a host.
- Node that supports SNMP as not supporting SNMP.
- The default router is shown as a host on the map.
- Error messages appear, such as "time-out" or "no such name."
- `netmon` incorrectly identifies a node that supports SNMP as not supporting SNMP.
- Multi-homed hosts show up as separate devices.

If the community name on the default router or the community name on nodes in the seed file does not match the configuration settings in NNM, `netmon` will not be able to get the information that it needs in order to discover the nodes on the network.

TIP

If NNM attempts to contact a node using SNMP and the SNMP request times out, NNM looks for a `netmon.cmstr` file that you can configure to contain additional community names for the node. If the `netmon.cmstr` file exists, and contains community names, the first community name from the netmon.cmstr file that results in a successful SNMP response is

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0033
3740
Doc:

stored in the SNMP configuration database for that node. See the *netmon.cmstr* reference page in NNM's online help (or the UNIX manpage) for more information.

If Community Names are Unavailable

If you need to manage critical devices, yet do not have access to their GET-community names, create a `hosts` file. This *optional* file allows NNM to identify multiple IP addresses as being within a single device (without obtaining this information from the device's SNMP agent). This file must be maintained manually, in the following format:

```
IPAddress       hostname       alias(optional)
```

If you are identifying multi-homed devices such as switches, you must implement alias assignments so that the hostnames of all boards within the device resolve to the same IP address.

```
IPAddress_1         hostname_1         hostname_2

IPAddress_2         hostname_1

IPAddress_3         hostname_1         hostname_3
```

Place your new `hosts` file in the following location. Make sure that the file does not have any extension, such as `.txt`:

- *Windows:* `\WinNT\system32\drivers\etc\hosts`
- *UNIX:* `/etc/hosts`

NOTE Name resolution order issues:

Windows: The default behavior is to search the `hosts` file before checking DNS. If you have altered this default order, this technique may not work.

UNIX: Ensure that the hostname resolution order reads your new `hosts` file. Open the `/etc/nsswitch.conf` file and verify the contents.

Subnet Mask Issues

If the subnet masks on the management station or configured on your network devices are incorrect, discovery will fail. If the subnet mask is too restrictive, not enough is discovered. If the subnet mask is not restrictive enough, too much is discovered.

Symptoms of incorrect subnet masks may include:

- `netmon` discovers and adds nodes from the internet that are outside of your administrative domain. This is caused by an un-subnetted or incorrectly subnetted network.
- Nodes in your management domain do not show up on the map. This is caused by incorrect subnet masks on those nodes.
- Strange networks appear on the map, such as a network having a Class A, Class B, or Class C network number when you expect a subnetted network number. This is caused by incorrectly configured subnet masks on the nodes mapped to those strange networks.
- Many `Inconsistent subnet mask` alarms show up in your Alarm Browser. This is caused by incorrect subnet masks on the nodes identified in the alarm messages.

For networks to be discovered correctly, subnet masks must be correctly configured on all IP interfaces on the following:

- The management station
- All gateways
- Any nodes in a seed file for `netmon`
- Any SNMP-enabled node within your management domain

NOTE

Non-contiguous subnet masks are not supported by NNM. Also, in hierarchical subnets, two subnets having the same IP subnet address but different subnet masks are not supported. See the white paper about subnet masks (page 75) for more information.

Proxy ARP (an alternative to defining extensive routing tables) is also not supported and will result in "misconfigured subnet mask" alarms. If you wish to prevent these alarms from posting, highlight one of the

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0034
3740
Doc:

alarms in the Alarm Browser and select `Action:Configure Event`. Then modify the event's configuration so that the alarm category is set to `Don't log or display`.

To identify the source of the problem caused by incorrect subnet masks, first check the management station to see which subnet masks it knows about, then check the subnet configuration on each network and each device that is causing the problem.

1. *Check the subnet mask information on the Management Station:* Check this information through both SNMP and non-SNMP tools to check for misconfigurations.
   - SNMP check:

     Use the `Edit:Find->Object by Selection Name` to locate the management station's symbol.

     Select the NNM management station's symbol and select `Configuration:Network Configuration->IP Addresses` to see which subnet masks are in use on the management station's interfaces.
   - Non-SNMP check using the tool provided by your operating system:
     - *Windows:* issue the `ipconfig /all` command

       `ipconfig /all` tells you how the system is actually configured; which may not be what the device's SNMP agent returns. For information, see your operating system documentation.
     - *UNIX:* issue the `ifconfig` *`interface`* command, where *`interface`* is usually `lan0`, `lan1`, and so forth. The `interface` command can be found in the `/usr/sbin/ifconfig` file.
2. *Check the subnet mask for each network:* If the subnet masks on the management system are correct (from the previous step), determine the subnet mask currently being used for each network. Do one of the following:

- Select a network symbol on any submap, then right-click on the symbol and select `Object Properties, IP Map`. Check to see that the subnet mask entry is correct. Repeat for each network symbol in question.
- From the command prompt, issue the `ovtopodump` command specifying each network. See the *ovtopodump* reference page in NNM's online help (or the UNIX manpage) for more information.

3. *Check the subnet mask on individual network devices:* To determine what subnet masks are returned to NNM from a device's SNMP agent, do one of the following:
   - On any node-level submap, select an interface board symbol, right-click on the symbol and select `Object Properties, IP Map`. Check the subnet mask entry.
   - On any submap, select the `Fault:Network Connectivity->Poll Node` menu item and type in the offending IP address and look at the results.
   - From the command prompt, type:

     `netstat -I nodename (or IP address)`

     Check the Windows operating system documentation or the UNIX manpage for more information about `netstat`.

4. To solve the subnet masks problems, follow these steps:
   a. Correct the problem with the subnet masks on the network objects that have the problem.

      Log into the network device itself and modify its network configuration to specify the correct subnet masks.

   b. Use the `Fault:Network Connectivity->Poll Node` menu item to verify that the new symbols have the correct subnet masks.

TIP If you discover a large number of inaccuracies, correct the problems and then redo discovery to reset NNM's databases ("Stop Everything and Start Discovery Over Again" on page 161).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0035
Doc: 3740

Running netmon with the Jumpstart (-J) option

The netmon jumpstart command (-J option) can force detected SNMP agents to generate ICMP broadcasts to populate their ARP tables, thus aiding NNM's discovery process. See the *netmon* reference page in NNM's online help (or the UNIX manpage) for more information.

CAUTION Generating ICMP broadcasts can cause a great deal of network traffic. Use this with caution.

netmon's default setting does not use the -J option. By default netmon generates, if necessary, just an ARP Request. There are several factors that determine whether netmon needs to generate an ARP Request:

- For nodes that are up but not on the same subnet with the management station, netmon generates just one ICMP echo request packet and gets back one response. In this case, no ARP Request is generated.

  Because the management station is on a different subnet, a request will go through a gateway. Gateways always have large ARP caches. netmon knows the gateway's link-level address and does not have to broadcast an ARP Request to that gateway. netmon only has to send one ICMP echo request through the gateway and gets back one response.

- For devices that are on the same subnet as the management station, netmon may generate just one ICMP echo request, or it may also generate one ARP Request as well. Because the nodes are on the same subnet, netmon does not have to go through a gateway. Broadcasting an ARP Request will depend on whether or not netmon already has the device's link-level address in the management station's own ARP cache.

- netmon will generate an ARP Request if the address that is being polled for status is not in the ARP cache of your management station.

  The presence of the address in the management station's ARP cache is affected by how many nodes are on the subnet and by how much physical memory is in your management station (some systems will automatically adjust the size of their ARP table).

If netmon is started with the -J option, netmon may cause a broadcast ICMP echo request on each subnet it discovers. These broadcasts will only be issued on a subnet if:

- No broadcast ICMP echo request has ever been issued on this subnet on behalf of this management station.
- An agent capable of issuing a broadcast ICMP echo request on netmon's behalf has been discovered on this subnet. All HP-UX SNMP agents have this capability.

IPX Discovery and Layout (Windows only)

- "General IPX Suggestions" on page 153
- "Network Issues with IPX" on page 154
  - "All IPX nodes are missing from my map" on page 154
  - "IP Network 0.0.0.0 Contains All IPX Nodes" on page 156
- "Router Issues with IPX" on page 156
  - "IPX routers are missing from my map" on page 156
- "Problems with Specific IPX Devices" on page 157
  - "Some IPX nodes are missing from my map" on page 157
  - "IPX nodes have incorrect names or labels" on page 157
  - "Nodes supporting both IP and IPX appear on the map as two separate nodes" on page 159
  - "Duplicate IP Address messages are in the Configuration Alarms list" on page 159

General IPX Suggestions

- Ensure that IPX is configured and installed correctly on the management station. See "Installing IPX Transport Software (Windows only)" on page 100. Pay particular attention to the Frame Type. All IPX nodes on the same IPX network must use the Frame Type configured on the IPX servers and routers.
- Ensure that nodes are running and responding to IPX diagnostic requests *and* SNMP requests. From the command prompt, issue the ipxping -b command. You should receive a response from each

RQS nº 03/2005 - CI
CPMI - CORREIC
Fls. Nº 0036
3740
Doc:



device configured to respond to IPX. If you don't receive any responses, your management station's IPX is probably not configured correctly. If a particular node does not respond, use `snmpget` and `snmpwalk` to check that device's configuration settings. Correct any problems that you discover.

- Ensure that the community name is configured correctly (see "GET- and SET-Community Name and SNMP Port Issues" on page 145).

  It may be necessary to add entries for the IP address and hostname in addition to the IPX address. The format for an IPX address is *<net>*:*<nodeaddr>*; for example, `00000100:080009ABCDEF`. You can drop the leading zeros of the *<net>* portion of the address in most cases. For example: `100:080009ABCDEF`.

- Ensure that the SNMP agent on the node is running.
- Ensure that the IPX objects are *managed* on your map.

Network Issues with IPX

All IPX nodes are missing from my map If NNM does not discover any IPX nodes when run for the first time, check the following:

- Make sure that IPX discovery is enabled via the `Options:Network Polling Configuration:IP/IPX` operation. Click the `IPX Discovery` tab and make sure that `Discover New Nodes` is checked. Also, if IPX discovery is configured for a particular time of day, no nodes will be discovered until that time.
- Make sure that the IPX transport is correctly configured and installed on your system. If `netmon` is started with IPX discovery enabled, but the IPX software is not installed, check the Alarm Browser window under the `Application Alert Alarms` category. You should see an application error event similar to `Could not get IPX RIP socket, disabling IPX discovery.`

  `netmon` will not perform IPX discovery until IPX is correctly configured and `netmon` is restarted.
- Check the Alarm Browser window under the `Application Alert Alarms` category for other errors that may indicate the problem. For example, an invalid license could prevent the system from starting.
- Verify that there is at least one server or router that will respond to the IPX RIP request.

1. Issue the following command at the command prompt:

   Windows: ***install_dir*\bin\ipxping -r -n 1 -d 5**

   This command sends one IPX RIP request and waits five seconds for responses. Responses will include the address of the responding server or router. Adding the -v option will include the IPX networks that can be reached from your management station.

   If you do not see a response and the management station is not also configured as an IPX/NetWare gateway, this indicates that there are either no servers or routers attached to this network, or there is a misconfiguration in your IPX Transport installation. In particular, verify that the IPX transport Frame Type is configured correctly, both on the management system and on the various servers and routers in the network.

   All nodes configured for the same IPX network must run the same Frame Type. For some installations, different IPX networks may be configured for different Frame Types on the same physical cable, but all nodes in the same IPX network must have the same Frame Type, which must match the types configured on the NetWare servers and IPX routers.

2. If the test above succeeded in producing RIP responses, verify that your system receives IPX diagnostic responses by issuing the following command:

   Windows: ***install_dir*\bin\ipxping -n 1**

   This command sends a single IPX diagnostic broadcast request to the local network. All NetWare clients and servers attached to the local network should respond. Lack of response indicates either there are no local NetWare clients, or there is a misconfiguration of the IPX transport on the management station or the target systems. Verify the IPX transport installation and configuration.

3. You can also verify communication with any given network by issuing the following command from the command prompt:

   Windows:
   ***install_dir*\bin\ipxping -n 1 -b <*IPX_net_addr*>**

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0037
Doc. 3740



For example: `bin\ipxping -n 1 -b 00000100` sends a single IPX broadcast diagnostic request to the IPX network 00000100. All NetWare clients and servers configured for the 00000100 network should respond.

IP Network 0.0.0.0 Contains All IPX Nodes If you are running this version of NNM on a collection station that forwards information to a management station running NNM 4.X, you may encounter errors on the management station's display of network information. NNM 4.X does not correctly handle IPX nodes and networks. All nodes with IPX interfaces end up in a single IP network with the IP address 0.0.0.0.

To avoid this, install a topology filter that includes *only* IP objects. You can find details on installing topology filters in *A Guide to Scalability and Distribution*. An example filter, `IPObjectsOnly`, is shipped with the system's filter configuration file for this purpose.

Router Issues with IPX

IPX routers are missing from my map

1. Verify connectivity with the router as described in "Some IPX nodes are missing from my map" on page 157.
2. If the router does not support IPX diagnostic protocols, you can expand the IPX discovery region beyond the router using the `Options:Network Polling Configuration` operation. Click the `IPX Discovery` tab, and use the controls to set the `Maximum Hops` to a larger value. Make sure the value is large enough to expand beyond the router, but not any larger than desired for your discovery purposes. To discover all IPX networks, set the value to 16—the maximum allowed by IPX (however, see note below).

NOTE

Setting the maximum hops to 16 can cause a large number of nodes to be discovered rapidly, causing both short-term and long-term system performance problems. Unless you are sure your system is appropriately configured to handle the number of IPX nodes in your environment, Hewlett-Packard recommends that you expand your management domain slowly.

There is no way to add the router manually if it does not respond to IPX diagnostic requests.

3. If you increased your IPX hop count, but no nodes are being discovered in some or all of the IPX networks, check the following:
   - If the IPX networks exist on your map, verify that the target networks are managed. Use `Edit:Manage Objects` to manage the target networks.
   - If you have IPX discovery configured to run only at a certain time of day, new node discovery will not happen on the newly discovered networks until that time. You can verify your IPX discovery configuration using `Options: Network Polling Configuration:IP/IPX`

Problems with Specific IPX Devices

Some IPX nodes are missing from my map If NNM discovers some, but not all nodes that support IPX:

1. Verify the installation and configuration of the IPX transport on the nodes that are not responding. In particular, check the IPX Transport Frame Type, making sure that it is either set to `Auto Detected` or set to match the Frame Type of the management system and servers.
2. Systems must respond to IPX diagnostic requests in order for NNM to add them to the databases and map. The following systems are known not to respond to IPX diagnostic requests:
   - Some dedicated routers (that is, not NetWare servers) do not support IPX diagnostic protocols.
   - Windows systems, including the management station itself.

To verify that a system responds to IPX diagnostic packets, you must know its IPX address, which is a combination of the IPX network number and its node hardware address. Once you know the IPX address, you can test connectivity to that IPX address by issuing the ***install_dir*\bin\ipxping <*IPX_address*>** command. For example: *install_dir*\bin\ipxping 00000100:080009ABCDEF sends an IPX diagnostic packet to the node with a LAN hardware address of 080009ABCDEF in the IPX network 00000100.

IPX nodes have incorrect names or labels NNM uses the following rules to choose the label for an IPX node:

RQS nº 03/2005 - CN
CPMI - CORREI
Fls. Nº 0038
3740
Doc:



- If the node has an IP hostname, then truncate the IP hostname to just the basename and use that—preference is given to the IP name of an object.
- If the node is a NetWare server, use the NetWare server name as the label. Otherwise, take the network number of the internal server address (that is, remove the 00000000000, which is the same for every server).
- If the node supports SNMP and reports an SNMP `sysName` value, use that as the label.
- If the node supports IP, use the IP address.
- If the node supports IPX, use the host-address portion of the IPX address, formatted to translate the vendor of the hardware. (For example, `100:080009ABCDEF` gets a label of `HP-ABCDEF`).
- Otherwise, if the node has an LLA/MAC, use the hardware address as the label, formatting the hardware vendor if possible.

Based upon this information, troubleshoot naming problems by doing the following:

- If the node label is an IP address instead of a node name, update the IP address-to-hostname mapping. Verify the DNS configuration under the Network TCP/IP Configuration, and make sure your hostname resolution is configured correctly.
- If the node supports both IP and IPX and the label is incorrect, verify the IP address-to-hostname mapping as above.
- If the node is a Netware Server, verify that the correct server name is being propagated by the IPX network protocols by checking IPX SAP packets that show the server name, server type, and server address. You can check IPX SAP packets by doing either:
  - Listen for the information. Every server on the local network should broadcast a set of SAP packets once per minute. You can see the contents of these packets by typing the following at the command prompt:
    ***install_dir*\bin\ipxping -s -1**
  - Query for the information. You can obtain the information immediately by typing the following at the command prompt:
    ***install_dir*\bin\ipxping -sbgv**

If the name returned via either of the above methods does not match your expectations, you will need to reconfigure the IPX Server name.

- If the node supports SNMP, verify that the SNMP `sysName` is configured correctly on the target node. View the SNMP `sysName`, as determined by netmon, using `Edit: Object Properties`. Select the `IP Map` application and click `Edit Attributes`. The System Name attribute will be the SNMP `sysName` variable. If this name is blank, either the system does not have a `sysName` configured, or the SNMP configuration for the node is incorrect. Many nodes are shipped with a pre-configured SNMP `sysName` which may cause several nodes to have the same label.
- If the discovered label is a hardware address, but no vendor translation is occurring, check the contents of the following file: *`install_dir`*`\conf\physAddr.conf`

  Make sure the vendor is listed correctly; for example: `080009 HP`

Nodes supporting both IP and IPX appear on the map as two separate nodes If nodes that support both IP and IPX are showing up as two separate nodes on the map, verify your SNMP configuration for the IPX addresses of the node. The nodes can only be determined to be the same node if the node supports SNMP over IPX, and reports the MIB-II `ipAddrTable` correctly.

SNMP could be misconfigured over IPX. At the command prompt, type: **`snmpwalk`** ***`IPXaddress system`***

If you do not receive a response, verify the community name configuration (see "GET- and SET-Community Name and SNMP Port Issues" on page 145).

Duplicate IP Address messages are in the Configuration Alarms list Some IPX nodes are shipped with the IP address 192.0.0.192 preconfigured. This normally does not cause problems for IP discovery, but might for IPX discovery. If multiple nodes support SNMP over IPX, and report the 192.0.0.192 address as a valid address, `Duplicate IP Address` alarms will be generated.

To fix this problem, configure a correct IP address on each IPX node in question.

To configure NNM to simply ignore the problem and prevent these particular `Duplicate IP Address` alarms from showing up in your Alarm Browser, do the following:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0039
3740
Doc:

1. From any submap, select `Options:Event Configuration`. Click the `OpenView` entry in the `Enterprises` section.
2. Select `OV_Duplicate_IP_Addr` from the event list.
3. From the `Event Configuration` window, use `Edit:Events->Copy` to make a copy of the event. A window will be displayed with the event information to be modified.
4. On the `Description` tab, enter a new event name; for example, **`Ignored_Dup_Addrs`**.
5. Click `Only specified sources`.
6. Click the `Sources` tab. Identify each node that is generating duplicate IP address alarms by doing one or more of the following:
   - Select each offending IPX node on the submaps and click the `[Add From Map]` button in the event configuration dialog box.
   - Type each node name or address into the `Source` entry area, and click `Add`. The source name should be the name listed in the `Source` column of the Alarm Browser.
   - Create an ASCII file listing the full host name or IP addresses of each offending IPX source, one per line. (Use of wildcard characters is allowed in this file.)

     Type the full path and name of this file into the `Source` entry area, and click `Add`.

   File names and sources can be intermixed in this list. See NNM's online help for more information.
7. Click the `Event Message` tab.
   a. Select either `Don't log or display`, or `Log only`.
   b. Click `[OK]`.
   c. Click `File:Save` to cause the event configuration to be updated.
   d. Click `File:Exit` to exit the `Event Configuration` window.

Stop Everything and Start Discovery Over Again

If a few aspects of your map do not look right, see "Troubleshooting Discovery" on page 131. However, if the entire map does not accurately represent your network or you decide to try discovering your network in a more limited fashion (page 124) and want to restart initial discovery, repopulate the databases, and generate a new map, do the following:

1. Stop all of NNM's services (background processes):

CAUTION

See *A Guide to Scalability and Distribution* for information about shutting down NNM in a distributed environment.

- *Windows:*
  Select `Start:Programs:HP OpenView:`
  `Network Node Manager Admin->NNM Services - Stop.`
- *UNIX:* As root, at the command prompt, type **ovstop**.

2. Since this step deletes NNM's topology, object, and map databases and your maps, you may wish to back up your existing databases before proceeding (see "Backup/Restore to Protect Your Investment of Time" on page 165).

   If you have customized NNM's configuration (discovery configuration, SNMP configuration, event configuration, or data collection and threshold monitoring, etc.) none of these configurations are affected by this step.

   Execute the following:

   - *Windows:* Use the Windows Explorer program to highlight the ***install_dir*\databases\openview** directory. Select all of the contents of that directory and delete the contents.
   - *UNIX:* Type

     ```
     cd $OV_DB/openview
     rm -rf $OV_DB/openview/*/*
     ```


RQS nº 03/2005 - CN
CPMI 161 CORREIOS
Fls. Nº 0040
Doc:
3740

NOTE If you are using a database other than the one embedded in NNM, see NNM's online manual, *Reporting and Data Analysis*.

3. Optional: To remove the old error messages and start again, execute the following:

   - *Windows:* Use the Windows Explorer program to highlight the ***install_dir*\databases\eventdb** directory. Select all of the contents of that directory and delete the contents.
   - *UNIX:* Type

     ```
     cd $OV_DB/eventdb
     rm -rf $OV_DB/eventdb/*/*
     ```

NOTE If you are using a database other than the one embedded in NNM, see NNM's online manual, *Reporting and Data Analysis*.

4. Restart NNM's services. NNM runs initial discovery, populates the databases, and generates a new map:

   - *Windows:*
     Select `Start:Programs:HP OpenView:`
     `Network Node Manager Admin->NNM Services - Start.`
   - *UNIX:* At the command prompt, type:

     ```
     xnmsnmpconf -clearCache
     $OV_BIN/ovstart ovwdb
     $OV_BIN/ovw -fields
     $OV_BIN/ovstart
     ```

See "Discover the Network... Let NNM Do It" on page 103 to start again.

6 Preserve Your Sanity: Backup and Polling Configuration

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0041
Doc. 3740

Before you begin to configure NNM to meet your team's needs, it is a good idea to make sure that the backup process for NNM is in place and working properly. For information about backing up NNM see page 165.

NNM monitors the devices on your network through standard network protocols. This means that network traffic is generated while accomplishing network management. NNM ships with a generic polling configuration already in place. Take time to learn about and customize the polling configuration to meet your particular business needs. For information about controlling the polling traffic generated by NNM see page 178.

Backup/Restore to Protect Your Investment of Time

Backing up NNM can be integrated into your regularly scheduled network backup scheme. The backup happens in the background while your team continues to monitor alarms on your network. NNM temporarily pauses all services (background processes) whose activities result in changes to the NNM databases (such as the ovw, ovwdb and ovtopmd databases), thus ensuring consistency among the NNM databases and minimizing the potential for database corruption.

After the synchronized files are copied to the backup directory, the services resume normal activity. Then the files that do not require services to be in a paused state are copied to the backup directory.

During the backup of synchronized information, your team's maps are frozen in time, but the Alarm Browser's list and all Data Collection & Threshold information stay current throughout the backup.

NOTE Do not initiate changes to NNM's configuration files from the command line during a backup. It may cause data corruption in the backup copies of the files.

You must ensure that the information copied to the backup directory is archived to the disaster-recovery media of your choice (such as tape).

Add NNM's backup command to your list of regularly scheduled maintenance jobs. This script needs to run prior to your regularly scheduled backup process:

- *Windows:* `install_dir\bin\ovbackup.ovpl`
- *UNIX:* `$OV_BIN/ovbackup.ovpl`

Add NNM's backup directory to the list of items in your regularly-scheduled backup procedure. The backup directory (staging area) on the management station is:

- *Windows:* `install_dir\tmp\ovbackup\`

RQS nº 03/2005 - CN - CPMI - CORREIOS 0042 Fls. Nº 3740 Doc:

- *UNIX:* `$OV_TMP/ovbackup/`

See the *ovbackup.ovpl* and/or *ovrestore.ovpl* reference pages in NNM's online help (or the UNIX manpages) for more information.

How Does the Backup Work?

The `ovbackup.ovpl` command encapsulates all the steps needed to create a backup copy of NNM's critical files. In addition, other HP OpenView programs may supply scripts to include their critical files in the backup process.

A backup consists of two phases. The purpose of these phases is to copy the directory structure and data to the backup staging area. Two distinct phases are required in order to ensure that NNM is paused for the shortest possible time.

- **Operational Phase**

  NNM runs each script located in the `pre_pause` directory. Affected applications take preparatory steps. Then, NNM broadcasts an `ovpause` command. *All* services configured to respond to NNM's `ovpause` command take appropriate action. In some cases, the service temporarily becomes inactive. In other cases, such as data collection (`snmpCollect`), the service is not completely inactive; data continues to be recorded in temporary files until the backup is complete.

  Once all services registered to respond to the pause have successfully paused, NNM runs each script located in the `operational` directory. Because all affected services are paused, the data copied during this phase is *synchronized*.

  Once all files are copied to the backup directory structure, NNM broadcasts the `ovresume` command to restart all services. Some services, such as the data collector (`snmpCollect`), then copy their data collected during the paused state from their temporary files to the regular files. In this way, even during a paused state, data collection is not interrupted. Finally, NNM runs each script located in the `post_resume` directory to return affected applications to an operational state.

- **Analytical Phase**

NNM runs each script located in the `analytical` directory. An affected service may or may not be paused and resumed during the backup process, depending on the settings in its local registration file. The backup scripts might also pause and resume affected applications, themselves.

It is your responsibility to ensure that your disaster recovery plan includes archiving NNM's backup directory during your regularly scheduled backup scheme.

CAUTION If you choose to run `ovbackup.ovpl`, you *must* deactivate the default `solid.ini` scheduled backup. Do not do both or neither. Running both programs will result in backups that may not restore properly. Running neither program may cause severe performance problems with the embedded database. See"Problem: Backup failed. SOLID Database Error 10019:Backup is already active" on page 175 or the *Reporting and Data Analysis with HP OpenView Network Node Manager* online manual for more information.

Backing Up and Archiving All Critical Files

Try the backup and archive procedure now, before you spend a lot of time customizing NNM! Then back up and archive NNM files periodically while you configure NNM for your specific site, and back up and archive NNM files regularly as part of your disaster recovery plan.

1. The scripts named `nnm_checkpoint.ovpl` back up all of NNM's critical data. Additional scripts could be provided by other HP OpenView application developers or by you. Backup scripts must be placed in one of the following directories:

   - *Windows:*

     install_dir`\conf\ovbackup\pre_pause` **or**
     install_dir`\conf\ovbackup\checkpoint\operational` **or**
     install_dir`\conf\ovbackup\checkpoint\analytical` **or**
     install_dir`\conf\ovbackup\post_resume`

   - *UNIX:*

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0043
Fls. Nº
3740
Doc:

```
$OV_CONF/ovbackup/pre_pause or
$OV_CONF/ovbackup/checkpoint/operational or
$OV_CONF/ovbackup/checkpoint/analytical or
$OV_CONF/ovbackup/post_resume
```

TIP

To prevent NNM from being paused for longer than necessary, scripts should be placed in the `analytical` directory unless the data needs to be synchronized with the NNM databases. Scripts placed in the `operational` directory are run while all services registered to respond to the `ovpause` command are paused. Scripts placed in the `analytical` directory pause and resume services one at a time or in groups, only if necessary. See "Custom Scripts" on page 176 for information about writing your own backup/restore scripts.

2. Check on disk space availability before backing up the databases.

   At a minimum, the destination directory must have space for the NNM data that `ovbackup.ovpl` copies. If additional scripts have been added by other applications or the administrator, then additional space is needed. To determine the minimum space requirements, calculate the sum of the space used by NNM in the directories listed in the following table.

TIP

As soon as you install NNM, data collection begins on certain MIB objects. Data collection consumes disk space. Backing up data collection files consumes additional disk space. Disk space being consumed by any SNMP data collection as well as the back-up of these files needs to be managed. For more information on network performance data collection, see page 447.

Table 6-1 Directories Included in Backup

Windows	UNIX
Operational files: *install_dir*\databases\openview*.* *install_dir*\databases\eventdb*.* *install_dir*\log*.* *install_dir*\conf*.* *install_dir*\registration*.* *install_dir*\lrf*.* *install_dir*\fields*.* *install_dir*\symbols*.*	*Operational files:* $OV_DB/openview/* $OV_DB/eventdb/* $OV_LOG/* $OV_CONF/* $OV_REGISTRATION/* $OV_LRF/* $OV_FIELDS/* $OV_SYMBOLS/*
Analytical files: *install_dir*\databases\snmpCollect*.* *install_dir*\databases\analysis*.*	*Analytical files:* $OV_DB/snmpCollect/* $OV_DB/analysis/*

After the backup, the ovbackup directory contains a duplicate copy of all directory structures as well as individual files. The backup process does not compress data, so depending on the size of the original database, the directory could become very large:

- *Windows:* *install_dir*\tmp\ovbackup\
- *UNIX:* $OV_TMP/ovbackup/

You can specify a different directory with the `ovbackup.ovpl -d` option. See the *ovbackup.ovpl* reference page in NNM's online help (or the UNIX manpage) for more information.

TIP

The following *analytical data* directories are *not* included in NNM's backup scripts:

- *Windows:*

  install_dir\backgrounds
  install_dir\bitmaps
  install_dir\www\htdocs\bitmaps
  install_dir\www\registration

- *UNIX:*

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0044
3740
Doc:

```
$OV_BACKGROUNDS
$OV_BITMAPS
$OV_WWW/htdocs/bitmaps
$OV_WWW_REG
```

If you make changes or additions to map backgrounds, bitmap files, or web registration files ensure that your new files are properly backed up. See "Custom Scripts" on page 176 for information about writing your own backup/restore scripts.

3. Decide how you will archive the backup copy of NNM's critical files. Implement measures to ensure that the files in the *install_dir*\tmp\ovbackup directory (`$OV_TMP/ovbackup`) are archived to the disaster-recovery media of your choice on a regular and timely basis *and NOT during the time that the NNM backup scripts are running*.

CAUTION

If you redirected the Data Warehouse storage from the SOLID database to another database of your choice: The information will not be included by the `ovbackup.ovpl` script. Be sure to back up the database files that are used by NNM's reporting feature and Data Warehouse feature. See your database provider's documentation for directions about backing up your data.

4. At the command line, type **`ovbackup.ovpl`** or create a script that issues the `ovbackup.ovpl` command at the scheduled time of your choice. Refer to the *ovbackup.ovpl* reference page in NNM's online help (or the UNIX manpage) for more information.

NOTE

Do not initiate changes to NNM's configuration files from the command line during a backup. It may cause data corruption in the backup copies of the files.

TIP

UNIX systems only issue: NNM's `ovw`, `ovwdb`, and `ovtopmd` databases use sparse files. Sparse files are RDBM files which are stored to disk with the NULs stripped out. Sparse files usually have the extension `.PAG`. NNM's backup program makes sure that sparse database files are *not* expanded. Do not use `tar` because it expands sparse files.

5. After the backup completes:
   a. Check the ASCII log file to ensure that NNM's critical files were copied successfully:
      - *Windows:* *`install_dir`*`\tmp\ovbackup.log`
      - *UNIX:* `$OV_TMP/ovbackup.log`
   b. At the command line, type **ovstatus** to verify that all NNM services were successfully restarted.
6. Copy the files to the disaster recovery media of your choice.
7. Verify that your archive process successfully ran to completion and that the files on your disaster-recovery media are valid.
8. Optional: to reclaim hard drive space on your management station, delete the archived files from *`install_dir`*`\tmp\ovbackup\*.*` (`$OV_TMP/ovbackup/*`).

Restoring All of NNM (procedures/options)

In the event of a disaster or equipment upgrade, you must restore NNM to the most recently backed up state:

1. Install NNM from the installation CD, if necessary, and install any patches.
2. Stop all of NNM's services (background processes):
   - *Windows:*
     Select `Start:Programs:HP OpenView:`
     `Network Node Manager Admin->NNM Services - Stop`.
   - *UNIX:* As root, at the command prompt, type **ovstop**.
3. Retrieve the latest NNM backup files from your disaster-recovery media and copy them to the management station's backup directory:

RQS nº 03/2005 - CN
CPMI - CORREIO
Fls. Nº 0045
3740
Doc:

- *Windows:* *install_dir*\tmp\ovbackup\
- *UNIX:* $OV_TMP/ovbackup/

TIP

UNIX systems only issue: NNM's ovw, ovwdb, and ovtopmd databases use sparse files. Sparse files are RDBM files which are stored to disk with the NULs stripped out. Sparse files usually have the extension .PAG. Make sure that the software being used to copy the files from your disaster-recovery media to the NNM management station does not expand sparse database files. Do not use tar because it expands sparse files.

4. Type **ovrestore.ovpl** from the command line to run the script files that update NNM's databases, log files, and configuration information files.

   The scripts named nnm_restore.ovpl restore all files found in the ovbackup directory. Additional scripts could be provided by other OpenView application developers or by you. See "Custom Scripts" on page 176 for information about writing your own backup/restore scripts. These restore scripts must be placed in one of the following directories:

   - *Windows:*

     install_dir\conf\ovbackup\restore\operational
     install_dir\conf\ovbackup\restore\analytical

   - *UNIX:*

     $OV_CONF/ovbackup/restore/operational
     $OV_CONF/ovbackup/restore/analytical

5. Verify that your files are safely restored.

   Optional: to reclaim hard drive space on your management station, delete the archived files from *install_dir*\tmp\ovbackup*.* ($OV_TMP/ovbackup/*).

6. Start all of NNM's services (background processes):

   - *Windows:*
     Select Start:Programs:HP OpenView:
     Network Node Manager Admin->NNM Services - Start.
   - *UNIX:* As root, at the command prompt, type **ovstart**.

Restoring Part of NNM (procedures/options)

The `ovrestore.ovpl` command allows you to specify that only the operational data (that must remain in a synchronized state) or only the analytical data be restored. It is not recommended that you restore smaller segments of NNM than these two categories. In fact, doing so could introduce data corruption.

See the *ovrestore.ovpl* reference page in NNM's online help (or the UNIX manpage) for more information. Remember that the following steps apply:

1. Stop all of NNM's services (background processes):
   - *Windows:*
     Select `Start:Programs:HP OpenView:`
     `Network Node Manager Admin->NNM Services - Stop.`
   - *UNIX:* As root, at the command prompt, type **`ovstop`**.
2. Retrieve the latest NNM backup information from your disaster-recovery media and copy it to the management station's backup directory:
   - *Windows:* *`install_dir`*`\tmp\ovbackup\`
   - *UNIX:* `$OV_TMP/ovbackup/`

TIP

UNIX systems only issue: NNM's `ovw`, `ovwdb`, and `ovtopmd` databases use sparse files. Sparse files are RDBM files which are stored to disk with the NULs stripped out. Sparse files usually have the extension `.PAG`. Make sure that the software being used to copy the files from your disaster-recovery media to the NNM management station does not expand sparse database files. Do not use `tar` because it expands sparse files.

3. Type **`ovrestore.ovpl`** (along with the parameter specifying either operational or analytical data) from the command line to run the script files that replace NNM's databases, log files, and configuration information files with the backup copy.

   The scripts named `nnm_restore.ovpl` restore NNM-specific data in either the operational or analytical files found in the `ovbackup` directory. Additional scripts could be provided by other HP

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0046
Doc: 3740

OpenView application developers or by you. See "Custom Scripts" on page 176 for information about writing your own backup/restore scripts. These restore scripts must be placed in one of the following directories:

- *Windows:*

  install_dir\conf\ovbackup\restore\operational
  install_dir\conf\ovbackup\restore\analytical

- *UNIX:*

  $OV_CONF/ovbackup/restore/operational
  $OV_CONF/ovbackup/restore/analytical

4. Verify that your files are safely restored.

   Optional: to reclaim hard drive space on your management station, delete the archived files from *install_dir*\tmp\ovbackup*.* ($OV_TMP/ovbackup/*).

5. Start all of NNM's services (background processes):

   - *Windows:*
     Select Start:Programs:HP OpenView:
     Network Node Manager Admin->NNM Services - Start.
   - *UNIX:* As root, at the command prompt, type **ovstart**.

Troubleshooting Information

At the completion of the backup, ensure that the backup completed without the errors. This section describes some errors which can occur. Look at the last entry in NNM's backup log file:

- *Windows:* *install_dir*\tmp\ovbackup.log
- *UNIX:* $OV_TMP/ovbackup.log

Problem: The system is already in a paused state.

Solution: An error occurred while pausing the services. ovpause logs an error and generates a trap. The backup is aborted. From the command line, type **ovresume.ovpl** and then try the backup again. If you are experiencing time-out errors for a particular service during the pause process, double the length of its pause time-out by altering the affected service's lrf file. See the *lrf* reference page in NNM's online help (or the

UNIX manpage) for more information. You must use the `ovaddobj` command to update NNM's configuration, and then use `ovstop` and `ovstart` to force NNM to acknowledge the change.

Problem: `The backup failed due to a file copy error.`

Solution: The original databases are not disturbed; however, the backup files cannot be used for a recovery. Fix the copy failure condition and then restart the backup. If the copy failed due to insufficient space, free up space in the staging area or use the `ovbackup.ovpl -d` option to copy files to a different directory. See the *ovbackup.ovpl* reference page in NNM's online help (or the UNIX manpage) for more information.

Problem: `The system is not in a paused state. ovresume cannot continue.`

Solution: The backup script assumes that there will be no operator interaction during the backup. Should someone on your team execute `ovresume` from the command line prior to the backup completing, the backup process may not run to completion. The original databases are not disturbed; however, the backup files cannot be used for a recovery. Restart the backup.

Problem: `Resume attempt FAILED.`

Solution: Check the backup log file. If you also see "Resume time-out" errors, see the *ovresume* reference page in NNM's online help (or the UNIX manpage) for information about the `-t` parameter to extend the time-out interval. If you see "Resume Error" messages, call HP customer support.

Problem: `Backup failed. SOLID Database Error 10019:Backup is already active`

Solution: If you are using NNM's reporting feature or Data Warehouse feature, historical information about your network is being stored in the SOLID database. By default, the SOLID database conducts a discreet backup of its own at 11 p.m. nightly. If you see this error in the `ovbackup.log` file, it means that the `ovbackup` was scheduled to run shortly after the SOLID database backup began.

To correct this problem you must deactivate the default `solid.ini` scheduled backup. The process for doing this is:

1. Copy the `$OV_DB/analysis/default/solid.ini` file to `$OV_DB/analysis/default/solid.ini.old` file.
2. Edit the `$OV_DB/analysis/default/solid.ini` file.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0047
3740
Doc:

3. Comment out the `At=<time> backup` entry, by inserting a semicolon (;) at the beginning of the line. An example would be:

```
;At=23:00 backup
```

4. Save the `$OV_DB/analysis/default/solid.ini` file.

   The embedded database will now be backed up only when the `ovbackup.ovpl` command is run. If the use of `ovbackup.ovpl` is stopped at a future time, the default backup should be reinstated by copying the `$OV_DB/analysis/default/solid.ini.old` back to `$OV_DB/analysis/default/solid.ini`.

Windows-only Problem: `WARNING: Could not do 'secure' copy for file <filename>.`

Solution: This is unavoidable when open files on the Windows operating system's NTFS are copied to the staging area. See the WARNINGS section of the *ovbackup.ovpl* reference page in NNM's online help for more information.

UNIX-only Problem: `WARNING: Symbolic link errors or warnings from <directory>.`

Solution: In most cases, this is not a problem and nothing needs to be done. It usually occurs when restore attempts to create a symbolic link for a file that is already there. See the WARNINGS section of the *ovbackup.ovpl(1m)* manpage for more information.

Custom Scripts

NNM's backup procedure and restore procedure are designed so that they can be extended by placing any executable script into the appropriate `operational` or `analytical` directory. The HP-supplied `nnm_checkpoint.ovpl` and `nnm_restore.ovpl` scripts all have the extension `*.ovpl`. The suffix means "OpenView Perl" and refers to a specific subset of the Perl language used to implement NNM automated backup. This subset is not supported for general use by HP customers.

You may use the scripts supplied by HP as a reference or example while creating your own Perl scripts. However, if you create your own Perl scripts, do not use the `*.ovpl` extension in your script's file name and do not invoke HP's unsupported subset of Perl. Instead, ensure that you have a complete version of Perl installed on your system and use that one.

If you have *specific files* that you wish to include in NNM's backup process, the simplest way is to:

- *Windows:* Write a `.BAT` file that copies your files to the backup staging area, *`install_dir`*`\tmp\ovbackup`. Make sure that you duplicate the directory structure to your files, if necessary.
- *UNIX:* Write a shell script that copies your files to the backup staging area, `$OV_TMP/ovbackup`. Make sure that you duplicate the directory structure to your files, if necessary.

After you place your script in the appropriate directory, NNM runs it during the next backup or restore process:

- *Windows:*

```
install_dir\conf\ovbackup\pre_pause or
install_dir\conf\ovbackup\checkpoint\operational or
install_dir\conf\ovbackup\checkpoint\analytical or
install_dir\conf\ovbackup\post_resume or
install_dir\conf\ovbackup\restore\operational or
install_dir\conf\ovbackup\restore\analytical
```

- *UNIX:*

```
$OV_CONF/ovbackup/pre_pause or
$OV_CONF/ovbackup/checkpoint/operational or
$OV_CONF/ovbackup/checkpoint/analytical or
$OV_CONF/ovbackup/post_resume or
$OV_CONF/ovbackup/restore/operational or
$OV_CONF/ovbackup/restore/analytical
```

CAUTION

If you write scripts to copy *specific files* to the backup staging area, you must either:

- Create scripts that restore those specific files to the correct location (upon execution of `ovrestore.ovpl`). Place the scripts in the appropriate restore directories.
- Remember to copy the files to their original locations after running `ovrestore.ovpl`.

Refer to the *ovbackup.ovpl* or *ovrestore.ovpl* reference page in NNM's online help (or the UNIX manpage) for more information.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0048
3740
Doc:

Controlling the Amount of Traffic Generated by NNM

NOTE

When you configure performance reports using the NNM web Reporting interface, the data collector starts collecting data. This data collection increases network traffic. You cannot control when or how frequently the collections are taken. If you need to reduce the amount of network traffic, you can suspend the generation of the report. See the NNM online help for more information.

Network Node Manager software automatically generates intense polling traffic at first as the network monitoring process is discovering your network.

After NNM's initial discovery of you network, *you* are in control of NNM's polling based upon your business needs. There are five types of polling in NNM that you need to know about. You can customize polling, or you can turn polling off completely. There are benefits and consequences to your decisions: less polling means less network traffic; however, reducing the amount of polling traffic by lengthening polling intervals may delay real-tim map updates, resulting in a less accurate map and less timely alarm logs. Turning polling off completely disables proactive management of you network.

You adjust NNM's polling through two dialog boxes accessed with the map menu's `Options:SNMP Configuration` and `Options:Network Polling Configuration` menu items.

Figure 6-1 Options:SNMP Configuration Dialog Box

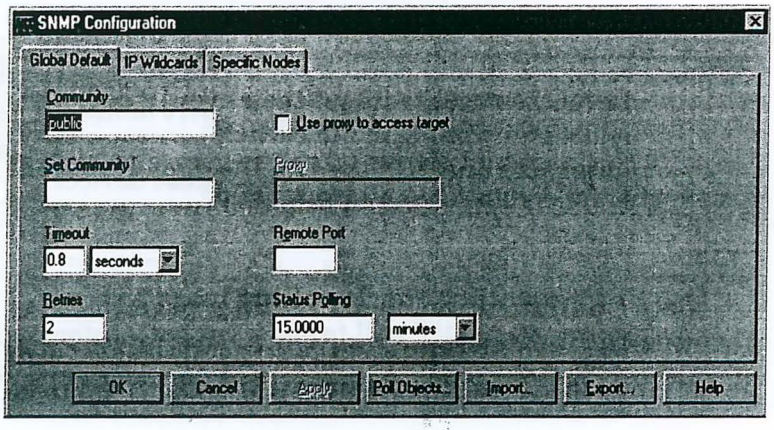
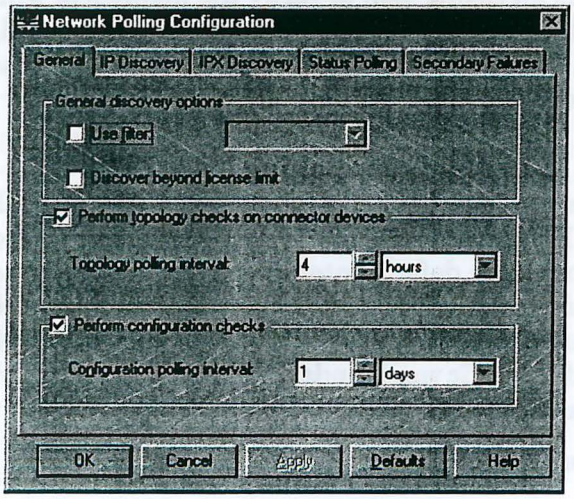


Figure 6-2 Options:Network Polling Configuration Dialog Box



Check the online help from these dialog boxes for more detailed information than you will find in this chapter. The five types of polling are:

- **Status polling** (See "Status Polling" on page 181)

  This is an ICMP `ping` sent to each interface of each managed device to verify if it is still accessible by the management station. In addition, a direct SNMP poll checks cached port tables on hubs and bridges to find the physical address listings of non-SNMP supported

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0049
Fls. Nº
3740
Doc:

devices, and a direct SNMP poll updates the designated list of DHCP addresses. Status polling intervals are configurable as described in this section. *Only management stations running a Windows operating system:* IPX diagnostic requests are also sent.

TIP

Level-2 devices (without their own IP address) whose physical addresses were found in cached port tables are included in NNM's databases and displayed on the map. However, no network polling traffic is generated on behalf of these devices.

- **Configuration check polling** (page 183)

  This is an SNMP poll to gather current information about managed devices. This information is used by NNM to keep the maps current. The default interval is once-per-24-hours for each managed device.

- **Topology check polling of connecting devices** (page 184)

  This is an SNMP poll to verify the manner in which managed connective devices (bridges and hubs via the Bridge MIB, Repeater MIB, and proprietary HP MIBs) service other devices on the network. The default interval is 4 hours.

- **New node discovery polling** (page 184)

  There are two categories of new node discovery, IP and IPX. IP is an SNMP poll that scans for previously unknown devices and updates the map. The default interval is dynamic. *Only management stations running a Windows operating system:* if the IPX stack is configured as part of your Windows operating system, IPX issues RIP, SAP, and IPX diagnostic commands to detect additions to your management domain.

- **Secondary failures polling** (page 192)

  This status polling works in conjunction with the Event-Correlation feature provided with NNM. During a network failure, NNM now identifies the device causing the problem and correlates failure messages from all other affected devices. Through this setting, you control how long NNM ignores devices other than the primary failure. You can also instruct NNM to never ignore certain critical devices, even if they are a secondary failure in an event stream.

- Also see suggestions for fine-tuning all of these polling settings on page 193.

Status Polling

For each managed IP device, an ICMP `ping` is issued to verify if it is still accessible by the management station. The `Global Default` interval for IP devices is once every 15 minutes. Often, the `Global Default` interval setting for every device is not optimal. Refer to the list of mission-critical devices that you developed in Chapter 4, "Planning Your NNM Configuration." You will probably want to poll mission-critical devices more frequently. Some customers decide not to poll certain devices at all, such as end-user PCs or certain printers.

Dynamic Host Configuration Protocol (DHCP) allows IP addresses to be allocated on a temporary basis (a lease). When the lease for an IP address expires, the address can be reused by a different node. This is useful in environments supporting mobile users who connect to the network with a laptop from many different places.

You can specify the range of IP addresses that your network is configured to assign dynamically for mobile devices. The default is OFF (no filter in use). If this filter is enabled, NNM keeps the map clean and the Alarm Browser list free of unnecessary messages about devices within this address range as they are repeatedly attached and detached from your network. Addresses are defined through a *filter* that you write using Boolean logic. See *A Guide to Scalability and Distribution* for information about writing, testing, and implementing the DHCP filter.

You can control status polling in the following ways.

In the Options:SNMP Configuration dialog box

- Set polling intervals on specific nodes by IP address, IPX address, or hostname.

  For IP addresses only, you can set polling intervals using IP address wildcards for a group of IP nodes (for example, `15.122.*.*`). You can also import a file that contains your configuration preferences; see the online help in this dialog box for information about using a file. The IP address wildcard is useful; for example, when you want to configure different values for time-outs or the number of retries for Wide Area Networks (WANs).

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0050
Fls. Nº
3740
Doc:

- Set the status polling interval to be used for any device not specifically listed. If you set it to 24-hours, polling begins at the time that you enter the setting. The actual time may drift depending on network conditions.
- Specify time-out and retry values. For example, you may want to increase the time-out and retry count values to prevent the management station from a premature time-out when making requests across a WAN because latency times are greater over WANs than LANs. Note that the time-out value is set in tenths of a second, and the time-out value doubles with each retry.
- Use filters to configure status polling by object classes. To view the current object class status polling interval configurations, click `Poll Objects` to open the `Status Polling Interval Configuration` dialog box. See the *OVfilterIntro* reference page (or the UNIX manpage) in NNM's online help for more information about defining filters. See the *netmon.statusIntervals* reference page (or the UNIX manpage) about modifying object-based status polling definitions.

NOTE

You may want to view or edit the current object class status polling interval configurations from a remote computer. To do this, use the following procedure:

1. Edit, as `root` (UNIX) or `Administrator` (Windows), the following file and follow the instructions contained in the file.
   - *Windows*:`install_dir\conf\remoteConfAllow.conf`
   - *UNIX*: `$OV_CONF/remoteConfAllow.conf`
2. From your remote computer, point your web browser to the following location:
   `http://hostname:3443/OvCgi/statusIntervalConf.ovpl`

In the Options:Network Polling Configuration dialog box

- Turn OFF/ON both IP and IPX status polling.
- Specify the interval of time that NNM should wait before deleting a "down node" from your maps. The default is 1 week.

- Identify your DHCP node list filter to specify a group of IP addresses that NNM should use for laptop computers. NNM handles this group of IP addresses differently, since devices will be connected and disconnected often from these addresses. Also specify the time interval that NNM should wait before deleting a disconnected node from your map.
- Designate your Discovery filter (if you created a filter of devices that should be excluded from polling). See "Create a Discovery Filter Identifying Which Devices to Include" on page 128.

NOTE One other status polling method, **SNMP status polling**, is used only in special cases to obtain device status information using SNMP queries. SNMP status polling is not configured to run automatically at installation and does not generate any network traffic until you configure it to run. SNMP status polling is covered in more detail on page 273.

Configuration-Check Polling

This type of polling gathers SNMP information about all currently managed devices for NNM's exclusive use. Configuration-check polling gathers information such as:

- Contact and location change
- Forwarding IP packets change
- Interface added
- Interface deleted
- Incorrect routing by a node
- Link address change
- Mismatch of link address
- Network mask change
- Node name change
- Object Identifier change
- Mismatches in link addresses
- World wide web capabilities

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0051
3740
Doc:

This information is used by NNM to keep the maps and databases current. The default interval is once-per-24-hours. This setting applies to all managed devices; it cannot be customized per node.

You can control configuration-check polling in the following ways.

In the Options:Network Polling Configuration dialog box

- Turn OFF/ON all configuration polling.
- Set the interval of time to wait between configuration polling, starting from the time that you set it. The time may drift depending on network conditions.

TIP To monitor status of devices outside your firewall, see "SNMP Status Polling" on page 273.

Connector Topology Polling

Connector topology polling monitors how hubs and bridges are connected in a network. All hubs and bridges are polled based upon the Bridge MIB (RFC1493), Repeater MIB (RFC2108), MAU MIB (RFC1515), and proprietary HP MIBs. You cannot set this polling on a per node basis. This setting helps keep your map current when you are moving devices around.

You can control connector topology polling in the following ways.

In the Options:Network Polling Configuration dialog box

- Turn it OFF/ON.
- Specify the interval of time. The default is 4 hours.

New Node Discovery Polling (IP, Level-2, and IPX)

New node discovery polling checks available ARP caches and Routing tables. This information is used to keep your maps current. This setting applies to all managed devices. It cannot be customized per node.

If you are running NNM on a Windows management station: For each managed IPX network, the following broadcasts occur for each discovery interval. The default interval is 6 hours:

- A single broadcast IPX Routing Information Protocol (RIP) request
- Two broadcast Service Advertising Protocol (SAP) requests
- Two broadcast IPX diagnostic requests per network, 10 seconds apart

You can control new node discovery polling in the following ways.

In the Options:Network Polling Configuration dialog box

For IP and Level-2 devices:

- Turn new node discovery polling OFF/ON. The default is ON for both IP and Level-2 devices. See "Controlling Level-2 Device Discovery and Layout" for more information about configuring NNM to discover level-2 devices.
- Select either the auto-adjust discovery interval or set your own polling interval. The default is auto-adjust, which is based upon the number of new nodes discovered. The range is between 15 minutes and 24 hours.

For IPX devices:

- Turn new-node discovery polling OFF/ON. The default is OFF.
- Set your polling interval or the desired specific time of day for polling.
- Specify the maximum number of sequential routers through which to poll. The default hop count is zero.

Controlling Level-2 Device Discovery and Layout

NNM discovers level 2 devices on both LANs and WANs and presents this information in a graphical format in the NNM map.

Table 6-2 on page 186 and Table 6-3 on page 190 summarize the information contained in this section. Table 6-2 shows the `netmon -k` keyword options and how these options work with the `Discover Level-2 Objects` check box to deliver the resulting NNM behaviors.

Table 6-3 shows how the `Discover New IP Nodes` check box and the `Discover Level-2 Objects` check box works with the `loadhosts` command to deliver the resulting NNM behaviors.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0052
Doc 3740

See "Controlling Level-2 Discovery: Detailed Information" on page 188 for more in-depth information about controlling level-2 discovery and layout.

Table 6-2 Controlling Level 2 Discovery and Layout

netmon -k Option	Discover Level2 Object Check Box Status	NNM Behavior
bridgeMIB=true	Checked	Level 2 nodes and interfaces are discovered and added to the topology database. Bridge MIB layout is done. Existing level 2 interfaces in the topology are unaffected.
bridgeMIB=false	Checked	Level 2 nodes and interfaces are discovered and added to the topology database. No Bridge MIB layout is done. Existing level 2 interfaces in the topology are unaffected.
bridgeMIB=true	Not checked	Level 2 interfaces are discovered and added to the topology database. Level 2 nodes are not discovered. Bridge MIB layout is done. Existing level 2 interfaces in the topology are unaffected.
bridgeMIB=false	Not Checked	Level 2 nodes and interfaces are not discovered. No Bridge MIB layout is done. Existing level 2 interfaces in topology are unaffected.

Table 6-2 Controlling Level 2 Discovery and Layout (Continued)

netmon -k Option	Discover Level2 Object Check Box Status	NNM Behavior
discoverLevel2Nets=true	Checked	L2Nets are created between pairs of routers with such routes. All level 2 interfaces on routers are discovered and added to the topology db. Existing level 2 interfaces in the topology are unaffected.
discoverLevel2Nets=false	Checked	L2Nets are not created between pairs of routers with such routes. All level 2 interfaces on routers are discovered and added to the topology db. Existing level 2 interfaces in the topology are unaffected.
discoverLevel2Nets=true	Not checked	Routers are examined for non-IP interfaces. L2Nets are created between pairs of routers with such routes. All level 2 interfaces on routers are discovered. Only level 2 interfaces on routers needed for L2Nets are added to the topology. Existing level 2 interfaces in the topology are unaffected.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0053
3740
Doc:

Table 6-2 Controlling Level 2 Discovery and Layout (Continued)

netmon -k Option	Discover Level2 Object Check Box Status	NNM Behavior
discoverLevel2Nets=false	Not Checked	Routers are not examined for non-IP interfaces. L2Nets are not created. No level 2 interfaces on routers are discovered. Existing level 2 interfaces in the topology are unaffected.

Controlling Level-2 Discovery: Detailed Information

NNM controls the discovery and layout of level 2 devices in the following manner:

- NNM discovers and adds views of level 2 devices that support the Bridge MIB (RFC 1493).
- NNM examines routers for non-IP interfaces and adds views of level 2 networks that exist between pairs of routers to the NNM map.

You can control the discovery and map layout of level 2 devices by using of the following NNM controls:

- Using the `netmon -k` options.
- By selecting the `Discover Level2 Objects` check box in the `IP Discovery` area of the `Network Polling Configuration` user interface.

You can use the `Discover Level2 Objects` check box together with the `netmon -k bridgeMIB` options to configure the following discovery and layout behaviors:

- If the `bridgeMIB` keyword is set to true (the default value) and the `Discover Level-2 Objects` check box is checked, the `netmon` process discovers level 2 interfaces and adds these interfaces to the topology database. The `netmon` process attempts to create new

segments for bridges and switches supporting the bridge MIB and places the devices on the NNM map. In some cases the netmon process creates and places level 2 nodes on the NNM map. The netmon process changes the names of these newly created level 2 nodes from MAC layer addresses to IP or IPX name references if it determines that the level 2 nodes are IP or IPX nodes. Existing level 2 interfaces in the topology are unaffected.

- If you change the `bridgeMIB` keyword to `false` and the `Discover Level-2 Objects` check box is checked, the `netmon` process discovers level 2 interfaces and adds these interfaces to the topology database. The `netmon` process will not attempt to create new segments for the bridges and switches supporting the bridge MIB nor will it place the devices on the NNM map. Existing level 2 interfaces in the topology are unaffected.
- If the `bridgeMIB` keyword is set to true and the `Discover Level-2 Objects` check box is not checked, the `netmon` process discovers level 2 interfaces and adds these interfaces to the topology database. The `netmon` process attempts to create new segments for bridges and switches supporting the bridge MIB and places the devices on the NNM map. The `netmon` process will not create nor will it place level 2 nodes on the NNM map. Existing level 2 interfaces in the topology are unaffected.
- If you change the `bridgeMIB` keyword to false and the `Discover Level-2 Objects` check box is not checked, the `netmon` process will not discover level 2 interfaces nor will it add these interfaces to the topology database. The `netmon` process will not create nor will it place level 2 nodes on the NNM map. The `netmon` process will not attempt to create new segments for bridges and switches supporting the bridge MIB, nor will it place the devices on the NNM map. Existing level 2 interfaces in the topology are unaffected.

See the `ovtopofix` reference page in NNM's online help (or the UNIX manpage) for information on reversing the effects of the `bridgeMIB` keyword. Look for information on the `ovtopofix -l` (el) and `-I` options.

You can use the `Discover Level2 Objects` check box together with the `netmon -k discoverLevel2Nets` options to configure the following discovery and layout behaviors:

- If the `discoverLevel2Nets` keyword is set to true (the default value) and the `Discover Level-2 Objects` check box is checked, the `netmon` process examines routers for non-IP interfaces and creates

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0054
3740
Doc:

L2Nets between pairs of routers with non-IP interfaces. All level 2 interfaces on routers are discovered and added to the topology database.

- If you change the `discoverLevel2Nets` keyword to false and the `Discover Level-2 Objects` check box is checked, the `netmon` process will not examine routers for non-IP interfaces nor will it create L2Nets between pairs of routers with non-IP interfaces. All level 2 interfaces on routers are discovered and added to the topology database.
- If the `discoverLevel2Nets` keyword is set to true and the `Discover Level-2 Objects` check box is not checked, the `netmon` process examines routers for non-IP interfaces and creates L2Nets between pairs of routers with non-IP interfaces. All level 2 interfaces on routers are discovered. Only level 2 interfaces on routers needed for L2Nets are added to the topology. Existing level 2 interfaces in the topology are unaffected.
- If you change the `discoverLevel2Nets` keyword to false and the `Discover Level-2 Objects` check box is not checked, the `netmon` process will not examine routers for non-IP interfaces nor will it create L2Nets between pairs of routers with non-IP interfaces. No level 2 interfaces on routers are discovered. Existing level 2 interfaces in the topology are unaffected.

When the `Discover New IP Nodes` check box is not checked, the `Discover Level-2 Objects` check box is grayed-out, but still impacts NNM behavior. Table 6-3 shows the resulting NNM behavior when the `Discover New IP Nodes` check box is not checked and new nodes are added by using the `$OV_BIN/loadhosts` command, netmon's seedfile, or when manually adding symbols to the map. The discovery of level 2 interfaces on these nodes is still controlled by the `Discover Level-2 Objects` check box.

Table 6-3 **Discovery Impact of Using `loadhosts` Command or a Seed File**

Discover Level-2 Objects Check Box Status	Discover New IP Nodes Check Box Status	NNM Behavior
Checked	Not checked	Adds both IP interfaces and level 2 interfaces

Table 6-3 **Discovery Impact of Using `loadhosts` Command or a Seed File (Continued)**

Discover Level-2 Objects Check Box Status	Discover New IP Nodes Check Box Status	NNM Behavior
Not checked	Not checked	Adds only IP interfaces

Changing `netmon -k` Options

You can use the following procedure to modify the netmon -k options:

1. Log in as:
   - *Windows*: Administrator
   - *UNIX*: root
2. Open the netmon local registration file in the ASCII editing software of your choice:
   - *Windows*: *install_dir*\lrf\netmon.lrf
   - *UNIX*: $OV_LRF/netmon.lrf
3. Add the text shown in bold to set the keyword to the stated value:
   - To set bridgeMIB= true:

```
netmon:netmon:

OVs_YES_START:ovtopmd,pmd,ovwdb:-P -k segRedux=true -k
bridgeMIB=true:OVs_WELL_BEHAVED:15:PAUSE::
```

   - To set bridgeMIB=false:

```
netmon:netmon:

OVs_YES_START:ovtopmd,pmd,ovwdb:-P -k segRedux=true -k
bridgeMIB=false:OVs_WELL_BEHAVED:15:PAUSE::
```

   - To set DiscoverL2Nets=true:

```
netmon:netmon:

OVs_YES_START:ovtopmd,pmd,ovwdb:-P -k segRedux=true -k
discoverLevel2Nets=true:OVs_WELL_BEHAVED:15:PAUSE::
```

   - To set DiscoverL2Nets=false;

```
netmon:netmon:
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0055
3740
Doc:

```
OVs_YES_START:ovtopmd,pmd,ovwdb:-P -k segRedux=true -k discoverLevel2Nets=false:
OVs_WELL_BEHAVED:15:PAUSE::
```

4. Turn off the netmon service (background process). At the command prompt, run **ovstop -c netmon.**
5. Force NNM to acknowledge the change. At the command prompt, run:
   - *Windows*: **ovaddobj *install_dir*\lrf\netmon.lrf**
   - *UNIX*: **ovaddobj $OV_BIN/ovaddobj $OV_LRF/netmon.lrf**
6. Turn on the netmon service (background process): At the command prompt, run: **ovstart -c netmon**

See the *netmon* reference page in NNM's online help (or the UNIX manpage) for more information; look for the -k keyword parameter and the bridgeMIB and discoverLevel2Nets keyword arguments.

Secondary Failure Polling

This setting allows you to fine-tune the behavior of the connector-down correlation circuit. The default is ON. See "NNM's Event Reduction Capabilities" on page 352 and "Connector Down Correlation" on page 361 for more information about the event correlation feature.

You can control secondary failure polling in the following ways.

In the Options:Network Polling Configuration dialog box

- Turn secondary failure polling OFF/ON.
- Specify the factor by which the normal polling interval should be extended for secondary devices during a failure.
- Designate the section that you wrote in the `filters` file that specifies which critical devices should always be excluded from the secondary status list regardless of their location during a failure event.

  See the *OVfilterIntro* reference page (or the UNIX manpage) in NNM's online help for more information about defining filters. See also *A Guide to Scalability and Distribution* for information about creating filters.
- Control the behavior of the map and event log during a failure event.

Fine-Tuning the Polling Services

The amount of network management traffic generated by status polling depends on your network's configuration, including:

- How many nodes are up and how many are down?
- How many nodes are on the same subnet?
- How many nodes are on other subnets?
- How large is the permanent ARP cache?
- How probable is it that a particular IP address can be found in the permanent ARP cache?

Polling is controlled by NNM's `netmon` service (background process). Because automatic polling is based upon managed nodes, you can reduce the amount of network-management traffic by unmanaging nodes. Simply select the node or nodes on the map, and then select the `Edit:Unmanage Objects` menu item. You can add nodes and change nodes from unmanaged to managed. It may take a while for polling changes to take effect. Polling is scheduled on a per node basis, but the `netmon` service can fall behind schedule if its polling load exceeds capacity limits.

TIP

To automatically set specific types of devices to unmanaged, such as all printers or all end-user systems, see the *oid_to_type* reference page in NNM's online help (or the UNIX manpage). See also "Modify the oid_to_type File to Unmanage Devices by Type" on page 129.

To determine if the polling process is overloaded, select the `Performance:Network Polling Statistics` menu item. If "Seconds until next status poll" or "Seconds until next SNMP poll" is a negative number, then the polling queue is overloaded and running behind.

If polling is continually running behind, you may want to change the startup parameter settings in the `netmon.lrf` file for queue length (`-q` controls the ICMP queue length, `-Q` controls the SNMP queue length, and -x controls the IPX queue length). The default queue setting is 3 on a management station running the Windows operating system and 20 on a management station running a UNIX operating system. Increasing queue length affects the management station's use of system resources and use of network bandwidth for network management.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0056
Doc: 3740

For information about parameter choices available to you for configuring NNM's polling service:

- See the *netmon* reference page in NNM's online help (or the UNIX manpage) for a wealth of choices about controlling polling from the command line and start-up parameter settings. The information in this reference page lists the parameters allowed in the `netmon.lrf` file. See "Create a Seed File Specifying Multiple IP Networks to Manage" on page 120 for information about the process of changing the `netmon.lrf` file (the seed file requires a modification to the `netmon.lrf` file).
- See the *xnmpolling* reference page in NNM's online help (or the UNIX manpage) for information about how to change polling configuration from the command line.
- See NNM's online help available from within the `Options:SNMP Configuration` dialog box and the `Options:Network Polling Configuration` dialog box for more information.

Information that is gathered during polling is stored in NNM's `ovsnmp.conf_db` database.

Watching NNM's Polling Queue

You can automate NNM to notify you whenever the `netmon` service is falling behind in the polling queue.

Use NNM's Data Collection & Thresholds feature (see page 447) to monitor two MIB values from HP's netmon MIB (provided on NNM's installation CD; use Load/Unload MIBs to access the `netmon` MIB):

- `nnmICMPSecsUntilNextPoll (.1.3.6.1.4.1.11.2.17.4.4.1.1.3)` and
- `nnmSNMPSecsUntilNext Poll (.1.3.6.1.4.1.11.2.17.4.4.1.2.3)`

Set the threshold configuration to generate a trap each time the polling queue falls behind to the negative amount that you specify.

Then use NNM's Event Configuration feature (page 422) to set up Automatic Action instructions for that trap instructing NNM to email a message to you or to page you each time that trap is received.

Running NNM Without Network Polling

It is possible to run NNM without the netmon service (background process) that polls your network to generate the map and detect changes. This may be useful if the only applications you have running under NNM do not rely on netmon's discovery functionality or if you are relying on collection stations to perform discovery and monitoring.

NOTE See *A Guide to Scalability and Distribution* for information about collection stations and how to proceed with this step when using collection stations.

To run NNM without automatic IP discovery, configuration checking, and polling by netmon, follow these steps:

1. Stop the currently running netmon service (background process). From the command line, type **ovstop -v netmon**
2. Remove netmon from NNM's start-up options. At the command prompt, type:

   Windows: **ovdelobj *install_dir*\lrf\netmon.lrf**

   UNIX: **ovdelobj $OV_LRF/netmon.lrf**

NOTE If you change your mind and want to restart netmon at a later time:

1. Add netmon to NNM's start-up options. At the command prompt, type:

   Windows: **ovaddobj *install_dir*\lrf\netmon.lrf**

   UNIX: **ovaddobj $OV_LRF/netmon.lrf**

2. Start the netmon service (background process):

   Windows: Select `Start:Programs:HP OpenView:Network Node Manager Admin->NNM Services - Start`.

   UNIX: As root, at the command prompt, type **ovstart**.

The pmd, ovwdb, and ovtopmd services must also be running before netmon can work properly. To generate a list showing the status of each of NNM's services:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0057
3740
Doc:



- *Windows:* Select `Start:Programs:HP OpenView:Network Node Manager Admin->NNM Services - Status`.
- *UNIX:* At the command line prompt, type **`ovstatus -c`**.

If any of the processes are not successfully running, see Appendix A, "NNM Services and Files," on page 539 for information about troubleshooting NNM's services before continuing.

7 Map Making Fundamentals

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0058
3740
Doc:



The following concepts are useful to understand before you start creating your own customized maps:

- maps versus submaps (page 199)
- objects versus symbols (page 203)

Maps versus Submaps

You can think of the relationship between maps and submaps as being much like the relationships between an atlas and its pages. The atlas is the map. The pages of the atlas are the submaps where you may view a particular continent, country, state, city, or even specific parts of a city. In NNM, when you view a part of your network map, you are actually viewing a submap. The view may be presented in a high-level submap that represents your entire network that spans the world, or in a more detailed submap of any portion of the network.

Maps

A **map** is a set of related objects, symbols, and submaps that provides a graphical and hierarchical presentation of your network and its systems. You can create multiple maps, but only one map is open at a time for any given session of NNM.

You do not view a map directly; instead, you always view the submaps that comprise the map. You can display multiple submaps at any given time. Submaps are typically organized hierarchically to show an increasing level of detail.

Different maps can be used for defining different management regions, or for different presentations of the same management region. Different maps can be tailored to the needs of individual users.

You can create multiple maps and customize how information about objects is displayed on each map. Different maps can display information about the same object because maps obtain their information from the same source, the object database. In NNM, you can create new maps, delete maps, and choose the map to display from existing maps.

When you start NNM, a map is automatically opened. You can specify a map by name, or you can let the ovw service open a default map. While a map is open for display, it is simply called an "opened map."

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0059
Doc: 3740



Pros/Cons of Multiple Maps

You can view your various maps through multiple NNM SESSIONS. HOWEVER, Only one map can be opened in a single session at any given time. A single user can open multiple maps by opening multiple NNM sessions. Different users can open the same map (at the same time) through different NNM sessions.

When multiple users access the same map, all users except the first one to access the map are limited to Read-Only access. This means that only the first users will be able to create map snapshots or access any modification features that you, the map administrator, made available to them.

Submaps

When you open a map, you actually view submaps of the map.

A **submap** is a particular view of the network environment. It consists of related symbols that are displayed in a single window. Each submap displays a different perspective of your map. NNM creates a root submap for each map. The root submap provides a standard, top-level submap for every map. Submaps are often organized in a hierarchical fashion for a given map, with the root submap at the top. You can also create independent submaps that are not associated with a hierarchy.

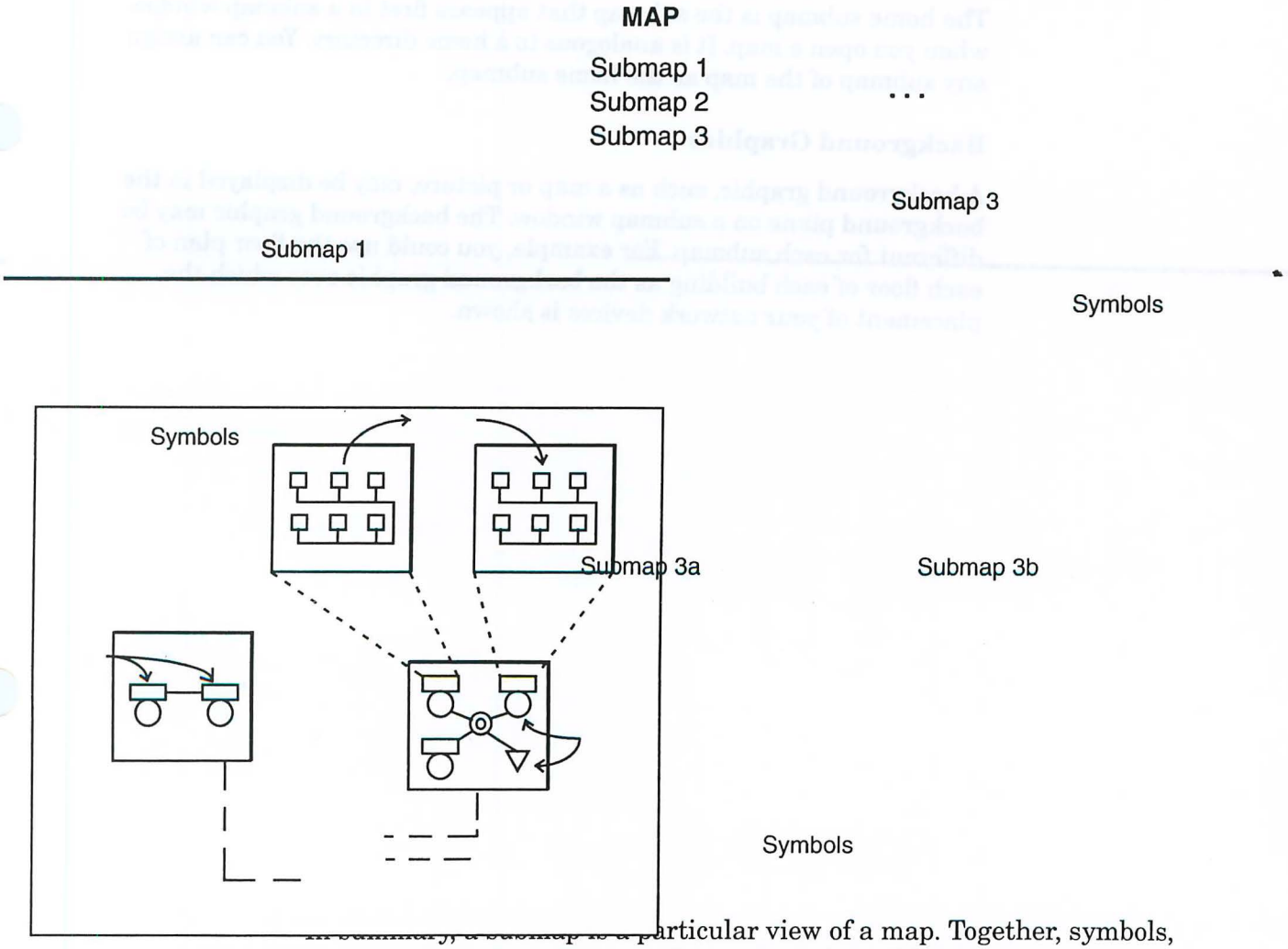
You can open and display multiple submaps of the open map at any given time, either by listing all the submaps of the open map and selecting the submaps to open, or by navigating from one submap to another. You can navigate among the submaps of the open map by double-clicking the mouse on explodable symbols. Double-clicking on an explodable symbol opens a submap that displays a more detailed view.

The hierarchical relationship of submaps creates a parent-child relationship between them. A submap may have several child submaps. The hierarchical relationship of submaps enables you to view your network from a distance, or to choose a more detailed view. For example, consider a submap that contains a single symbol that represents an entire organization. From this high-level view of the map, you can double-click on the symbol to open a child submap. The child submap may display a view of your network map from the perspective of a particular location. From there, you can select a specific department,

then a specific node. You can customize the organization of submaps in a map to suit your purposes; for example, to reflect the organization of your company.

The following figure shows how submaps and their symbols can be used to graphically display network or system management information in a network map.

Figure 7-1 Symbols and Submaps in a Map



In summary, a submap is a particular view of a map. Together, symbols, submaps, and maps make up the presentation of NNM.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0060
Doc 3740



Root Submap

The root submap is the highest-level submap of the map. The first time a map is opened, the root submap is set as the default home submap.The root submap is a system-created submap that allows for the placement of very high-level objects by multiple applications. The root submap cannot be deleted. You can easily return to the root submap at any time by pressing the Home toolbar button.

Home Submap

The home submap is the submap that appears first in a submap window when you open a map. It is analogous to a home directory. You can assign any submap of the map as the home submap.

Background Graphics

A background graphic, such as a map or picture, may be displayed in the background plane on a submap window. The background graphic may be different for each submap. For example, you could use the floor plan of each floor of each building as the background graphic over which the placement of your network devices is shown.

Understanding Objects versus Symbols

An **object** represents a particular entity or resource in a networked systems environment. An object might represent a physical piece of equipment on the network, the components of a node on the network, or parts of the network itself. The object represents the resource by modeling the characteristics (attributes) of the resource. An object exists on a map by virtue of being represented by a symbol on a submap in a map.

A **symbol** is a graphical representation of an object. A single object can be represented by multiple symbols. Multiple symbols for the same object can exist on the same submap, on multiple submaps of the same map, or on submaps of different maps. This enables multiple users on different maps to view a symbol of the same object at the same time. A symbol never represents more than one object at a time.

In addition to representing objects, symbols have other functions:

- Symbols let you navigate through the submaps of a map. Most symbols are explodable—when you double-click on an explodable symbol, a new submap window opens to let you "look inside" the object represented by the symbol.
- Some symbols execute actions. When you double-click on an executable symbol, a predefined action is executed on a predefined target.
- Symbols can be configured to reflect the status of the object that they represent or of objects in child submaps.

The following figure shows how symbols and objects are related. This figure contains two submaps that contain different symbols. Object Y is represented by a single symbol in the root submap, while Object X is

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0061
Doc: 3740

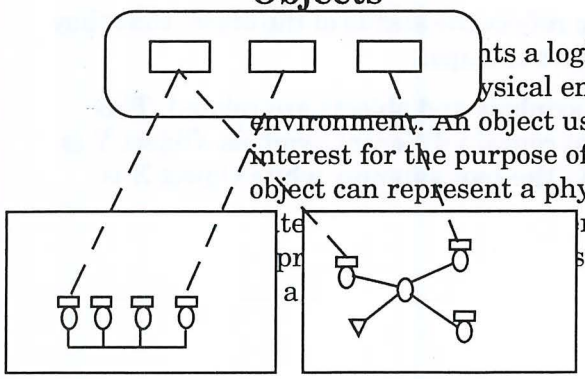
represented by symbols in both the root submap and submap2. Changes made to object X, such as a change in status, can be displayed in both symbols in the two submaps.

Figure 7-2 Object-Symbol Relationships





Objects



nts a logical or physical entity or resource, or a group of ysical entities or resources that exist in a network environment. An object usually represents any particular thing of interest for the purpose of doing network or systems management. An object can represent a physical item (such as a PC, a workstation, a te rface card, or an RS-232 connection), or it can pr such as a group of PCs, all 486 PCs, or all nodes a

Object Attributes/Properties

Each object stored in the map database contains attributes that define the object. An **attribute** is a characteristic of an object to which values can be assigned.

You can think of an attribute as a field that has a specific value. In an application dialog box that displays certain attributes of an object, the labeled fields represent the object' s attributes, and the data in the fields are the object's attribute values, such as:

- hostname
- address
- status
- description
- owner

Every object has a special attribute called a **selection name**. The selection name is a textual name that uniquely identifies the object. An object can have multiple names, but each name must be unique for its name space. For example, an object might have a hostname (for TCP/IP networks) and a fully distinguished name (for OSI networks). Either name could be used as the selection name.

The phrase **selection list** appears throughout this manual and relates to objects. The selection list is a list of objects that are represented by the symbols selected by the user. The selection list is one of the primary ways that you pass arguments to NNM.

The attributes of an object are displayed via the `Edit:Object Properties` dialog box. This dialog box displays the selection name of the object and displays any comments that you, or another user, may have entered about this object.

In the `Edit:Object Properties` dialog box, there is a list of attribute categories, such as General and Capabilities. These categories are accessed by applications that may be managing or monitoring certain attributes about the object. Applications may also add their own attribute category. You can view/modify the object attributes in each category.

- The `General Attributes` dialog box provides a place for applications and users to display attributes in one common location. The `General Attributes` dialog box may display attributes of an

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0062
Doc: 3740

object from multiple applications. These fields may also be displayed in application-specific dialog boxes. The specific fields that are displayed in this dialog box depend on the applications that register a field for this dialog box. Check NNM's online help in this dialog box for more information.

You can set the values of these attributes from the dialog box. Note that values set in this dialog box are not verified. Applications or users may add additional fields to this dialog box by setting a general flag for the field in the field registration file.

- The `Capabilities` dialog box includes the object attributes that determine menu graying. The capabilities of the objects on the current selection list determine which menu items are enabled or disabled. All attributes displayed in the `Capabilities` dialog box are read-only.

  The default for this dialog box is that unset capability fields are not displayed. You can change the behavior of this dialog box so that the unset fields *are* displayed by modifying your Windows system registry or UNIX `$APP_DEFS/OVw` file and changing the value of `showUnsetCapabilitiesFields` to `TRUE`.

The same information is available in the `Edit:Add Object` dialog box. This enables you to assign attribute values during object creation.

Operations on Objects

Check NNM's online help for information about the operations you may commonly perform on objects, such as:

- adding an object
- selecting one or more objects
- locating objects
- adding attributes to an object
- changing an object's description
- changing the vendor and SNMP agent values
- deleting an object
- hiding an object
- showing a hidden object

Symbols

A symbol provides a graphical representation of a particular object. NNM uses two varieties of symbols for display on the map: icon symbols and connection symbols.

- *Icon symbols*, usually referred to simply as a symbol, consists of a geometric shape. A symbol graphic, or icon, usually appears inside the shape.
- *Connection symbols* connect two icon symbols or an icon symbol and a backbone. On a submap, connection symbols appear as lines. However, connection symbols are not merely lines. They represent objects and can display status. NNM uses connection symbols to show the current state of connections between resources on your network.

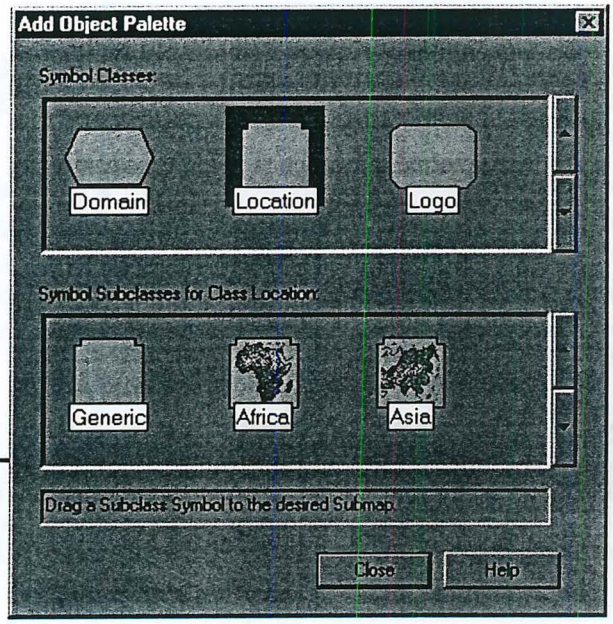
Icon Symbols

Icon symbols include many symbol types. A symbol type consists of the symbol class and symbol subclass. The symbol class is indicated by the outside shape of the symbol. Each symbol class is further divided into

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0063
Doc: 3740

subclasses. Figure 7-3 displays the palette as it appears when you select the `Location` class. The subclasses of the selected symbol class are displayed in the lower portion of the palette.

Figure 7-3 Subclasses in the Location Class



NNM contains a variety of predefined symbols. You can view the available symbols by browsing through the palette or by looking at the `Display Legend` dialog box. To view the legend, select `Help:Display Legend` from the menu bar. The classes and respective subclasses that are registered by NNM are listed in the `Add Object Palette`.

Connection Symbols

A connection symbol is a line that graphically connects two icon symbols or an icon symbol and a backbone (a bus or a ring backbone) on a submap. The connection symbol displays the status of a connection between two objects. Connection symbols behave like icon symbols in the following ways:

- A connection symbol represents an object, just like an icon symbol.
- Connection symbols may reside on the application plane or the user plane.

- You can display a symbol pop-up menu for the connection, and open the `Symbol Properties` dialog box to view or change symbol characteristics.
- You can assign a label to the connection symbol.
- You can change the type of a connection symbol.

Like an icon symbol, the connection symbol may be explodable or executable.

Symbol Characteristics

The following list discusses characteristics of symbols.

Symbol Variety — Symbols come in two varieties: the icon symbol and the connection symbol.

Symbol Type — Symbol type consists of the symbol class and subclass.

- **Class** — You can distinguish the symbol class by the outer shape of the symbol. For example, a circle, square, diamond, and so on.
- **Subclass** — A subclass is a further definition of the class. Each symbol class has a unique set of subclasses.

Status — NNM displays status information by changing the color of the class (or outer shape) of the symbol. The ten status states are categorized as either administrative or operational (see page 270).

Label — You can label each symbol that appears on your network map. The label appears below the symbol. You can choose whether or not to display the label of a symbol.

Location — A symbol can reside on one of two planes: the application plane or the user plane. If an object is not managed by any application, then symbols of that object reside on the user plane of the submap and have a box displayed around them. If an object is managed by one or more applications in a particular submap, then symbols of that object reside on the application

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0064
Doc: 3740

	plane of that submap. This enables you to visually distinguish between objects that are being managed by applications and those objects that are not.
Behavior	Behavior defines how the symbol behaves when you double-click on the symbol. A symbol may behave in one of two ways. It may open a child submap (explode the child submap), or it may execute an application.
Status Source	A symbol may present status information from one of three sources (see page 273). This characteristic enables applications to have more control over the presentation of status. In general, you do not need to change these settings.

Operations on Symbols

Check NNM's online help for information about the operations you may commonly perform on symbols. Many of these symbol operations can be performed from the symbol pop-up menu:

- Adding a connection symbol
- Adding an executable symbol
- Adding an icon symbol
- Changing symbol behavior
- Changing a symbol label
- Changing a symbol type
- Cutting and pasting symbols
- Copying a symbol

See also Appendix D, "Changing All the Symbols for a Particular Device," on page 661.

8 Map Customization

RQS nº 03/2005
CPMI - CORR
Fls. Nº 006
3740
Doc:

Putting It All Together

After you create the initial map and clean up any network problems that were identified, you have the *default* map. (See Chapter 5, Initial Network Discovery: Options and Troubleshooting, if you need to create the default map.) The purpose of the default map is to display a map of your network quickly when you first run NNM. Now you are ready to create copies of the default map and customize the copies for your specific needs.

You can create multiple maps and customize the way in which information about objects is displayed on each map. This enables you to distribute resources over your map to better match how your network and/or team is organized. Multiple maps can display information about the same object because all maps obtain their information from the same source, the object database.

Which Maps for Which Users

In Chapter 4, Planning Your NNM Configuration, you identified the groups or individuals within your organization who need access to the maps. You also identified which aspects of your network each group or individual needs to see on their maps.

Identifying the Purpose of Each Map

As you develop your custom maps, keep in mind the type of problem each group or individual is trying to prevent or solve by using the map. Design their map so that the amount of information displayed is limited to the minimum relevant information and that the information is presented in such a way that it makes their job easier. For example: the map for printer maintenance may show only printers and print servers with backgrounds showing actual floor plans to aid quick response efforts; the map for network troubleshooters might need to contain network infrastructure devices across the entire company; and the map for upper-management to use during client visits might need to show everything possible to look large and impressive.

Determining How Many People Need Access to Each Map

In Chapter 4, you built a model of your customer base and network support team to understand how NNM can be customized to most effectively help your team.

Can any of the groups that you identified share a map, or do their information needs require completely different maps?

Keep in mind that a number of people can view one map simultaneously or multiple maps by using remote console access (see *A Guide to Scalability and Distribution* for information) or by using NNM's new web access (see Chapter 14, NNM on the Web,). When multiple people are accessing a single map, only the first user to open the map has read-write permission (provided that they have read-write permission to the map file), which means that only one person will be able to make changes to the map. However, everyone accessing NNM can acknowledge/delete alarms from the Alarm Browser as issues are resolved.

The number of remote access logins that can be supported is dependent upon a number of factors. See the *Performance and Configuration Guide* that was included with NNM's installation package.

Planning Your Efforts

The remainder of this chapter presents a series of possible map customizing changes. Focus on customizations that help your team meet a business need. After initial map customizing, NNM users tend to use the Alarm Browser on a day-to-day basis and only use the map while troubleshooting a specific network alarm. So keep map customizations to a workable minimum. The customizing options are:

- "Copying the Default Map" on page 215
- "Controlling the Display of Devices Attached to Switches or Bridges" on page 217
- "Giving Your Network Symbols Meaningful Names" on page 221
- "Turning Connection Labels on or off" on page 223
- "Configuring Trunking and Meshing" on page 225
- "Establishing Submap Persistence Settings" on page 229
- "Controlling Which Devices Appear on the Map" on page 232

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0066
3740
Doc:

- "Changing/Adding Object Attribute Fields" on page 235
- "Making the Maps Look Like Your World" on page 240
- "Creating Your Own Map Symbols" on page 263
- "Specifying the Placement and Size of the Submap Windows" on page 266
- "Miscellaneous Configuration Changes" on page 268
- "Controlling Symbol Status" on page 270
- "Creating New NNM Features to Meet Your Team's Needs" on page 278

Customizing the maps requires a substantial time commitment and should be done by someone who understands NNM and your network. To protect your efforts, you may want to remove functionality from the maps so that your team cannot accidentally make changes to your customizations. See Chapter 9, "Controlling Map Access," on page 283.

Copying the Default Map

When you start NNM, the default map is automatically opened with the home submap displayed. You can create multiple maps and specify which map NNM displays initially. Only one map can be opened in a single session at any given time. Different users can open the same map (at the same time) through different NNM sessions, although only the first session opened would include read-write capabilities (provided that they have read-write permission to the map file). All other instances of the same map would be set to read-only.

The `Map:Save As` menu item copies only the currently *open* map and saves it under the new name you specify. Do this when you want to:

- Create multiple maps with similar characteristics.
- Create a specific map for each user. By copying one map, they all initially have similar or identical characteristics; although as changes are made, the maps will diverge.
- Create a writable version of the current map if the currently open map is set to `read-only`.

See the NNM online help if you need more information. See also the *ovw* reference page in NNM's online help (or the UNIX manpage) for information about command line options for copying maps.

The new map is not automatically opened. You can open the new map by selecting the `Map:Open` menu item and selecting the map name that you specified.

Copy the default map now and open the copy before you start making customizations. You can always return to your default map if you make a mistake.

Your Map Strategy

Refer to your worksheets from Chapter 4, Planning Your NNM Configuration, where you identified which maps were needed by your organization. This chapter leads you through the map customization process. Think about how you might leverage your work from one map to another to keep this process as simple as possible. For example, first

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0067
3740
Doc:

make customizations that are common to all required maps. Then make multiple copies of that map before making the finishing touches for each department.

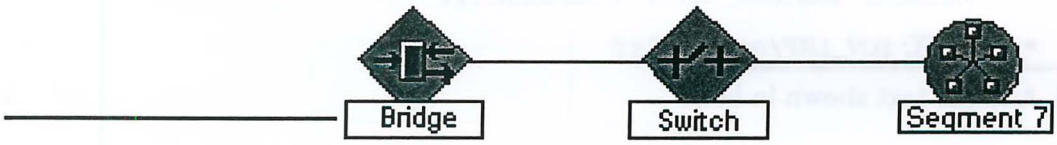
You can set a different Home submap for each user of the map, if you wish (page 287).

Controlling the Display of Devices Attached to Switches or Bridges

NNM has two methods for displaying the devices that are directly attached to ports on switches or bridges:

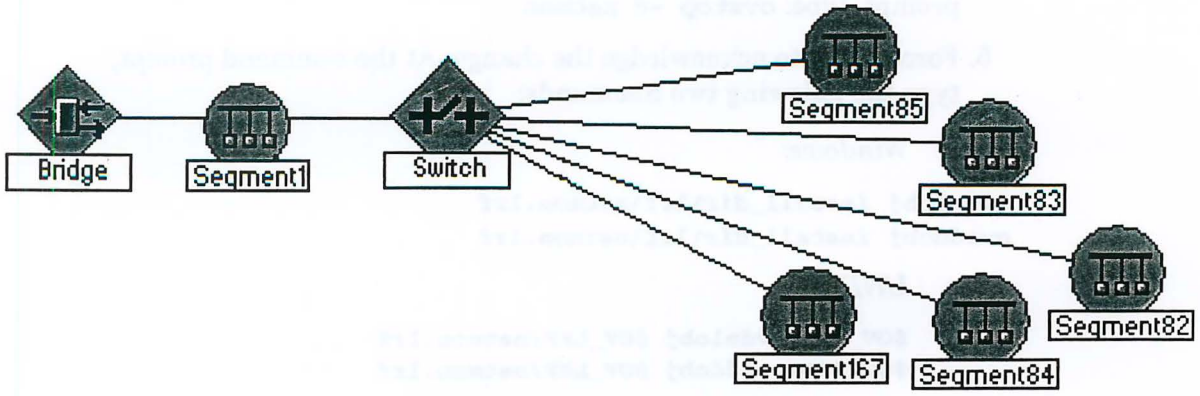
1. Each attached device is presented as part of a star configuration. You double-click on the star segment icon that is attached to a switch or bridge to display all attached devices on one submap. The star segment presentation is the recommended choice. Your map is less cluttered and easier to use when troubleshooting problems.

Figure 8-1 SegRedux On



2. Each attached device is presented as a separate bus segment. You can check the status of each device on its own separate bus segment.

Figure 8-2 SegRedux Off



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0068
Doc: 3740

Turning On Star Configuration for Attached Devices

If you installed NNM for the first time, devices that are directly attached to ports on switches or bridges are automatically displayed in the star configuration. If you *upgraded* NNM from a previous version, you need to take the following steps in order to update your map and NNM's databases so that devices directly attached to ports on switches or bridges are displayed in the star configuration.

1. Log in as:
   - *Windows:* `Administrator`
   - *UNIX:* `root`
2. Open the `netmon` local registration file in the ASCII editing software of your choice:
   - *Windows:* *`install_dir`*`\lrf\netmon.lrf`
   - *UNIX:* `$OV_LRF/netmon.lrf`
3. Add the text shown in bold:

```
netmon:netmon:
OVs_YES_START:ovtopmd,pmd,ovwdb:-P -k segRedux=true:OVs_WELL_BEHAVED:15:PAUSE::
```

   See the *netmon* reference page in NNM's online help (or the UNIX manpage); read about the `-k` keyword parameter and the `segRedux` keyword argument for more information.
4. Turn off the `netmon` service (background process). At the command prompt, type: **`ovstop -c netmon`**
5. Force NNM to acknowledge the change. At the command prompt, type the following two commands:
   - *Windows:*

```
ovdelobj install_dir\lrf\netmon.lrf
ovaddobj install_dir\lrf\netmon.lrf
```

   - *UNIX:*

```
$OV_BIN/ovdelobj $OV_LRF/netmon.lrf
$OV_BIN/ovaddobj $OV_LRF/netmon.lrf
```

6. Turn on the `netmon` service (background process). At the command prompt, type: **`ovstart -c netmon`**

NNM now displays all devices that are directly attached to the ports on a switch or bridge in one star segment submap.

Turning Off Star Configuration for Attached Devices

If you want to turn off this feature, you need to take the following steps in order to update your map and NNM's databases.

1. Log in as:
   - *Windows:* `Administrator`
   - *UNIX:* `root`
2. Open the netmon local registration file in the ASCII editing software of your choice:
   - *Windows:* *`install_dir`*`\lrf\netmon.lrf`
   - *UNIX:* `$OV_LRF/netmon.lrf`
3. Change the *true* to *false* (or delete the text shown in bold):

```
netmon:netmon:
OVs_YES_START:ovtopmd,pmd,ovwdb:-P -k segRedux=true:OVs_WELL_BEHAVED:15:PAUSE::
```

   See the *netmon* reference page in NNM's online help (or the UNIX manpage); read about the `-k` keyword parameter and the `segRedux` keyword argument for more information.
4. Turn off the `netmon` service (background process). At the command prompt, type: **`ovstop -c netmon`**
5. Force NNM to acknowledge the change. At the command prompt, type the following two commands:
   - *Windows:*

```
ovdelobj install_dir\lrf\netmon.lrf
ovaddobj install_dir\lrf\netmon.lrf
```

   - *UNIX:*

```
$OV_BIN/ovdelobj $OV_LRF/netmon.lrf
$OV_BIN/ovaddobj $OV_LRF/netmon.lrf
```

6. Clean up NNM's databases to update the configuration information. At the command prompt, type:
   - *Windows:* **`ovtopofix -l`**

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0069
Doc: 3740

- *UNIX:* **$OV_BIN/ovtopofix -l**

See the *ovtopofix* reference page in NNM's online help (or the UNIX manpage); read about the `-l` parameter for more information.

7. Turn on the `netmon` service (background process). At the command prompt, type: **ovstart -c netmon**

   NNM displays a separate bus segment for each device directly attached to a port on a switch or bridge.

Giving Your Network Symbols Meaningful Names

You can easily provide meaningful names for your network symbols, rather than their IP addresses; for example, Finance, R&D, or Manufacturing. Simply make additions to the list in the following file:

- *Windows:* `\WinNT\system32\drivers\etc\networks`
- *UNIX:* `/etc/networks`

Follow the directions at the top of this ASCII file. Make a list of all your network IP addresses and the corresponding names that would be most meaningful to your team. To force NNM to acknowledge the change, at the command prompt type:

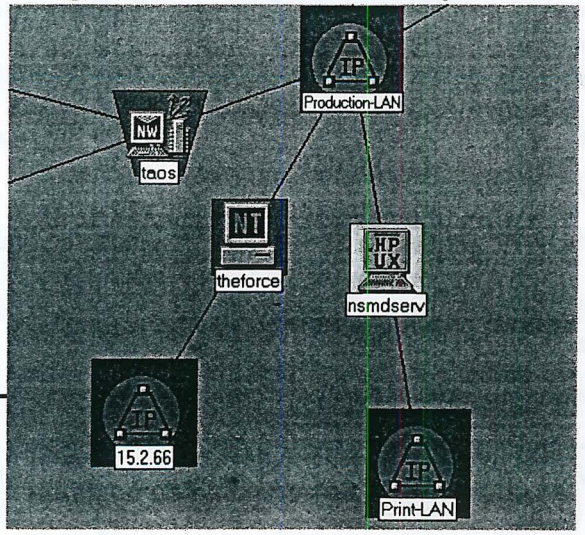
```
ovstop netmon
ovstart netmon
```

Once NNM synchronizes, the new names appear on your maps. Your changes to this file are preserved when applying NNM patches or upgrades.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0070
Doc. 3740

NOTE This change is visible from remote consoles and web access after the map is reloaded or refreshed on each system.

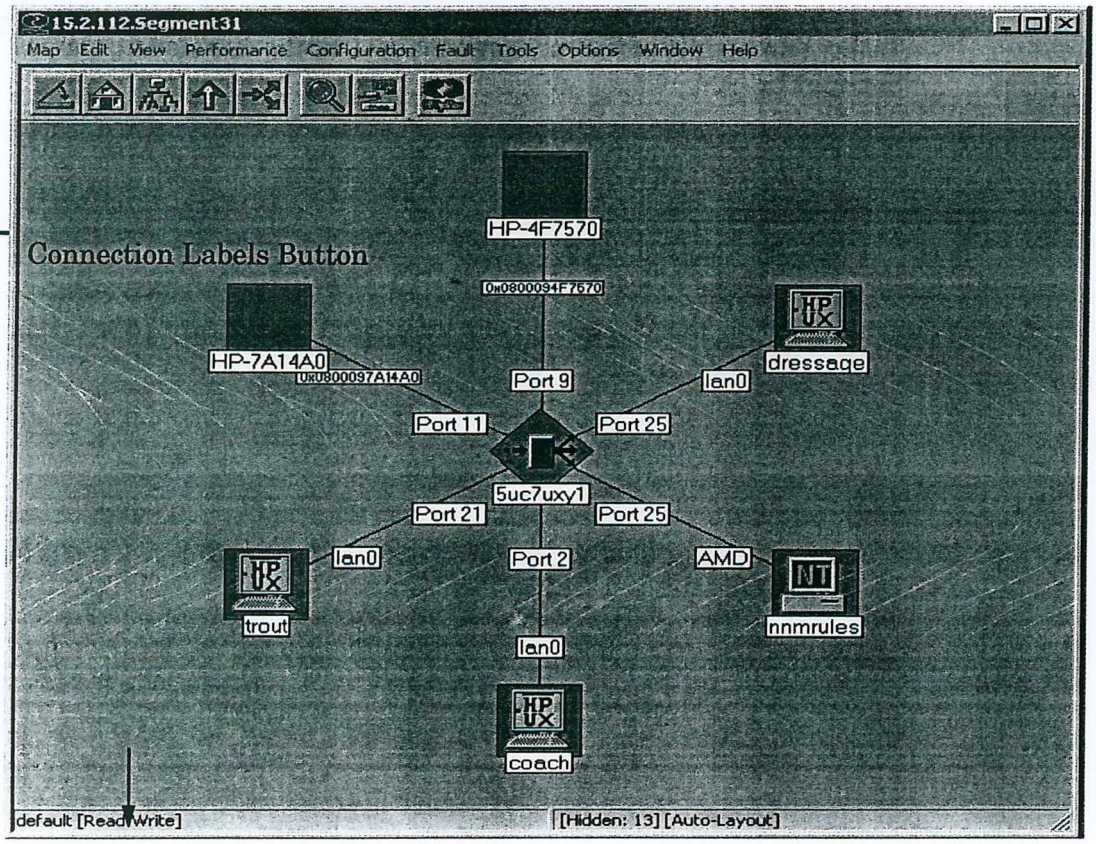
Figure 8-3 Meaningful Names for Network Symbols



Turning Connection Labels on or off

Connection labels indicate the port used to connect one network interface to another. Use either the `View:Show Connection Labels` menu item or the `Connection Labels` button to turn this feature on or off. On a Windows operating system you can control the connection label feature through the `View` tab contained in the `Map:Properties` or `Submap:Properties` pull-down menus.

Figure 8-4 Show Connection Labels Enabled



NNM labels each end of a connection unless one end is a container object such as a segment, network, or location. Connection labels are created from information made available by equipment manufacturers. Since

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0071
Doc: 3740

devices return information in varying formats, connection labels vary from device to device. If NNM cannot read or understand the information from a device, it will not label the connection.

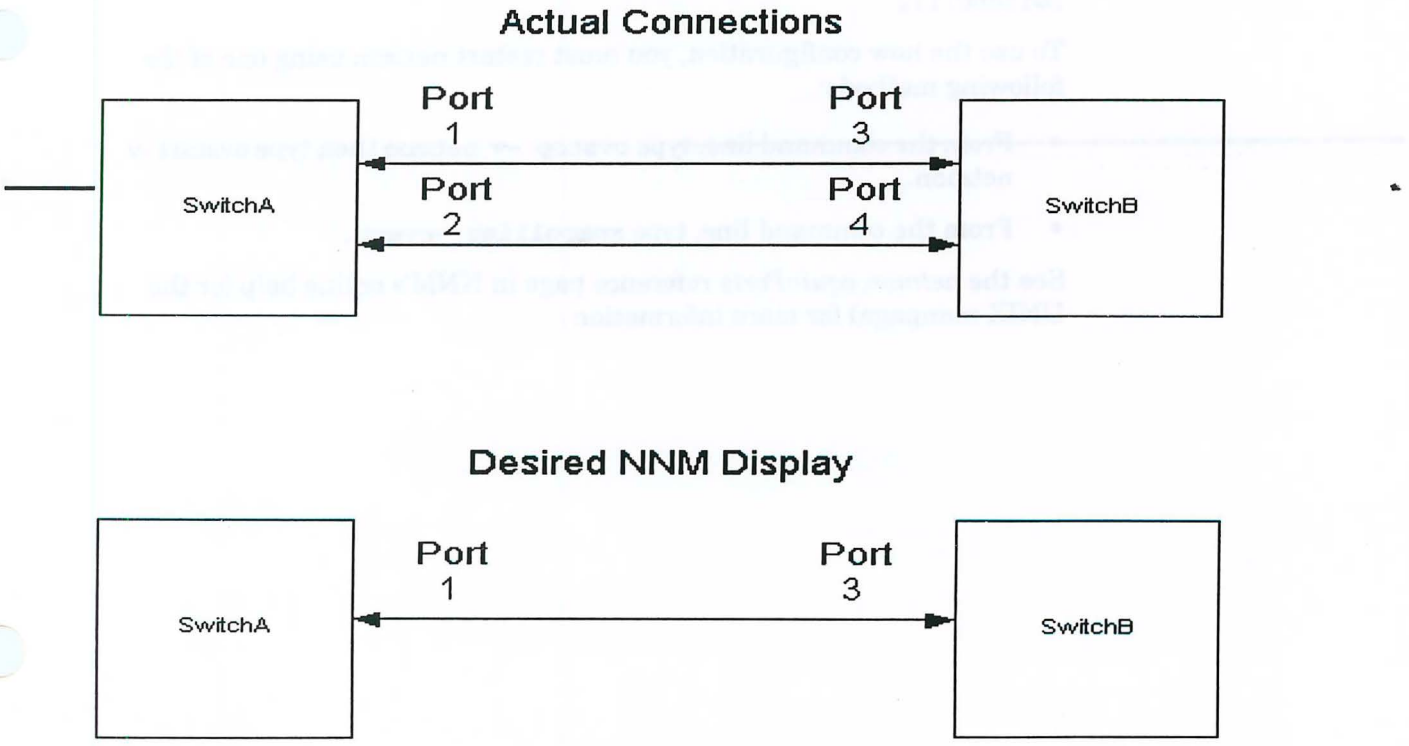
For devices that do not respond to SNMP requests, the connection label usually defaults to the IP address of the node. One common cause of devices not responding to SNMP requests is a mismatched community name. If you suspect that your GET-Community names are not matching up with the settings on your management station, see"GET- and SET-Community Name and SNMP Port Issues" on page 145.

The connection label depends on information gathered during discovery and may be updated during a configuration poll. Changes on the devices may not appear on the connection label until the next configuration poll. To force an update of the connection labels, at the command prompt, type **`ovtopofix -U`**.

Configuring Trunking and Meshing

Configuring two or more ports between two network devices into a single group is referred to as **port trunking**. This is done to increase the available bandwidth between two devices. For example, look at the actual connections diagrammed in Figure 8-5. The available bandwidth between switches A and B increases when ports 1 and 2 on switch A and ports 3 and 4 on switch B are connected in a trunk configuration.

Figure 8-5 **A Port Trunking Example**



NNM is unable to detect port trunking and meshing automatically. For example, NNM will move devices around on your map depending on which port in the trunk or mesh configuration it last heard the device. To control NNM's representation of this topology, you can enter port trunking configuration information into the following file:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0072
3740
Doc:

To specify a mesh, add a line in the `netmon.equivPorts` file for each switch participating in the mesh. The `netmon.equivPorts` file consists of parameters in the format *`host`*`:`*`port-spec`*`:`*`port-spec`*`: [`*`port-spec`*`]` where *`host`* is an object identifier such as a host name, IP address, or MAC address, and *`port-spec`* is a combination of *`group_number`*, *`port_number`*.

When labeling any of the ports participating in a mesh relationship, NNM labels the object with the first *`port-spec`* parameter from the `netmon.equivPorts` device line entry.

For example, to achieve the results shown in Figure 8-6, the `netmon.equivPorts` file would have the following entries:

```
SwitchB:1:2

SwitchC:1:2
```

To use the new configuration, you must restart `netmon` using one of the following methods:

- From the command line, type **`ovstop -v netmon`** then type ovstart -v netmon.
- From the command line, type **`xnmpolling -event.`**

See the *netmon.equivPorts* reference page in NNM's online help (or the UNIX manpage) for more information

Establishing Submap Persistence Settings

The persistence settings allow you to control the number of submaps that are retained in memory (RAM) so that they are available at all times, rather than generated upon demand. There are several of things to keep in mind when making your choices:

- Persistent submaps display faster.
- The greater the number of persistent submaps, the greater the need for RAM on the management station.
- Only those submaps that are persistent are included when a map snapshot is created.
- Only those submaps that are persistent are included in the initial scoping pane list for NNM's web access.
- You can set persistence by logical level of network structure (such as internet level, network level, or segment level).
- You can establish a persistence filter that specifies making persistent all submaps that contain certain devices, that you specify (page 230).
- Any time that you make an editing modification directly to a l all related parent submaps up to the internet level become persistent; for example, turn off auto-layout, set window geometry, add a background graphic, or add an

NOTE If you add background graphics to your submaps, they automatically become persistent. Keep in mind that graphic files are quite large and may significantly increase the amount of memory required to keep the submap in RAM.

NNM's default setting for this feature:

- *Windows:* Only the Internet level and the containment realm of the map are persistent.
- *UNIX:* All levels of the map are persistent.

RQS nº 03/2005 - CPMI - CORREI
Fls. Nº 0073
3740
Doc:

NOTE The selection that you make affects remote consoles and the web display after the map is reloaded or refreshed on each system.

By Logical-level of Your Network's Structure

If you choose to set the persistence by logical level, select the `Map:Properties` menu item, select the `Applications` tab, and double-click the `IP Map` entry. The level to which submaps should be persistent can be one of the following values:

`Unset`	*Windows:* Same as `Internet Level`. *UNIX:* Same as `All Levels`.
`All Levels`	Specifies all submaps as persistent.
`Segment Level and Higher`	Specifies that Segment-, Network-, and Internet-level submaps are persistent.
`Network Level and Higher`	Specifies that Network- and Internet-level submaps are persistent.
`Internet Level`	Specifies that Internet-level submaps are persistent.

By Presence of Specific Devices

A persistence filter describes which specific network devices should have their submaps retained in memory (RAM) at all times.

This may be useful if you want to use the snapshot feature (see Appendix B, "Network Troubleshooting Tools," on page 553 or NNM's online help) as part of your normal business procedures and need to make sure the snapshots always include information about specific critical devices. It may also be a useful way to keep the number of submaps retained in memory (RAM) to a minimum when you are using an HP OpenView program that requires the submaps containing certain devices to remain present in RAM.

The persistence filter is defined in the `filters` file (the same file that contains any discovery filters, DHCP filters, etc.):

- *Windows:* *`install_dir`*`\conf\C\filters`
- *UNIX:* `$OV_CONF/C/filters`

NNM includes a predefined persistence filter section for your convenience as a starting point, or you may define your own. For detailed information about how to develop a filter, refer to *A Guide to Scalability and Distribution*.

After you create your persistence filter:

- Select the `Map:Properties` menu item, select the `Applications` tab, and double-click the `IP Map` entry.
- Click on `Persistence Filter` and type the name of the section in NNM's `filters` file that you just created.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0074
3740
Doc:

Controlling Which Devices Appear on the Map

You can control which devices are visible on a particular map. It is important to remember that all maps derive their information from the same database, so *deleting* an object (specific device) from the database eliminates it from all maps (until the next discovery polling interval). Rather than using delete, consider the following choices:

- Map Filter:

  A map filter allows you to remove nodes from view on the map. You write the map filter using Boolean logic and place it in the `filters` file with all the other NNM filters. You can create multiple map filters and assign a unique filter to each map.

- Hide Feature:

  The hide feature enables you to modify which group of symbols is displayed on any submap in an interactive way (without needing to write a filter using Boolean logic).

NOTE These changes are visible from remote consoles and web access after the map is reloaded or refreshed on each system.

Creating a Map Filter

A map filter allows you to remove certain nodes from view on the map while continuing to monitor them and receive alarms from them in the event/alarm portion of NNM. Map filters are defined in the `filters` file (the same file that contains any discovery filters, DHCP filters, and so on):

- *Windows:* `install_dir\conf\C\filters`
- *UNIX:* `$OV_CONF/C/filters`

See *A Guide to Scalability and Distribution* for information about creating filters.

You can create multiple map filters and assign a unique filter to each map. See the `filters` file for predefined examples as a starting point. Your filter can be applied/changed at any time by opening the map, selecting `Map:Properties`, selecting the `Applications` tab, and opening the configuration dialog box for `IP Map`.

Testing Your Filter

See *A Guide to Scalability and Distribution* for information about testing and troubleshooting your filters.

Using the Hide Feature

The hide feature allows you to customize individual submaps as well as all submaps in a map. For example, you may wish to hide everything except printers to create a special set of submaps specifically for monitoring printers, or hide everything except routers to create a special submap specifically for monitoring routers. Because all maps derive their information from the same database, if you delete all instances of any symbol, the underlying object in the database is also deleted. The hide feature enables you to modify the group of symbols displayed on any submap in an interactive way (without needing to learn Boolean logic in order to write a filter).

NOTE If the submap is transient, it becomes persistent when you hide a symbol. (Use the map filter if you wish to hide symbols without effecting persistence.)

If devices are hidden on a particular submap:

- `[Hidden:#]` appears on the right side of the status bar giving notice about how many devices are hidden (# = number of hidden objects).
- There is no way to determine which devices are hidden, only how many are hidden.
- If you wish to show a hidden object on a particular submap, you must show all hidden objects. There is no way to specify which hidden objects to show.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0075
Doc: 3740



To hide a symbol, select the symbol or symbols that you wish to hide, select `View:Hidden Objects`, and select `Hide Selected From This Submap` or `Hide Selected From All Submaps`. You can use the Find feature in partnership with the Hide feature to hide groups of symbols such as all routers.

Testing and Troubleshooting

If you choose to hide a symbol from all submaps but change your mind later, to undo the action you must show ALL hidden symbols on ALL submaps.

To display hidden symbols on individual submaps, open each affected submap and select `View:Hidden Objects->Show Hidden On This Submap`.

To display hidden symbols on all submaps, open any submap and select `View:Hidden Objects->Show Hidden On All Submaps`.

Backing Up Your Efforts

The next time NNM's backup process runs, your modifications will be included.

Changing/Adding Object Attribute Fields

You may wish to modify or add object attribute field definitions so that your team can search on custom criteria when resolving network problems or so that a new application can manage the object.

NOTE You can only add fields, you cannot delete them. Adding fields does not affect submap persistence.

An NNM object represents a logical or physical entity or resource, or a group of such logical or physical entities or resources that exist in a network environment. In NNM, an object usually represents any particular thing of interest for the purpose of doing network or systems management. An object can represent a physical item (such as a PC, a gateway, a router, or an interface card) or it can represent a logical item (such as a group of PCs, all 486 PCs, or all nodes in a single department). An object is represented on the map graphically by a symbol.

An object is constructed of individual characteristics that are called attributes. Attributes include the name of the object and various characteristics that are used to classify the object. An object, for example, might have the name `IP Hostname` and an attribute such as `isDevice`.

To view the attributes assigned to any object, select any symbol that represents the object and then display the `Edit:Object Properties` dialog box. A list of attribute categories is displayed, such as `Capabilities`, `General Attributes`, and application-specific categories such as `IP Map` (an application included in NNM). Select any category to display its list of attribute names and values.

The attribute names represent fields in the NNM object database, and the data in the fields are the object's attribute values. Possible modifications/additions to the information in the object database:

- Change the current value in an attribute field through the object properties' `General Attributes` dialog box.
- Change a symbol's *type* in order to switch to a different set of attribute fields.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0076
Doc: 3740

- Add underlying definitions of attribute fields by editing field registration files (FRF).

These changes are visible from remote consoles and NNM's web interface after the map is reloaded or refreshed on each system.

TIP

The following *analytical data* directories are *not* included in NNM's backup scripts:

- *Windows:*

  ```
  install_dir\backgrounds
  install_dir\bitmaps
  install_dir\www\htdocs\bitmaps
  install_dir\www\registration
  ```

- *UNIX:*

  ```
  $OV_BACKGROUNDS
  $OV_BITMAPS
  $OV_WWW/htdocs/bitmaps
  $OV_WWW_REG
  ```

If you make changes or additions to map backgrounds, bitmap files, or web registration files ensure that your new files are properly backed up. See "Backup/Restore to Protect Your Investment of Time" on page 165 for more information.

Changing the Value in an Attribute Field

You can change the description of an object by modifying the values assigned to its attributes (characteristics) in the `General Attributes` dialog box. See NNM's online help for more information.

To change object attribute values:

- *Windows:* Select a symbol; then select `Edit:Object Properties`. Alternately, right-click the a symbol and select `Object Properties` from the pop-up menu. The values in the `General Attributes` dialog box can be modified. To edit these values, click on the attribute name.

- *UNIX:* Select a symbol; then select `Edit:Object Properties`. Alternately, click mouse button 3 on a symbol and select `Object Properties` from the pop-up menu. The values in the `General Attributes` dialog box can be modified. To edit these values, click on the attribute name.

For example, clicking on `isSNMPSupported` will toggle the value between `TRUE` and `FALSE`; clicking on `SNMPAgent` will pop-up a dialog box from which you can choose the SNMP agent.

NOTE This change is visible from remote consoles and the web interface after the map is reloaded or refreshed on each system.

Changing Symbol Type to Switch Attribute Sets

You can assign a new set of attributes to an object by changing the symbol type of the object.

NOTE This step adds fields, but does not delete or change values in existing fields.

l and select `Change Symbol Type` from the pop-up menu.

UNIX: Click mouse button 3 on a symbol and select `Change Symbol Type` from the pop-up menu.

NOTE This change is visible from remote consoles and the web interface after the map is reloaded or refreshed on each system. Changing the symbol type forces the submap to become persistent.

See NNM's online help for more information about changing symbol type. See also the *OVwRegIntro* reference page in NNM's online help (or the UNIX manpage) for more information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0077
Doc: 3740

NOTE

The ipmap service automatically assigns a symbol type and label based upon information it receives from the netmon service. This means that if you modify the symbol label or symbol type of an object that is managed by NNM, your changes will be replaced by the values assigned by NNM the next time configuration polling runs.

You can turn off this ipmap capability by setting the environment variable IPMAP_NO_SYMBOL_CHANGES=TRUE. See the *ipmap* reference page in NNM's online help (or the UNIX manpage) for information about the -u parameter.

Alternately, you can modify the oid_to_sym file to specify that a different symbol be associated with a specific *type* of device (determined by sysObjectID). See the *oid_to_sym* reference page in NNM's online help (or the UNIX manpage) for more information. See "Changing All the Symbols for a Particular Device" on page 661 for a complete example.

Adding Attribute Fields in the Object Database

If you want to add a specific attribute field that is not yet defined in the object database, you simply create or modify the field registration files (FRF):

- *Windows:* *install_dir*\fields\C*.*
- *UNIX:* $OV_FIELDS/$LANG/*

See NNM's online manual, *Creating and Using Registration Files*, for complete information about changing fields or adding fields.

See the *OVWRegIntro* reference page in NNM's online help (or the UNIX manpage) for more information.

TIP

Set the Locate and General flag for the field when you define it. Locate enables your new field to appear in the Edit:Find->Object by Attribute dialog box. General enables the field to show up in the Object Properties, General Attributes category.

After you have modified the field registration files:

1. Display a list of currently running sessions. At the command prompt type:

   ovstatus -v ovuispmd

   You may want to print out this information so that you have the hostnames and session IDs for restarting the sessions later. You may wish to notify those users who are currently accessing NNM to warn them about the shutdown.

2. Stop all sessions. At the command prompt, type:

   ovstop -c ovuispmd

   (This terminates any sessions and stops only the `ovuispmd` service--the maps are all closed, but your network is still being monitored by NNM.)

3. Force NNM to update the field definitions in the object database. At the command prompt, type:

   ovw -fields

4. To start new NNM sessions, at the command prompt, type:

   ovstart -c ovuispmd

5. Open NNM's user interface to begin one or more sessions.

parsed for correctness and checked for errors which are reported to:

- *Windows:* The error message pop-up `Console` window. Messages are always appended to the end of the Console file. It is a good idea to clear the contents of this file (`Edit:Clear`) each time that you see it.
- *UNIX:* `stderr`

Close the NNM interface and reopen the maps to view your changes (see "Closing All Current Sessions" on page 319).

NOTE These changes are visible from remote consoles and web access after the map is reloaded on each system.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0078
3740
Doc:

Making the Maps Look Like Your World

Review the worksheet from Chapter 4, Planning Your NNM Configuration, where you identified the maps that your organization needs and the network devices that need to be present on each map. Now customize the look of each map to meet the needs of your team. When you edit a map, your changes affect only the *open* map. If you want the same customizations on multiple maps, make the changes once, then copy the modified map. A map can be customized in the following ways:

- By controlling the placement of the symbols on your map.
  By default, NNM controls how symbols are placed on your submaps, but you can take control of how symbols are placed on individual submaps. You can also turn off auto-layout for the whole map.
- By adding your own submaps:
  - *Partitioned Internet* submaps (child submaps at the Internet-level) to break the Internet symbols into smaller groups of information, such as by country, city, building, department, or floor by using container objects (location symbols). These changes (*and these changes only*) can be copied to other maps using the `Map:Export` and `Map:Import` feature.
  - *Child* submaps (at the Network-, Segment-, or Node-level) to add more information to an explodable symbol.
  - *Meta-connection* submaps automatically created by NNM whenever there are multiple connections between two symbols. Double-click on the connecting line to explode a submap showing each connecting-line symbol.
  - *Independent* submaps to create your own custom hierarchy of submaps that is independent of the hierarchy automatically created.
- By adding background graphics such as map images, site-specific images, or floor plans ("Background Graphics" on page 260). Use *.GIF files to ensure that the background graphics are visible over web access.

NOTE These changes are visible from remote consoles after the map is reloaded or refreshed on each system. These changes are immediately visible in NNM on the web.

Controlling the Placement of the Symbols on Your Map

NNM's auto-layout controls the placement of symbols on the maps (see "Automatic Discovery and Layout" on page 56 for more information about how auto-layout works). If you want to make changes to the placement of symbols, you must first turn off auto-layout. Auto-layout can be turned `On/Off` for a single submap or for all submaps in the open map.When auto-layout is turned off, the `[Auto-Layout]` message at the bottom of each affected submap disappears, and the `New Object Holding Area` appears across the bottom of the submap. Any time a new object is discovered, a map symbol is moved to another submap, a bridge or hub is moved within a network submap, or a hidden object is set to show on your network, the affected symbols will show up in the `New Object Holding Area` to await your decision about placement.

TIP When accessing NNM over the web, there is no `New Object Holding Area`. However, the status bar notifies you if objects are currently in the `New Object Holding Area`.

Auto-Layout Algorithms (Default Layout Rules)

The layout algorithm for a submap is set when the submap is created. If an application (such as NNM) creates the submap, it specifies a layout algorithm. NNM's default layout algorithm for a submap is based upon the symbol type of the parent object and cannot be changed after the submap is created.

The possible layout algorithms are:

- None. Symbols are arranged by the user or are left in the `New Object Holding Area`.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0079
3740
Doc:

- Point To Point. Symbols are arranged as an arbitrarily interconnected set of nodes and connections.
- Row/Column. Symbols are arranged in rows and columns.
- Bus. Symbols are arranged along a snake-like backbone representing the linear array of nodes on a segment.
- Star. Symbols are arranged in a star consisting of a circle and a center symbol. You can set the star center using the symbol pop-up menu.
- Ring. Symbols are arranged in a circle.

If automatic layout is enabled:

- `[Auto-Layout]` appears on the right side of the status bar.
- When a new symbol is added to the submap, NNM places the symbol on the submap according to the assigned layout algorithm.
- Although you can move the symbols in the submap, all symbols in the submap snap back to their original position when the `ipmap` service checks for changes.

By default, auto-layout is turned on. If you turned it off and change your mind, to turn auto-layout on:

- *Windows:*

  For all submaps, select `Map:Properties` and access the `View` tab.

  For one submap, select `Map:Submap->Properties` from that submap and access the `View` tab. Select the `Auto Layout` field.

- *UNIX:* Select either:

```
View:Automatic Layout->On For All Submaps
View:Automatic Layout->On For This Submap
```

Do-It-Yourself Layout

If you want to create a customized placement (for example, to place symbols on a background graphic that shows their geographical location), you need to turn off automatic layout for the submap you want to customize.

NOTE If the submap is transient, it becomes persistent when you turn off auto-layout.

If automatic layout is disabled:

- A `New Object Holding Area` is created in the lower portion of the submap. Symbols in the `New Object Holding Area` are shown without their connections. Connections are automatically added when you remove the symbol from the holding area and place it on the map.
- Symbols added to the submap are placed in the `New Object Holding Area`. You can move symbols from the `New Object Holding Area` to the submap.
- You can move symbols within the submap window by dragging and dropping them with the mouse.
- You cannot move a symbol from the submap to the `New Object Holding Area`.
- You can arrange symbols in the submap according the assigned layout algorithm by selecting `View:Redo Layout`.
- When hidden symbols are unhidden, they are placed in the `New Object Holding Area`.

To disable auto-layout:

- *Windows:*

  For all submaps, select `Map:Properties` and access the `View` tab.

  For one submap, select `Map:Submap->Properties` from that submap and access the `View` tab. Deselect the `Auto Layout` field.

- *UNIX:* Select either:

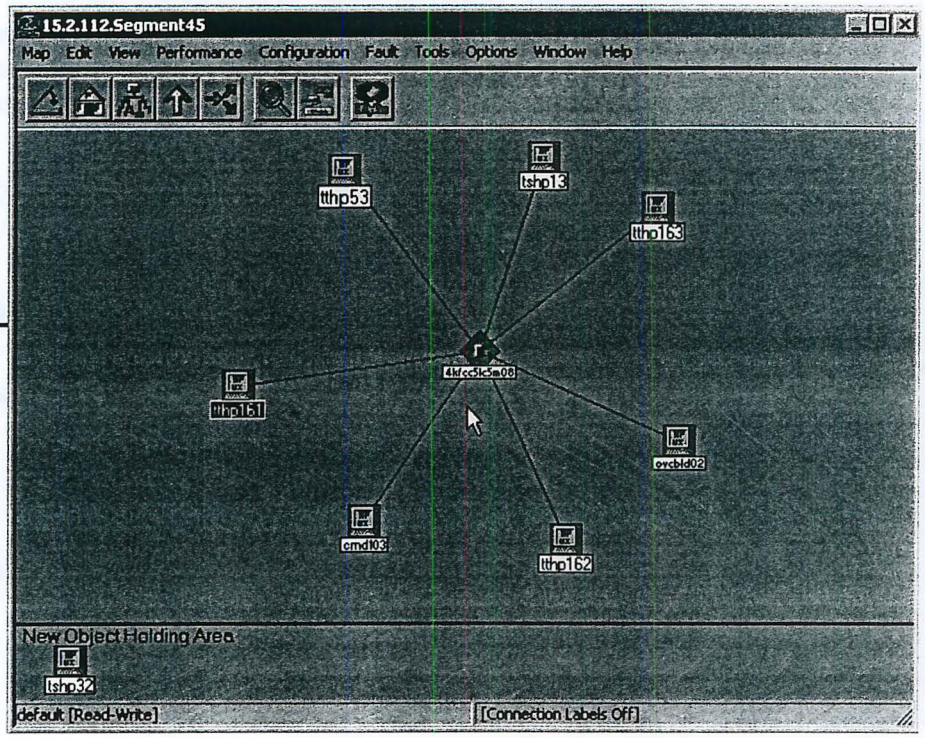
```
View:Automatic Layout->Off For All Submaps
View:Automatic Layout->Off For This Submap
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0080
3740
Doc:

New Object Holding Area

A `New Object Holding Area` (Figure 8-7) appears on the lower portion of each submap window if the submap has no layout algorithm or if the assigned layout algorithm is disabled (automatic layout is turned off). Symbols in the `New Object Holding Area` are shown without their connections.

Figure 8-7 **The New Object Holding Area**



New Object Holding Area

Adding Your Own Submaps

You can create submaps that show a particular view of some aspect of your network. For example, you may create one submap to show all the nodes on a particular network segment, and create another submap that shows all the software subsystems of a particular node.

Child Submap or Independent Submap?

The method you use to create a new submap determines whether the submap is a *child submap* or an *independent submap*.

- A *child submap* is related to a parent object. To create a child submap, double-click on an explodable symbol. If no child submap exists, you are prompted to create one (for example, when you create a new container object).
- An *independent submap* is created from the `Map:Submap->New` menu item. The submap has no associated parent object and is independent of any existing hierarchy of submaps. To display an independent submap, select a submap entry in the `Edit:Find->Submap` dialog box.

TIP You cannot open the independent submap by double-clicking on a symbol unless you manually add a symbol to the root-level submap that invokes your independent submap.

An independent submap can be used as the beginning of a new submap hierarchy. You must create any child submaps starting from the independent submap to build an additional submap hierarchy into the map. NNM cannot automatically generate these child submaps for you. NNM also cannot update your independent hierarchy as new nodes are discovered or changes occur to the connections.

The map must be open with read-write access before you can create a submap.

Meta-Connection Submaps (for multiple connections)

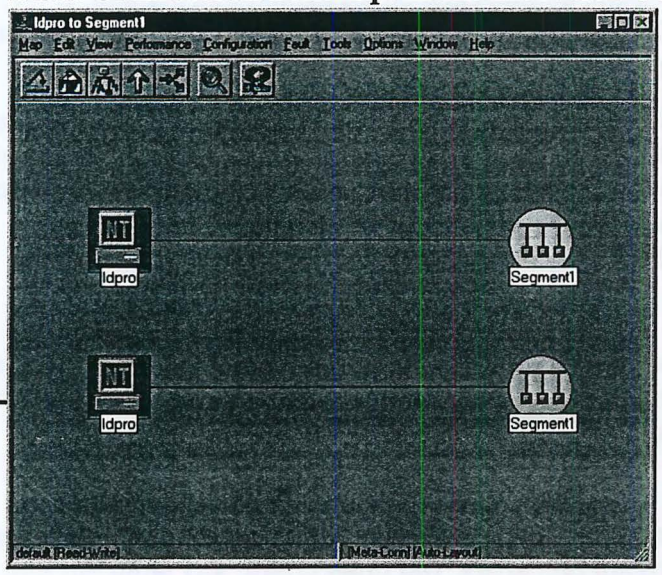
If two devices represented by symbols on your map communicate over *multiple* connections, you can double-click upon the connecting line to display a meta-connection submap. The meta-connection line (symbol) on your submap looks the same as a regular line on your map (connection symbol).

NNM does not display multiple lines between the two objects; instead, each individual connection between the two symbols is displayed on the line's meta-connection submap. NNM automatically creates a meta-connection submap when you (or an application) add a connection

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0081
3740
Doc:

symbol between two symbols in a regular submap that already have a connection. You can add an unlimited number of connections between two symbols in a regular submap. Each of these connections is automatically added to the meta-connection submap with the two symbols as end points.

Figure 8-8 Meta-Connection Submap: Multi-Interface Connections



A *meta-connection submap* displays the status of each connection between two symbols or a symbol and a backbone. Compound status colors from the meta-connection's submap are propagated to their parent submap differently as compared to regular submaps (page 274). The meta-connection symbol in the parent submap displays the compound status of the multiple connections in the meta-connection submap. Any unconnected objects in the meta-connection submap also contribute to compound status. However, the connected icon symbols in a meta-connection submap do not propagate their status. Their status is maintained by the symbols in the parent submap above the meta-connection submap. (Meta-connection submaps are not accessible over NNM's web interface.)

You can:

- Create a child submap from a meta-connection submap by double-clicking on any of the objects in the meta-connection submap. Therefore, the meta-connection submap can be a parent of other regular submaps.

- Select objects in the meta-connection submap.
- Add unconnected objects to a meta-connection submap.
- Add connections at the parent level submap. (You cannot add connections directly on a meta-connection submap.)
- Delete the meta-connection submap by deleting the last object from the meta-connection submap.

Customizing the Internet Level of Your Network Map

As a result of the initial discovery process, NNM displays one Internet symbol on the root submap *and creates one Internet submap*. Within the Internet submap are symbols representing IP and IPX networks, and IP- and IPX-addressable gateways (routers). This section provides definitions and procedures that you can use when editing the internet level of your network map (for information about editing the network, segment, or node levels, see page 256). In order to understand your options, you need to know:

- What are container objects.
- rnet submaps.
- What is the containment realm.
- How to expand the single Internet submap into multiple partitioned internet submaps.
- the partitioned internet submaps.

NOTE To manage IPX networks, you must be running NNM on a management station using a Windows operating system. If you are running NNM on a management station using a UNIX operating system, you can configure a system that uses the Windows operating system to serve as a collection station that forwards IPX information to the UNIX system. This requires another copy of NNM to be running on the system with the Windows operating system. See *A Guide to Scalability and Distribution* for information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0082
3740
Doc:

Container Objects to Hold Part of Your Map

You can group the symbols on the Internet-level submap into logical submaps that reflect the physical or logical reality of your network and working style.

First, you add symbols called *container objects* to the Internet submap. The container objects allow you to create maps by location, building, department, or whatever makes sense to you. Each container object explodes into a new submap called a *partitioned internet submap*. Container objects can be either the Internet symbol (in the Network class) or any of the symbols in the Location class (see NNM's online help Display Legend for a quick look at your choices).

Partitioned internet submaps can contain gateway router symbols and subnet symbols. To maintain the map hierarchy, partitioned internet submaps are only allowed between the Internet-level submap and the Network-level submap. NNM maintains the connection between devices as you create the partitioned internet submaps.

Partitioned Internet Submaps

The symbol of a container object opens a special submap called a partitioned internet submap. You can add symbols from the Location class and the Internet symbol from the Network class to any partitioned internet submap. Thus, you can create a hierarchy of partitioned internet submaps as many levels deep as you wish. For example, you may want to subdivide your management domain by continent, then by country, then by city, showing your IP and IPX networks, and IP and IPX-addressable gateways (routers) only at the city level.

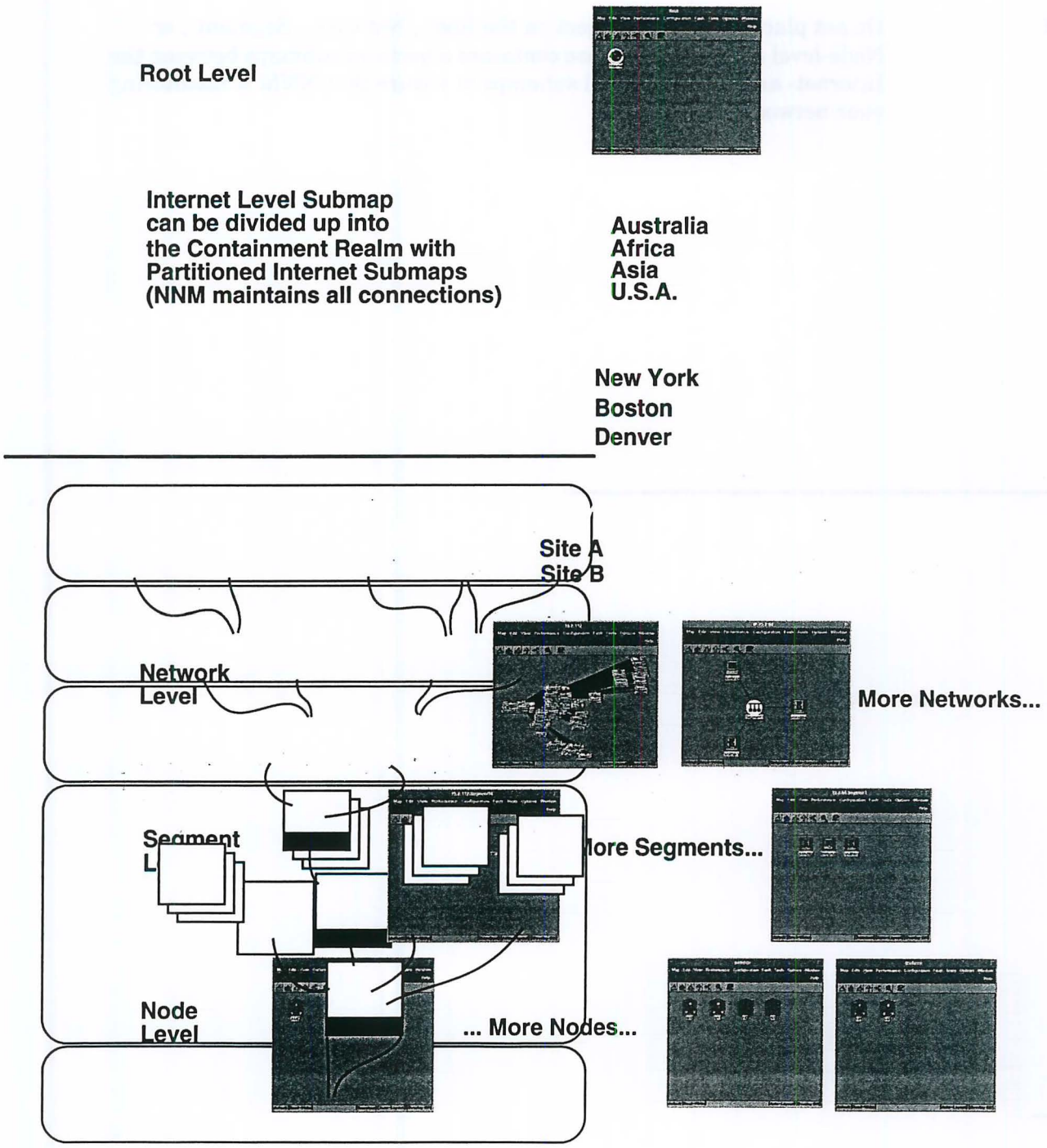
The Internet submap always remains at the top of your hierarchy of partitioned internet submaps and is opened whenever the Internet symbol is selected from the root map.

You can create multiple levels of partitioned internet submaps to rearrange how your network map is displayed. NNM maintains the connections and monitors the devices placed within a container object as long as the container objects are on submaps between the Internet-level submap and any Network-level submaps. If you use container objects at other levels of the map, NNM cannot manage the devices that are contained in the submaps, so connections are lost and status is not updated.

NOTE Do not place a container object on the Root-, Network-, Segment-, or Node-level submaps. Only use container objects on submaps between the Internet- and Network-level submaps to ensure that NNM is monitoring your network devices.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0083
3740
Doc:

Figure 8-9 Containment Realm: Partitioned Internet Submaps



Creating a Partitioned Internet Submap

To create a partitioned internet submap, add the Internet symbol from the Network class or any of the symbols from the Location class to the Internet submap or any partitioned internet submap. The new symbol represents a special object, called a container object. Symbols of container objects open into a partitioned internet submap. You can then cut and paste IP and IPX network and gateway (router) objects from your Internet submap into your partitioned internet submap. NNM maintains all connections between your IP and IPX network and gateway (router) objects.

NOTE It is important to follow these directions *exactly*.

To add a container object to an Internet or partitioned internet submap:

1. Select the `Edit:Add Object` menu item. The `Add Object Palette` appears.
2. From the `Add Object Palette`, select either:
   - the `Network Class`'s Internet symbol
   - the `Location Class` (any symbol)

   Drag the symbol onto the Internet submap or the partitioned internet submap of your choice. The `Add Object` dialog box appears.
3. Specify your choices in the `Add Object` dialog box.
4. Click on `[OK]`. The newly added symbol resides on the submap, and an empty child submap (partitioned internet submap) for that symbol is automatically created. To open the new partitioned internet submap, double-click on the new symbol.

NOTE Until you add objects to your new partitioned internet submap, the container symbol displays an unknown status. In the new container symbol's `Object Properties` dialog box, `IP Map` is not listed as a configurable application because the `IP Map` service does not require any information about the container object.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0084
3740
Doc:

5. Use `Edit:Cut` and `Edit:Paste` to place the desired IP and IPX network and gateway (router) objects into the new partitioned internet submap.

All submaps, objects, symbols, and connections that are contained under a cut-and-pasted symbol remain intact. Symbol behavior and status are maintained. For example, if the symbol you paste onto a map explodes into a child submap, that capability also exists for the new symbol.

The Containment Realm

The Internet submap and the hierarchy of partitioned internet submaps make up the **containment realm**. You can populate a manually created partitioned internet submap by cutting and pasting IP and IPX network and gateway (router) symbols from the Internet submap to a partitioned internet submap. Only one symbol is allowed for each IP and IPX network and gateway (router) symbol; however that symbol can be placed in any location within the containment realm.

Within the containment realm, when you cut and paste these symbols the hierarchical and topological relationship between symbols is maintained. When you cut these symbols from the Internet submap and paste them on a partitioned internet submap, the hierarchical [illegible] wn the map hierarchy. In other words, that symbol's child submaps along with all associated symbols and objects are [illegible]

In addition to the hierarchical relationship, all topological relationships between symbols are maintained. NNM maintains the connections between symbols after they are pasted onto a partitioned internet submap by redrawing their connections to the symbol of the container object.

Editing Guidelines

NOTE You must follow these directions *exactly* in order to maintain the connections between devices on your map as you work and in order to maintain NNM's monitoring of your network devices.

This section discusses the types of editing operations you can perform in the containment realm *while maintaining the connections between symbols*.

To maintain connections between symbols in the containment realm:

Use `Edit:Cut/Edit:Paste` or drag-and-drop.

However, you must also follow these guidelines:

- You can cut and paste symbols between the Internet submap and any partitioned internet submap.
- You *cannot* cut from and/or paste symbols onto the Root submap or the Network, Segment, and Node submaps. In other words, cut/paste is only allowed on the Internet or containment realm level.
- You *cannot* cut and paste or drag and drop container symbols themselves. If you paste a container object on one of these submaps, the containment information is broken; that is, the symbol will no longer maintain its relationship to other symbols. Connections between that symbol and other symbols are also broken.

Once a cut and paste or drag and drop operation has been made between submaps, IP Map will need to resynchronize. You cannot perform any other operations until this resynchronization is complete.

Example of an Internet Submap

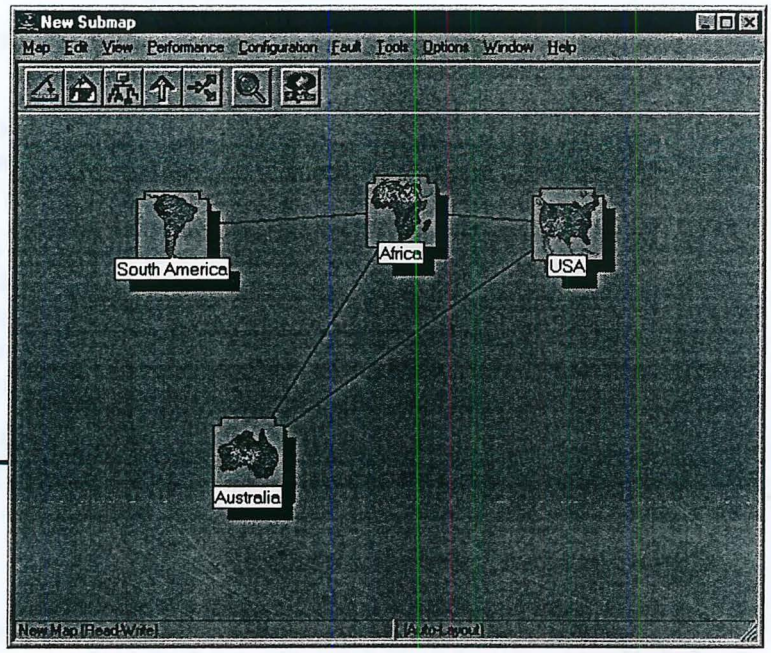
On the Internet submap, you can place a map of the world and add symbols that represent container objects of countries or continents. Each container object opens into its own submap. You can then cut symbols that represent your resources in a particular country or continent from the Internet submap and paste them into the appropriate partitioned internet submap.

The following figure shows an Internet submap in which four container objects were added. The symbols of the container objects represents Australia, U.S.A., South America, and Africa. In addition, all symbols of objects discovered by NNM have been cut from the Internet submap and pasted in lower-level partitioned internet submaps. NNM maintains the

IRQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0085
Doc: 3740

connections between the symbols of discovered objects in the lower-level submaps. Also, NNM creates the proper connections between the symbols of the container objects.

Figure 8-10 IP Internet Submap

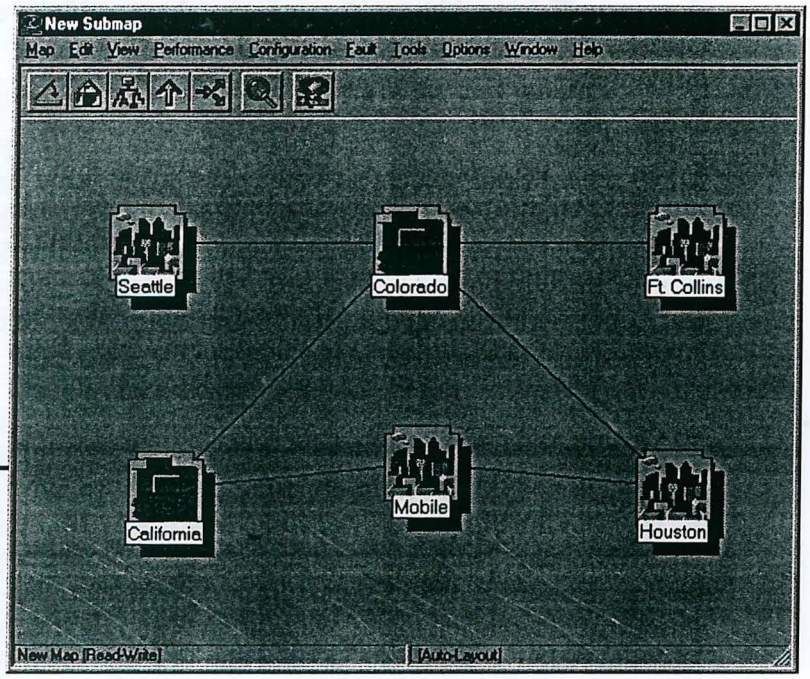


Example of Partitioned Internet Submap

The following figure shows the U.S.A. submap. Six container objects have been created in this submap. This submap may also contain symbols representing IP and IPX networks or gateways. From this submap, you can double-click on any of the six container objects and open a

partitioned internet submap, which may display an additional partitioned internet submap containing other container objects or symbols that represent IP and IPX networks and gateways.

Figure 8-11 Partitioned Internet Submap of the USA



Maintaining the Containment Realm

As you customize your submaps, NNM tracks any editing changes you make to the open map. The Internet submap and all partitioned internet submaps make up the containment realm. NNM continues to manage objects that have been moved within the containment realm with the network monitoring process (`netmon`).

If new IP- and IPX-addressable resources are added to the network, NNM discovers these resources, creates objects for them, and adds a symbol for each object to the appropriate submap or submaps. NNM always places IP- and IPX-addressable gateways (routers) and networks that have been discovered on the original, highest-level Internet submap.

You can maintain the customized organization of your network map by distributing these symbols ("Editing Guidelines" on page 252) to the partitioned internet submap of your choice.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0086
3740
Doc:

When creating multiple maps on one management station, using the `Map:Import` and `Map:Export` feature is an easy way to copy your *containment-realm customization* changes from map to map.

CAUTION Always make an export file of any map before importing changes from another map. This enables you to undo the changes if you don't like what happened.

All your container objects as well as the objects that NNM automatically placed at the internet level are included. Changes to the lower-levels of the map (network/segment/node) and any executable symbols (page 279) are not included in the export/import nor are they affected in any way by the import/export. If you need multiple maps that include your customizations to *all* levels of the map, use `Map:Save As` instead.

TIP The `Map:Export/Map:Import` feature *may* be useful if you are configuring NNM on a test machine and plan to move changes to a production machine at a later time. Make sure that exactly the same HP OpenView and 3rd party products are installed on both machines to ensure a successful map export/import operation. See NNM's online help for more information about Map Import/Map Export. If you need to move customization at all levels of your map, rather than just at the Internet and containment realm levels, use NNM's backup and restore feature instead (page 165).

Customizing Network-, Segment-, or Node-Level Submaps

Editing the lower-level network submaps enables you to distribute resources over your map to better match how your network is organized. You can:

- Copy or move symbols within or between submaps.
- Add symbols to your submaps.

Copying or Moving Symbols

Copying or cutting and pasting are convenient ways to edit your network map. The cut and paste operation is the means for changing a symbol's location from one submap to another, and is essentially a move operation. You can cut and paste multiple symbols simultaneously.

If you cut and paste symbols at the network, segment, or node levels, NNM will *not* maintain the previous connections between these symbols. Therefore, after cut and paste operations, you must add a connection between the desired symbols. Use the dialog box accessed through `Edit:Add Connection`.

The sections that follow show you how to add network, segment, node, and interface objects to your network map so that they can be managed by NNM.

Changing Symbol Location on One Submap After auto-layout is turned off, simply select the symbol and, while holding down the left or center mouse button, drag the symbol to the new location within the submap.

Copying/Moving Symbols from Submap to Submap You can easily copy or move symbols from one submap into any other submap in the open map. Select the symbols, then:

- To copy the symbols, select the `Edit:Copy` menu item and `Edit:Paste` menu item. The copy operation does not remove the symbols or selected objects from their original location.
- To move the symbols, select the `Edit:Cut` menu item and `Edit:Paste` menu item.

  Sometimes the cut (or delete) operation applies only to a symbol or set of symbols, without affecting the object or objects represented by the symbols. Sometimes the cut operation applies to the object as well as the symbol. When you cut a symbol, if the object that the symbol represents is represented by another symbol, in any map, the symbol is cut, but the object is not deleted from the database. If the symbol is the only symbol that represents the object, the object is cut (or deleted) along with the symbol.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0087
Fls. Nº
Doc: 3740

NOTE If you are using NNM for UNIX operating systems, you can also move the symbol by dragging and dropping symbols from one submap to another.

Adding Object Symbols to Your Submaps

You can add segment, node, or interface objects to your maps.

Adding a Segment Object If NNM can identify which network segment a node is on, it places the node on that segment. If NNM cannot identify the segment, it places the node on the default segment submap for that network. The default segment submap for each network is the first submap created by the `ipmap` service when NNM ran initial discovery (named Segment 1). If this submap has been deleted, the oldest segment submap (lowest segment number) becomes the default segment submap.

NOTE You may wish to check the oldest segment submap for each network (Segment 1) periodically to check for stray objects.

NNM discovers new nodes on segments attached to connector devices that support the Bridge MIB (RFC1493) and Repeater MIB (RFC2108), as well as HP SNMP bridges and multi-port repeaters (hubs) that have IP or IPX addresses.

A Network submap may contain symbols in the Network and Connector classes. NNM recognizes the following symbols on a Network submap.

Table 8-1 Symbols Managed on a Network Submap

Class	Symbol
Network	Bus
Network	Star
Network	Token Ring
Network	FDDI Ring

Table 8-1 Symbols Managed on a Network Submap (Continued)

Class	Symbol
Connector	Gateway (Router)
Connector	Bridge
Connector	Repeater
Connector	Multi-Port (Hub)
Connector	Switch (supplied by vendors)

You can add a segment object to a Network submap. When you add a segment, an empty Segment submap is created. Double-clicking on the symbol opens the Segment submap. See NNM's online help for more information.

Adding a Node Object You can add an object that represents a node or a network device to your Segment submap by placing one of the supported symbols on a Segment submap. Double-clicking on the node symbol opens a Node submap. NNM manages the following symbols from the Computer, Connector, and Net Device classes in a Node submap. See NNM's online help for more information.

Table 8-2 Symbols Managed in a Segment Submap

Class	Symbol
Computer	Generic
Computer	PC
Computer	Workstation
Computer	Mini
Computer	Main Frame
Connector	Bridge
Connector	Gateway (Router)
Connector	Repeater
Connector	Multi-port (Hub)

RQS nº 03/2005 - CN - CPMI - CORREIOS
0088
Fls. Nº
3740
Doc:

Table 8-2 Symbols Managed in a Segment Submap (Continued)

Class	Symbol
Net Device	Analyzer
Net Device	Modem
Net Device	X.25
Net Device	PBX

Adding an IP or IPX Interface Object You can add an interface to a Node submap by placing an interface symbol on the Node submap. To do this, enter the address of the interface in the `Add Object` dialog box. See NNM's online help for more information.

Table 8-3 Symbols Managed in a Node Submap

Class	Symbol
Cards	IP Interface
Cards	IPX Interface

Background Graphics

A background graphic, such as a map or picture, may be displayed in the background plane of a submap window. The background graphic may be different for each submap. NNM includes an extensive collection of background graphics for your convenience. You can also create your own background graphics.

Keep in mind that graphic files are quite large and may significantly increase the time required to open each submap and significantly increase the amount of memory required to view a submap. If the submap is transient, it becomes persistent when you add a background graphic. Supported file formats for background graphics are as follows:

- *NNM for all platforms:*
  - GIF (CompuServe Graphics Interchange Form)
- *NNM for a Windows or UNIX operating system:* Supports these graphic file formats (not displayed when accessing NNM over the web):

— BMP (Bitmap)
— TIFF (Tag Image File Format)

- *NNM for UNIX operating systems only:* Supports these graphic file formats
(not displayed in NNM for Windows or NNM on the web):

— XBM (X11 monochrome bitmap format)
— PCX
— Image
— Starbase
— XPM (X Pixmap format)
— XWD (X Window Dump)

- *NNM for UNIX and NNM on the web only:* Supports these graphic file formats (not displayed in NNM for Windows):

— JPEG (Joint Photographics Experts Group)

TIP

The following *analytical data* directories are *not* included in NNM's backup scripts:

```
install_dir\backgrounds
install_dir\bitmaps
install_dir\www\htdocs\bitmaps
install_dir\www\registration
```

- *UNIX:*

```
$OV_BACKGROUNDS
$OV_BITMAPS
$OV_WWW/htdocs/bitmaps
$OV_WWW_REG
```

If you make changes or additions to map backgrounds, bitmap files, or web registration files ensure that your new files are properly backed up. See "Backup/Restore to Protect Your Investment of Time" on page 165 for more information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0089
Doc: 3740

Adding or Replacing a Background Graphic

You can add a graphic to the background of a submap or replace a graphic with a new graphic. Background graphics shipped with NNM are stored in:

- *Windows:* `install_dir\backgrounds\*.*`
- *UNIX:* `$OV_BACKGROUNDS`

A graphic can serve as a background for the symbols in a submap. A graphic helps provide contextual information such as a floor plan for systems, a map of geographically diverse sites, and so on. Both users and applications can specify a background graphic for a submap.

The map must be open with read-write access to choose a new background graphic. Select `Map:Submap->Properties` and specify the name of the graphic file that you wish to use.

NOTE When using a background graphic, symbols cannot be placed outside the dimensions of the background graphic.

Creating Your Own Map Symbols

You can create your own symbols to use on maps. You might want to do this to customize the appearance of existing symbols, or you might need a symbol to represent a new object. Each symbol is comprised of two graphic elements: the class that determines the background shape of the symbol and changes color according to current status, and the subclass that determines the graphic displayed within the background shape. Several steps are required. See "Changing All the Symbols for a Particular Device" on page 661 for a detailed example of these steps:

- Create a set of *.GIF images according to the specifications in NNM's online manual, *Creating and Using Registration Files*.
- Create a symbol registration file to define the characteristics and appearance of the new symbol.
- Develop custom online help information about the your new symbol. This online help information will be available through the symbol's pop-up menu. See NNM's online manual, *Creating and Using Registration Files*.

NOTE These changes are visible from remote consoles and web access after the map is reloaded or refreshed on each system. Your new symbol will also display in `Help:Display Legend`.

What Is a Symbol

A **symbol** is a graphical representation of an object (page 203). A single object can be represented by multiple symbols. Multiple symbols of the same object can exist on the same submap, on multiple submaps of the same map, or on submaps of different maps.

In addition to representing objects, symbols have other functions:

- Most symbols are explodable--when you double-click an explodable symbol, a new submap opens to let you "look inside" the object representing the symbol.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0090
Doc: 3740

- Some symbols are executable. When you double-click on this type of symbol, a predefined action is carried out on a predefined target.
- Symbols can reflect the status of the object that they represent or of objects in child submaps.

When you create a new symbol type you can define the following characteristics:

Symbol Variety Symbols come in two varieties: the icon symbol and the connection symbol.

- **Icon Symbol** These symbols represent the objects or groups of objects managed by NNM.
- **Connection Symbols** These symbols represent logical connections between devices that are managed by NNM. Connection symbols do not represent actual physical connectors.

Symbol Type Symbol type consists of the symbol class and subclass (see Note on page 265):

- **Class** You can distinguish the symbol class by the outer shape of the symbol. For example, a circle=a network, square=a computer, diamond=a connective device, and so on.
- **Subclass** A subclass is a further definition of the symbol that is represented by a bitmap within the outer shape that represents the class.

Status Source A symbol may present status information from one of three sources. This characteristic allows applications to have more control over the presentation of status. See "Controlling Symbol Status" on page 270 for more information. In general, Hewlett-Packard recommends that you do not change these settings.

Label A label may appear below each symbol. This label is simply a name to help you identify a specific symbol. (see Note on page 265).

Behavior	Behavior defines how the symbol behaves when you double-click the symbol. A symbol may behave in one of two ways: it may open a child submap (explode), or it may execute an action (execute).
Default Layout	When an explodable symbol opens a new submap, its default layout specifies the layout algorithm (Ring, Bus, Star, Point to Point, or Row/Column) for the submap.

NOTE

The `ipmap` service automatically assigns a symbol type and label based upon information it receives from the `netmon` service.

This means that if you modify the symbol type or symbol label of an object that is managed by NNM, your changes will be replaced by the values assigned by NNM the next time configuration polling runs.

You can turn off this `ipmap` capability by setting the environment variable `IPMAP_NO_SYMBOL_CHANGES=TRUE`. See the *ipmap* reference page in NNM's online help (or the UNIX manpage) for information about changing this environment variable.

Alternately, you can modify the `oid_to_sym` file to specify that a different symbol be associated with a specific *type* of device (determined by `sysObjectID`). See the *oid_to_sym* reference page in NNM's online help (or the UNIX manpage) for more information. See "Changing All the Symbols for a Particular Device" on page 661 for a complete example.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0091
3740
Doc:

Specifying the Placement and Size of the Submap Windows

You can control the size and placement of the submap windows through the menu choices `Window Geometry` and `Submap Overlay`. The choices you make here affect the way that the submaps are displayed on the management station and on remote consoles, but not through web access.

Window Geometry

NOTE Window geometry settings are visible from remote consoles when the map is reloaded on each system. This change does not impact maps accessed over the web.

Select `View:Window Geometry` to explicitly save the size and placement of submap windows so that they are consistent each time they are opened. This feature allows you to override any settings that an application may specify for the size and placement of its submap

When you specify the size or placement of a submap window in a read-write map, those settings will be used in that session and in all subsequent sessions. You cannot change window geometry on read-only maps.

If the submap is transient, it becomes persistent when you save its window geometry.

Submap Overlay

NOTE Submap overlay settings are visible from remote consoles when the map is reloaded on each system. This change does not impact maps accessed over the web.

Select `View:Submap Overlay` to minimize the number of windows on your screen during submap navigation. By default, NNM automatically reuses submap windows. Each new submap that you access by double-clicking on it is placed in the window from which you accessed it. This eliminates the display of submaps that you are merely passing through as you navigate the hierarchy. By using submap window overlay, you no longer have to close unneeded submaps that are on your display.

You can change this behavior so that a new window is presented whenever you access a new submap. The overlay feature is set on a per-submap basis. You cannot change submap overlay on read-only maps.

If the submap is transient, it becomes persistent when you turn off overlay.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0092
Doc. 3740

Miscellaneous Configuration Changes

A variety of configurable settings are stored in:

- *Windows:* The system registry.
- *UNIX:* The X Windows resource files (page 269).

The changes discussed in this section affect only the local management system's display of NNM or the local remote console's display of NNM. NNM accessed over the web is not affected.

Windows Operating System

See the *app-defaults* reference page in NNM's online help for detailed information about which NNM settings can be controlled through the Windows system registry.

You can customize the appearance and behavior of NNM by editing the Windows system registry. Check your Windows operating system documentation for more information about editing the system registry files.

Changing the Windows system registry on the management station affects *only* the sessions run on the management station. Each management station and each remote console could have different settings.

Possible settings include:

- Map fonts
- Status colors for symbols and map background color

These settings are stored in the registry under the following keys:

- `\HEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\Network Node Manager\OVw\Map Fonts`
- `\HEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\Network Node Manager\OVw\Map Colors`

TIP After making your changes, check `Help:Display Legend` to verify that your color choices are working successfully.

UNIX Operating Systems

You can also customize the appearance and behavior of NNM by editing the application defaults files and the X resources files used by your X Windows resource manager.

Open the `$APP_DEFS/OVw` file and read the instructions within the file.

Changing the `$APP_DEFS/OVw` file on the management station affects *only* the sessions run on the management station. Each management station and each remote console could have different settings. Each user on the system can have a private X resources file that can override the `$APP_DEFS/OVw` file.

The UNIX `$APP_DEFS/OVw` file for NNM lets you customize things such

- Map background color
- Status colors for symbols
- Submap window height and width
- Timers for response to requests to close a map
- Timers for queries
- Keyboard focus policy
- Fonts for dialog boxes

To change general X Windows behavior and color, refer to the online help for the window manager that is being used on your computer. Refer to documentation on your window manager for the location of the X resources file for that window manager.

TIP After making status color changes, check `Help:Display Legend` to verify that your color choices are working successfully.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0093
3740
Doc:

Controlling Symbol Status

You can customize the status color and status propagation of the symbols:

- Control the colors used to indicate the status of network objects.
- Control the way in which critical status is propagated up the map's network hierarchy ("Compound Status" on page 274).
- Monitor the status of router interfaces outside of your firewall ("SNMP Status Polling" on page 273).

Object Status Colors

NNM displays status conditions via the colors of the symbols. The colors used to display status in NNM's web interface cannot be changed. However the colors used to display status in NNM for a Windows or UNIX operating system can be changed; colors used for both device symbols and connection symbols are defined and documented in:

- *Windows:* The system registry.
- *UNIX:* $APP_DEFS/Ovw

You can view the current colors using `Help:Display Legend`.

Someone on your team may need to change their colors, for example to address color blindness issues. Keep in mind that your changes affect *only the local display* of the management station or remote console, and must be redone each time you upgrade NNM.

TIP After making your changes, check `Help:Display Legend` to verify that your color choices are working successfully.

To change the colors, see "Miscellaneous Configuration Changes" on page 268.

Symbol Status

Status is displayed by a symbol on a submap. There are two categories of status conditions: administrative and operational. These two categories are important because they interact with the status propagation schemes in very different ways.

In the **status propagation** schemes, rules are used to determine how the status of a symbol in a child submap is transmitted to the symbols of objects in parent submaps. Administrative status conditions are ignored by the propagation schemes, which means that status information from a child submap is not transferred to a parent symbol. Operational status conditions, on the other hand, may indicate problems that must be propagated through the use of the schemes.

NNM recognizes ten status conditions, shown in the following table:

Table 8-4 Default Status Conditions

Category	Status Condition	Meaning of Status
Administrative	Unmanaged	Users can set this value, which indicates that the object should not be monitored and that the operational status should be ignored.
Administrative	Testing	An application sets the status to "testing" when an object is undergoing temporary diagnostic or maintenance procedures.
Administrative	Restricted	An application sets the status to "restricted" when an object is functioning normally, but it may not be available to all users.
Administrative	Disabled	An application sets the status to "disabled" when an object is inactive (although there may not be anything necessarily wrong with the object).

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0094
3740
3740
Doc:

Table 8-4 Default Status Conditions (Continued)

Category	Status Condition	Meaning of Status
Operational	Unknown	An application sets the status to "unknown" when the status of an object cannot be determined.
Operational	Normal	An application sets the status to "normal" when the object is in a normal operational state.
Operational	Warning	An application sets the status to "warning" when an object may face a potential problem.
Operational	Minor/Marginal	An application sets the status to "minor/marginal" when an object has a minor problem; the device itself may continue to operate normally.
Operational	Major	An application sets the status to "major" when an object has serious problems; the device itself probably no longer operates normally.
Operational	Critical	An application sets the status to "critical" when the device represented by the object is not functioning.

The status of a particular symbol represents an application's interpretation of the status of certain object attributes, or characteristics, as defined in NNM's object database.

For example, the `ipmap` service determines the status of a node object based upon the operational status of IP and IPX interfaces installed in the node. If all of its IP or IPX interfaces are down, then NNM determines that the node's state is critical. From the perspective of the `ipmap` service, the node is nonfunctional. However, another application may consider the same node functional because that application

monitors a different protocol, and it finds that the interfaces for that protocol are fully functional. Multiple symbols for the node object could be used to represent these status states separately.

Status Source

Status may be obtained from three possible sources. This feature is mainly used by applications so that they can set the status of specific symbols. In general, Hewlett-Packard recommends that you do not change the status source of a symbol. The status source of a symbol is automatically set depending on the application that manages the object.

The three sources of status are:

Symbol Status Source This source of status is used by applications that may want to set status on a particular symbol of the object. This allows other applications to set states for other symbols of the same object.

Object Status Source This source of status is used by applications that want to set and display the same status state among all the symbols of a particular object.

Compound Status Source NNM determines the status state of the symbol based upon compound status rules. Compound status determines how status propagates from symbols in child submaps to symbols in parent submaps.

The following subsections discuss the significance of each status source.

NOTE If you change symbol source, the submap containing the symbol is forced to become persistent.

SNMP Status Polling

In some cases a router may have interfaces to which the NNM management station has no route (for example, interfaces located outside of a firewall). You can obtain status information from the SNMP agent for the device, just as you can for layer-2 interfaces, via SNMP queries for `ifAdminStatus` and `ifOperStatus`.

To configure an IP interface for SNMP status polling, use the following procedure.

IRQS nº 03/2005 - CN
CPMI - CORREIOS
0095
Fls. Nº
3740
Doc:

1. If the file `netmon.snmpStatus` file does not exist you will need to create it in the location listed below.
   - *Windows:* `install_dir\conf\netmon.snmpStatus`
   - *UNIX:* `$OV_CONF/netmon.snmpStatus`
2. Add a line to the `netmon.snmpStatus` file with the IP wildcards you want to have SNMP status polled.
3. To make your changes take effect, do one of the following.
   - From the command line, type **`ovstop -v netmon`** then type ovstart -v netmon.
   - From the command line, type **`xnmpolling -event.`**
   - Click `Apply` in the `Options:Network Polling Configuration` dialog box.

See the `netmon` and `netmon.snmpStatus` reference pages in NNM's online help (or the UNIX manpages) for more information.

Compound Status

NNM uses compound status to propagate the status of a symbol in a low-level submap up to parent submaps, to alert you about a problem. [illegible] occurs only when a symbol is given one of the six operational status conditions (unknown, normal, warning, [illegible]ical). The administrative status conditions (unmanaged, testing, restricted, and disabled) are not propagated.

You can set compound status in the `Status Propagation` section of the `Map Properties` dialog box.

NOTE The selections that you make affect remote consoles and the web display after the map is reloaded or refreshed on each system.

From the perspective of a compound status scheme, a symbol is either:

- **unknown**: a symbol's current status has not yet been determined by an application.
- **normal**: a symbol is functioning as intended and responding appropriately when contacted by an application.

- **abnormal**: a symbol is given one of the four abnormal status conditions (warning, minor/marginal, major, or critical), and is either potentially or currently having problems.

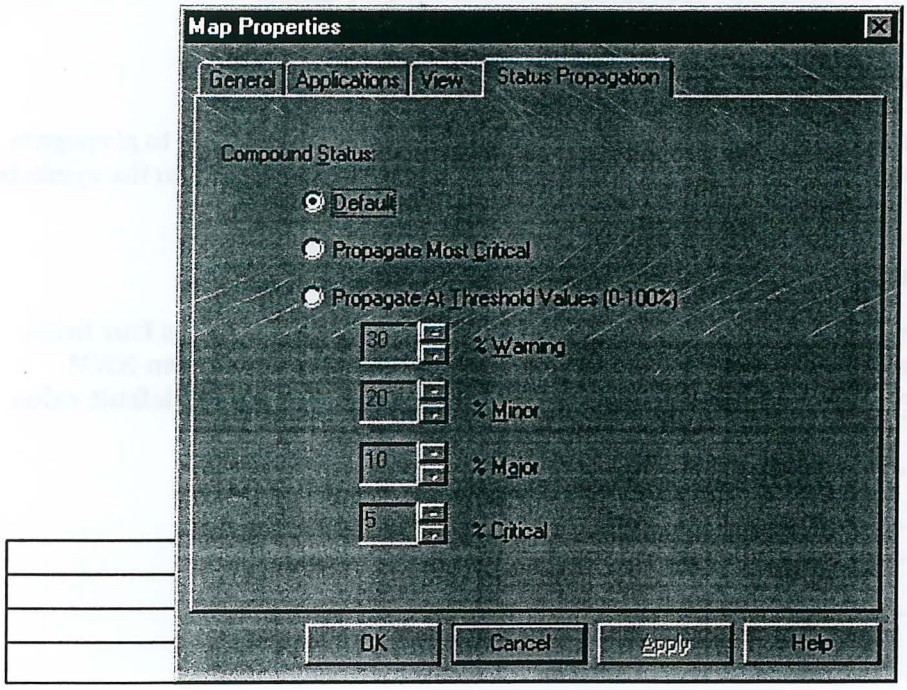
The mapping of the compound status categories to the operational status conditions is described in the following table.

Table 8-5 Compound Mapping

This Compound	Maps to This Operational Status Condition
Unknown	Unknown
Normal	Normal
Abnormal	Warning, Minor/Marginal, Major, or Critical

The following subsections discuss each of the three compound status schemes: default, propagate most critical, and propagate at threshold value.

Figure 8-12 Status Propagation Settings



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0096
Doc: 3740

Default

Selecting the default propagation scheme causes NNM to propagate status according to the algorithms described in the following table:

Table 8-6 Default Status Propagation

Condition of Symbols in Child Submap	Status of Symbols of Parent Object
No symbols are normal and no symbols are abnormal.	Unknown
All symbols are normal.	Normal
One symbol is abnormal; all other symbols are normal.	Warning
More than one symbol is abnormal and more than one other symbol is normal.	Minor/Marginal
One symbol is normal; all other symbols are abnormal.	Major
All symbols are abnormal.	Critical

Propagate Most Critical

Selecting the propagate most critical scheme causes NNM to propagate the status of the most critical symbol in the child submap to the symbols of the parent object.

Propagate At Threshold Value (0 - 100%)

Selecting the propagate at threshold value scheme displays four fields that enable you to set threshold values that determine when NNM propagates status. The number shown for each field is its default value.

% warning	30
% minor	20
% major	10
% critical	5

The specified value indicates the minimum percentage of symbols that must be in that status state in order for that status state to be propagated. If the percentage is met or exceeded in more than one status state, then the most severe of those states is propagated.

RQS nº 03/2005 - CN
CPMI - CORREIO
Fls. Nº 0097
Doc: 3740

Creating New NNM Features to Meet Your Team's Needs

Adding to NNM's Menu Structure

You can add your own choice of features to NNM's pull-down menus, pop-up menus, and tool bars. This is useful for providing quick access to commonly used tools or to specific network management scripts that your team developed. You may wish to designate a menu location where you post tools developed by team members as a way to share best practices, or designate a menu location to post software tools provided by specific vendors.

There are two ways to make additions to NNM's menu choices:

- NNM provides an easy way to add menu access to MIB-based applications that are written using NNM's MIB Application Builder program. See "Using the MIB Application Builder" on page 443 for more information.
- You can also make modifications to NNM's registration files to add any menu or toolbar items that you want. Complete information about registration files is available in NNM's online manual, *tration Files*.

NOTE The changes that you make using these two options appear on the management station and from remote consoles. They do not show up when NNM is accessed over the web. See Chapter 14, "NNM on the Web," for information about modifying NNM's web user interface.

TIP You can develop your own *context* settings for your new menu items to make them appear on only specific submaps. See "Using the Context Feature to Control Menu Choices" on page 296. You can also establish *selection rules* that make the menu item unavailable unless an

appropriate device is selected on the map. See NNM's online manual, *Creating and Using Registration Files* for complete information about establishing selection rules.

Creating Executable Symbols with Custom Behaviors

Symbol Behavior

The setting for a symbol's behavior defines how the symbol behaves when you double-click on it. A symbol may behave in one of two ways. It may explode into a submap, or it may execute an action.

A single object may be represented by both an explodable and an executable symbol. Note that when you change an existing explodable symbol to executable, you can open the child submap only from the `Map:Submap->Open` dialog box, or from another explodable symbol of the parent object.

Explodable Symbols

If a symbol's behavior is set as explodable (the default), the symbol enables you to view the components of an object. When you double-click on an explodable symbol, NNM opens another submap, called a child submap. The contents of this child submap may be determined by you or an application.

For example, NNM creates a child submap for a node that contains the IP interfaces installed in the node. If you double-click on a computer workstation managed by NNM, a node submap is opened that displays symbols of the node's IP and/or IPX interfaces.

If no child submap exists for the object, when you double-click on the symbol you are prompted to create a child submap. See "Making the Maps Look Like Your World" on page 240 for information about creating child submaps.

Executable Symbols

You can distinguish executable symbols from explodable symbols by the three dimensional appearance of each executable symbol. A square appears around the symbol indicating that it is executable (button-like). If a symbol's behavior is set as executable, the symbol enables you to

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0098
3740
Doc:



associate the double-click with an action other than opening a child submap. For example, by double-clicking on a conveniently placed symbol, you could:

- Launch a management tool.
- Open a window for remote login on a particular workstation.
- Execute a script that checks the disk space available on a selected system's hard drive and causes a message to display with the results of the check.

You can choose one or more objects as the target objects of the action from among the objects represented on the map. The chosen target objects must be appropriate for the action selected.

TIP *NNM over the web:* You will see the executable symbol with a box around it; however, you cannot run the executable.

Creating an Executable Symbol

Using NNM for a Windows or UNIX operating system, you can create a new executable symbol that performs an action. You can copy and paste a symbol, then change the duplicate symbol's behavior so that it executes some action. Or you can change the behavior of an existing symbol from explodable to executable.

When you add an executable symbol to your map, you must select the action that the symbol will execute and the target objects on which it will act. You can choose an action from among the actions supplied:

- `Edit:Add Object` dialog box, choose the `Executable` setting.
- Right-click on a symbol, choose `Symbol Properties`, select the `Executable` setting.

Or you can designate your own action by setting up an application registration file (ARF). The application registration file defines the action and adds it to the list in the `Add Object` dialog box and the `Symbol Properties` dialog box.

For more information about establishing your own custom actions:

- See NNM's online help.
- See NNM's online manual, *Creating and Using Registration Files*.

NOTE If an executable symbol is placed on a submap, that submap becomes persistent.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0099
Doc: 3740



9 Controlling Map Access

IRQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 010
Doc: 3740

Customizing the maps requires a substantial time commitment and a level of expertise in the intricate workings of NNM. To protect your efforts, you may want to remove functionality from some maps so that inadvertent detrimental changes cannot be made.

As you are setting up maps for various users/groups, you need to decide how much control you want to maintain over the map. If you allow your team to maintain the map, provide training (see page 286). If you want to maintain control over changes to the map, there are several choices for controlling how NNM looks and functions for each user or group:

- "Setting User Preferences Within NNM" on page 287.

  Simply log in as each user/group and set their options. NNM tracks these options by user/group and invokes them each time that user/group accesses NNM. Keep in mind that your team can change these settings if they wish.

- "Using Command Line Startup Options" on page 289.

  To use the command line options, you need to develop scripts for each user/group that enforce your choices. Your team member runs the script rather than the regular `ovw` command to open NNM's interface.

- "Using Operating-System Level File Permissions for the Map" on page 292.

  You control access to specific maps through setting operating system level permissions on the `snapinfo.dir` file within each map's directory.

- "Using the Context Feature to Control Menu Choices" on page 296.

  Control which features are accessible through the menus by selecting from predefined "context" identifiers or defining your own. Keep in mind that your team can change these settings if they wish.

- "Using ARF Files to Control Menu Choices" on page 299.

  Control which features are accessible through the menus by modifying the underlying application registration files (ARFs). The example provided makes NNM "fool-proof" by removing all access to configuring NNM, yet without limiting the use of NNM. This choice provides you with the ultimate control.

- "Allowing Others to View NNM from Many Computers" on page 317. Learn how to set up multiple systems to run the NNM interface while accessing the common database on the management station. You can set up remote consoles and/or web access.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0101
Doc: 3740

Establishing and Communicating a Process for Requesting Changes to the Map

Now that your maps are set up just the way you want them, think about how you will handle ongoing changes to the maps.

Not Allowing Team Members to Make Changes

Provide procedures for your team members to follow when requesting changes to their maps. Who should your team members contact and how. Designate one person to maintain the maps.

Allowing Team Members to Make Changes

If you are allowing your team members to have access to editing features, think about what training they will need in order to understand how NNM works and make wise decisions as they use the map. For example:

- All maps use the same database information. Don't delete symbols from the map. Use the hide feature.
- If more than one person uses a particular map, only the first person to open the map will have read/write permissions. Identify which team member has read-write permission for each map.
- If you are viewing a map in read-only mode, use `Map:Refresh` to display the most recent changes.
- Explain what to do when symbols show up in the `New Object Holding Area`. Explain why this might happen, such as when a new device added to your network.
- If they are allowed to modify their submaps, provide information about how to edit maps so that the connections between devices are maintained, and/or how to reestablish connections that are lost from the map.

Setting User Preferences Within NNM

You can define the following user preferences for each user/group. Simply log into the system as each user/group and set the preferences. NNM keeps track of each user's settings. These settings can be changed by each team member. You may want to simply provide training about these choices and leave it up to each team member, or you may wish to set them up for each team member and then remove the menu choices that allow changes (see page 299):

- Set the default map.
- Set a home submap.
- Set the toolbar to be hidden or displayed.
- Create a list of frequently accessed submaps by adding symbols to the Quick Navigator (this is customized per map rather than per user).

Table 9-1 User Preference Settings

User Preference	Setting
The **home** submap is the first submap that appears when you open a map. The home submap is always persistent.	Define the home submap: 1. Open the submap you want to be displayed each time you open the current map. 2. Select `Map:Submap->Set This Submap as Home` (Not available in NNM on the web.)
The map that NNM first displays upon startup is called the **user default map**.	Define the user's default map: 1. Select `Map:Open`. 2. Select a map name. 3. Click `Set User Default`.
The toolbar provides quick access to frequently-used menu items.	*UNIX only:* Display or hide the tool bar by selecting `View:Toolbar`

RQS nº 03/2005 - CN
CPMI - CORREIC
Fls. Nº 0102
3740
Doc:

Table 9-1 User Preference Settings (Continued)

User Preference	Setting
The Quick Navigator provides quick access to frequently used submaps.	• Add a submap symbol to the Quick Navigator: 1. Open the submap you want to access from the Quick Navigator. 2. Select `Edit:Add to Quick Navigator->Add This Submap`. • Remove a submap symbol from the Quick Navigator: 1. Select the symbol in the Quick Navigator and display the symbol pop-up menu. 2. Select `Delete Symbol` from the pop-up menu. Remember that your team members can change these settings at any time unless you remove the menu choices for making those changes (see page 299).

Using Command Line Startup Options

This section discusses details about the ovw command that you may use to start NNM from the command line prompt. You can write scripts for each user/group that specify their specific startup options.

TIP It may be useful to enter these into each user's login script. For security purposes, remove the *write* permissions to the login scripts after you are done.

These commands may be useful for customizing NNM per user group or useful when running multiple sessions of NNM at the same time.

Options

The ovw command contains the following options. See the *ovw* reference page in NNM's online help (or the UNIX manpage) for more information.

```
ovw [-ro|-rw][-map map_name][-submap submap_name][-propagation
scheme][-server][-verify][-fields][-copyMap source_map_name
destination_map_name ...][deleteMap map_name] [mapcount]
```

Table 9-2 Startup Options for NNM

Option	Meaning
`ovw -ro`	Open all maps as read-only.
`ovw -rw`	Open all maps as read-write if possible. *UNIX:* This is the default. It is necessary only if the X resources specify read-only as a default behavior.
`ovw -map` *map_name*	Open map *map_name*. Create the map, *map_name*, if it does not exist.
`ovw -submap` *submap_name*	Open *submap_name* as the initial submap if it exists on the map being opened. If *submap_name* does not exist, then NNM initially opens the home submap of the map being opened.

FRQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0103
Doc: 3740

Table 9-2 Startup Options for NNM (Continued)

Option	Meaning
`ovw -propagation` *scheme*	Sets the propagation scheme for a new map or changes the scheme for an existing map. The propagation schemes are default, most critical, and threshold.

Examples

Table 9-3 provides examples that show you various ways you can use the `ovw` command to start NNM from a command line prompt.

Table 9-3 Using the ovw Command to Start NNM

Command Entered	Effects
`ovw`	Runs NNM and opens the map assigned as the user default map.
`ovw -map Admin_Map`	Runs NNM and opens the map named `Admin_Map`. `Admin_Map` does not need to be the user default map.
`ovw -map world -propagation threshold:40:30:20:5`	Runs NNM and creates a new map named `world` using the threshold propagation scheme with a warning threshold of 40%, a minor threshold of 30%, a major threshold of 20%, and a critical threshold of 5%.
`ovw -ro`	Runs NNM and opens the map assigned as the user default map. The user default map, and all maps subsequently opened during this session, are opened with read-only access.
`ovw -ro -map Europe2`	Runs NNM and opens the map called `Europe2`. All maps during this session of NNM are opened with read-only access.
`ovw -rw`	Runs NNM and opens the map assigned as the user default map. Maps can be opened with read-write access if permissions allow. The `-rw` option is the default and is necessary only if read-only is specified as the default behavior.

Table 9-3 Using the ovw Command to Start NNM (Continued)

Command Entered	Effects
`ovw -map Admin_Map -submap Main`	Runs NNM and opens map named `Admin_Map`, and first displays the submap named `Main` instead of the home submap.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0104
3740
Doc:

Using Operating-System Level File Permissions for the Map

Two factors determine whether a map is opened with read-write access or with read-only access when a map is opened. First, only one user can have a specific map opened with read-write access at any one time (the first person to access the map). Second, you can use the file system to purposely allow specific users read-write or read-only access to a map by setting permission to the files.

TIP If you want several users to have simultaneous read-write access, make copies of the map for each user. See "Copying the Default Map" on page 215. Keep in mind that if your team members make changes to their map, it will then be out of sync with the other maps. To prevent team members from making changes to the map, see page 299.

Possible permission settings are:

Read-write Access A map opened with read-write access is completely editable. You can add objects, add connections, create submaps, and change object attribute values. Only one user can have a specific map open with read-write access at any one time. If another user has the map open with read-write access, when you open the same map, you have read-only access to it. This is the case even if you have read-write permission from the operating system.

Read-only Access A map opened with read-only access is not editable by the user, although the map still can receive status from applications. In a map open with read-only access, you can view status changes, perform locate operations on objects, and update topological changes using the `Map:Refresh Map` menu item. However, you cannot add, delete, or modify items in the map, including symbols, objects, submaps, and map snapshots.

CAUTION: Using `Map:Open` or `Map:Save as`, it may be possible to navigate to a read-write map.

	You can use command line options to make *all* maps read-only (page 289) or remove these menu choices (page 299).
No Access	You cannot open a map that is set with No Access.

Windows: Setting Permissions

User access to maps is governed by the file permissions of the snapinfo.dir file in each individual map directory. If NNM is installed on:

- *FAT file system*, you can make each map read-only or read-write for *everyone* on the system. HP recommends that you install NNM on an NTFS file system if more individualized map access permissions are a concern.
- *NTFS*, you have a fine level of control over access to maps. For example, using the Windows Explorer's `Security` tab, you can adjust the permissions so that specific users/groups have write access to specific maps only.

FAT file systems

CAUTION Close the NNM interface before changing map permissions (see "Closing All Current Sessions" on page 319). NNM checks permissions only when it opens the map. If, for example, you change permissions for an open map from read-write to read-only, you risk map database corruption.

Each NNM map is comprised of a group of files. NNM needs to be able to make continuous changes to these files. A special file that controls users' access to the map files themselves is provided for each map. You can set individual maps to `read-write` or `read-only` by setting the attributes on the following file:

`install_dir``\databases\openview\mapdb\`*`mapname`*`\snapinfo.dir`

Log in as Administrator. Use the Windows Explorer to access the file properties of the `snapinfo.dir` file. When you set this file to `read-only`, all the files that comprise the map are read-only protected for *all* users. The next time the map is opened, your changes take affect.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 105
3740
Doc:

NTFS

CAUTION

Close the NNM interface before changing map permissions (see "Closing All Current Sessions" on page 319). NNM checks permissions only when it opens the map. If, for example, you change permissions for an open map from read-write to read-only, you risk map database corruption.

Each NNM map is comprised of a group of files. A special file that controls users' access to the map files themselves is provided for each map. You can set customized permissions for each user/group on individual maps. Set `read-write` or `read-only` attributes on the following file:

`install_dir``\databases\openview\mapdb\`*`mapname`*`\snapinfo.dir`

Log in as Administrator. Access the file properties of the `snapinfo.dir` file and use the Windows Explorer's `File:Properties-> Security` tab. Set the appropriate permissions for each user or group that accesses this file. When you set this file to `read-only`, all the files that comprise the map are read-only protected for *the specific user/group*. The next time the map is opened, your changes take affect.

UNIX: Setting Permissions

CAUTION

Close the NNM interface before changing map permissions (see "Closing All Current Sessions" on page 319). NNM checks permissions only when it opens the map. If, for example, you change permissions for an open map from read-write to read-only, you risk map database corruption.

Each NNM map is comprised of a group of files. A special file that controls user's access to the map files themselves is provided for each map. You can set customized permissions for each user/group on individual maps. Set `read-write` or `read-only` attributes on the following file:

`$OV_DB/Openview/mapdb/`*`mapname`*`/snapinfo.dir`

To change map permissions, log in as root. Use the commands provided by NNM. *Do not use the UNIX file permission commands* (chmod, chgrp, chown) *from your operating system.*

NNM provides several commands to let you change permissions:

ovwchmod	Changes the mode of individual maps.
ovwchgrp	Changes the group ownership of individual maps.
ovwchown	Changes the ownership of individual maps.
ovwperms	Lists the available maps and their current permissions.

See the *ovwperms* reference page in NNM's online help (or the UNIX manpage) for more information.

To change permissions of *other* NNM configuration files and database files, use the UNIX chown, chmod, and chgrp commands. You may need to stop and start NNM's services (background processes) in order to force NNM to acknowledge the changes. You do not need to stop and start any services to force NNM to acknowledge the change in *map* permissions. The next time the map is opened, your changes take affect.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 0106
3740
Doc:

Using the Context Feature to Control Menu Choices

NOTE This feature is not available when accessing NNM over the web.

If you want to remove completely a menu choice from all submaps rather than from specific submaps, see page 299.

If you want to add menu choices, the context feature allows you to control in which submaps your new choices display. See "Creating New NNM Features to Meet Your Team's Needs" on page 278, and see also "Using the MIB Application Builder" on page 443.

This feature allows you to remove or display specific *groups* of pull-down menu items and pop-up menu items on a submap-by-submap basis.

There are two components to the context feature:

- Application Registrations Files (ARFs)

  Menu items are defined in application registration files. Each menu item is set to display in one or more *contexts*.

- `Map:Submap->Properties / Context` tab

  Each submap is configured to display one or more *contexts*.

NNM provides multiple predefined *contexts* for your use. You can also create your own *contexts*.

Anyone with read-write access to the map can change the contexts assigned to a submap.

Using NNM's Predefined Contexts

NNM's predefined context identifiers that are provided for your convenience are:

- `isInternet`

  Displays menus, toolbar buttons, and commands pertaining to an Internet network.

- `isIP`

  Displays menus, toolbar buttons, and commands pertaining to an Internet Protocol (IP) network.

- `isIPX`

  Displays menus, toolbar buttons, and commands pertaining to an Internet Packet Exchange (IPX) network.

- `isNetwork`

  Displays menus, toolbar buttons, and commands pertaining to network management.

- `isNode`

  Displays menus, toolbar buttons, and commands pertaining to node management.

You can add and remove these predefined context identifiers through the `Context` tab in the `Map:Submap Properties` dialog box or the New Submap Wizard. See NNM's online help from these dialog boxes for more information.

NOTE If you see the `NoGeneric` or `NoDefault` context identifier in a submap's properties, do not change it. These are special contexts utilized by application developers.

Creating Your Own Contexts

Contexts are specified on a menu-item by menu-item basis in the application registration files (ARFs) that control HP OpenView or third-party applications. (See page 305 for an example ARF file.)

To create your own context IDs:

- See NNM's online manual, *Creating and Using Registration Files,* for details about editing application registration files (ARFs).
- See the *OVwRegIntro* reference page in NNM's online help (or the UNIX manpage) for more information.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0107
Doc: 3740

NOTE



If you don't want a menu item to show up everywhere, delete the `AllContexts` identifier associated with that menu item in the ARF file, and replace it with a more specific context identifier.

Close the NNM user interface (`ovw` service) and reopen it to force NNM to acknowledge changes to the ARF files.

Using ARF Files to Control Menu Choices

NOTE These changes do not affect NNM over the web. NNM's web-based user interface is read-only for all maps, so you do not need to do anything to prevent team members who have web access from making changes to the map.

You can configure NNM so that your team cannot accidentally change your map customizations while accessing maps from remote consoles or on the management station itself. In this example, all features that allow access to modifying NNM are removed *without* setting the map to read-only. By leaving the read-write access to the map, your team retains full use of NNM and can still make map snapshots as needed. You are left in complete control over how NNM operates. Your team can use NNM, but cannot change any configuration settings. All access to configuration settings is removed from your team's view of the software, but remains in your view of the software.

See NNM's online manual, *Creating and Using Registration Files*, for details about editing application registration files (ARFs).

1. Establish *login accounts* for each user/group on your team. NNM needs to be able to differentiate between them in order to provide customized menu selections.
2. Create a unique directory for each user/group to hold their custom registration files. For example:
   - *Windows:* You should be the only user with read-write access:

     ```
     install_dir\registration\connectivity_reg\C\*.*
     install_dir\registration\printers_reg\C\*.*
     install_dir\registration\servers_reg\C\*.*
     ```

   - *UNIX:*

     ```
     /etc/opt/OV/share/registration/connectivity_reg/C/*
     /etc/opt/OV/share/registration/printers_reg/C/*
     /etc/opt/OV/share/registration/servers_reg/C/*
     ```

     (Set your new directories and the files that you place within them to have at least permissions of `r-xr-xr-x`.)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0108
3740
Doc:



TIP Placing your custom registration files in this location ensures that your work is included in the NNM backup and restore process.

3. *Copy* NNM's default registration directory to the new empty directories. NEVER MODIFY THE ORIGINAL FILES:

   - *Windows:* in Windows Explorer, select the contents of `install_dir\registration\C\*.*` and paste it into each new directory that you created in the previous step.
   - *UNIX:* repeat the following command for each new directory that you created in the previous step.

```
# cd $OV_REGISTRATION/C
# find .| cpio -pdumv $OV_REGISTRATION/each new directory/C/
```

4. Delete the following files from each new directory that you just populated:

   - `dataWarehouse`

     To disable access to NNM's data warehouse feature that exports the NNM database contents to a relational database.

   - `xnmpolling`

     To disable access to NNM's polling configuration settings.

   - `ovsnmp/xnmbuilder`

     To disable access to NNM's Application Builder program.

   - `ovsnmp/xnmcollect`

     To disable access to setting up or changing data collection and threshold monitoring.

   - `ovsnmp/xnmloadmib`
     To disable access to changing the SNMP MIBs loaded on your system.

   - `ovsnmp/xnmsnmpconf`

     To disable access to customizing NNM's record of your network's SNMP configuration settings such as GET- and SET-community names and port settings.

   - `ovsnmp/xnmtrap`

TIP Placing your custom registration files in this location ensures that your work is included in the NNM backup and restore process.

3. *Copy* NNM's default registration directory to the new empty directories. NEVER MODIFY THE ORIGINAL FILES:
   - *Windows:* in Windows Explorer, select the contents of *install_dir*\registration\C*.* and paste it into each new directory that you created in the previous step.
   - *UNIX:* repeat the following command for each new directory that you created in the previous step.

```
# cd $OV_REGISTRATION/C
# find .| cpio -pdumv $OV_REGISTRATION/each new directory/C/
```

4. Delete the following files from each new directory that you just populated:
   - `dataWarehouse`

     To disable access to NNM's data warehouse feature that exports the NNM database contents to a relational database.
   - `xnmpolling`

     To disable access to NNM's polling configuration settings.
   - `ovsnmp/xnmbuilder`

     To disable access to NNM's Application Builder program.
   - `ovsnmp/xnmcollect`

     To disable access to setting up or changing data collection and threshold monitoring.
   - `ovsnmp/xnmloadmib`
     To disable access to changing the SNMP MIBs loaded on your system.
   - `ovsnmp/xnmsnmpconf`

     To disable access to customizing NNM's record of your network's SNMP configuration settings such as GET- and SET-community names and port settings.
   - `ovsnmp/xnmtrap`

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0109
Doc: 3740



To disable access to customizing NNM's event configuration settings.

5. In each of the new directories that you just created, open the following application registration file (ARF): ...\C\ovw

   Use an ASCII editor program and comment out or delete the following blocks of code that provide potentially destructive functionality to the user interface. To comment out a section, use the /* characters at the beginning and the */ characters at the end of the section that you wish NNM to ignore. Although you can delete these sections, for the convenience of troubleshooting and changing your mind later, it is better to simply comment them out.

TIP Never place comments within comments.

The ARF file controls which menu choices show up in the NNM interface. If you find it confusing to read the file, refer to the NNM user interface for clues about what you are seeing. Refer to the *OVwRegIntro* reference page in NNM's online help (or the UNIX manpage) for information about the syntax of the file.

- In the `MenuBar <100> "Map" _M` section, delete or comment out the following sections to remove Map pull-down menu items from the user interface (see the example ARF file on page 305):

```
"New..."
"Open..."
"Save As..."
"Export..."
"Import..."
"Delete..."
"Properties..."
"Submap..."

Menu Submap
"New..."
"Open..."
"Delete..."
"Delete This Submap"
"Set This Submap As Home"
"Make This Submap Persistent"
"Properties..."
"Close
```

- In the `MenuBar <100> "Edit" _E` section, delete or comment out the following sections to remove Edit pull-down menu items from the user interface (see the example ARF file on page 305):

```
"Add Object..."
"Add Connection..."
"Cut"
"Copy"
"Paste"
"Delete"
"Manage Objects"
"Unmanage Objects"
"Object Properties..."

Menu Delete
"From This Submap"
"From All Submaps"
```

- In the `MenuBar <100> "View" _V` section, delete or comment out the following sections to remove View pull-down menu items from the user interface (see the example ARF file on page 305):

```
"Hidden Objects"
"Automatic Layout"
"Redo Layout"

Menu "Hidden Objects"
"Hide Selected From This Submap"
"Hide Selected From All Submaps"
"Show Hidden On This Submap"
"Show Hidden On All Submaps"
```

- In the `Menu Find` section, delete or comment out the following sections to remove Find menu items from the user interface (see the example ARF file on page 305):

```
"Submap..."
```

- Delete or comment out all of the following to disable access to NNM customization through the pop-up menus (see the example ARF file on page 305):

```
"Change Symbol Type"
"Symbol Properties"
"Delete"
"Hide"
"Set Star Center"
```

6. Verify that your changes are valid. At the command prompt, type:

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0110
Doc: 3740

```
ovw -verify
```

7. In each of the new directories that you just created, open the following application registration file (ARF): ...\C\ipmap

   Use an ASCII editor program and comment out or delete the following blocks of code that provide potentially destructive functionality to the user interface. To comment out a section, use the /* characters at the beginning and the */ characters at the end of the section that you wish NNM to ignore. Although you can delete these sections, for the convenience of troubleshooting and changing your mind later, it is better to simply comment them out.

TIP Never place comments within comments.

   The ARF file controls which menu choices show up in the NNM interface. If you find it confusing to read the file, refer to the *OVwRegIntro* reference page in NNM's online help (or the UNIX manpage) for information about the syntax of the file.

   In the `MenuBar "Map"` section, delete or comment out the following sections to remove pull-down menu items from the user interface:

```
"Import..."
"Export..."
```

8. Verify that your changes are valid. At the command prompt, type:

```
ovw -verify
```

9. Set the ovw environment variable `OVwRegDir` in each user/group's path so that the new registration files are used each time this user logs in:

   - *Windows:* Edit the system registry files:

     a. Select `Start:Run` and type **regedit**.

     b. Add a new string value to `HKEY_USERS\`*S-id#*`\Environment`. For example:

        Name: **OVWRegDir**

        Data: **c:*install_dir*\registration\printers_reg\C**

1852

NOTE If you are unsure which `S-id#` (systemID number) is the correct `user id#`, you can reference the registry entry and check the `ProfileImagePath` data. Look at the last 3 or 4 digits in the `S-id#`:
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\current version\ProfileList\S-id#`.

- *UNIX:*
  C shell users, enter the following in each `.cshrc` file; for example:

```
setenv OVwRegDir=/etc/opt/OV/share/registration/printers_reg/C/
```

  Borne and Korn shell users, enter the following in each `.profile` file; for example:

```
export OVwRegDir=/etc/opt/OV/share/registration/printer_reg/C/
```

10. Log in as the user you just established, and test the look and feel of the user interface to make sure you obtained the results that you had in mind. Try out several submaps with a variety of context settings.

TIP If it isn't working as you expected, you can always return to the untouched original files. In a Windows operating system, however, the registry entries will not be automatically reset.

11. When everything is working as you planned, set the file permissions on your custom registration files as follows:

    - *FAT file system in Windows*, you can set individual files to `read-only` for *everyone* on the system. Log in as Administrator. Use the Windows Explorer to access the file properties of each file in the custom registration directory. Set these files to `read-only` to prevent all users from changing your customizations.

TIP As a workaround for the limited user-level permissions in FAT, consider creating an NTFS partition on your hard drive. Then use the partitioned space for your customized registration

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0111
3740
Doc:

directory in order to gain more control over access security. However, if you do this, your customized registration files are no longer automatically included in NNM's backup routine.

- *NTFS in Windows*, you have a fine level of control over file permissions. Log in as Administrator. Using Windows Explorer's `File:Properties->Security` tab, set up the appropriate permissions for the *directory* that holds your customized registration files. Be sure to select both `Replace Permissions on Subdirectories` and `Replace Permissions on Existing Files`. Set the permissions to `read-only` for each user/group to prevent them from changing your customizations.
- *UNIX:* set the appropriate permissions on each file using the standard UNIX `chmod` and `chown` commands. For example:

```
# chmod -R 500 /etc/opt/OV/share/registration/printers_reg/C
# chown -R printers /etc/opt/OV/share/registration/printers_reg/C
# chgrp -R bin /etc/opt/OV/share/registration/printers_reg/C
```

ARF File Modifications Example

The following is a printout of the `ovw` ARF file with bold type showing the sections discussed in the previous section. Place comment symbols /* */ around all the sections in bold type to implement the suggested changes on your management station.

TIP Do not place comments within comments.

```
 /*
 **
 **  @(#)HP OpenView Windows Menu Registration
 **
 **  $Revision: /main/PULSAR/5 $
 **  $Date: 1998/07/06 18:43 UTC $
 */
Application "OpenView Windows"
{
    Description {
        "HP OpenView"
```

```
        "Application registration fiel for various menu items",

        "which present themselves from the ovw menu bar."

    Version "Network  Node Manager X.X (copy_proot modifies)";
    Copyright {
        "Copyright (c) 1990-19XX Hewlett-Packard Company (copy_proot modifies)",
        "All rights reserved."
    }
    }
#ifndef NT
    HelpDirectory "OVW";
#endif /* NT */

    /*
    **
    ** OVw Menu Bars
    **
    */
    MenuBar <100> "Map" _M
    {
#ifndef SPECIAL_EDITION

        <100>   "New..."                _N      Ctrl<Key>N
                Context (AllContexts || WantMapMenus)
                f.new_map;
        <100>   "Open..."               _O      Ctrl<Key>O
                Context (AllContexts || WantMapMenus)
                f.avail_maps;
        <100>   "Refresh"               _f
                Context (AllContexts || WantMapMenus)
                f.refresh_map;
        <100>   "Save As..."    _A      Ctrl<Key>S
                Context (AllContexts || WantMapMenus)
                f.save_map;

        /* 99 is used for ipmap and map customization */

        <98>    "Delete..."             _D
                Context (AllContexts || WantMapMenus)
                f.avail_maps;
#endif /* !SPECIAL_EDITION */
        <98>    "Properties..."    _r
                Context (AllContexts || WantMapMenus)
                f.map_desc;
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0112
3740
Doc:

```
        <98>    "Separator 1"
                Context (CantTouchThis)
                        f.separator;
#ifndef NT
        <98>    "Print Window"  _P              Ctrl<Key>P
                        Context (AllContexts || WantMapMenus)
                        f.action Print_Window;
#endif /* !NT */
        <98>    "Submap"                _S
                        Context (AllContexts || WantMapMenus)
                        f.menu "Submap";
#ifndef SPECIAL_EDITION
        <98>    "Snapshot"              _h
                        Context (AllContexts || WantMapMenus)
                        f.menu "Snapshot";
#endif /* !SPECIAL_EDITION */
        <0>             "Exit"                  _x
                        Context (CantTouchThis)
                        f.exit;
    }
#ifndef NT
        Action "Print_Window" {
                Command "printwindow";
        }
#endif /* NT */
    Menu Submap
    {
        <100>   "New..."                        _N
                        Context (AllContexts || WantMapMenus)
                        f.new_submap;
        <100>   "Open..."                       _O
                        Context (AllContexts || WantMapMenus)
                        f.list_submaps;
        <100>   "Delete..."                     _D
                        Context (AllContexts || WantMapMenus)
                        f.list_submaps;
        <100>   "Delete This Submap"    _T
                        Context (AllContexts || WantMapMenus)
                        f.delete_smap;
        <100>   "Set This Submap As Home"       _H
                        Context (AllContexts || WantMapMenus)
                        f.set_home_submap;
#ifndef NT
        <100>   "Make This Submap Persistent"   _M
                        Context (AllContexts || WantMapMenus)
                        f.persistify;
```

```
#endif /* !NT */
        <100>   "Properties..."          _r
                        Context (AllContexts || WantMapMenus)
                        f.submap_desc;
    <1>         "Close"          _C      <Key>Escape
                        Context (AllContexts || WantMapMenus)
                        f.close_smap;
        }
#ifndef SPECIAL_EDITION
    Menu "Snapshot"
    {
        <100>   "New..."                 _N
                        Context (AllContexts || WantMapMenus)
                        f.create_snap;
        <100>   "Open..."                _O
                        Context (AllContexts || WantMapMenus)
                        f.avail_snaps;
        <100>   "Delete..."              _D
                        Context (AllContexts || WantMapMenus)
                        f.avail_snaps;
        <100>   "Properties..."          _r
                        Context (AllContexts || WantMapMenus)
                        f.snap_desc;
        <100>   "Close"                  _C
                        Context (AllContexts || WantMapMenus)
                        f.close_snapshot;
    }
#endif /* !SPECIAL_EDITION */


    MenuBar <100> "Edit" _E
    {
        <100>   "Add Object..."          _A
                        Context (AllContexts || WantEditMenus)
                        f.add_obj;
        <100>   "Add Connection..."      _n
                        Context (AllContexts || WantEditMenus || WantEditObjs)
                        f.add_conn;
        <100>   "Separator 1"
                Context (CantTouchThis)
                        f.separator;
        <100>   "Cut"                    _t     Ctrl<Key>X
                        Context (AllContexts || WantEditMenus || WantEditCut)
                    f.cut_obj_smap;
        <100>   "Copy"                   _C     Ctrl<Key>C
                        Context (AllContexts || WantEditMenus || WantEditCut)
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
0113
Fls. Nº 0740
Doc:

```
                    f.copy_obj_smap;
    <100>   "Paste"                 _P      Ctrl<Key>V
                    Context (AllContexts || WantEditMenus || WantEditCut)
                    f.paste;
    <100>   "Delete"                _D
                    Context (AllContexts || WantEditMenus || WantEditObjs)
                    f.menu Delete;
<100>   "Selected Objects List..."      _L      Ctrl<Key>L
                    Context (AllContexts || WantLocateMenus)
                    f.sel_objs;
    <100>   "Find"              _F
        Context (AllContexts || WantEditMenus || WantLocateMenus)
                    f.menu Find;
    <50>    "Separator 2"
            Context (CantTouchThis)
                    f.separator;
    <50>    "Manage Objects"        _M
                    Context (AllContexts || WantMapMenus)
                    f.manage_objects;
    <50>    "Unmanage Objects"      _U
                    Context (AllContexts || WantMapMenus)
                    f.unmanage_objects;
    <1>         "Object Properties..."      _r
                    Context (AllContexts || WantEditMenus || WantEditObjs)
                    f.obj_desc;
    }

Menu Delete
{
    <100>   "From This Submap"      _T
                    Context (AllContexts || WantEditMenus || WantEditObjs)
                    f.delete_obj_smap;
    <100>   "From All Submaps"      _A
                    Context (AllContexts || WantEditMenus || WantEditObjs)
                    f.delete_obj;
}
Menu Find
{
    <100>   "Submap..."                     _S
                    Context (AllContexts || WantLocateMenus)
                    f.list_submaps;
    <100>   "Object By Selection Name..."   _N      Ctrl<Key>F
                    Context (AllContexts || WantLocateMenus)
                    f.locate_name;
    <100>   "Object By Attribute..."        _A      Ctrl<Key>A
                    Context (AllContexts || WantLocateMenus)
```

```
                    f.locate_attr;
        <100>   "Object By Comment..."          _C
                    Context (AllContexts || WantLocateMenus)
                    f.locate_comment;
        <100>   "Object By Status..."    _u
                    Context (AllContexts || WantLocateMenus)
                    f.locate_status;
        <100>   "Object By Symbol Type..."      _T
                    Context (AllContexts || WantLocateMenus)
                    f.locate_type;
        <100>   "Object By Label..."    _L
                    Context (AllContexts || WantLocateMenus)
                    f.locate_label;
    }
    MenuBar <100> "View" _V
    {
        <100>   "Highlights"            _H
            Context (AllContexts || WantEditMenus )
                    f.menu Highlights;
        <100>   "Hidden Objects"                        _n
                    Context (AllContexts || WantEditMenus || WantEditHide)
                    f.menu "Hidden Objects";
#ifdef NT
        <100>   "Toolbar"               _T
                    Context (AllContexts || WantViewMenus)
                    f.submap_toolbar_toggle;
        <100>   "Status Bar"            _S
                    Context (AllContexts || WantViewMenus)
                    f.submap_status_toggle;
#else /* NT */
        <100>   "Toolbar"               _T
                    Context (AllContexts || WantViewMenus)
                    f.toolbar_toggle;
#endif /* NT */
        <100>   "Pan and Zoom"          _Z
                    Context (AllContexts || WantViewMenus)
                    f.show_panner;
#ifndef NT
        <100>   "User Plane"    _U
                    Context (AllContexts || WantViewMenus)
                    f.user_plane;
        <100>   "Automatic Layout"      _A
                    Context (AllContexts || WantViewMenus)
                    f.auto_layout;
        <100>   "Submap Overlay"        _O
                    Context (AllContexts || WantViewMenus)
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0114
Doc: 3740

```
                        f.overlay_toggle;
#else /* NT */
        <100>   "Submap Overlay"        _O
                        Context (AllContexts || WantViewMenus)
                        f.nt_overlay_toggle;
#endif /* NT */
        <100>   "Window Geometry"       _G
                        Context (AllContexts || WantViewMenus)
                        f.menu "Window Geometry";
        <100>   "Redo Layout"           _R
                        Context (AllContexts || WantViewMenus)
                        f.redolayout;
    }
    Menu Highlights
    {
        <100>   "Select Highlighted"    _S   Ctrl<Key>H
                        Context (AllContexts || WantEditMenus)
                        f.select_highlighted;
        <100>   "Clear Highlighted"     _C
                        Context (AllContexts || WantEditMenus)
                        f.clear_highlights;
    }
    Menu "Hidden Objects"
    {
        <100>   "Hide Selected From This Submap"        _T
                        Context (AllContexts || WantEditMenus || WantEditHide)
                        f.hide_obj_smap;
        <100>   "Hide Selected From All Submaps"        _A
                        Context (AllContexts || WantEditMenus || WantEditHide)
                        f.hide_obj;
        <100>   "Show Hidden On This Submap"    _S
                        Context (AllContexts || WantEditMenus || WantEditHide)
                        f.unhide;
        <100>   "Show Hidden On All Submaps"    _O
                        Context (AllContexts || WantEditMenus || WantEditHide)
                        f.unhide_all;
        }

        Menu "Window Geometry"
        {
                <100>   "Save For This Submap"  _T
                        Context (AllContexts || WantViewMenus)
                        f.geometry_smap;
                <100>   "Save For All Open Submaps"     _A
                        Context (AllContexts || WantViewMenus)
                        f.geometry_all;
```

```
            <100>   "Clear For This Submap" _S
                    Context (AllContexts || WantViewMenus)
                    f.geometry_smap_off;
            <100>   "Clear For All Open Submaps"    _O
                    Context (AllContexts || WantViewMenus)
                    f.geometry_all_off;
        }
    MenuBar <100> "Performance" _P
    {
    }
    MenuBar <100> "Configuration" _C
    {
    }

    MenuBar <100> "Fault" _F
    {
    }
    MenuBar <100> "Accounting" _A
    {
    }
    MenuBar <100> "Security" _S
    {
    }
    MenuBar <100> "Tools" _T
    {
    }
    MenuBar <100> "Options" _O
    {
    }
    MenuBar <100> "Window" _W
    {
        <100>   "Separator 1"
                Context (CantTouchThis)
                    f.separator;
#ifdef NT
        <100>   "Cascade Submaps"                   _C
                    Context (AllContexts || WantLocateMenus)
                    f.cascade_submaps;
        <100>   "Separator 2"
                Context (CantTouchThis)
                    f.separator;
#endif /* NT */
        <100>   "Root"                              _R
                    Context (AllContexts || WantLocateMenus)
                    f.goto_root;
        <100>   "Home"                              _H
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0115
Doc: 3740

```
                    Context (AllContexts || WantLocateMenus)
                    f.goto_home;
        <100>   "Parent"                        _P
                    Context (AllContexts || WantLocateMenus)
                    f.goto_parent;
        <51>   "Separator 3"
                Context (CantTouchThis)
                    f.separator;
    }
    MenuBar <0> "Help" _H
    {
        <90>    "Display Legend"        _D
                    Context (AllContexts || WantHelpMenus)
                    f.disp_legend;
#ifndef NT
        <80>    "Mouse and Keyboard"    _M
                    Context (AllContexts || WantHelpMenus)
                    f.help_browser "ovw:mousenkeyboard";
        <80>    "On Window"
                    Context (AllContexts || WantHelpMenus)
                    f.help_browser "ovw:overv";
        <60>    "Using Help"                    _H
                    Context (AllContexts || WantHelpMenus)
                    f.on_help;
    <50>    "Misc"              _i
            Context (AllContexts || WantHelpMenus)
            f.menu "Misc Help";
#endif /* !NT */

        <43>    "Release Notes" _L f.action "ReleaseNotes";

        <40>    "About HP OpenView..."      _A
                    Context (AllContexts || WantHelpMenus)
                    f.about_ovw;
    }
    Action "ReleaseNotes"
    {
       Command "ovweb -ReleaseNotes README.html";
    }
#ifndef NT
    Menu "Misc Help"
    {
        <98>    "Tasks"                 _T
            Context (AllContexts || WantHelpMenus)
                    f.task_index;
        <98>    "Functions"             _F
```

```
            Context (AllContexts || WantHelpMenus)
                        f.function_index;
    }
#endif /* !NT */

    /*
     *  OVw Popup menu
     */
    PopupItem <100> "Open" Context (AllContexts || WantPopupMenus)
                    TargetSymbolType ANY f.open_symbol;
    PopupItem <100> "Change Symbol Type..." Context (AllContexts ||
WantPopupMenus)
                    TargetSymbolType ANY f.change_symbol;
    PopupItem <100> "Symbol Properties..." Context (AllContexts ||
WantPopupMenus)
                    TargetSymbolType ANY f.sym_desc;
    PopupItem <100> "Delete" Context (AllContexts || WantPopupMenus)
                    TargetSymbolType ANY f.delete_symbol;
    PopupItem <100> "Hide" Context (AllContexts || WantPopupMenus)
                    TargetSymbolType ANY f.hide_symbol;
    PopupItem <100> "Set Star Center" Context (AllContexts || WantPopupMenus)
                    TargetSymbolType ANY f.star_center_symbol;
    PopupItem <100> "PopupSeparator1" Context (AllContexts || WantPopupMenus)
                    TargetSymbolType ANY f.separator;
    PopupItem <100> "Object Properties..." Context (AllContexts ||
WantPopupMenus)
                    TargetSymbolType ANY f.obj_desc;


    /*
     *  Toolbar buttons with text
     */

#ifndef SPECIAL_EDITION
    /* Uncomment these for text buttons */

/*  ----  Remove this line for text buttons on the toolbar ----

    ToolbarButton <100> "Close" Context "AllContexts" f.close_smap;
    ToolbarButton <100> "Home" Context "AllContexts" f.goto_home;
    ToolbarButton <100> "Root" Context "AllContexts" f.goto_root;
    ToolbarButton <100> "Parent" Context "AllContexts" f.goto_parent;
    ToolbarButton <100> "TBAR_SEP1"  Context "AllContexts" f.separator;
    ToolbarButton <100> "Pan" Context "AllContexts" f.show_panner;
    ToolbarButton <100> "TBAR_SEP2"  Context "AllContexts" f.separator;
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0116
Doc 3740

```
    ToolbarButton <100> "Open View" Context "AllContexts" f.about_ovw;

    ----  Remove this line for text buttons on the toolbar ----  */
#endif /* !SPECIAL_EDITION */
    /*
     *  Toolbar buttons with icons - icon paths are relative to OV       bitmaps
     *  directory.
     */
    ToolbarButton <100>
#ifdef NT
                @"toolbar/close.bmp,Close"
#else /* NT */
        @"toolbar/close.24.pm:toolbar/noclos.24.pm"
#endif /* NT */
                Context "AllContexts" f.close_smap;

    ToolbarButton <100>
#ifdef NT
                @"toolbar/home.bmp,Home"
#else /* NT */
                @"toolbar/home.24.pm:toolbar/nohome.24.pm"
#endif /* NT */
                Context "AllContexts" f.goto_home;
    ToolbarButton <100>
#ifdef NT
                @"toolbar/root.bmp,Root"
#else /* NT */
                @"toolbar/root.24.pm:toolbar/noroot.24.pm"
#endif /* NT */
                Context "AllContexts" f.goto_root;
    ToolbarButton <100>
#ifdef NT
                @"toolbar/parent.bmp,Parent"
#else /* NT */
        @"toolbar/parent.24.pm:toolbar/noparent.24.pm"
#endif /* NT */
                Context "AllContexts" f.goto_parent;
    ToolbarButton <90> "TBAR_SEP1" Context "AllContexts" f.separator;
    ToolbarButton <90>
#ifdef NT
                @"toolbar/pan.bmp,Pan && Zoom"
#else /* NT */
        @"toolbar/pan.24.pm:toolbar/nopan.24.pm"
#endif /* NT */
                Context "AllContexts" f.show_panner;
    ToolbarButton <0> "TBAR_SEP2" Context "AllContexts" f.separator;
```

```
    ToolbarButton <0>
#ifdef NT
                @"toolbar/hpov.bmp,About HP OpenView"
#else /* NT */
        @"toolbar/hpov.24.pm:toolbar/nohpov.24.pm"
#endif /* NT */
                Context "AllContexts" f.about_ovw;
}
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0117
Doc: 3740

Allowing Others to View NNM from Many Computers

There are two ways to access NNM from multiple computers while it is running on your management station.

- Remote consoles

  Allows multiple people to use NNM as if they were sitting at the management station.

- NNM's web interface

  Allows multiple people to have read-only access to the maps and limited read-write access to the alarm tracking system. The web interface updates dynamically to display current network activity.

- Microsoft Terminal Services

  Allows multiple people to use NNM as if they were sitting at the management station.

Remote Consoles

A number of people can view one map simultaneously or multiple maps by using remote console access (see *A Guide to Scalability and Distribution* manual for information). Remote consoles access the NNM services (background processes) and databases running on the management station, yet run NNM's user interface locally.

This is a great way to distribute the work load among your team. The map and alarms browser list are updated dynamically so everyone on your team knows the current network status. Everyone accessing NNM can acknowledge/delete alarms from the Alarm Browser as issues are resolved.

The number of remote access logins that can be supported is dependent upon a number of factors. See the *Performance and Configuration Guide* that was included with NNM's installation package.

Keep in mind that each remote station generates some network traffic in order to operate.

NNM's Web Interface

Your team can remotely access the NNM session that is running on the management station through the web interface. See Chapter 14, "NNM on the Web," for more information.

Microsoft Terminal Services

In the Terminal Server multiuser environment, a terminal emulator allows a user to locally display the Windows 2000 desktop of a remote server and manage NNM on that remote server. To enable this functionality, the server must have Microsoft Terminal Services enabled and the local workstation must have Microsoft Terminal Services Client installed. See the *Installation Guide* for more information.

The Terminal Server machine becomes a core server that allows multiple users the ability to connect and display its desktop on their local machines via a Terminal Services Client application. A user can connect (via Terminal Services Client) to multiple Terminal Servers, or connect multiple times to the same Terminal Server and locally display multiple desktops.

The Microsoft Terminal Services client is a small executable that resides on each client workstation. Its function is to display the remote Windows 2000 user interface to the user.

See *A Guide to Scalability and Distribution* manual for more information.

RQS nº 03/2005 - C
CPMI - CORREIOS
Fls. Nº 0118
3740
Doc:

Closing All Current Sessions

Sometimes, in order to configure, update, or troubleshoot NNM, it is necessary to stop and start the NNM user interface (you *don't* need to stop all the services/background processes). To close all sessions (local, remote, and web) that your team is currently using, do the following:

1. To display a list of currently running sessions, at the command prompt, type:

   ovstatus -v ovuispmd

   You may want to print out this information so that you have the hostnames and session IDs for restarting the sessions later. You may wish to notify users who are currently accessing NNM to warn them about the shutdown.

2. To stop all sessions, at the command prompt, type:

   ovstop -c ovuispmd

   (This terminates any sessions and stops the ovuispmd service--the maps are all closed but your network is still being monitored by NNM services/background processes.)

3. To start new NNM sessions, at the command prompt, type:

   ovstart -c ovuispmd

4. Now open NNM's user interface to begin one or more sessions.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0119
3740
Doc:



10 Keeping Up with Events on Your Network: Beyond the Maps

Once you have verified the accuracy of NNM's maps of your network, you can be sure that communications are established with all important devices. It is now time to turn your attention to the second aspect of NNM, the event system.

In this chapter, you will find:

- *Background Information* (page 323).
  An explanation about how the NNM event system works.
- *NNM's Alarm Browser Overview* (page 329).
  The Alarm Browser provides a convenient central location for your team to monitor critical events on your network.
- *Alarm Browser Customization (*page 342).
  You can control the way the Alarm Browser looks and operates.

See Chapter 11, "Event Reduction Capabilities: Getting to the Root Cause," for information about the event reduction tools that are included with NNM. Also learn how you can use event correlation and the de-duplication feature to automatically determine the root cause of a problem, eliminate unuseful alarms, and in response to a pattern of events, generate new alarms that contain exactly the data you need for troubleshooting.

See Chapter 12, "Customizing Events: Doing It Your Way," for an explanation about how you can implement your own custom event monitoring strategies using NNM's Event Configuration, Application Builder, and Data Collection & Threshold features. You will also learn how to utilize vendor-specific MIBs and MIFs using NNM's MIB Load/Unload, MIB Browser, and DMI Browser features.

See Chapter 13, "Using Event Data," for an explanation about how you can take advantage of the information that has been gathered. NNM provides tools for using this information for analytical purposes and allows you to port the data to the application of your choice. You will learn about NNM's MIB Grapher and the data warehouse features.

ECT nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0120
3740
Doc:

How NNM's Event System Works

Many services (background processes) within NNM and other HP OpenView compatible programs, gather information and generate **events** that are forwarded to NNM. Events can also be emitted from agents on managed nodes, or from management applications residing on the management station or on specific network nodes. Unsolicited SNMP events or notifications are called **traps**. NNM provides one centralized location, the Alarm Browser, where the events and traps are visible to your team. You can control which events and traps are considered important enough to show up as **alarms**. You and your team can easily monitor the posted alarms and take appropriate action to preserve the health of your network. Examples of alarms include:

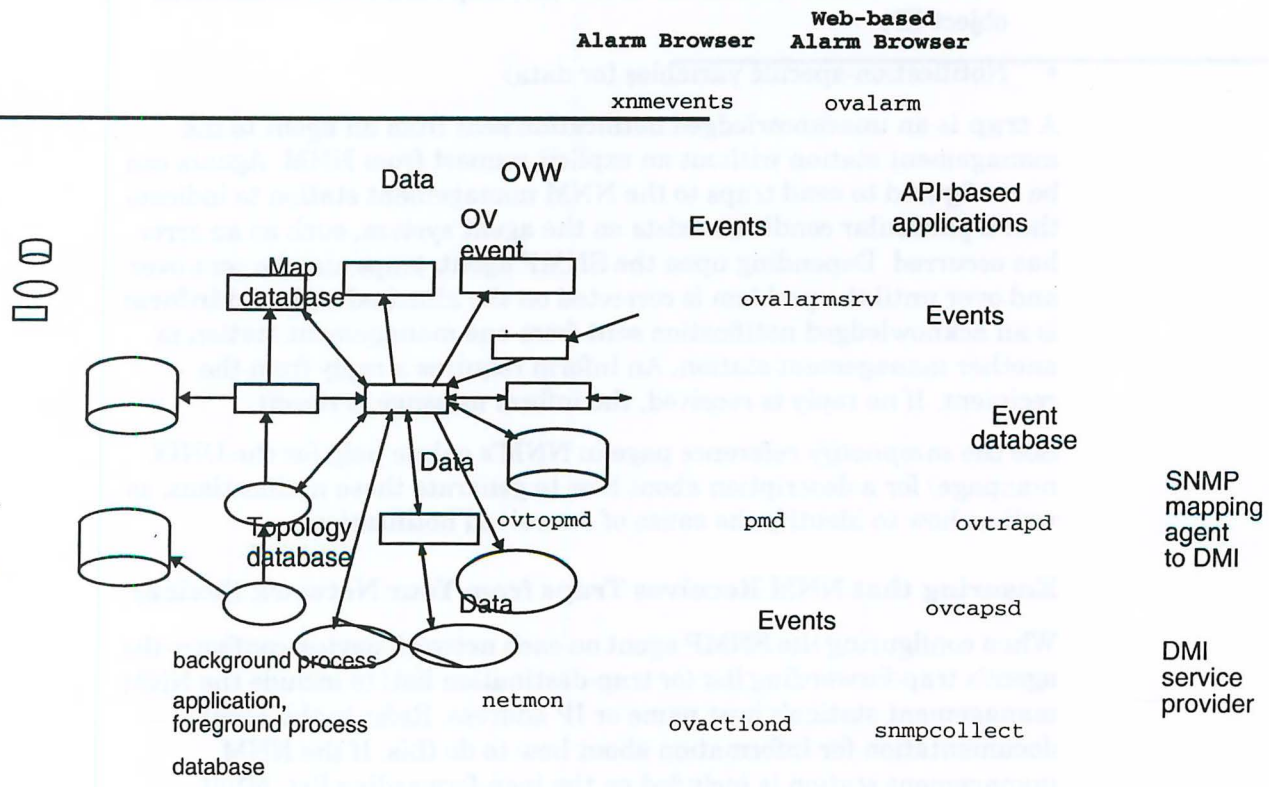
- A critical router exceeded its threshold of traffic volume that you configured in NNM's Data Collection & Thresholds feature (`snmpCollect` service).
- The shell script that you wrote or the MIB application that you created using NNM's Application Builder feature gathered the specific information you needed and posted it to the Alarm Browser.
- An unauthorized network topology change was detected (`netmon` or `ovrepld` services).
- At 3 a.m., you receive a page notifying you that one of your mission-critical servers is using its UPS battery power. You received this page because of the way you configured the underlying DMI event `dmtfUPSBatteryUtilityPowerLostSystemOnBattery` (`ovcapsd` service and `ovactiond` service).
- The theft of a network printer was detected during NNM's regularly scheduled polling cycle (`netmon` service).
- An SNMP agent on a managed critical server forwarded a trap to NNM (`ovtrapd` service) because it was overheating and about to fail.

All events are passed to NNM's `pmd` service, which then logs them in the event database and sends them on to all applications that subscribe to them. For example, the Alarm Browser subscribes to all events configured to *display in a category* of the Alarm Browser.

NOTE Alarms are not received by or displayed in the Alarm Browser if the pmd service is not running. See "Make Sure NNM's Services Are Successfully Running" on page 106 for information about how to verify that pmd is running. Refer to Appendix A, "NNM Services and Files," on page 539 for more information about these services (background processes).

If additional actions were configured to automatically execute upon the pmd services' receipt of a certain alarm (such as dialing a pager or sending an email message), the alarm is also forwarded to NNM's ovactiond service.

Figure 10-1 pmd Interactions with Other NNM Services



By default, NNM's Event Configuration feature includes preconfigured definitions for all standard traps. However, by default not all definitions are configured to post alarms into the Alarm Browser. Use NNM's Event

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0121
3740
Doc:

Configuration feature to specify which traps are important to you and should, therefore, be posted in the Alarm Browser category of your choice (see "Event Configuration Overview" on page 422).

SNMPv1 Traps / SNMPv2c Traps and Informs

An SNMP notification is a message sent from an agent to notify another system of an event on the local system. The notification may either be acknowledged (SNMPv2c `InformRequest`) or unacknowledged (SNMPv1 `TrapResponse` or `SNMPV2cTrap`).

NNM provides you with useful troubleshooting information each time a notification is received:

- The name or address of the node from which the notification came (also called an agent address)
- The notification identification (that is, trap number or notification object ID)
- Notification-specific variables (or data)

A **trap** is an unacknowledged notification sent from an agent to the management station without an explicit request from NNM. Agents can be configured to send traps to the NNM management station to indicate that a particular condition exists on the agent system, such as an error has occurred. Depending upon the SNMP agent, traps may be sent over and over until the problem is corrected on the attached node. An **inform** is an acknowledged notification sent from one management station to another management station. An inform requires a reply from the recipient. If no reply is received, the inform message is resent.

See the *snmpnotify* reference page in NNM's online help (or the UNIX manpage) for a description about how to generate these notifications, as well as how to identify the cause of a received notification.

Ensuring that NNM Receives Traps from Your Network Devices

When configuring the SNMP agent on each network device, configure the agent's trap-forwarding list (or trap-destination list) to include the NNM management station's host name or IP address. Refer to the agent's documentation for information about how to do this. If the NNM management station is included on the trap-forwarding list, NNM receives notice from the agent when something goes wrong (even if the device does not show up on your NNM maps).

If your network device is using the HP SNMP EMANATE agent, NNM's `netmon` service automatically updates the agent's trap-forwarding list upon initial discovery, provided your network's SET-community names are configured within NNM. See "GET- and SET-Community Name and SNMP Port Issues" on page 145.

NOTE

For your convenience, NNM lets you view the currently configured trap-forwarding list on remote HP 9000 or Sun SPARCstations running the HP OpenView SNMP Agent software. On any submap, select the symbol for the HP 9000 or Sun SPARCstation running the HP OpenView SNMP Agent software, then do one of the following:

- Select the `Configuration:SNMP Trap Recipients` menu item.
- Use NNM's MIB Browser and the HP-UNIX MIB's object: `.1.3.6.1.4.1.11.2.13.1.2`

(You must first configure your correct community names. See "GET- and SET-Community Name and SNMP Port Issues" on page 145.)

Sending SNMP Traps from the NNM Management Station

To forward SNMP trap and inform messages originating from the NNM management station to another location of your choice, you must configure the SNMP agent on the NNM management station to include the destination host name or IP address in its trap-forwarding list. You must also manually configure the protocol versions that the destination supports. Use the `xnmsnmpconf -setVersions` command to configure this feature. Refer to the *xnmsnmpconf* reference page in NNM's online help (or the UNIX manpage) for more information.

For example, to configure protocol versions SNMPv1 and SNMPv2C for the default port for system `robert`, use the following command:

```
xnmsnmpconf -setVersions robert/162 1,2C
```

NOTE

For information about forwarding alarms from one management station to another management station, see *A Guide to Scalability and Distribution*.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0122
Doc. 3740

DMI Events (Indications)

The Desktop Management Interface (DMI) is a parallel management strategy to SNMP. DMI standards were developed by the Desktop Management Task Force (DMTF). Although DMI is entirely independent from the SNMP protocol, there are many similarities:

- The DMI **client** is similar to the SNMP management station.
- The DMI **service provider** is similar to the SNMP agent and must be running on each remote DMI device.
- The DMI **MIF** (Management Information Format) file is similar to the SNMP MIB file and defines the management information that can be provided by the service provider (event) or requested by the client (get/set).
- The **DMI event** is similar to the SNMP trap.

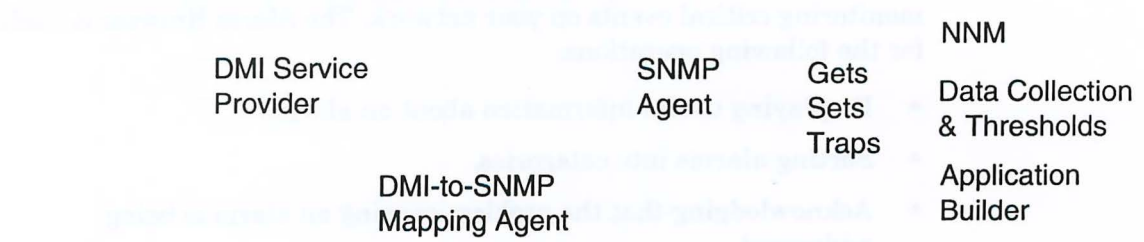
If your management station is running NNM on a Windows operating system, during discovery polling, NNM subscribes to receive DMI events from all managed systems running DMI version 2.0. All DMI events are received by NNM's ovcapsd service (background process) and converted to SNMP traps as specified in the Desktop Management Task Force's DMI to SNMP Mapping Standard. See the *ovcapsd* reference page in NNM's online help for more information.

NOTE

If your management station is running NNM for a UNIX system, you must communicate with the DMI service provider indirectly through an SNMP agent installed on the remote DMI-enabled device itself along with a DMI-to-SNMP mapping agent (such as Intel's). See the following figure.

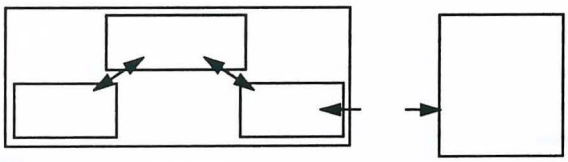
The SNMP agent then handles all communications. Therefore, NNM doesn't need to subscribe to the DMI service provider in order to receive DMI events from this node.

Figure 10-2 Remote DMI Enabled Node



All of the Desktop Management Task Force's standard DMI events that were available at the time of NNM's release are preconfigured in NNM's event system to post automatically to the Alarm Browser. You can customize the behavior of these events in the same manner that you can customize any SNMP event (see "Event Configuration Overview" on page 422 for information about customizing event configurations).

In addition to the DMTF's standard DMI MIF definitions, third-party vendors may have developed custom MIFs with their own custom events. NNM will receive these custom events and translate them to a generic DMI Event Received message until the vendor-specific DMI-to-SNMP mapping is configured in NNM. See "Loading DMI-to-SNMP Event Mappings" on page 419 for information about configuring a DMI-to-SNMP mapping for a custom MIF file.



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0123
3740
Doc:



Alarm Browser Overview

NNM's Alarm Browser provides a convenient central location for monitoring critical events on your network. The Alarm Browser is useful for the following operations:

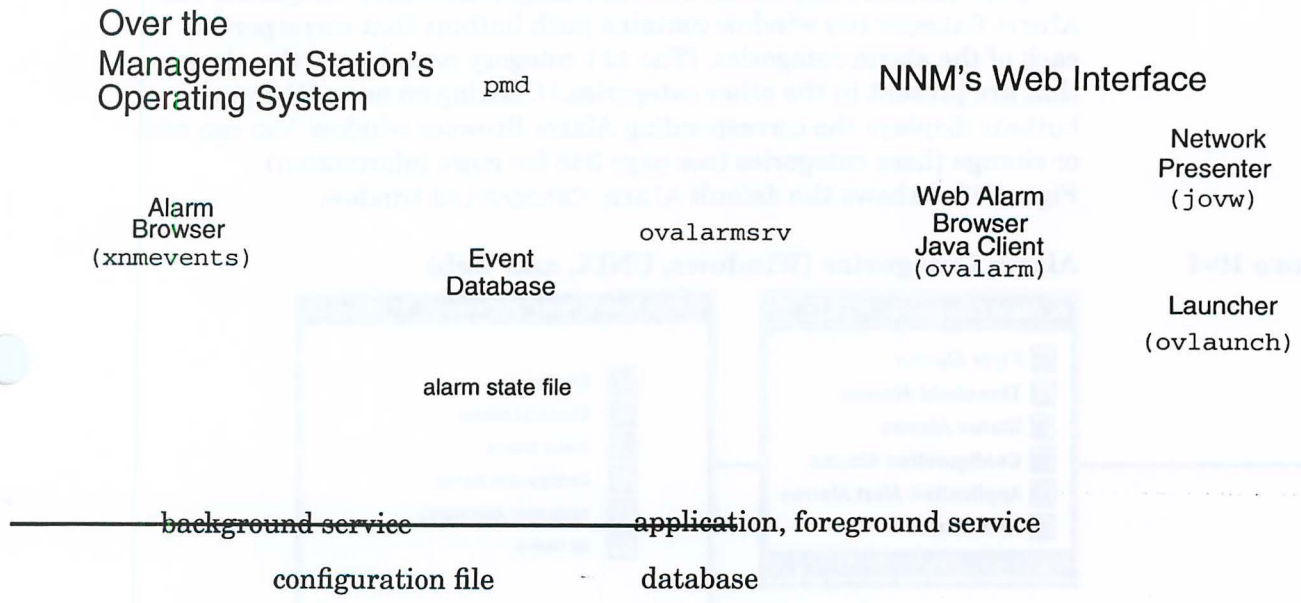
- Displaying useful information about an alarm.
- Sorting alarms into categories.
- Acknowledging that the problem causing an alarm is being addressed.
- Dynamically filtering the alarm list in multiple ways to make the information more useful; for example, by specific node.
- Deleting alarms from the list after they are resolved.
- Specifying additional actions that can be executed upon selected alarms.

There are actually two NNM Alarm Browser programs:

- one that runs under the management station's operating system
- one that runs within NNM's Java-based web interface

Both programs *share* the event database and configuration files for alarms as shown in the following figure. Therefore, no matter which Alarm Browser you use, the displayed list of alarms remains current at all times. Whenever someone acknowledges an alarm, deletes an alarm, or changes severity for an alarm everyone on the team sees the change.

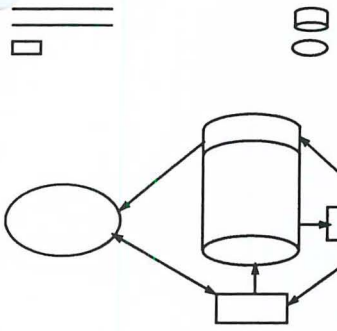
Figure 10-3 Relationship Between the Two Alarm Browsers



Displaying Alarms

To view alarms, open the NNM user interface, then:

- *Windows or UNIX:* Either,
  - In the `Alarm Categories` window, click on the button that corresponds to the category you wish to view.
  - In any submap, select the `Fault:Alarms` menu item to display the `All Alarms Browser` window. If any symbols are selected on your map, the alarm list is *filtered* to show only alarms related to the selected symbols.
- *Java-based web interface:* Either,
  - In the Launcher, select the `Tools` tab, then select `NNM:Alarm Browser`. In the `Alarm Categories` window, click on the button that corresponds to the category you wish to view.
  - In Network Presenter, select the `Fault` menu, then select `Alarm Browser`. In the `Alarm Categories` window, click on the button that corresponds to the category you wish to view.



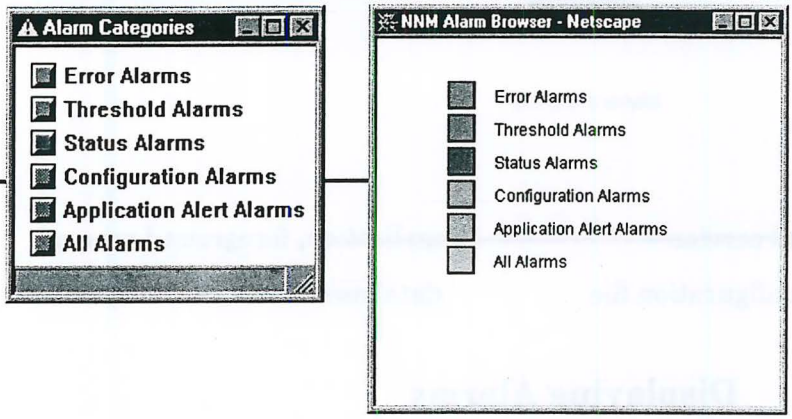
RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0124
3740
Doc:

To exit any of the Alarm Browser windows, select `File:Close`.

Alarm Categories/Alarm Browser Windows

For your convenience, NNM sorts incoming alarms into categories. The `Alarm Categories` window contains push buttons that correspond to each of the alarm categories. (The `All` category contains all the alarms that are present in the other categories.) Clicking on one of the push buttons displays the corresponding Alarm Browser window. You can add or change these categories (see page 348 for more information). Figure 10-4 shows the default `Alarm Categories` window.

Figure 10-4 **Alarm Categories (Windows, UNIX, and Web)**



The push buttons in this window change color to indicate that alarms have been received. The color of the push button reflects the most severe unacknowledged alarm in the category, or it remains the background color if no alarms are present or all alarms are acknowledged. By default, alarm severity is indicated by the following colors:

Normal	Green
Warning	Cyan
Minor	Yellow
Major	Orange
Critical	Red
No alarms	Background color
All alarms acknowledged	White

When you select a category, the corresponding Alarm Browser window is displayed. The Alarm Browser window contains a scrollable list of alarms belonging to the associated category. The Alarm Browser window also displays status about the number of alarms in the window and their severity. Figure 10-6 shows the `All Alarms Browser` window.

To view details about alarms:

- *Windows or UNIX:*
  - Click the right mouse button on any alarm message to display a pop-up window that contains a summary.
  - Select the `Actions:Alarm Details` for complete details.
- *Java-based web interface:*
  - Click on the  button for complete details.
  - Select the `Actions:Alarm Details` for complete details.

It is possible to sort the alarm list:

- *Windows or UNIX:* Select `Actions:Additional Actions` for sorting choices.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0125
3740
Doc:

- *Java-based web interface:* Click once or twice on any column heading.

Figure 10-5 All Alarms Browser Window (Windows or UNIX)

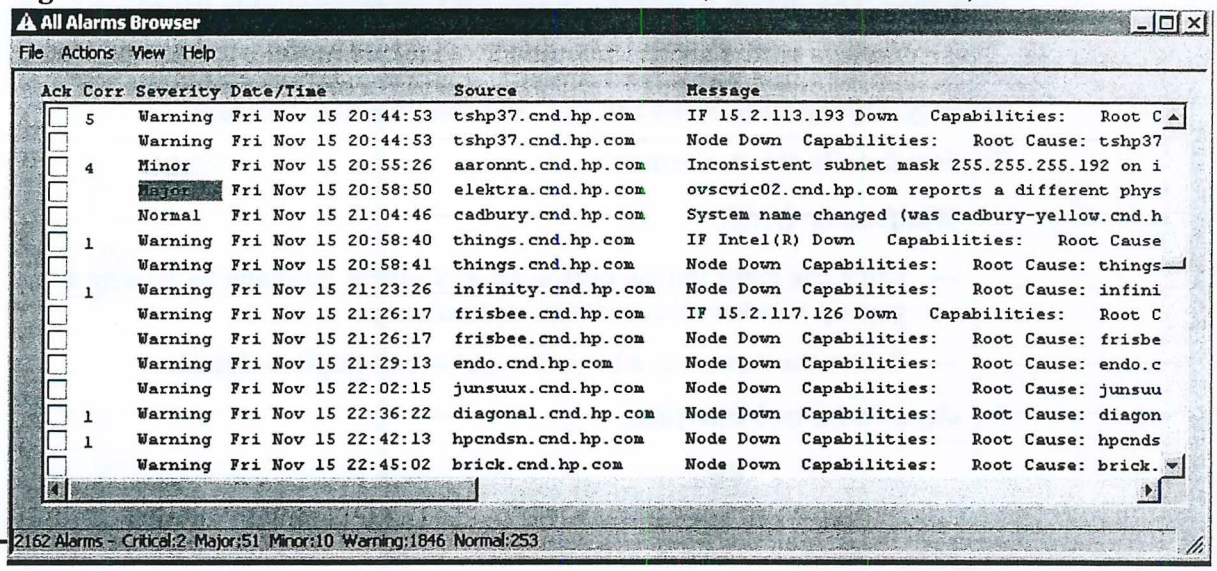
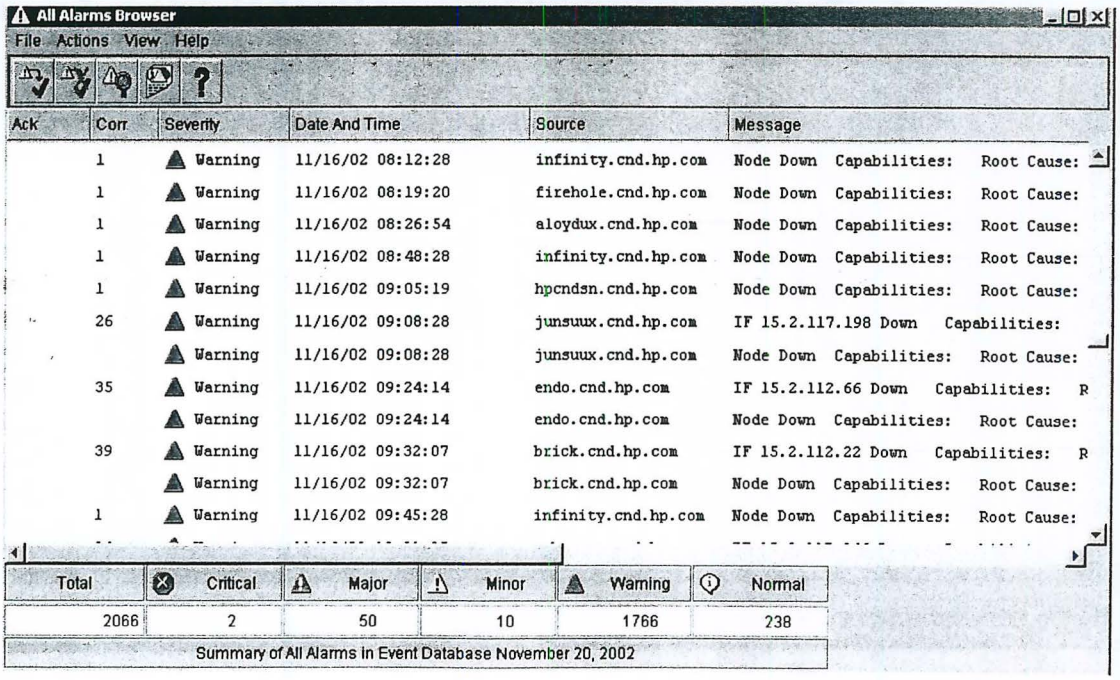


Figure 10-6 All Alarms Browser Window (Web)



The Alarm Browser window lists all undeleted alarms for the indicated category. By default, the alarms are in chronological order with the most recent event at the *bottom* of the list.

For each alarm, the list displays the following:

`Ack`	A check mark indicating whether the alarm is acknowledged or unacknowledged.
`Corr`	A number in this column indicates that this is a primary (root cause) alarm for a group of alarms identified by the Event Correlation System. This number represents the quantity of related or duplicate events correlated beneath the most recent alarm. If you double-click on this number, NNM displays all of the events nested under the alarm.
`Severity`	The severity of the alarm.
`Date/Time`	The day of the week, date, and time when the alarm was received.
`Source`	An identifier (such as a node name) for the network object where the alarm originated.
`Message`	A brief description of the alarm.

Acknowledging Alarms

In order to keep track of which alarms are being worked on, members of your team can acknowledge an alarm, yet not delete it. When an alarm is acknowledged, everyone who has access to the Alarm Browser sees the change. This is a great way for your team to communicate about which issues are being addressed.

Once acknowledged, an alarm remains visible but does not affect the color propagated into the `Alarm Categories` window. To acknowledge selected alarms:

- *Windows and UNIX:*
  Either select the `Actions:Acknowledge` menu item or click in the `Ack` field.
- *Java-based web interface:*
  Either select the `Actions:Acknowledge` menu item or click the  button.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: Nº 0126
3740
Doc:

Filtering Alarms

Filtering allows you to limit the number of alarms displayed. You display only the alarms that are meaningful to your particular troubleshooting efforts at the time; for example, all alarms related to a specific node. Your filtering choices do not affect the Alarm Browser lists being viewed by other members of your team. When you close any Alarm Browser window, the filters are automatically cleared.

Each person using NNM can dynamically filter their displayed alarm list based upon one or more criteria. The criteria must all be true for an alarm to display in the list:

- Severity level
- Source IP addresses or use wildcards to specify a range of IP addresses or node names
- Acknowledged or unacknowledged alarms
- Alarm time span
- Message string word search
- Event type

Filters are available from any Alarm Browser window under `View:Set Filters`.

- *Windows or UNIX:*
  If filtering is on, the status message at the bottom of the Alarm Browser window indicates that filtering is applied.

  Each Alarm Browser window can use unique alarm filter settings. Only one filter dialog box can be displayed at a time. The title bar of the filter dialog box indicates which Alarm Browser window is currently affected. If the filter dialog box is displayed and the `View:Set Filters` menu item is selected from a different Alarm Browser window, the name in the filter dialog box title bar changes and the filter settings in the dialog box change to reflect current filter settings for that Alarm Browser window.

  You can perform operations based upon the filtered alarms, the selected alarms, or all the alarms in the category. For example, to see all the `Critical` alarms, pick the `All Alarms` category. From the `All Alarms Browser` window pick `View:Set Filter`, then ensure that only `Critical` severity is selected and click `[Apply]` or `[OK]`. The filter modifies the list of alarms currently displayed in the Alarm

Browser window. You now see all the critical alarms. After resolving all these alarms, delete them using `Actions:Delete->Filtered Alarms`. The category light in the `Alarm Category` window changes from red to the next most severe color.

You can save and restore the filters you have set by using the `[Save]` and `[Restore]` buttons in the `Set Filters` dialog box (not available in the web-based Alarm Browser).

- *Java-based web interface:*
  If filtering is on, the status message at the bottom of the Alarm Browser window indicates that filtering is applied.

  You can perform operations based upon the filtered alarms and the selected alarms. For example, to see all the `Critical` alarms, pick the `All Alarms` category. From the `All Alarms Browser` window pick `View:Set Filter`, then ensure that only `Critical` severity is selected and click `[Apply]` or `[OK]`. The filter modifies the list of alarms currently displayed in the Alarm Browser window. You now see all the critical alarms. After resolving all these alarms, delete them using `Actions:Delete->All in Browser`. The category light in the `Alarm Category` window changes from red to the next most severe color.

  Each Alarm Browser window can use unique alarm filter settings. Select the `View:Set Filters` menu item from any Alarm Browser window to set its filter.

NOTE

Two additional alarm filters are available on a user-by-user basis; they need to be implemented on each management station and each remote console. These filters are not available through NNM's web interface:

- `filterByMap`
  Display only alarms that apply to devices on the current map.
- `filterByMapManaged`
  Display only alarms that apply to managed devices on the current map.

These two filters are invoked through settings in:

- *Windows:* The system registry settings for `xnmevent`
  See the *app-defaults* reference page in NNM's online help.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0127
3740
Doc:

- *UNIX:* `$APP_DEFS/XNmevents` file
  See the comments within this ASCII file.

Deleting Alarms

Alarms remain visible in an Alarm Browser window until someone deletes them or until the specified maximum number of alarms for the browser has been reached. If you do not delete (or acknowledge) alarms, each button in the `Alarm Categories` window will continue to show status color for all alarms, and you may not know when new alarms occur. When an alarm is deleted, it is removed from everyone's alarm list.

You can delete alarms either individually or all at once, using choices under the `Actions:Delete` menu item in each Alarm Browser window. Whenever you delete alarms, a confirmation window pops up.

Once deleted, the same alarm instance does not reappear. You need only delete the alarm in one Alarm Browser window. This clears the alarm from every Alarm Browser window in which it appears.

See "Controlling the Size of the Alarm Browser's State File" on page 344 for information about controlling the maximum number of alarms; the

NOTE

If you want to turn off the confirmation dialog box:

- *Windows:* In the system registry, set `XNevents/warnOnDelete` to false. See the *app-defaults* reference page in NNM's online help.
- *UNIX:* In the `$APP_DEFS/XNevents` file, set `warnOnDelete` to false. See the comments in this ASCII file for more information.

  The confirmation dialog box does not appear over the web-based interface.

TIP

If you plan to delete a large number of alarms and wish to be able to undo the delete, see "Copy or Restore the Alarm Browser's State File" on page 347.

1618

NNM's Map and the Alarm Browser

The map and the Alarm Browser are tightly integrated. When you double-click on an alarm from the Alarm Browser, NNM displays the source node in the submap, zooms to the highlighted object, and displays the panner window. Conversely, from a submap, NNM makes it easy to display all alarm messages related to selected symbols.

Highlighting an Alarm Message and Displaying the Relevant Submap

NOTE Selecting alarm messages in an Alarm Browser window does not affect the current object selections on your map.

To jump directly from an alarm message to the corresponding submap, select the alarm in the Alarm Browser window. Select:

- *Windows or UNIX:* `Actions:Highlight Source on Map` or simply double-click on the alarm message. The submap containing the source of the alarm is displayed. The label for the source object is *highlighted*. Any map symbols that were previously highlighted or previously selected remain so.
- *Java-based web interface:* `Actions:Show Node in Network Presenter`. If accessing a map other than the *default* map, you must type in the correct map name before proceeding. A new instance of the Network presenter is started. Any previously running instance of the Network Presenter is closed. The submap containing the source of the alarm is displayed. Only the symbol for the source object is *selected*.

On the submap, use NNM's menu items to obtain more information to help you resolve the problem that has caused the alarm.

TIP You may receive alarms for nodes that do not appear on the map. For example:

- If an SNMP agent is not in your management region, but is configured to send traps to the NNM management station, the Alarm Browser receives alarms for that agent (for example, when it starts up).

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0128
3740
Doc:



- If you are displaying a map's snapshot, the alarms are for the current map itself, not the snapshot.

Selecting Map Symbols and Displaying Associated Alarm Messages

To access alarm information about objects on the map:

- *Windows or UNIX:* Select the objects on the map and then select `Fault:Alarms`. The `All Alarms Browser` window displays automatically filtering out all alarms except those associated with the selected objects.
- *Java-based web interface:* From any submap, select the `Fault:Alarms` menu item; or select an object on the map, then right-click and select `Alarm Browser`. The `Alarm Category` window is displayed. To view alarms for specific devices, open the All Alarms list and use `View:Set Filters` to limit the alarm list.

Specifying Additional Actions on Alarms

You can select alarms and pipe the alarms into user-written programs (shell commands via standard input), using the menu item `Actions:Additional Actions`. The output of the command will be displayed.

NOTE This feature is not available in the web-based Alarm Browser.

Only one `Additional Actions` dialog box can be displayed at a time. The `Additional Actions` dialog box affects alarms in the browser that is indicated in its title bar. If this dialog box is displayed and the `Actions:Additional Actions` menu item is selected in a different Alarm Browser window, the name in the title bar changes to reflect the alarm category for the most recently selected browser.

Specify the scope of the action. You can select one of five different scopes for the action. These are:

- Selected Alarms
- Filtered Alarms

- Acknowledged Alarms
- Unacknowledged Alarms
- All Alarms in Category

Clicking `[Describe]` when an action is highlighted provides a description of the action, including what command is executed, and how long NNM waits for the command to complete before terminating the command.

See the *trapd.conf* reference page in NNM's online help (or the UNIX manpage) for an explanation about how to write additional action commands. The command is a program that expects input in a predefined format. See "Defining Additional Actions" on page 441, which describes how to define additional actions.

Launching Specific Views or URLs from Alarms

You can configure up to 50 URLs in the `xnmeventsExt.conf` file for the `Actions:Views` menu. These URLs can be one of the NNM views or any other URL that you prefer. NNM views are available from NNM's `Tools` menu.

To configure an alarm to launch a specific URL, edit the following file:

- *UNIX*:`$OV_CONF/$LANG/xnmeventsExt.conf`
- *Windows:* `install_dir\conf\C\xnmeventsExt.conf`

Editing instructions are included in the file.

After you modify xnmeventsExt.conf, do the following for the changes to take effect:

1. Close the NNM Alarm Browser.
2. Stop the `ovalarmsrv` process:
   - *Windows*: Run the `install_dir\bin\ovstop ovalarmsrv` command.
   - *UNIX*: As root, run the `$OV_BIN/ovstop ovalarmsrv` command.
3. Start the `ovalarmsrv` process:
   - Windows: Run the `install_dir\bin\ovstart ovalarmsrv` command.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0129
3740
Doc:

- UNIX: As root, run the `$OV_BIN/ovstart ovalarmsrv` command.

4. Run the `xnmevents` command to restart the NNM Alarm Browser:
   - *Windows*: Run the *`install_dir`*`\bin\xnmevents.exe` command.
   - *UNIX*: Run the `$OV_BIN/xnmevents.exe` command.
5. Restart any web-based Alarm Browsers to view the new menu items.
6. Use the `Fault:Alarms` menu item to open the Alarm Browser. The `Actions:Views` menu in the Alarm Browser should contain the new menu items.

See *Using Network Node Manager Extended Topology* for more information.

Configuring the Alarm Browser

You can configure the Alarm Browser in the following ways:

- Set the maximum size of the event database (default is 16MB).
- Set the maximum number of alarms in the Alarm Browser's state file (default is 3500).
- Set the number of alarms that should be deleted each time the state file reaches maximum capacity.
- Copy or restore the Alarm Browser's state file.
- Control the look and behavior of the Alarm Browser.
- Assign alarm categories:
  - Moving alarms from one category to another.
  - Changing the default alarm category for a specific MIB object.
  - Creating new alarm categories and assigning alarms to the new category.

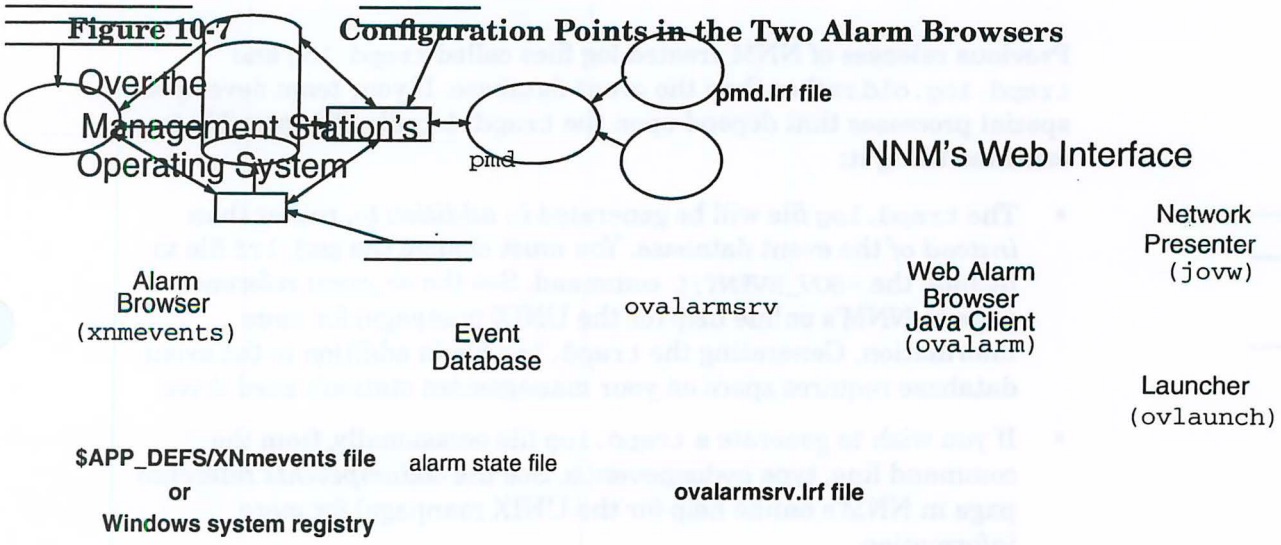


Figure 10-7 Configuration Points in the Two Alarm Browsers

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0130
Doc. 3740

Controlling the Size of the Event Database

All events are entered into the event database. The most important ones are posted to the Alarm Browser. Many NNM services rely upon the information stored in the event database. The default maximum size setting is 16MB. The event database is divided into four files. In the default configuration of 16MB, this means that each file has a maximum size of 4MB. When all four files are full, the oldest log is truncated and new events are written into the reclaimed space.

You can change the amount of disk space that is reserved on the management station for the event database by setting the `b` parameter in the `pmd.lrf` file. See the *ov_event* and *pmd* reference pages in NNM's online help (or the UNIX manpages) for information about changing this setting. Information from the event database can be archived into the data warehouse for trend analysis by selecting the menu item `Tools:Data Warehouse->Export Events`.

NOTE The event database is accessed by all versions of NNM running on your management station: NNM for Windows *or* NNM for UNIX, and NNM on the web.

TIP Previous releases of NNM created log files called `trapd.log` and `trapd.log.old` rather than the event database. If your team developed special processes that depend upon the `trapd.log` file, it is possible to continue using it:

- The `trapd.log` file will be generated *in addition to*, rather than *instead of* the event database. You must change the `pmd.lrf` file to include the `-SOV_EVENT;t` command. See the *ov_event* reference page in NNM's online help (or the UNIX manpage) for more information. Generating the `trapd.log` file in addition to the event database requires space on your management station's hard drive.
- If you wish to generate a `trapd.log` file occasionally, from the command line, type `ovdumpevents`. See the *ovdumpevents* reference page in NNM's online help (or the UNIX manpage) for more information.

Controlling the Size of the Alarm Browser's State File

Events that are configured to post as alarms in the Alarm Browser are sent to the Alarm Browser's state file. The contents of this state file provides the starting point for displayed alarms each time you open the NNM interface. The state file maintains all user edits to the alarm list, such as acknowledgments or deletes.

To modify the number of alarms being stored and displayed, you must change the setting in two places.

- The `-a` parameter in the `ovalarmsrv.lrf` file.
  Changes in the `ovalarmsrv.lrf` file control what is stored in the state file. Remember that this setting affects all users who have access to NNM. Consider RAM and hard drive space on your management station when changing this setting.
- The `maxEvents` setting.
  This parameter is in the UNIX's `$APP_DEFS/XNmevents` file or in the Windows system registry's `xnmevents` entry. It controls how many messages display in the Alarm Browser window itself (independent of the number stored in the underlying state file).

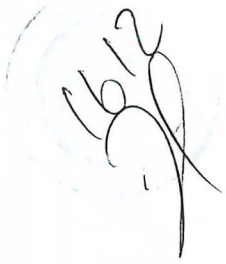
To change the `ovalarmsrv.lrf` file setting that controls the state file:

1. Make your changes to the `-a` parameter and save your changes:
   - *Windows:* `install_dir\lrf\ovalarmsrv.lrf`
   - *UNIX:* `$OV_LRF/ovalarmsrv.lrf`

   See the *lrf* reference page in NNM's online help (or the UNIX manpage) for more information.
2. Update NNM's configuration file. At the command prompt, type:
   `ovaddobj ovalarmsrv.lrf`
3. To force NNM to acknowledge the change, at the command prompt, type:
   `ovstop ovalarmsrv`

TIP This causes the Alarm Browser to close in all currently running NNM sessions.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0131
3740
Doc:



Then at the command prompt, type:
ovstart.

To change the `maxevents` setting that controls the display of messages, on each management station and each remote console (not required for the web-based Alarm Browser):

1. Make your changes to the `maxEvents` parameter and save your changes:
   - *Windows:* The system registry
     `MKEY_LOCAL_MACHINE:SOFTWARE:Hewlett-Packard:OpenView:Network Node Manager:xnmevents:maxEvents`
   - *UNIX:* `$APP_DEFS/XNmevents` file
2. To force NNM to acknowledge your changes, simply close the Alarm Browser; then reopen the Alarm Browser.

See the *ovalarmsrv, app-defaults,* and *xnmevents* reference pages in NNM's online help (or the UNIX *ovalarmsrv* and *xnmevents* manpages) for more information.

TIP Previous releases of NNM used per-user state files (`xnmevents.user`). Do not try to restore these old state files into this version of NNM.

Controlling How Many Alarms to Delete Automatically

Each time the Alarm Browser's state file reaches maximum capacity, the oldest alarms (at the top of the list) are deleted to make room for the new ones.

To control the number of alarms deleted each time, you must change the setting in two places.

- The `-d` parameter in the `ovalarmsrv.lrf` file.
  Remember that this setting affects all users who have access to NNM. Consider the frequency of pause time required to rewrite the state file's alarm list if you change this setting. The higher the number the less frequent the pause.

- The `deleteNumber` setting.
  This parameter is in UNIX's `$APP_DEFS/XNmevents` file or in the Windows system registry's `xnmevents` entry. It controls how many messages are deleted each time the Alarm Browser window itself reaches maximum size (independent of the number stored in the underlying state file).

To change the `ovalarmsrv.lrf` file setting that controls the state file:

1. Make your changes to the `-d` parameter and save your changes:
   - *Windows:* *`install_dir`*`\lrf\ovalarmsrv.lrf`
   - *UNIX:* `$OV_LRF/ovalarmsrv.lrf`

   See the *lrf* reference page in NNM's online help (or the UNIX manpage) for more information.
2. Update NNM's configuration file. At the command prompt, type:

   `ovaddobj ovalarmsrv.lrf`
3. To force NNM to acknowledge the change, at the command prompt, type:

   `ovstop ovalarmsrv`

TIP This causes the Alarm Browser to close in all currently running NNM sessions.

Then at the command prompt, type:

`ovstart`

To change the `deleteNumber` setting that controls how many messages are deleted from the Alarm Browser display window, on each management station and each remote console (not required for the web-based Alarm Browser):

1. Make your changes to the `deleteNumber` parameter and save your changes:
   - *Windows:* In the system registry, add the following parameter and specify the number:
     `MKEY_LOCAL_MACHINE:SOFTWARE:Hewlett-Packard: OpenView:Network Node Manager: xnmevents:deleteNumber`

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0132
3740
Doc:

- *UNIX:* `$APP_DEFS/XNmevents` file

2. To force NNM to acknowledge your changes, simply close the Alarm Browser; then reopen the Alarm Browser.

See the *ovalarmsrv*, *app-defaults*, and *xnmevents* reference pages in NNM's online help (or the UNIX *ovalarmsrv* and *xnmevents* manpages) for more information.

Copy or Restore the Alarm Browser's State File

The state file records all actions that have been applied to specific alarms, such as acknowledging an alarm, deleting an alarm, changing an alarm's category, or changing an alarm's severity rating. Remember that the state file affects all users who access NNM (unlike the filtering or sorting of alarm messages, which is controlled by each individual user).

There may be times when you want to delete a large number of alarms, yet be able to change your mind and undo the deletion. This is possible if you first save the state file.

NNM provides a tool for you to use that makes sure all services (background processes) are in the correct state, then copies or restores the state file for you.

See the *ovalarmadm* reference page in NNM's online help (or the UNIX ut copying and restoring the Alarm Browser's state file.

CAUTION

Do not work directly with the encoded binary state file:

- *Windows:* `install_dir\databases\eventdb\statelog`
- *UNIX:* `$OV_DB/eventdb/statelog`

All changes to this file are made through the Alarm Browser.

Controlling How the Alarm Browser Looks

If there are compelling reasons that you need to change aspects of the Alarm Browser such as the color used to indicate the severity of alarms, Explore the possibilities in:

- *Windows:* The system registry
  See the *app-defaults* reference page in NNM's online help for more information.
- *UNIX:* `$APP_DEFS/XNmevents` file
  See the information included in this ASCII file for more information.

Assigning Alarm Categories

You can control the category into which an alarm message is displayed by:

- Moving an existing alarm message to another category (affecting only that instance of the particular alarm).
- Changing the default category for alarms received from a specific MIB object.
- Creating an entirely new alarm category and assigning alarms to the new category.

Moving an Existing Alarm Message to Another Category

To move an alarm to a different category, in any Alarm Browser window, select the alarms that you want to recategorize. Then select `Actions:Assign Category` from the menu bar. Refer to the online help if you need more information.

This change only affects the selected instances of the alarms. Future alarms of the same type will continue to be posted in the old category's list, unless you reconfigure the alarm as described next.

Changing the Default Category for an Alarm

NOTE You cannot do this through NNM's web interface.

To permanently change the category assignment for a specific alarm message, you must change the configuration settings for the specific underlying event's MIB object. Access the `Event Configuration` dialog box:

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0133
3740
Doc:

- From any Alarm Browser window, select the alarm you wish to reconfigure, and select the `Actions:Configure Event` menu item. The `Event Configuration` dialog box displays the underlying event's current configuration.
- From any submap, select the `Options:Event Configuration` menu item. It is up to you to navigate to the MIB object that defines the event you wish to reconfigure.

Prerequisites are:

- The MIB for which you want to configure events must be loaded into NNM's MIB database. The `Options:Load/Unload MIBs:SNMP` operation lists all MIB modules currently in NNM's MIB database. If the enterprise-specific MIB is not loaded, see "Loading MIBs in the MIB Database" on page 413 for more information.
- Make sure you understand the enterprise-specific MIB. To configure events, you need to understand the trap definitions for the device and what they do. Most device vendors include documentation about their enterprise-specific traps with their product. This documentation typically describes the trap and when the trap is generated. In addition, some vendors include overview information describing strategies for how to manage their specific device. The vendor documentation can give you the conceptual understanding that you need to configure effective event formats and actions.

Refer to "Event Configuration Overview" on page 422 for information about reconfiguring an event to always post its alarm into a specific category of the Alarm Browser.

Creating a New Alarm Category

NOTE You cannot create a new alarm category through NNM's web interface. However, once you establish a new alarm category, it will show up in the web-based Alarm Browser.

You can configure NNM's Alarm Browser to contain custom categories that fit your organization's needs.

For example, you could add a category called `Link Address Alarms`. Once added, you could change all SNMP link address events so that new alarms of this type are posted into the new category.

To add a new category:

1. Access the `Event Configuration` dialog box from either any Alarm Browser window (`Actions:Configure Event`) or from any submap (`Options:Event Configuration`).
2. From the `Event Configuration` menu bar, click `Edit:Alarm Categories`. The `Alarm Categories` window appears.
3. Check NNM's online help that is available within the `Alarm Categories` window for more information.
4. In the `Event Configuration` window, click `File:Save` to save the changes you have made. The new event category appears in the `Alarm Categories` window.

NOTE You must now assign specific SNMP events (associated with specific MIB objects) to this new category; otherwise, it will remain empty. For information about assigning specific events to this category, see "Event Configuration Overview" on page 422.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0134
3740
Doc:

11 Event Reduction Capabilities: Getting to the Root Cause

1605

NNM's Event Reduction Capabilities

Event reduction is the process by which NNM can identify relationships between events. Once identified, a smaller number of new events with the same or higher information content can be generated. This simplifies diagnosing network faults. There are three event reduction strategies within NNM:

- "De-Duplication of Alarms" on page 358

  Multiple, identical alarms are often sent to the NNM Alarm Browser. NNM can retain these alarms, but not display all of them by using *de-duplication* to nest the duplicate alarms beneath the most recent alarm. By reducing the quantity of alarms displayed in the Alarm Browser, you can easily determine the important alarms. You control which events are nested in this manner by making entries in the `dedup.conf` file.

- "ECS Correlations" on page 360

  NNM includes built-in event correlation logic that evaluates incoming events and nests certain related events under a single meaningful alarm. Event correlation helps you quickly identify the primary cause of the problem. For example, you don't need to sift through hundreds of alarms to identify the root cause when a router goes down. High-speed correlation minimizes network bandwidth utilization and improves the quality of customer network services. The fundamental design principle is to correlate events in real-time.

- "Correlation Composer Correlators" on page 386

  NNM provides additional built-in event correlation logic, called correlators, through the Correlation Composer. The Correlation Composer provides a new easier-to-use interface for configuring and creating correlation rules.

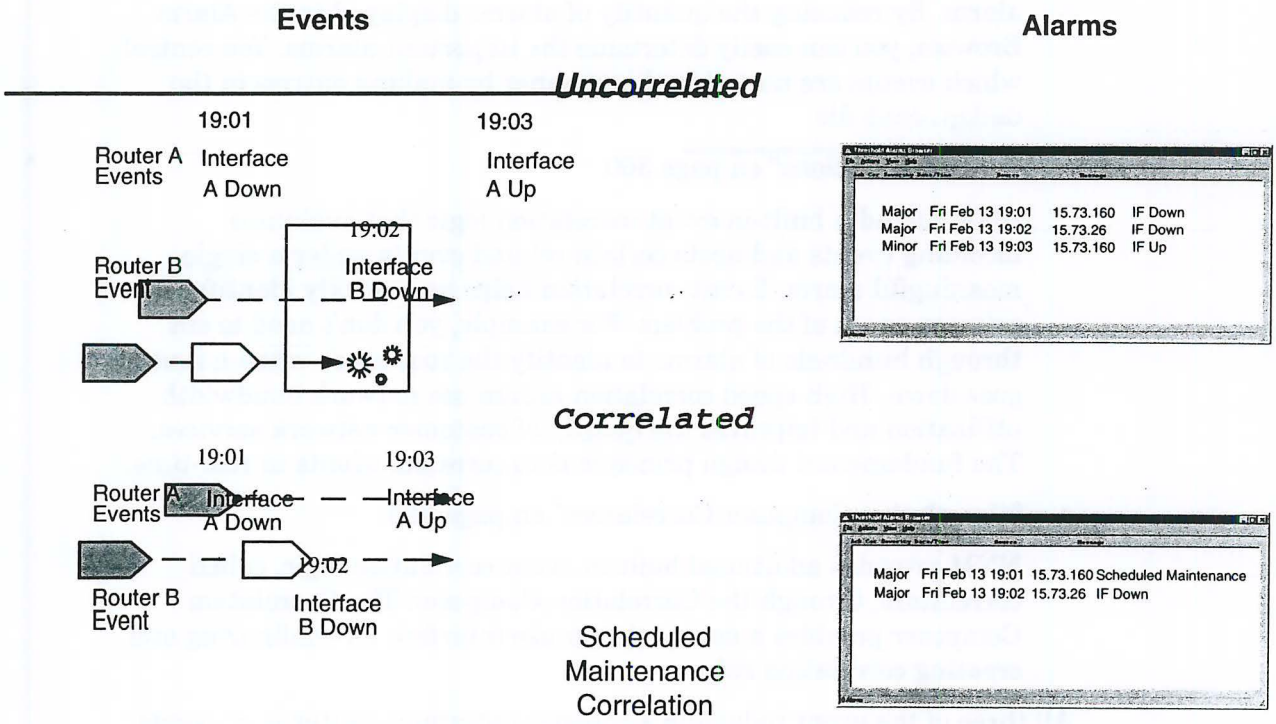
All three of the event reduction strategies determine patterns of events by monitoring the *SNMP MIB Object ID*, the sending *SNMP-agent / IP-address*, and a specific combination of *SNMP variable-binding values*. See "What is an SNMP Variable-Binding and How Do I Identify One?" on page 404 to learn about determining SNMP variable-binding values.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0135
Doc: 3740

Event reduction modifies the flow of events by recognizing patterns of events, then either nesting related events in the Alarm Browser, discarding the events, or replacing the events with fewer more meaningful events. Event reduction strategies can dramatically reduce the number of alarms and improve the value of alarms displayed in your Alarm Browser. Instead of displaying the whole event storm typically generated by equipment and link failures, a correlated event stream displays only the most meaningful alarms, resulting in faster and easier identification of network problems.

For example, one of the correlations included with NNM is called the `ScheduledMaintenance` correlation. Once configured, it suppresses router events generated during routine maintenance.

Figure 11-1 With/Without Scheduled Maintenance Correlation



In Figure 11-1 on page 353, Router A is undergoing planned maintenance (for example, it is being moved to a new rack). The `ScheduledMaintenance` correlation has been configured to post a Scheduled Maintenance alarm notification and suppress all other events

generated by this device during the maintenance period. Because the device has powered down within the maintenance period, the correlation suppresses both events from Router A. However, the Interface Down event from Router (Interface) B is passed through because it is not one of the devices specified for maintenance. The result is two events instead of three, and a higher confidence level that the alarm represents a real problem requiring attention from your team.

This simple correlation eliminates false alarms caused by maintenance activities. Where previously an automated paging facility would have resulted in unnecessary pages, with event correlation it may be feasible to generate meaningful pages.

As illustrated by this example, a single correlation recognizes event patterns caused by a particular fault type. Once you understand how a correlation works, you can modify its parameter values.

A detailed description of each of the supplied correlations and correlators is provided. Before changing any parameter settings, carefully read the description in the configuration window to learn how each correlation and correlator works, its effect, and its deployment requirements.

Correlation Concepts

This section discusses the following concepts:

- "Enabling/Disabling Event Correlations" on page 354.
- "Static and Dynamic Parameters" on page 355.
- "Multiple Correlations and Correlators" on page 355.
- "Event Streams" on page 356.
- "Recommendations" on page 356
- "Event Reduction in Distributed Environments" on page 357.

Enabling/Disabling Event Correlations

When you install NNM, several correlations and correlators are loaded and **enabled**, meaning that they are actively filtering incoming events.

Correlations and correlators can be enabled and disabled at any time through the `ECS Configuration` window and `Correlation Composer` window.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0136
3740
Doc:

- Test the effect of the event reduction strategy to be sure it does what you expect.
- Ensure that all members of your team know which event reduction strategies are in effect.

Event Reduction in Distributed Environments

The NNM correlation engine feeds information for all event reduction features into the ECS default event stream. In a distributed environment this has two main benefits:

- The correlation processing load is distributed over several collection stations.
- Network traffic is reduced.

See *A Guide to Scalability and Distribution* manual for further information about distributed network management concepts.

This point is especially important when you introduce a new correlation or correlator. You must make sure that the new one does not break any existing event reduction configurations: de-duplication, ECS correlations, and Correlation Composer correlators.

Event Streams

A **stream** is a logically separate flow of events. All streams originate from a common source (the postmaster, pmd service). However, each stream can have a different set of correlations applied to it and is directed to a different destination.

NNM listens only to the *default* stream. You may wish to establish separate streams for special network management applications that you add to your OpenView suite. The ECS correlations can be used on the new streams. However, the Correlation Composer correlators only work on the default stream; do not enable them on any other stream.

If you configure NNM's ECS feature with multiple streams, you can choose different combinations of your correlations for each stream. Each correlation can be enabled only once on a selected event stream. However, you can enable the same correlation on several different event streams. *The configuration settings for the correlation remain the same across all streams.* Refer to the *ecsmgr* reference page in NNM's online help (or the UNIX manpage) for more information.

Recommendations

The most detailed source of information about each correlation or correlator is the descriptive information displayed in each correlation's configuration window. Review this information before using the correlation or correlator.

To minimize disruption to the event reduction service, it is suggested that you:

- Plan changes ahead of time where possible.
- Choose a time when network activity is low.
- Do not make ad hoc changes to static parameters.
- Avoid inconsistent states by applying all parameter modifications at the same time, rather than applying each individual parameter change.
- Avoid changing static parameters in the middle of an event storm.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0177

- Test the effect of the event reduction strategy to be sure it does what you expect.
- Ensure that all members of your team know which event reduction strategies are in effect.

Event Reduction in Distributed Environments

The NNM correlation engine feeds information for all event reduction features into the ECS default event stream. In a distributed environment this has two main benefits:

- The correlation processing load is distributed over several collection stations.
- Network traffic is reduced.

See *A Guide to Scalability and Distribution* manual for further information about distributed network management concepts.

De-Duplication of Alarms

NNM de-duplication affects only those alarms listed in the `dedup.conf` file. The *newest* de-duplicated alarm always becomes the parent alarm, visible in the Alarm Browser. Only those alarms that are displayed in the Alarm Browser are monitored by de-duplication. In other words, de-duplication runs on alarms after they have passed through the event correlation system.

NOTE All de-duplication configurations, correlators defined within Correlation Composer, and all correlations defined within ECS must *work well together* on your NNM management station. Before you begin, it is critical that you print out and read the following white paper:

`Developing_NNM_Event_Reduction.pdf`

- *Windows: NNM_install_dir*`\Doc\WhitePapers\`
- *UNIX:* `$OV_DOC/WhitePapers/`

This information explains how to ensure that you do not break existing implementations.

You *might* need to install the white papers on Windows-based NNM management stations. See "White Papers" on page 75.

You can modify the `dedup.conf` file to change the list of affected alarms. For example, if you have multiple, identical alarms that you want to nest under the most recent instance of the alarm, do the following:

1. Open the `dedup.conf` file from the following location:
   - *Windows*: *`install_dir`*`\conf\dedup.conf`.
   - *UNIX*: `$OV_CONF/dedup.conf`.
2. Make the following changes to increase de-duplication:
   - Add the SNMP MIB Object ID of the alarm.
   - Add the event SNMP-agent/IP-address source pair (optional).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0138
Doc: 3740

- Add the specific SNMP variable-binding (optional). See "What is an SNMP Variable-Binding and How Do I Identify One?" on page 404 for more information about SNMP variable-bindings.

See the *dedup.conf* reference page in NNM's online help (or the UNIX manpage) for more information about how to edit the `dedup.conf` file.

NOTE If you need to disable the de-duplication feature, remove the # from the following line of the `dedup.conf` file.

```
#DEDUPLICATION=OFF
```

To deploy any changes you made to the `dedup.conf` file, you must restart the `ovalarmsrv` process. This causes NNM to read the contents of the `dedup.conf` file. To restart the `ovalarmsrv` process, use the following procedure:

1. Stop the `ovalarmsrv` process.
   - *Windows:* As administrator, run `ovstop ovalarmsrv`.
   - *UNIX:* As root, run `ovstop ovlarmsrv`.
2. Start the `ovalarmsrv` process.
   - *Windows:* As administrator, run `ovstart ovalarmsrv`.
   - *UNIX:* As root, run `ovstart ovlarmsrv`.

Once you complete this process, alarms that were already posted to the Alarm Browser before you implemented the de-duplication are not removed. The de-duplication feature nests all new matching alarms as they arrive. The *newest* de-duplicated alarm always becomes the parent alarm, visible in the Alarm Browser.

ECS Correlations

NNM's Built-In Correlations

NNM includes a set of event correlations (the Bundled Edition correlations):

- Connector Down Correlation System (page 361)
  This feature encompasses more than event correlation. NNM's map processes and alarm monitoring processes have been enhanced to help you speed up the task of identifying the source of a problem on your network as it occurs.
- Frame Relay Correlation (page 365)
  This correlation detects and reports specific problems with virtual connections. It distinguishes between failures within the provider network and failures within the local network.
- ManageX Server Down Correlation (page 369)
  When certain ManageX services become unavailable, this correlation combines HP OpenView ManageX events with NNM's topology events, creates new high level ManageX messages, and forwards them to the ManageX message reader. These messages explain why ManageX services are unavailable. Events sent to NNM by ManageX appear in the NNM Alarm Browser. Enable this correlation only if ManageX and NNM will be used together.
- Pair Wise Correlation (page 371)
  This correlation matches a *parent* event to one or more previously occurring *child* events; for example, an Interface Down alarm (OV_IF_Down) followed by an Interface Up alarm (OV_IF_Up) within a designated time frame. You can configure the behavior of alarms passing through this correlation.
- Repeated Event Correlation (page 375)
  This correlation identifies multiple duplicate alarms which are associated with a single physical event and bundles them together under a single alarm.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0139
3740
Doc:

- Scheduled Maintenance Correlation (page 379)
  When conducting planned network maintenance that requires multiple devices to be off-line for a certain amount of time, this correlation allows you to exclude events generated because of the maintenance activity.

Connector Down Correlation

Use of this correlation can prevent event storms when a router (or other connector device) goes down. In the event of a network failure, NNM automatically determines:

- Which device is malfunctioning.
- Which other network devices are impacted by this failure. That is, which functional network devices are now *inaccessible to the management station* over the network because of the failing device. These inaccessible devices are referred to as *secondary failures*.
- Which *inaccessible* network devices are *important* to the productivity of the organization and thus should be given high priority.

Behavior NNM automatically determines the route to a node that is down and checks each connector device along the path to that node to determine the primary malfunction.

Only the alarm about the primary device is logged to the Alarm Browser, making it easy for you to determine the root cause of the problem. To view the error messages regarding devices considered secondary failures:

- From the Alarm Browser, select the correlated alarm's message and select `Actions:Show Correlated Events` or double-click on the correlated column.
- From the web-based Alarm Browser, select the correlated alarm's message and select `Actions:Alarm Details` and select the `Correlations` tab.

NNM slows down polling traffic to all affected devices (i.e. devices considered secondary failures other than the primary malfunction) until the primary device is recovered. The map automatically updates to indicate the primary failure and the affected secondary failures below the primary failure.

You can establish a list of mission-critical devices (Important Node filter) that are never considered secondary failures.

Setting Parameters There are several configuration parameters for the `ConnectorDown` correlation contained within the correlation, itself. However, the `ConnectorDown` correlation is mainly controlled by NNM rather than the Event Correlation Service. It is recommended that you do not modify the correlation itself.

To set parameters for the `ConnectorDown` correlation, from any NNM submap, select `Options:Network Polling Configuration`. (See "Secondary Failure Polling" on page 192 for instructions.)

Make sure that the `Secondary Failures Polling Options` field is enabled because this field determines whether the `ConnectorDown` correlation is being used. The settings in the other fields are up to you (see the following examples for information about the behavior of different choices).

- Important Node Filter
  Designate the name of the filter you created which lists all nodes that are mission-critical and should, therefore, never be placed in secondary-failure status. In the case of a failure resulting in devices contained in the list becoming inaccessible, alarm messages pertaining to these devices would continue to appear in the Alarm Browser window. (See "Router/Switch Health" on page 390 for information about the correlation of alarms from nodes listed in the Important Nodes filter.)

  This filter resides in the same file that contains any discovery filters, DHCP filters, etc.:

  — *Windows:* `install_dir\conf\C\filters`

  — *UNIX:* `$OV_CONF/C/filters`

  See the *OVfilterIntro* reference page (or the UNIX manpage) in NNM's online help for more information about defining filters. See also *A Guide to Scalability and Distribution* for information about creating filters.

- Important Node Behavior
  Designate which status change you prefer to receive for the devices listed in the important-node filter: Down (red on map) or Unknown (blue on map).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0140
3740
Doc:

- Secondary Node Polling Multiplier
  To prevent the generation of unnecessary polling traffic, specify a multiplier by which any scheduled polling should be extended during the failure for devices designated as secondary devices.
- Secondary Node Behavior
  Designate which status change you prefer to receive for devices determined to be secondary failures: Down (red on the map), Unknown (blue on the map), or Unchanged (no change reflected on the map).
- Secondary Failure Alarm Suppression
  Designate whether or not you want to prevent alarm messages about secondary failures from being posted to the Alarm Browser's main categories. If this function is selected, the secondary devices' alarm messages are displayed by selecting the primary alarm message in the Alarm Browser window and selecting the `Actions:Show Correlated Events` menu item.

NOTE See *A Guide to Scalability and Distribution* for information about configuring this feature on collection stations and their corresponding management station.

The following examples illustrate how these settings affect the behavior of NNM.

Example 11-1 Example 1 Default Settings without Using a Filter

```
Important Node Filter File: None
Important Node's Failure Status: Down (irrelevant because no devices are
identified in the filter)
Secondary Node Failure Status: Unknown (blue on the map)
Suppress Alarms for Secondary Failures: True
Secondary Node Polling Multiplier: 2
```

During a network failure:

- The node determined to be the primary cause of the failure appears as a red (critical) symbol on the map, an alarm message is posted in the Alarm Browser, and polling intervals remain constant.
- Since no filter has been specified, no secondary nodes are considered important.

- All secondary-failure nodes are displayed as blue symbols (unknown) on the map. The alarm messages for all secondary devices do not appear in the Alarm Browser list. To view secondary alarm messages, select the corresponding primary alarm and select the `Actions:Show Correlated Events` menu item. Once a node is identified as a secondary failure, its polling intervals are doubled.

Example 11-2 Example 2 Default Settings with a Filter

```
Important Node Filter File: YourFilterName
Important Node's Failure Status: Down (red on the map)
Secondary Node Failure Status: Unknown (blue on the map)
Suppress Alarms for Secondary Failures: True
Secondary Node Polling Multiplier: 2
```

During a network failure:

- The device determined to be the primary cause of the failure appears as a red (critical) symbol on the map, an alarm message is posted in the Alarm Browser, and polling intervals remain constant.
- Any affected device that is specified as an important device in your filter file appears as a red symbol (critical) on the map, polling intervals remain constant, and alarm messages are posted in the Alarm Browser window.
- All secondary-failure interfaces on all nodes are displayed as blue symbols (unknown) on the map. The alarm messages for all secondary devices do not appear in the Alarm Browser list. To view secondary alarm messages, select the corresponding primary alarm and select the `Actions:Show Correlated Events` menu item. Once a node is identified as a secondary failure, it's polling intervals are doubled.

Example 11-3 Example 3 Minimum Network Traffic During Event Correlation

```
Important Node Filter File: YourFilterName
Important Node Behavior: Unknown (blue on the map)
Secondary Node Behavior: Ignore (no change on the map)
Secondary Failure Alarm Suppression: True
Secondary Node Polling Multiplier: 10
```

During a network failure:

- The device determined to be the primary cause of the failure appears as a red (critical) symbols on the map, an alarm message is posted in the Alarm Browser, and polling intervals remain constant.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0141
3740
Doc:

- Any affected device that is specified as an important device in your filter file appears as a blue symbol (unknown) on the map, polling intervals remain constant, and alarm messages are posted in the Alarm Browser window.
- All secondary-failure interfaces on all nodes are ignored, no change is reflected on the map. No alarm messages are generated for secondary devices. Once a node is identified as a secondary failure, its polling intervals are multiplied by 10.

Example 11-4 Example 4 Behavior Like Previous Releases of NNM

To disable the *secondary device* strategy and configure NNM to consider all devices as primary, deselect the `Secondary Failures Polling Options` field to disable the Connector Down correlation. This will have the following effect.

```
Important Node Filter File: None
Important Node Behavior: (irrelevant because no devices identified in the filter)
Secondary Node Behavior: Down (red on the map)
Secondary Failure Alarm Suppression: False (all alarms posted)
Secondary Node Polling Multiplier: 1 (no change)
```

During a network failure:

- The device determined to be the primary cause of the failure appears as a red (critical) symbol on the map, an alarm message is posted in the Alarm Browser, and polling intervals remain constant.
- Since no filter has been specified, no secondary nodes are singled out as important nodes.
- All secondary-failure interfaces on all nodes are displayed as red symbols (critical) on the map. The alarm messages for all secondary devices are sent directly to the Alarm Browser list. No polling intervals are changed.

Frame Relay Correlation

The `FrameRelay` correlation detects and reports problems with frame relay virtual connections. This correlation narrows the troubleshooting area for frame relay problems and reduces the number of events in the Alarm Browser by reporting only one alarm that represents all affected virtual connections.

Behavior

NOTE The `FrameRelay` correlation detects and analyzes `frDLCIStatusChange` traps from devices that support the circuit state changes described in RFC2115.

This correlation begins when a frame relay device generates several `frDLCIStatusChange` traps as shown in Example 11-5 on page 366. Notice that each `frDLCIStatusChange` trap contains an SNMP variable-binding named `state` that is set to `active`, `inactive`, or `invalid`. The `FrameRelay` correlation counts each time a `frDLCIStatusChange` trap's `state` value changes from `invalid/inactive` to `active`.

The `FrameRelay` correlation counts two state transitions for the traps shown in Example 11-5: the first at 10:10:10 and the second at 10:10:30. Two minutes after the first state change, the `FrameRelay` correlation generates an `OV_FrameRelayReset` event. Two minutes is the default `Window` setting and can be modified. See "Setting Parameters" on page 368 for more information.

Example 11-5 The frDLCIStatusChange Trap

```
01/01 10:10:00 frDLCIStatusChange: ifIndex=1, DLCI=401, state=inactive
01/01 10:10:10 frDLCIStatusChange: ifIndex=1, DLCI=401, state=active
01/01 10:10:20 frDLCIStatusChange: ifIndex=1, DLCI=401, state=invalid
01/01 10:10:30 frDLCIStatusChange: ifIndex=1, DLCI=401, state=active
```

The `frDLCIStatusChange` trap indicates a problem with the PVC or the local equipment. NNM further analyzes this trap and reports whether the problem's root cause is located within the local network or the provider network.

To use the `FrameRelay` correlation you must enable SNMP trap forwarding on the frame relay routers and enable the `FrameRelay` correlation as shown in "Setting Parameters" on page 368. The router must support RFC2115.

Below are three examples of how to use the `FrameRelay` correlation to help you diagnose problems.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0142
3740
Doc:

Figure 11-2 The Frame Relay Network

Router A	DSU/CSU A	Frame Relay Cloud	DSU/CSU B	Router B

Example 11-6 NNM Reports a Problem with an Abnormal State Change Frequency

Refer to Figure 11-2 for this example. The following steps illustrate when NNM would generate an `OV_FrameRelayReset` event:

1. Router A generates a large number of `frDLCIStatusChange` traps within a configurable period of time.
2. The `FrameRelay` correlation counts several state transitions after analyzing the `frDLCIStatusChange` traps.
3. NNM generates an `OV_FrameRelayReset` event, indicating that there is a problem with either the frame relay network or the local router serial interface.

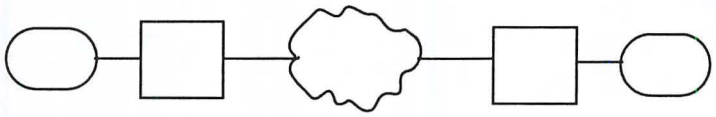
   The `OV_FrameRelayReset` event indicates that a problem exists due to a number of state transitions occurring within a certain time period as reported by Router A.

   You need to do some manual troubleshooting to diagnose this problem.

The `OV_FrameRelayReset` alarm contains an interface index on which the virtual connections are layered. This alarm reports the interface index along with the affected DLCIs and the number of times a reset occurs within the time period. For example, if an `OV_FrameRelayReset` alarm message contains `[(401, 2), (402, 1)]`, this indicates there were two resets for DLCI 401 and one reset for DLCI 402.

Example 11-7 NNM Reports a Problem with a Local Router Interface

Refer to Figure 11-2 on page 367 for this example. The following steps illustrate when NNM would generate an `OV_FrameRelayLocalCircuitProblem` event:



1. Router A generates a large number of `frDLCIStatusChange` traps within a configurable period of time. The status is currently `inactive`, and is toggling between `active` and `inactive`.
2. Either before or after the `frDLCIStatusChange` traps occur, router A sends a `link_Down` trap with the *`ifLocalReason`* variable-binding set to `LMI failed`. That indicates a possible LMI failure on Router A.
3. NNM generates an `OV_FrameRelayLocalCircuitProblem` event, indicating that there is a router serial interface failure on Router A.

   You need to troubleshoot the serial interface on Router A.

Example 11-8 NNM Reports a Problem with the Frame Relay Network

Refer to Figure 11-2 on page 367 for this example. The following steps illustrate when NNM would generate an `OV_FrameRelayCarrierProblem` event:

1. Local Router A generates a large number of `frDLCIStatusChange` traps within a configurable period of time.
2. The `frCircuitState` variable-binding within the `DLCIStatusChange` trap is invalid for the DLCIs generating the `DLCIStatusChange` events.
3. NNM generates an `OV_FrameRelayCarrierProblem` event, indicating that there is a problem with the frame relay network.

   You need to call your service provider.

Setting Parameters Complete the following steps if you want to view more information about or modify the `FrameRelay` correlation.

TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.

FRQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0143
3740
Doc:

3. If you want to enable or disable the `FrameRelay` correlation: from the `ECS Configuration` window, highlight the `FrameRelay` correlation, then select either `Enable` or `Disable`.
4. From the `ECS Configuration` window, highlight the `FrameRelay` correlation and select `Describe` to review the correlation description.
5. From the `ECS Configuration` window, highlight the `FrameRelay` correlation and select `Modify` to bring up the `FrameRelay-Modify` screen.

   The `Window` parameter, used as a time window for counting status transitions from the `frDLCIStatusChange` trap, is the only configurable parameter for the `FrameRelay` correlation.
6. To view the parameter description or modify the configurable parameter, select the parameter, then select `View/Modify`.

NOTE If you modify the `Windows` parameter, set the parameter to a value between two and five minutes. As you set the value higher, the `FrameRelay` correlation consumes more memory resources.

ManageX Server Down Correlation

The `MgXServerDown` correlation analyzes the network health, generates new high level ManageX messages, and delivers these messages to the ManageX message reader. The resulting messages explain why certain ManageX services are unavailable. ManageX messages also appear in the NNM Alarm Browser once this correlation is configured and enabled.

The message information is of value to the ManageX system administrator as it explains what portions of the network are interfering with ManageX operation. This information eliminates the need for the ManageX administrator to contact the network administrator and improves the efficiency of both the network administrator and the system administrator.

Behavior ManageX console events are picked up by the *NNM Lights Out policy* (nnmIntegration.mxc) and converted to an SNMP trap which is sent to NNM. These events route through the ECS `MgXServerDown` correlation for evaluation by NNM.

If NNM discovers that a ManageX device is down, the ECS `MgXServerDown` correlation will determine if the interface-down event is due to a problem on a connector device (router interface, switch, etc.). The result of the analysis is encapsulated in an event that NNM converts into an SNMP trap and sends to the ManageX NNM WMI policy (nnmWmiEventPolicy.mxw) where it is converted into a ManageX console message for display in the ManageX message reader.

Setting Parameters There are numerous configurable parameters contained in the `MgXServerDown` correlation. Complete the following steps if you want to review parameter definitions or modify parameters contained within the `MgXServerDown` correlation.

TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

`Options:Event Configuration`. This launches the `Event Configuration` window.

2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.
3. From the `ECS Configuration` window, highlight the `MgXServerDown` correlation and select `Describe` to review the correlation description.
4. From the `ECS Configuration` window, highlight the `MgXServerDown` correlation and select `Modify` to bring up the `MgXServerDown-Modify` screen.
5. To view parameter descriptions or modify any of the configurable parameters, select the parameter, then select `View/Modify`.

TIP From the `View/Modify` window, select `Help` for general information on making correlation modifications.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0144
3740
Doc:

Pair Wise Correlation

This correlation matches a *parent* event to one or more previously occurring *child* events. You can configure child events to:

- Display in the Alarm Browser while awaiting arrival of a parent event, or
- Only display in the Alarm Browser if the specified time window is exceeded without the arrival of a matching parent event,
- Upon arrival of a parent event, be removed from the Alarm Browser and nested beneath the parent event, or set to Acknowledged.

For example, consider several repeated OV_IF_Down events followed by an OV_IF_Up event within a designated time frame. This correlation could be configured to either remove or acknowledge the OV_IF_Down events upon arrival of the OV_IF_Up event. The OV_IF_Down events are nested under the OV_IF_Up alarm message in the Alarm Browser.

You can add SNMP traps and events to the `PairWise` correlation, provided that you know how the source that is sending the trap is identified. The SNMP MIB Object ID (OID) works in combination with one of the following to specify the source. The combination being used is determined by the developer of the underlying MIB. You must know the appropriate combination in order to configure additional events into this correlation:

- `agent-addr` attribute
- Any source wildcard (your choice)
- SNMP variable-binding name
- SNMP variable-binding position

Behavior You control the behavior of this correlation. The following three examples explain some of your choices. Remember that in order for an event to be displayed within the Alarm Browser, the event's configuration must *not* be set to:

- Don't log or display
- Log only

See "Event Configuration Overview" on page 422 for information about setting an event's configuration.

Example 11-9 **Don't Display the Child Events or the Parent Event**

```
ChildEventImmediateOutput = False
InhibitParentOfInhibitedChild = True
```

The correlation monitors the defined event parent/child relationships in the background. You never see the parent or any child events in the Alarm Browser unless the time of the defined window period is exceeded and no parent event arrives. If no parent is received, the child events are displayed in the Alarm Browser.

Example 11-10 **Display the Parent Event, Nest Child Events Beneath Parent**

```
ChildEventImmediateOutput = False
InhibitParentOfInhibitedChild = False
```

The correlation monitors the defined event parent/child relationships in the background. When the parent event is received, the parent event is displayed in the Alarm Browser with the child events nested beneath. If no parent is received within the defined window period, the child events are displayed in the Alarm Browser.

Example 11-11 **Display Both the Parent and Child Events in the Alarm Browser**

```
ChildEventImmediateOutput = True
InhibitParentOfInhibitedChild = ignored (True or False)
```

Child events are displayed in the Alarm Browser upon arrival. The correlation monitors the defined event parent/child relationships, and when the parent event is received, the parent event is displayed in the Alarm Browser with the child events nested beneath. You choose whether the child events are removed from the Alarm Browser list or set to Acknowledged upon arrival of the parent event.

To view nested child alarms:

- From the Alarm Browser, select the parent alarm message and select `Actions:Show Correlated Events` or double-click on the correlated column.
- From the web-based Alarm Browser, select the parent alarm message and select `Actions:Alarm Details` then select the `Correlations` tab. You can also select the parent alarm message, click on the view button and then select the `Correlations` tab.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0145
3740
Doc:

Setting Parameters Complete the following steps if you want to review parameter definitions or modify parameters contained within the `PairWise` correlation.

TIP

There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.
3. From the `ECS Configuration` window, highlight the `PairWise` correlation and select `Describe` to review the correlation description.
4. From the `ECS Configuration` window, highlight the `PairWise` correlation and select `Modify` to bring up the `PairWise-Modify` screen.
5. To view parameter descriptions or modify any of the configurable parameters, select the parameter, then select `View/Modify`.

TIP

From the `View/Modify` window, select `Help` for general information on making correlation modifications.

This correlation allows configuration of the following parameters.

These two tables define which events are being monitored by the correlation and define the parent/child relationships:

- The `InputEventTypeListStringSources` table is used when the event source is a simple string which is not an IP address. This table is used to set event types for input into the correlation and determine the parent and child event sources.

1583

- The `InputEventTypeList` table is used when the event source is an IP address. This table is used to set event types for input into the correlation and determine the parent and child event sources.

The following two parameters control when alarms appear in the Alarm Browser:

- The `ChildEventImmediateOutput` parameter determines whether the `PairWise` correlation outputs child events immediately or if it holds onto child events for further processing and possible cancellation by a parent event.

  `False` = The `PairWise` correlation holds onto child events for the duration of the `PairedTimeWindow`. If the `PairWise` correlation receives a matching parent event from the same source, within the appropriate amount of time, the child event is nested beneath the parent event in the Alarm Browser. If the `PairWise` correlation does not receive a matching parent event within the `PairedTimeWindow`, the child event is displayed in the Alarm Browser.

  `True` = Child events are displayed in the Alarm Browser upon arrival. Child events may be deleted or acknowledged in the Alarm Browser at a later time if a matching parent event arrives.

- The `InhibitParentOfInhibitedChild` parameter determines whether parent events are displayed in the Alarm Browser.

  `ateOutput` is true, the `PairWise` correlation ignores the `InhibitParentOfInhibitedChild` parameter and sends parent events to the Alarms Browser immediately.

  `True` = The correlation monitors the defined event parent/child relationships in the background. You never see either parent or child alarms in the Alarm Browser unless the time of the defined window period is exceeded and no parent event arrives. If no parent is received, the child events are displayed in the Alarm Browser.

  `False` = The parent event is displayed in the Alarm Browser upon arrival, with all child events nested beneath.

The following parameters fine tune the correlation:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0146
3740
Doc:

- The `DeleteOrAcknowledge` parameter determines whether a child event is deleted or acknowledged from the Alarm Browser once it is matched to a parent event (assuming that `ChildEventImmediateOutput = True`).
- The `PairedTimeWindow` is the maximum time that the child event waits for a parent event. However, the `PairWise` correlation has a built in *pattern delete* feature. If a parent event arrives outside of the defined window, the Alarm Browser is scanned for any defined child events from the same source as the parent event.
- The `IgnoreSecondaryFailureEvents` parameter determines whether this correlation monitors events from devices identified as secondary failures. When set to `True`, secondary failures are monitored by the `ConnectorDown` correlation (page 361), and not by the `PairWise` correlation.

Repeated Event Correlation

This correlation allows multiple alarms which are associated with a single physical event to be bundled together and replaced by a single alarm in NNM's Alarm Browser.

For example, the OpenView `OV_PhysAddr_Mismatch` alarm is one of several alarms that are configured and active by default. When the physical address of a device changes, NNM generates multiple events as neighboring systems discover the change and NNM reads this conflicting information. The `RepeatedEvent` correlation suppresses the multiple instances of the physical address change alarms and correlates them into one alarm for any particular node. You specify the time interval; for example, after receipt of the first of many repeated alarms, suppress duplicates for 2 hours. Then generate another alarm and resume suppression of duplicate alarms for two more hours.

You can add other SNMP traps to the `RepeatedEvent` correlation for suppression of duplicate alarms, provided that you know the following information. Event Identifiers (MIB OIDs) work in combination with one of the following to specify how to obtain the source of the incoming trap:

- `agent-addr` attribute
- Any source wildcard (your choice)
- SNMP variable-binding name
- SNMP variable-binding position

The combination being used is determined by the developer of the underlying MIB. You must know the appropriate combination in order to configure additional events into this correlation.

Behavior In NNM's Alarm Browser, all traps with the same key identifier [OID +source specifier] are nested under the first trap received for the specified time period. Only the first alarm in the series is posted into the Alarm Browser's main list. To view the rest of the alarms:

- From the Alarm Browser, select the primary message and select `Actions: Show Correlated Events` or double-click on the correlated column.
- From the web-based Alarm Browser, select the primary message and select `Actions:Alarm Details`, then select the `Correlations` tab. You can also select the primary message, click on the view button and then select the `Correlations` tab.

Setting Parameters Complete the following steps if you want to review parameter definitions or modify parameters contained within the `RepeatedEvent` correlation.

TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit: Event Correlation`. This brings up the `ECS Configuration` window.
3. From the `ECS Configuration` window, highlight the `RepeatedEvent` correlation and select `Describe` to review the correlation description.
4. From the `ECS Configuration` window, highlight the `RepeatedEvent` correlation and select `Modify` to bring up the `RepeatedEvent-Modify` screen.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0147
Fls. Nº
3740
Doc:

5. To view parameter descriptions or modify any of the configurable parameters, select the parameter, then select `View/Modify`.

TIP From the `View/Modify` window, select `Help` for general information on making correlation modifications.

The `RepeatedEvent` correlation contains the following parameters:

- The *`HoldFirstEventTime`* parameter sets an overall maximum time that initial events are held for later correlation with future events.
- The *`MaxHoldFirstEvents`* parameter sets an overall maximum number of first events to hold for later correlation with future events.
- The `InputEventTypeList` is a table that specifies the event types and event source identifiers that are input to this correlation. The following `Generic Trap Strings` and `Input Event OID` descriptions are included as event types in the `InputEventTypeList` table.

  `Generic Trap String`: The following generic trap names are contained within the correlation. Valid generic trap names are:

  coldStart

  warmStart

  linkDown

  linkUp

  authenticationFailure

  egpNeighborLoss

  By default, all of the generic traps are set to false (event not enabled) and are not evaluated by the `RepeatedEvent` correlation.

  `Input Event OID`: The Specific Event Types (Input Event `OID`) specify the trap `OID`. Two Input Event `OID`s are set to true (by default):

  `OV_PhysAddr_Mismatch (1.3.6.1.4.1.11.2.17.1.0.58982401)`

  `OV_Node_Added (.1.3.6.1.4.1.11.2.17.1.0.58785794)`

Enabling a particular row in the `InputEventTypeList-Modify` screen allows the event to be used as an input event into the correlation.

TIP

Make sure that the Event Configuration settings for the trap you are enabling is *not* set to either of the following. If it is, your correlated alarm will never show up in the NNM Alarm Browser:

— Don't log or display

— Log only

See "Event Configuration Overview" on page 422.

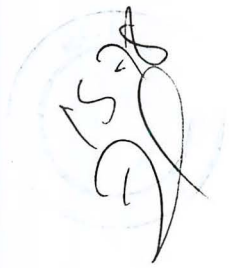
- The `RepeatedTimeWindow` parameter sets an overall maximum time to correlate duplicate events. This value is used for both fixed (`RollingWindow=false`) and rolling (`RollingWindow=true`) time windows.

- The `CreateUpdateEvent` parameter allows you to specify whether or not to delete the original alarm from the Alarm Browser and create a new summary event when the time limit for this correlation is exceeded. If `CreateUpdateEvent` is true, the `RepeatedEvent` correlation creates a new, identical summary event that contains a count of the correlated events. If `CreateUpdateEvent` is false, the original alarm is not deleted from the Alarm Browser and no update event is created.

- Setting the `RollingWindow` parameter to true means that the time window is not fixed to a set time duration. The rolling time window resets each time the correlation receives another duplicate event.

  For example, the `RepeatedTimeWindow` parameter is set to 10 minutes with the `RollingWindow` parameter set to true. An event reports a conflicting MAC layer address. A second identical event arrives (repeats) within 10 minutes of the initial event. The time window for the correlation extends for another 10 minutes and the event is nested beneath the initial event in the Alarm Browser.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0148
Fls. Nº
3740
Doc:



Scheduled Maintenance Correlation

Computer nodes and network segments are occasionally scheduled for maintenance. Such an occurrence typically results in a number of SNMP traps or HP OpenView events being generated. The `ScheduledMaintenance` correlation prevents unnecessary alarms during maintenance.

Behavior When the `ScheduledMaintenance` correlation detects the first event from a specified node or network segment within the specified time range, an event is generated and posted in the NNM Alarm Browser with the message: `Scheduled Maintenance`. The triggering event and all subsequent matching events are nested beneath the Scheduled Maintenance alarm. To view the nested alarms:

- From the Alarm Browser, select the primary message and select `Actions:Show Correlated Events` or double-click on the correlated column.
- From the web-based Alarm Browser, select the primary message and select `Actions:Alarm Details` and select the *Correlations tab.*

Setting Parameters Complete the following steps if you want to configure and enable the `ScheduledMaintenance` Correlation.

TIP

There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the [?] tab. Click Tasks, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.
3. If you want to enable or disable the `ScheduledMaintenance` correlation: from the `ECS Configuration` window, highlight the `ScheduledMaintenance` correlation. Then select either `Enable` or `Disable`.

4. From the `ECS Configuration` window, highlight the `ScheduledMaintenance` correlation and select `Describe` to review the correlation description.
5. From the `ECS Configuration` window, highlight the `ScheduledMaintenance` correlation and select `Modify` to bring up the `ScheduledMaintenance-Modify` screen.
6. To view or modify the affected network devices, or set the name of the planned outage, or activate/deactivate a planned outage: select `MaintenanceList` from the `ScheduledMaintenance-Modify` window and click on `View/Modify`.
7. To view or modify the date, time, and duration of a planned outage: Select `OutageTimeSpecification` from the `ScheduledMaintenance-Modify` window and click on `View/Modify` to make changes. It's important to note that a time window name is specified and configured in the `OutageTimeSpecification-Modify` window. This time window name is then referenced in the `MaintenanceList` definition.
8. To view any other parameter descriptions or modify any of the other configurable parameters, select the parameter, then select `View/Modify`.

TIP From the `View/Modify` window, select `Help` for general information on making correlation modifications.

Command Line Control

You can enable, disable, and control correlations from the `Options:Event Configuration` or `Edit:Event Correlation` menu item. However, if you need to debug a test correlation or enable tracing or logging for support purposes, use the `ecsmgr` command line utility. Possible tasks include:

- Starting or stopping event logging.
- Configuring error logging and trace logging.
- Creating a new stream.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0149
3740
Doc:

See the *ecsmgr* reference page in NNM's online help (or the UNIX manpage) for more information.

Correlation File Structure

Each correlation is comprised of four files. Correlations are stored in the following directory:

- *Windows:* `install_dir\conf\ecs\circuits\*.*`
- *UNIX:* `$OV_CONF/ecs/circuits/*.*`

Do not edit these files directly. Only the `*.ds` file can be altered by using the `Options:Event Configuration`, or `Edit:Event Correlation` menu items.

Table 11-1 Correlation File Structure

correlation`.eco`	Compiled correlation file (not editable).
correlation`.ds`	Data Store file containing externally configurable parameter values (text).
correlation`.fs`	Optional Fact Store file containing topological or other information describing relationships (text).
`C/`*correlation*`.param` or `$LANG/`*correlation*`.param`	Parameter file that describes the parameters configurable by the ECS Event Configuration window (text).

Troubleshooting

Correlation Not Displayed

If the correlation you want is not displayed:

- In the ECS Event Configuration window, click `[Update View]` to refresh the list display. Updates made by other users and updates made from the command line are not reflected in the list of correlations until you click `[Update View]`.
- The correlation may not have been loaded (installed).



Correlation Status Incorrect

If the Status of the correlation appears to be incorrect:

- In the ECS Event Configuration window, select the appropriate stream. Correlations are enabled in the selected stream only and the correlation status reflects the status for the selected stream only. A correlation may be enabled in one stream and disabled in others.
- Click `[Update View]` to refresh the list display.

ECS Event Configuration Window Hangs

If the ECS Event Configuration window appear to hang when you click `[Verify Table]` or `[OK]` after modifying a parameter value:

- Wait until the server responds. Verification is performed on the server and can take some time if the server is very busy.
- Check that the connection with the server has not been severed.

Too Many Alarms Are Showing Up

Did you change the NNM Event Configuration default settings for any events from "log-only" to display in the NNM Alarm Browser? Consider changing some of them back to "log-only" For example, you do not need to display the Link Down events received from your Cisco router because NNM is already monitoring status. The NNM `OV_IF_Down` event is the same as the hardware's Link Down trap.

Expand the configuration of de-duplication to include any repetitive events (see "De-Duplication of Alarms" on page 358).

Obtaining Additional Event Correlations

NNM includes several **Bundled Edition** correlations. No additional license or software is required to use these correlations. HP tests and supports these correlations.

There are three additional sources for correlations that can run in NNM:

- **Contributed Edition** correlations are provided by HP OpenView Partners. Check the HP OpenView web page for links (also check OpenView partners' web sites for access to these correlations). No

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0150
Doc: 3740

additional license or software is required. HP does not test or support the Contributed Edition correlations. They are tested and supported by the partner.

- **Extended Edition** correlations can be obtained from system integrators, such as HP Consulting Service (see "HP Consulting Service" on page 76) and others. They are tested and supported by the supplier.
- **Designer Edition** correlations are written by you. You must purchase and use the HP OpenView ECS Designer product. HP does not test or support the Designer Edition correlations. They must be tested and supported by you.

If you add correlations to NNM, they must be installed and their initial parameter values configured. When a correlation is enabled, its memory tables must fill with events before correlation becomes effective. Like the correlations supplied with NNM, you can then make further modifications to the parameter values while the correlation is enabled.

So You Want To Develop Your Own Correlation?

Developing your own event correlations is a powerful option but a non-trivial task. You should consider carefully whether this is something you want to do or whether it might be quicker, simpler, and cheaper to contract with a specialist to supply the correlation or correlations you need.

If you need only one or two special correlations, then it is probably not worthwhile developing them yourself. Instead, you should consider contracting a specialist to develop them for you. Contact HP Consulting Service (see "HP Consulting Service" on page 76) or other system integrators for assistance.

To develop a correlation you need to:

- Purchase the HP OpenView ECS Designer product, a separately licensed component.
- Learn to develop correlations (ECS Designer training, and/or documentation).
- Design and debug the correlation, data store file, and parameter file.
- If required, develop processes to use the ECS Annotation and/or Event I/O APIs, as described in the *HP OpenView ECS Developer's Guide*.

- Deploy the correlation to each management station and collection station, as described in the documentation that you received when you purchased ECS Designer.

When to Design Your Own Event Correlations There are several key factors which indicate that a new correlation is required, or that an existing correlation needs to be reconstructed:

- No existing correlation provides the correlation you need.
- Parameters of an existing correlation need to be set to values that are outside the minimum and maximum allowed in the ECS Event Configuration window.
- The correlation requires access to external data (for example, to look up an inventory database) and therefore needs to use ECS annotation.
- Special event I/O requirements exist.

What is Involved

NOTE All de-duplication configurations, correlators defined within Correlation Composer, and all correlations defined within ECS must *work well* ement station. Before you begin, it is critical that you print out and read the following white paper:

`Developing_NNM_Event_Reduction.pdf`

- *Windows:* *`NNM_install_dir`*`\Doc\WhitePapers\`
- *UNIX:* `$OV_DOC/WhitePapers/`

This information explains how to ensure that you do not break existing implementations.

You *might* need to install the white papers on Windows-based NNM management stations. See "White Papers" on page 75.

To design an effective correlation, you must:

- Understand typical network event patterns and what they mean.
- Know the architecture of your network management system.
- Identify external data access (ECS Annotation) requirements.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0151
3740
Doc:



- Define the problem concisely in terms of filtering and time-related if-then statements.
- Determine if all data is available from the events themselves. If not determine if:
  - — The external data is subject to change or is relatively stable.
  - — The required data is small enough to store in memory.
  - — The access speed and reliability is sufficient when extracting from your database (particularly if the database is remote).

Then, to develop the correlations, in addition to purchasing the HP OpenView ECS Designer product, you need to:

- Set up a test platform.
- Obtain or develop sample logs of events (perhaps use NNM backup files).
- If Event I/O or Annotation is required, refer to the *HP OpenView ECS Developer's Guide* (provided and obtain an ANSI C/C++ compiler.
- If ASCII events must be correlated, use the ASCII Module of the HP OpenView ECS Designer product.

Correlation Composer Correlators

NNM's Built-In Correlators

NNM includes a set of correlators:

- "Cisco Chassis Failure" on page 387.
  Monitors Cisco traps for three error conditions: temperature, fan failure, and power supply fault. Generates a new alarm if the condition persists for the specified time period.
- "Router/Switch Intermittent Status Changes" on page 393.
  Listens for `OV_IF_Down` alarms from routers and switches, and creates a new alarm when more than *N* interface-down events are received within *M* minutes from a specific interface (defaults N=5, M=30min). Only the new `OV_Intermittent` alarm appears in the NNM Alarm Browser.
- "Router/Switch Health" on page 390.
  (actually a group of three correlators) Correlates Interface status alarms with their related router or switch Node status alarm. `OV_IF_Unknown` and `OV_IF_Down` status alarms from interfaces within routers or switches are suppressed and nested beneath the Node-status alarm.
- "Multiple Reboots on Routers/Switches" on page 388.
  Listens for `coldStart` and `warmStart` traps and creates a new alarm when more than *N* `coldStart`/`warmStart` traps are received within *M* minutes from a specific SNMP-agent/IP-address pair (defaults N=4, M=5min).
- "HSRP Group Health" on page 394.
  (actually a group of 6 correlators on UNIX only) If you purchased the NNM Extended Topology product, this group of six correlators analyzes an HSRP group status change and notifies you of the results by generating an `OV_HSRP_`*x* status alarm, with related alarms nested beneath.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0152
3740
Doc:

Cisco Chassis Failure

Correlates events forwarded from switches supporting the `CISCO-STACK-MIB.my` MIB.

Behavior Certain Cisco and HP routers and switches that support the CISCO-STACK MIB can be configured to send traps that report chassis error conditions to the NNM management station. This correlator monitors the SNMP variable-binding data within the Cisco traps that provides information about the reasons for a failure.

If a *temperature*, *fan failure*, or *power supply* fault condition persists for a period longer than the configured time interval, one of the following events is generated and sent to the NNM Alarm Browser:

- `OV_Chassis_Temperature` (.1.3.6.1.4.1.11.2.17.1.0.58982424)
- `OV_Chassis_FanFailure` (.1.3.6.1.4.1.11.2.17.1.0.58982425)
- `OV_Chassis_PowerSupply` (.1.3.6.1.4.1.11.2.17.1.0.58982426)

Conditions that persist for a time less than the specified Window Period are discarded.

Setting Parameters Complete the following steps if you want to review parameter definitions or modify parameters contained within the `OV_Chassis_Cisco` correlator.

TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.
3. From the `ECS Configuration` window, select the `'default'` stream. Then, highlight `Composer` in the correlation table and select `Modify`. The `Correlation Composer` window appears in your web browser.

1569

4. In the `Correlation Composer` window, right-click the `OV_Chassis_Cisco` correlator and select `Modify` to display the `Description` tab.
5. Carefully read the information in the `Description` tab. Do not change any parameters other than the one specifically listed:
   - Window Period
6. Click the `Definition` tab to access the parameter settings. Click `[Help]` for information about each field.
7. After making the desired changes, close the correlator configuration window and return to the `Correlation Composer` main window.
8. Exit the `Correlation Composer` main window.
9. Save your changes when prompted to do so. This updates the NNM correlator fact store file.

Multiple Reboots on Routers/Switches

The Multiple Reboots correlator detects and reports problems with routers and switches that reboot multiple times within a specified time window.

Behavior The ECS `PairWise` correlation (page 371) suppresses `OV_Node_Down` alarms when the corresponding `OV_Node_Up` alarm arrives. Therefore, you may never see these events in the NNM Alarm Browser. This `OV_MultipleReboots` correlator detects a repetitive down/up situation within routers and switches and generates an `OV_Multiple_Reboots` alarm to warn you of a potential problem.

If a `coldStart` or `warmStart` trap arrives and no such traps have previously been seen for this SNMP-agent/IP-address pair, a new interval is started. If `coldStart` or `warmStart` traps already exist for this system, a counter is updated and checked to see if the number of counts exceeds the configured threshold. If the count exceeds the threshold and the trap is still within the current interval for this system, an `OV_Multiple_Reboot` alarm is posted in the NNM Alarm Browser. All further `coldStart` or `warmStart` traps within the specified time interval are nested under the `OV_Multiple_Reboot` alarm.

Once the interval expires, the sequence begins again.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0153
Doc: 3740

Setting Parameters Complete the following steps if you want to review parameter definitions or modify parameters contained within the `OV_MultipleReboots` correlator.

TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.
3. From the `ECS Configuration` window, select the `'default'` stream. Then, highlight `Composer` in the correlation table and select `Modify`. The `Correlation Composer` window appears in your web browser.
4. In the `Correlation Composer` window, right-click the `OV_MultipleReboots` correlator and select `Modify` to display the `Description` tab.
5. Carefully read the information in the `Description` tab. Do not change any parameters other than those specifically listed:
   - Count
   - Window Period
6. Click the `Definition` tab to access the parameter settings. Click `[Help]` for information about each field.
7. After making the desired changes, close the correlator configuration window and return to the `Correlation Composer` main window.
8. Exit the `Correlation Composer` main window.
9. Save your changes when prompted to do so. This updates the NNM correlator fact store file.

Router/Switch Health

Suppresses interface status alarms from devices other than routers or switches so that these alarms never appear in the NNM Alarm Browser. The assumption is that you do not wish to see end-node interface status alarms.

Displays, in the NNM Alarm Browser, the important interface status alarms from your routers and switches. Suppresses the unimportant interface status alarms from those same routers and switches.

Router/switch health is actually determined by a group of three correlators:

- OV_NodeIf_NodeDown
- OV_NodeIf_NodeNotConnector
- OV_NodeIF_PrimaryIFUnknown

Behavior Suppresses interface status alarms from devices other than routers or switches.

Suppresses interface status alarms from unused (unconnected) ports within routers or switches.

Addresses the following failure scenarios that the ECS `ConnectorDown` correlation (page 361) doesn't detect:

- If fewer than *all* the interfaces on a router or switch fail, the interface status alarms display in your Alarm Browser. Intermediate node status alarms (`OV_Node_Warning`, `OV_Node_Marginal`, or `OV_Node_Major`) are configured as *log-only*, so they never appear in your Alarm Browser.
- If *all* the interfaces on a router or switch fail, `OV_Node_Down` alarm displays in your Alarm Browser with the interface alarms nested underneath.
- If a router or switch failure is a secondary failure (for example a Switch B is inaccessible due to a Switch A failure), then the ECS `ConnectorDown` correlation suppresses all of the events associated with Switch B. The suppressedInterface alarms are nested under the primary Switch A `OV_Node_Down` alarm.

  However, if the Secondary Failure Polling configuration identifies Switch B as an **Important Node** (listed in your Important Node filter, see page 361 and page 192) the Switch B secondary failure

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0154
3740
Doc:

events are not suppressed by the ECS ConnectorDown correlation. In this case, the Switch B OV_Node_Unknown alarm is displayed in the NNM Alarm Browser. The OV_NodeIf group of correlators nest the associated Interface status alarms beneath the parent node alarm. The Switch B OV_Node_Unknown alarm is not nested under the Switch A alarm.

Setting Parameters Complete the following steps if you want to review parameter definitions or modify parameters contained within the OV_IF_NodeDown correlator.

TIP There are several ways to access the event correlation features. For more information, from any submap, select Tools:HP OpenView Launcher. Select the [?] tab. Click Tasks, Event Correlation Management. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select Options:Event Configuration. This launches the Event Configuration window.
2. From NNM's Event Configuration window, select Edit:Event Correlation. This brings up the ECS Configuration window.
3. From the ECS Configuration window, select the 'default' stream. Then, highlight Composer in the correlation table and select Modify. The Correlation Composer window appears in your web browser.
4. In the Correlation Composer window, right-click the OV_IF_NodeDown correlator and select Modify to display the Description tab.
5. Carefully read the information in the Description tab. Do not change any parameters other than the one specifically listed:
   - Window Period
6. Click the Definition tab to access the parameter settings. Click [Help] for information about each field.
7. After making the desired changes, close the correlator configuration window and return to the Correlation Composer main window.
8. Exit the Correlation Composer main window.

9. Save your changes when prompted to do so. This updates the NNM correlator fact store file.

Disabling the OV_NodeIF Correlator Group In releases prior to NNM 6.31, *node-status-events* were displayed in the Alarm Browser, and *interface-status-events* were configured as log-only so that they never displayed in the Alarm Browser. In this release of NNM, interface status events are usually displayed unless a catastrophic failure is detected (all interfaces within a node are down). If a catastrophic event is detected, the node alarm is displayed with the interface alarms nested beneath.

This procedure explains how to return to the old NNM behavior, if desired:

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. Select `OpenView`.
3. Sort the events using the `View:Sort->Sort by Event Name` command.
4. Edit the `OV_IF_Unknown` and `OV_IF_Down` events and change the `Category` field to `Log only`.
5. Edit the following events and change the `Category` field to `Status Alarms` instead of `Log only`:
   - OV_Network_Major
   - OV_Network_Critical
   - OV_Segment_Major
   - OV_Segment_Critical
   - OV_Node_Warning
   - OV_Node_Marginal
   - OV_Node_Major
   - OV_Remote_Mgr_Up
6. Select `[OK]`.
7. Save your changes using the `File:Save` command.
8. Exit using the `File:Exit` command.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0155
3740
Doc:

Once you have the events reconfigured, complete the following to disable the group of three `OV_NodeIF` correlators:

1. From any NNM submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click:
   - `Tasks`
   - `Event Correlation Management`
   - `Correlation Composer`
   - Read the information in the *Disabling a Correlator* topic.
2. Access the `Correlator Composer` main window and disable the following three correlators. You must disable *all* of them:
   - OV_NodeIf_NodeDown
   - OV_NodeIf_NodeNotConnector
   - OV_NodeIF_PrimaryIFUnknown

Router/Switch Intermittent Status Changes

Identifies routers or switches that are reporting intermittent up/down status.

Behavior If an interface is continuously going down and then coming up, the ECS `PairWise` correlation (page 371) cancels the `OV_IF_Down` event when the `OV_IF_Up` event arrives. Therefore, you would never see these events in the NNM Alarm Browser.

This correlator (`OV_Connector_IntermittentStatus`) detects a repetitive interface down/up situation within a router or switch and generates an `OV_Intermittent` alarm if the `OV_IF_Down` event occurs the specified number of times (Count) during the specified time (Window Period).

Setting Parameters Complete the following steps if you want to review parameter definitions or modify parameters contained within the `OV_Connector_IntermittentStatus` correlator.

1563

TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.
3. From the `ECS Configuration` window, select the `'default'` stream. Then, highlight `Composer` in the correlation table and select `Modify`. The `Correlation Composer` window appears in your web browser.
4. In the `Correlation Composer` window, right-click the `OV_Connector_IntermittentStatus` correlator and select `Modify` to display the `Description` tab.
5. Carefully read the information in the `Description` tab. Do not change any parameters other than those specifically listed:
   - Count
   - Window Period
6. Click the `Definition` tab to access the parameter settings. Click `[Help]` for information about each field.
7. After making the desired changes, close the correlator configuration window and return to the `Correlation Composer` main window.
8. Exit the `Correlation Composer` main window.
9. Save your changes when prompted to do so. This updates the NNM correlator fact store file.

HSRP Group Health

If you purchased the NNM Extended Topology product, six correlators work together to monitor HSRP group status within your networking environment. These six HSRP correlators are only provided with NNM management stations installed on a UNIX operating system. All six are required to calculate HSRP group health:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0156
Fls. Nº
3740
Doc:

- OV_HSRP_StatusChange
- OV_HSRP_If
- OV_HSRP_NewNNMEtTopo
- OV_HSRP_ProcessIfEvent
- OV_HSRP_ProcessTrap
- OV_HSRP_Trap_DrillDown

Behavior The following sequence is followed:

1. Listens for any *interface-status-change* alarms from an interface that is assigned to an HSRP group. If detected, initiates an `OV_Force_If_Group_Status_Polling` event for the identified HSRP group.

   Also, listens for any HSRP *trap*. If detected, initiates an `OV_Force_If_Group_Status_Polling` event for the identified HSRP group.

2. Runs the correlator logic to calculate the health of the HSRP group being monitored by using the results of the `OV_Force_If_Group_Status_Polling`. Posts one of the following alarms in the NNM Alarm Browser reporting the results:

   - `OV_HSRP_Up`
     An HSRP group is completely normal, and providing routing functionality.
   - `OV_HSRP_State_Transition`
     An HSRP group has changed either its active router or standby router or both.
   - `OV_HSRP_Marginal`
     An HSRP group has all interfaces in either Unknown or Normal status only, with at least one in each status.
   - `OV_HSRP_Warning`
     An HSRP group has all interfaces with Unknown status, except for one with Normal status.
   - `OV_HSRP_Unknown`
     An HSRP group has all interfaces in Unknown IP status. Network problems exist between the management station and all the interfaces. This HSRP group is providing routing only if an



interface with an Unknown IP status is actually functioning, but due to other network problems, cannot be reached from the NNM management station.

- `OV_HSRP_Major`
  An HSRP group has one or more interfaces with Critical IP status, and one or more interfaces with Unknown IP status. There are no interfaces with a Normal IP status. This HSRP group is providing routing functionality only if an interface with an Unknown IP status is actually functioning, but due to other network problems, cannot be reached from the NNM management station.

- `OV_HSRP_Down`
  An HSRP group is completely down. No active or standby interfaces in this HSRP group could be identified.

3. Nests all related *interface-status-change* alarms, from members of an HSRP group, under the relevant `OV_HSRP_x` status alarm.

   Also, nests all related HSRP *traps* under the relevant `OV_HSRP_x` status alarm.

4. Restarts the HSRP analysis process if any change is detected within the NNM Extended Topology database during the time that the ated.

Setting Parameters Complete the following steps if you want to review parameter definitions or modify parameters contained within the lator. This is the *only* correlator within the HSRP group of correlators that can be modified.

TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0157
3740
Doc:

3. From the ECS Configuration window, select the 'default' stream. Then, highlight Composer in the correlation table and select Modify. The Correlation Composer window appears in your web browser.
4. In the Correlation Composer window, right-click the OV_HSRP_StatusChange correlator and select Modify to display the Description tab.
5. Carefully read the information in the Description tab. Do not change any parameters other than the one specifically listed:
   - NetmonGroupPollWaitTime (in seconds)
6. Click the Definition tab to access the parameter settings. Click [Help] for information about each field.
7. After making the desired changes, close the correlator configuration window and return to the Correlation Composer main window.
8. Exit the Correlation Composer main window.
9. Save your changes when prompted to do so. This updates the NNM correlator fact store file.

Correlator Fact Store File

The correlators, themselves, are all stored within one file. You should never edit this file directly; only make changes through the Correlator Composer window. The file is automatically included when ovbackup and ovrestore are run (see "Backup/Restore to Protect Your Investment of Time" on page 165). If you are planning to make experimental changes to the correlator parameter settings, you may wish to make a backup of this file before proceeding.

All correlator configurations are stored within one NNM fact store file. No other correlator fact store files are allowed within NNM:

Windows: `\NNM_install_dir\conf\ecs\circuits\Composer.fs`

UNIX: `$OV_CONF/ecs/circuits/Composer.fs`

Troubleshooting

For troubleshooting information about the Correlation Composer, see the following references:

- Access the following pdf format manual from the NNM main window, select `Help:Documentation:`

  — *HP OpenView Correlation Composer's Guide*

- Access the following pdf-format white paper file: `Developing_NNM_Event_Reduction.pdf`

  — *Windows:* `NNM_install_dir\Doc\WhitePapers\`

  — *UNIX:* `$OV_DOC/WhitePapers/`

  This information explains how to ensure that you do not break existing event reduction implementations. It also explains the process required for carefully merging your new correlators into the NNM correlator fact store file.

  You *might* need to install the white papers on Windows-based NNM management stations. See "White Papers" on page 75.

- The `TroubleshootingEventReduction.txt` file explains how to create event logs and play them back into the NNM event correlation system for testing purposes:

  — *Windows:* `NNM_install_dir\contrib\ecs\`

  — *UNIX:* `$OV_CONTRIB/ecs/`

  You *might* need to install the contib files on Windows-based NNM management stations. See "The contrib Directory" on page 74.

Creating Additional Correlators

NOTE All de-duplication configurations, correlators defined within Correlation Composer, and all correlations defined within ECS must *work well together* on your NNM management station. Before you begin, it is critical that you print out and read the following white paper:

`Developing_NNM_Event_Reduction.pdf`

- *Windows:* `NNM_install_dir\Doc\WhitePapers\`
- *UNIX:* `$OV_DOC/WhitePapers/`

This information explains how to ensure that you do not break existing implementations.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0158
Doc: 3740

You *might* need to install the white papers on Windows-based NNM management stations. See "White Papers" on page 75.

Correlation Composer provides templates for the most commonly used correlation logic. These templates make it easy for you to develop your own:

- **Enhanced**
  Used to trigger the creation of one or more new alarms or to augment the information content of an alarm.
- **MultiSource**
  Used to define a relationship between an arbitrary number of alarms, potentially from different sources, that together form a logical set that identifies a problem. The set of alarms must all arrive within a defined time period. Upon completion of the set, the alarms can be discarded, modified, or a new more meaningful alarm can be generated.
- **Rate**
  Used to measure the number of incoming events within a defined time period. When a specified number is received, you can choose to discard the alarms and generate a new more meaningful alarm.
- **Repeated**
  Used to either discard duplicate alarms within a defined time period, or generate a new alarm each time an additional alarm is received so that the current number of alarms received can be specified in the alarm message text.
- **Suppress**
  Used when a specific category of alarms needs to be discarded, so that they never appear in the NNM Alarm Browser.
- **Transient**
  Used to detect a defined number of paired event occurrences within a defined time period, such as node up/node down. The paired events can be discarded, and a new more meaningful alarm can be generated.

NOTE Support for the correlator template named **User Defined** is not included. If you wish to use the Correlation Composer **User Defined** template, contact HP to purchase a Partner Care Extended support contract before beginning.

Correlators can be chained together to accomplish complex tasks (see "Router/Switch Health" on page 390 and "HSRP Group Health" on page 394 for examples of correlator groups).

If you wish to use external calls, contact HP to purchase a Partner Care Extended support contract before beginning.

Print out and read the following reference materials:

- Access the following pdf format manual from the NNM main window, select `Help:Documentation:`
  - — *HP OpenView Correlation Composer's Guide*
- Find the *csmerge* reference page in NNM's online help (or the UNIX manpage) for information about Correlation Composer's tool for merging new correlators (that are developed and tested in an isolated environment) back into the NNM correlator fact store file on your production NNM management station.
- Access the following pdf-format white paper file: `Developing_NNM_Event_Reduction.pdf`
  - — *Windows:* `NNM_install_dir\Doc\WhitePapers\`
  - — *UNIX:* `$OV_DOC/WhitePapers/`

  This information explains how to ensure that you do not break existing event reduction implementations. It also explains the process required for carefully merging your new correlators into the NNM correlator fact store file.
- The `TroubleshootingEventReduction.txt` file explains how to create event logs and play them back into the NNM event correlation system for testing purposes:
  - — *Windows:* `NNM_install_dir\contrib\ecs\`
  - — *UNIX:* `$OV_CONTRIB/ecs/`

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0159
Doc: 3740

Developing your own event correlators is a powerful option, but a non-trivial task. You should consider carefully whether this is something you want to do or whether it might be quicker, simpler, and cheaper to contract with a specialist to supply the correlator or correlators you need. Contact HP Consulting Service (see "HP Consulting Service" on page 76) or other system integrators for assistance.

To develop a correlator you need to:

- Learn to develop correlators through Correlation Composer training and/or documentation.
- Design and debug the correlator on an isolated test machine.
- Deploy the correlator to each NNM management station and collection station, as described in the `Developing_NNM_Event_Reduction.pdf` white paper.

When to Design Your Own Event Correlators

There are several key factors which indicate that a new correlator is required, or that an existing correlator needs to be reconstructed:

- No existing correlator provides the correlation you need.
- Parameters of an existing correlator need to be set to values that are outside the minimum and maximum allowed.
- The correlator requires access to external data (for example, to look up an inventory database) and therefore needs to use ECS annotation.
- Special event I/O requirements exist.

What is Involved

To design an effective correlator, you must:

- Understand typical network event patterns and what they mean.
- Know the architecture of your network management system.
- Identify external data access (ECS Annotation) requirements.
- Define the problem concisely in terms of filtering and time-related if-then statements.
- Determine if all data is available from the event's variable-bindings. If not determine if:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0160
Doc 3740

— The external data is subject to change or is relatively stable.

— The required data is small enough to store in memory.

— The access speed and reliability is sufficient when extracting from your database (particularly if the database is remote).

Then, to develop the correlators, you need to:

- Set up a test platform.
- Develop sample logs of events. See the following file for information about how to create log files of events, and how to feed them into the NNM event correlation system in your test environment:

  — *Windows:*

  NNM_install_dir\contrib\ecs\TroubleshootingEventReduction.txt

  — *UNIX:*

  $OV_CONTRIB/ecs/TroubleshootingEventReduction.txt

- Your NNM support contract includes coverage for the use of the following Correlation Composer templates (provided that you do not invoke calls to APIs, libraries, scripts, or programs that are not included as part of the Correlation Composer product embedded within NNM):

  — Enhanced

  — MultiSource

  — Rate

  — Repeated

  — Suppress

  — Transient

  If you wish to use external calls, contact HP to purchase a Partner Care Extended support contract before beginning.

NOTE

Support for the correlator template named **User Defined** is not included. If you wish to use the Correlation Composer **User Defined** template, contact HP to purchase a Partner Care Extended support contract before beginning.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0161
Doc:

What is an SNMP Variable-Binding and How Do I Identify One?

When an SNMP event or trap is generated, a group of *variables* are included in the data. These variables are defined within the MIB file from which the event or trap originates. These variables are often referred to as *var-binds* because they are bound to a particular instance of the SNMP event or trap. The *SNMP variable-binding list* associated with a particular trap or event can provide a wealth of valuable information for you to use when creating your own event reduction strategies using NNM de-duplication, ECS correlation, or Correlation Composer correlator. This section explains a couple of ways to determine the available SNMP variable-bindings:

- "Look within the MIB File" on page 404.
- "Check the Alarm Message Text in the Alarm Browser" on page 405.

This section also explains the SNMP variable-bindings contained within the NNM *interface-status* and *node-status* alarms on page 405, because they can be very useful when defining event reduction implementations.

Look within the MIB File

The most direct way to determine the available SNMP variable-bindings is to locate the MIB file, open the MIB file with an ASCII editor, and look up the variable list for that particular trap or event. Check the documentation that came with your router or switch to locate the MIBs currently in use. If you do not have a copy of the MIB file, try using the MIB Depot web site. It may be a good resource for obtaining MIBs:

`http://www.mibdepot.com`

Otherwise, contact the vendor who created that particular MIB to obtain a copy.

See also "Exchanging Management Information" on page 27 for more information about MIB files.

Check the Alarm Message Text in the Alarm Browser

The alarm messages that display within the NNM Alarm Browser are controlled by the NNM Event Configuration settings. Usually the alarm message text includes a specified subset of available SNMP variable-binding values, as defined through the NNM `Event Configuration` window.

NOTE

For more information about NNM's Event Configuration feature and the choices for controlling alarm message text, see "Event Configuration Overview" on page 422. The event configuration settings are stored in the `trapd.conf` file.

You can easily modify the alarm message configuration settings. See "Variables and Special Characters Allowed" on page 436 for information about alarm message configuration choices. Some very useful alarm message variables are:

$# = prints out the total number of SNMP variable-bindings defined within the originating MIB of the incoming trap

$* = prints out the value passed with each of the defined SNMP variable-bindings

You can use the alarm message information as a starting point for your event reduction strategy, even if you do not have a copy of the MIB.

Any incoming traps whose MIBs have not been loaded into NNM (see "Loading MIBs in the MIB Database" on page 413) are displayed as generic traps called `EnterpriseDefault` (.1.3.6.1.4.1.*). The alarm message for the "generic" trap is defined as follows:

```
no format in trapd.conf. $# args: $*
```

Special SNMP Variable-Bindings within NNM Interface and Node Status Alarms

The OpenView interface and node status events include a wealth of information transported in SNMP variable-bindings. They are of particular interest when developing new de-duplication configurations, correlations, and correlators.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0162
3740
Doc:

NOTE The first variable in the SNMP variable-binding list is traditionally considered to be var-bind "1" (one). If you are developing a Correlation Composer correlator, the first variable in the SNMP variable-binding list is var-bind "0" (zero).

OpenView Interface Status Variable Bindings

- **Var-Bind 1:** The ID of application sending the event.
- **Var-Bind 2:** The hostname of the node that caused the event.
- **Var-Bind 3:** The HP OpenView object identifier of the node that caused the event.
- **Var-Bind 4:** The database name, if applicable.
- **Var-Bind 5:** A time stamp for when the event occurred.
- **Var-Bind 6:** The HP OpenView object identifier of the interface that caused the event.
- **Var-Bind 7:** The name or label for the interface that caused the event.
- **Var-Bind 8:** The IP address for the interface that caused the event, or "0" if unavailable.
- **Var-Bind 9:** The NNM management station ID.
- **Var-Bind 10:** Event correlation event UUID which identifies the primary failure.
- **Var-Bind 11:** Number of bits in the subnet mask of interface.
- **Var-Bind 12:** Locale neutral description of the interface (typically `ifAlias`). Note that the regular label for the interface is transmitted in var-bind 7 and so the presence of this new variable-binding allows the interface name (for example, lan0) and the interface `ifAlias` to be displayed simultaneously.
- **Var-Bind 13:** Locale neutral comma separated list of capabilities of the interface. For example, `isSwitch,isIPRouter`. Not all capabilities are included that may be available in NNM. The primary purpose of this interface is to identify connector devices within event reduction implementations.

- **Var-Bind 14:** Name of the primary failure host if available.
- **Var-Bind 15:** Name of the primary failure entity if available.
- **Var-Bind 16:** The HP OpenView object identifier of primary failure entity if available.
- **Var-Bind 17:** Locale neutral description of the primary failure entity if available.
- **Var-Bind 18:** Locale neutral comma separated list of capabilities of the primary failure entity if available.

Variable-binding 14 through 18 describe the primary failure. For example, node C may be inaccessible due to a failure on router R. Node R would be the primary failure and node C would be the secondary failure. If node R is a primary failure then variable-binding 12 through 15 will describe node R and all the other variable-binding describe node C. If node C is a primary failure then all the SNMP variable-bindings describe node C. See "Connector Down Correlation" on page 361 and "Secondary Failure Polling" on page 192 for more information about designating primary and secondary failures.

OpenView Node Status Variable Bindings

- **Var-Bind 8:** Locale neutral comma separated list of capabilities of the entity. For example, `isSwitch`, `isIPRouter`.
- **Var-Bind 9:** Name of the primary failure host if available.
- **Var-Bind 10:** Name of the primary failure entity if available.
- **Var-Bind 11:** The HP OpenView object identifier of primary failure entity if available.
- **Var-Bind 12:** Locale neutral description of the primary failure entity if available.
- **Var-Bind 13:** Locale neutral comma separated list of capabilities of the primary failure entity if available.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0163
Doc.
3740

1548

12 Customizing Events: Doing It Your Way

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0164
3740
Doc:

NNM allows you to take control of the event system through the use of several built-in applications. This chapter explains the purpose and use of each of these standard NNM applications:

- *SNMP MIB Browser* (page 412) and *Load/Unload MIBs* (page 413). Allows you to load and explore the functionality of the MIBs of your choosing. Once the MIB is loaded, you can query to determine the remote device's status, configuration, and available resources. You can also *set* MIB object values, provided you configured your network's community names into NNM.
- *DMI Browser* (page 417) and mapping MIFs (page 419). *NNM for the Windows operating system only:* Allows you to explore and access the functionality of a network device's Desktop Management Interface (DMI) service provider to which NNM subscribes. You can query to determine the remote device's status, configuration, and available resources.
- *Event Configuration* (page 422). Allows you to customize events, such as changing standard wording of MIB-generated error messages to more meaningful messages for your organization. You can control which Alarm Browser category the event is assigned to and also configure:
  - Automatic Actions, such as dialing a pager, that execute whenever NNM receives a specific event. An Automatic Action command is tied to a particular event and can be limited to a specified list of IP hostnames and/or IPX addresses.
  - Additional Actions that provide access to batch files or executables that your team uses occasionally. You configure the additional actions to show up in NNM's menu bar. Additional Actions can be applied to any alarm or specified groups of alarms.
- Information gathering applications:
  - *MIB Application Builder* (page 443). Allows you to set up new menu items within NNM that provide access to your choice of useful MIB objects on an as-needed basis.

— *Data Collection & Thresholds* (page 447).
Allows you to configure NNM to gather your choice of SNMP-MIB objects automatically (scheduling specific collections, establishing threshold monitoring of devices, and controlling what shows up in the Alarm Browser as a result).

— *MIB Expressions* (page 460).
You can create MIB expressions (mathematical formulas using MIB objects for analysis) to be used by Data Collection & Thresholds.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0165
3740
Doc:

SNMP MIB Browser

The SNMP MIB Browser is available from any submap under `Tools:SNMP MIB Browser`. The SNMP MIB Browser is useful for:

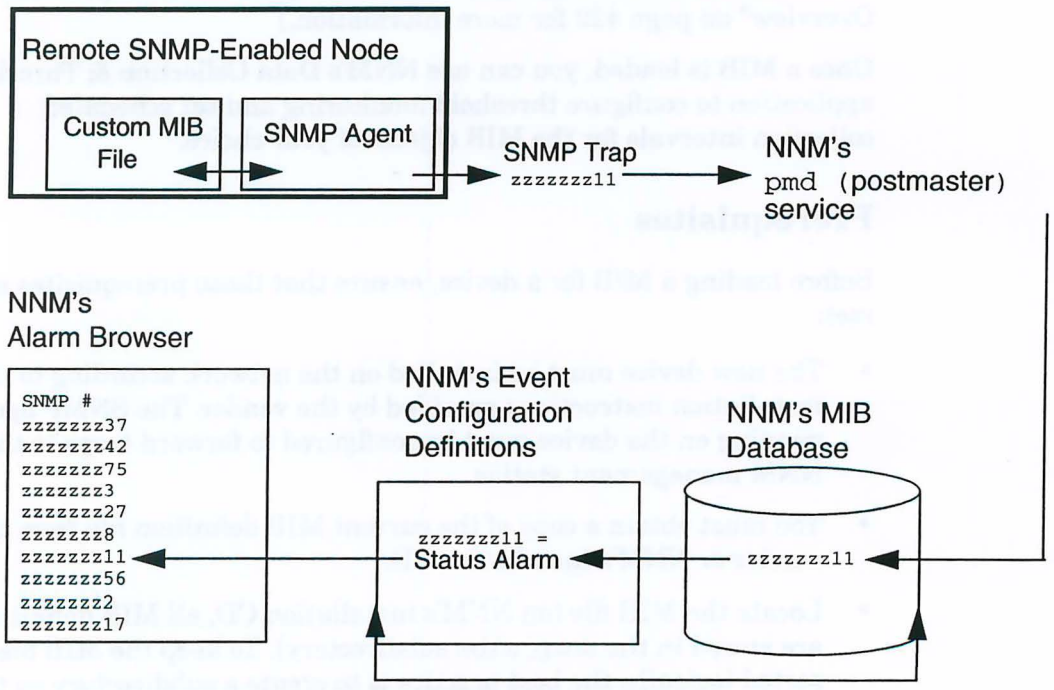
- Exploring your MIBs and their objects to become familiar with the network management capabilities that they provide. It serves as a useful reference tool. Type in any MIB number and view the description of what it is intended to do. Click on any leaf in any loaded MIB tree to view the MIB object's description.
- Querying MIB objects and viewing the returned instances for a network device that you selected on the submap or specified by typing in the IP address. You can view real-time MIB values for a selected node. You can also collect multiple instances by specifying a time interval for queries and display a graph of the results. The node for which you want to view MIB objects must support SNMPv1 or SNMPv2C.
- Setting MIB values on a network device. Prerequisites are:
  - The selected node on which you want to set MIB objects must support SNMPv1 or SNMPv2C.
  - The SNMP agent on the selected node must be configured to respond to SNMP SetRequests.
  - You must know the agent's SET-community name.

For more information about what you can do with NNM's SNMP MIB Browser, see the online help available within the SNMP MIB Browser window.

Loading MIBs in the MIB Database

When you install NNM, the standard SNMP version 1 and 2 MIBs are automatically loaded and configured for your convenience. Often devices on your network have their own custom vendor-specific MIBs that allow for monitoring specific aspects of that vendor's devices, and allow you to customize NNM to proactively manage the devices. If you are running extensible SNMP agents on your devices, the agents may be using custom MIB files. Before you can take advantage of these custom MIB capabilities, the MIB definition loaded into NNM's MIB database must match the version of the MIB in use on the device itself.

Figure 12-1 Configuring Custom MIB File Definitions



RQS nº 03/2005 - CN -
CPMI - CORREIOS
0166
Fls. Nº
3740
Doc:

NOTE To obtain the most recent version of a MIB file, check NNM's installation CD, contact the vendor who wrote the MIB file, or search the WWW (`ftp://ftp.isi.edu/mib/`) for quick access to the MIB file. Make sure the MIB definition loaded into NNM's MIB database matches the version of the MIB in use on the device itself.

The NNM installation CD includes hundreds of vendor-specific MIBs for your convenience. Simply load the MIBs that are relevant and useful for your specific network configuration. When you load a MIB into NNM's MIB database, that MIB's trap definitions are automatically added to the Event Configuration application so that you can customize NNM's use of each one. Use NNM's Event Configuration to identify which traps are forwarded to NNM's Alarm Browser. (See the "Event Configuration Overview" on page 422 for more information.)

Once a MIB is loaded, you can use NNM's Data Collection & Thresholds application to configure threshold monitoring and set scheduled collection intervals for the MIB objects of your choice.

Prerequisites

Before loading a MIB for a device, ensure that these prerequisites are met:

- The new device must be installed on the network according to the installation instructions provided by the vendor. The SNMP agent running on the device must be configured to forward traps to the NNM management station.
- You must obtain a copy of the current MIB definition file from the vendor or NNM's installation CD.
- Locate the MIB file (on NNM's installation CD, all MIB definitions are stored in the `snmp_mibs` subdirectory). To keep the MIB files sorted logically, the best practice is to create a subdirectory on the management station labeled with the vendor's name. Then copy the MIB file to that subdirectory on the management station before loading it. For example:
  - *Windows:* `install_dir\snmp_mibs\vendor\MIB`
  - *UNIX:* `$OV_SNMP_MIBS/vendor/MIB`

- The MIB must conform to *RFC 1155*, *RFC 1212*, *RFC 1902*, *RFC 1903*, or *RFC 1904*.
- If you have unloaded all the MIBs from the management station, it is recommended that you load MIB-II before you load an enterprise-specific MIB.

Procedure Tips

TIP

Close NNM's `Event Configuration` window prior to loading any MIB file. NNM automatically establishes a preliminary event configuration for you of each trap in the new MIB (provided the `Event Configuration` window is closed).

To load a MIB:

1. Place the NNM installation CD into the management station's CD drive. By default, NNM assumes you want a MIB from the installation CD. If the enterprise-specific MIB that you want to load is located elsewhere, you can enter the full path name to the file after opening the `Load/Unload MIB` window (in the field labeled `MIB File to Load`).
2. From any submap, select `Options:Load/Unload MIB:SNMP`. See NNM's online help from within the `Load/Unload MIB:SNMP` window for more information.
3. If the MIB file contains trap definitions, a dialog box appears asking if you would like to establish generic configurations for each trap in NNM's Event Configuration.

You can use the `Tools:SNMP MIB Browser` operation to view the new MIB objects. See "SNMP MIB Browser" on page 412.

If a MIB does not load properly, you will receive an error message. The problem could be:

- A syntax error in the MIB.

  The Load/Unload MIB program's error message identifies the MIB object where the error is occurring.
- Mismatched versions of the vendor's MIB.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0167
Doc: 3740

For example, the vendor's MIB on the NNM installation CD might not match the installed MIB version on the vendor's device on your network. In this case, obtain the MIB version that matches the MIB currently on the device.

In either case, contact the vendor to resolve the problem.

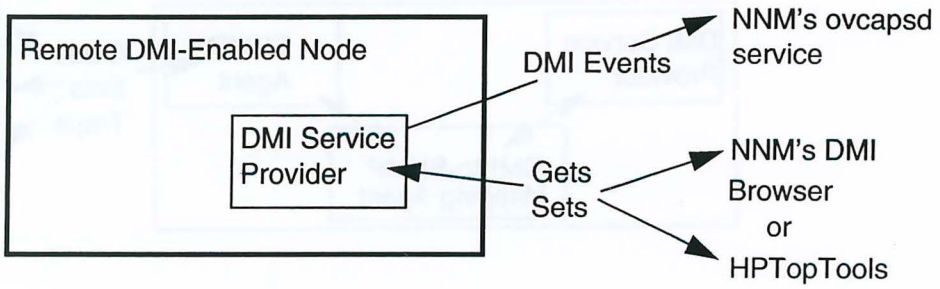
DMI Browser

The DMI Browser is available on NNM management stations running a Windows operating system. From any submap under `Tools:DMI Browser`. The DMI Browser allows you to view real-time MIF values for the DMI-enabled device currently selected on your submap.

Creating DMI Queries

In addition to DMI events, DMI also supplies GET and SET capabilities for some attributes.

Figure 12-2 Queries to a DMI Service Provider



- *DMI version 2:*

  To run DMI queries of devices running any DMI 2.0 service provider, use NNM's DMI Browser application. See the online help from within the DMI Browser for more information.

- *DMI version 1.1:*

  To run DMI queries of devices running the HP-RDMI service provider, use the HPTopTools application provided in the contributor's subdirectory on the NNM installation CD. See the `readme` file in the contributor's directory (see page 74).

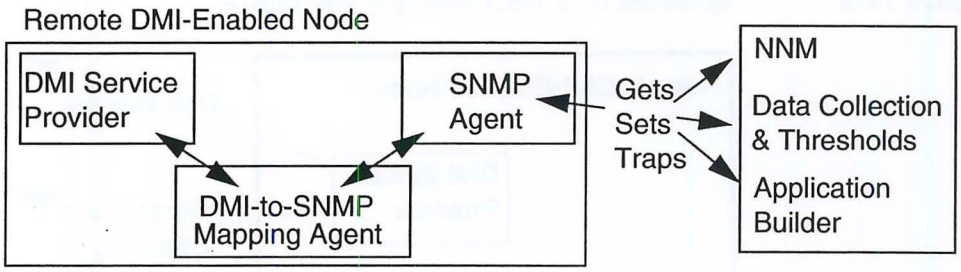
NOTE As an alternative, rather than communicating directly with the DMI service provider on your device, you can communicate with the DMI service provider indirectly through an SNMP agent installed on the

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0168
3740
Doc:

device along with a DMI-to-SNMP mapping agent. (Intel provides a mapping agent in their DMI 2.0 Service Provider Software Development Kit.) See the following figure.

The SNMP agent then handles all communications. Therefore, NNM tools such as the MIB Browser, MIB Application Builder, Data Collection & Thresholds application, and SNMP Grapher can be used to query DMI data via the DMI-to-SNMP mapping agent. NNM no longer subscribes to the DMI service provider to receive DMI events from devices running a DMI-to-SNMP mapping agent.

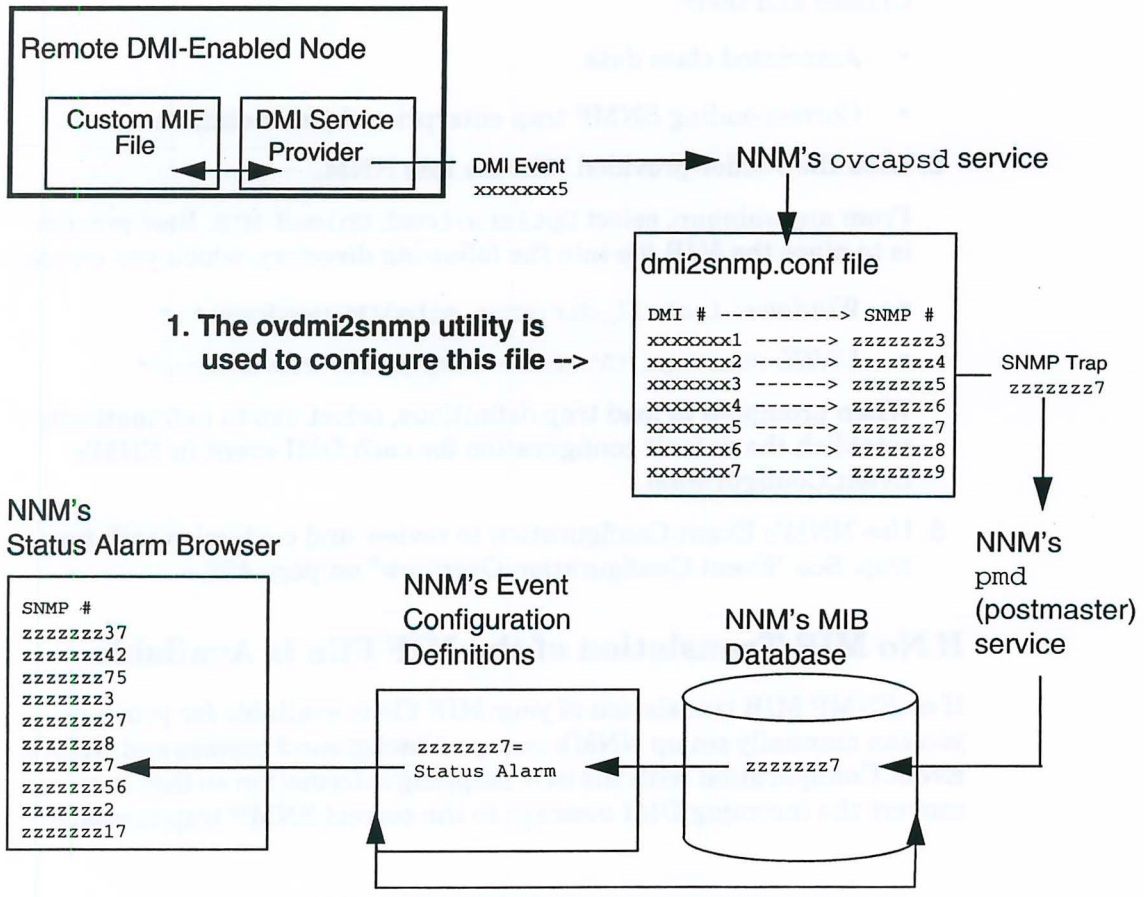
Figure 12-3 Bypassing a DMI Service Provider with an SNMP Agent



Loading DMI-to-SNMP Event Mappings

If your DMI service provider software is using a vendor-specific MIF instead of or in addition to the DMTF's standard MIF, you must configure NNM to understand the custom MIF events. Otherwise, a generic DMI event message (based upon the `dmiEventIndication` definition) is posted to the Alarm Browser each time the vendor-specific DMI event is received. To customize NNM's treatment of these events, you need to complete several steps, as shown in the following figure.

Figure 12-4 Configuring Custom MIF File Definitions



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0169
Doc: 3740

If a MIB Translation of the MIF File Is Available

The vendor of the DMI MIF may provide an SNMP MIB translation for your use. This allows you to load the MIB file and work with the event configurations in the same manner as you work with any SNMP MIB. However, an additional step is required. You must also provide the `ovcapsd` service with the new mapping information so that it can convert the incoming DMI event message to the correct SNMP trap message.

1. Update `ovcapsd`'s mapping file.

   A tool is provided to assist with this task. See the *ovdmi2snmp* reference page in NNM's online help for information about how to do this step. You will need to know each of the MIF's Event Generation Classes and their:

   - Associated class data.
   - Corresponding SNMP trap enterprise object identifier.

2. Load the vendor-provided MIB file into NNM.

   From any submap, select `Options:Load/Unload MIB`. Best practice is to place the MIB file into the following directory, which you create:

   - *Windows:* `install_dir\snmp_mibs\DMIvendors\*.*`
   - *UNIX:* `/var/opt/OV/share/snmp_mibs/DMIvendors/*`

   When prompted to load trap definitions, select `YES` to automatically establish the default configuration for each DMI event in NNM's Event Configuration.

3. Use NNM's Event Configuration to review and customize each new trap. See "Event Configuration Overview" on page 422.

If No MIB Translation of the MIF File Is Available

If no SNMP MIB translation of your MIF file is available for your use, you can manually set up NNM's `ovcapsd` background process and NNM's Event Configuration with the new mapping information so that it can convert the incoming DMI message to the correct SNMP trap message.

TIP MIF-to-MIB translation tools that convert any MIF file to a MIB file are available. Intel provides one in their DMI 2.0 Service Provider Software Development Kit.

1. Update ovcapsd's mapping file.

   A tool is provided to assist with this task. See the *ovdmi2snmp* reference page in NNM's online help for information about how to do this step. You will need to know each of the MIF's Event Generation Classes and their:

   - Associated class data.
   - Unique SNMP trap enterprise object identifier for the DMI Event Generation Class, which you choose.
   - SNMP trap ID, which is equal to the DMI Event ID.

   If your company has a registered "enterprise branch" assigned through the Internet Assigned Numbers Authority (IANA), use one of those available numbers. Otherwise, you may create a new OID that is unique to your installation under the `hpOVUserDefnEvents` branch (`1.3.6.1.4.11.2.17.9.xxxxx`).

2. Use NNM's Event Configuration to create a new trap configuration manually for each DMI event in your MIF file. Be sure to use the same corresponding SNMP trap enterprise object identifier and event/trap ID that you used in step 1 for each event. See "Event Configuration Overview" on page 422.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0170
Doc: 3740

Event Configuration Overview

SNMP events are the building blocks of network management. Alarms are generated when NNM receives certain events. Thoughtful planning and use of event configuration will allow NNM to monitor your network effectively, taking the pressure off of you and your team. The Event Configuration application enables you to control and enhance the way in which NNM handles events. This section describes the following few suggestions among numerous possibilities:

- Control alarm message posting and text.
  - — Control which alarms are posted into NNM's Alarm Browser and which alarms are ignored.
  - — Assign an Alarm Browser category for the event's alarm.
  - — Customize alarm messages to make them more meaningful or to provide specific troubleshooting information to your team.
- Establish automatic actions for NNM to perform whenever a specific event is received (such as dialing a pager).
- Place access to a commonly used batch file command or any executable (such as launching commonly used troubleshooting tools) on NNM menus for your team's convenience.

For more ideas about customizing NNM's event system, review the choices in the `Event Configuration` window and refer to NNM's online help available from within the `Event Configuration` window.

Prerequisites

- The MIB for which you want to configure events must be loaded into NNM's MIB database. From any submap, select `Options:Load/Unload MIBs:SNMP` to display the list of all MIBs currently in NNM's MIB database. If the MIB you wish to use is not loaded, see "Loading MIBs in the MIB Database" on page 413.
  - — A generic configuration for each trap from the MIB is automatically set up in NNM's event configuration feature when you load the MIB.

— MIB objects that are not *traps* can be manually set up in NNM's Event Configuration program. You can then generate GET, SET, or data collection events based upon the new event configuration.

- Make sure that you understand the enterprise-specific MIB. To configure events, you need to understand the trap definitions for the device and what they do. Most device vendors include documentation about their enterprise-specific traps with their product. This documentation typically describes the trap and when the trap is generated. In addition, some vendors include overview information describing strategies for how to manage their specific device. The vendor documentation can give you the conceptual understanding that you need to configure effective event formats and actions.

Event Configuration Window

TIP You cannot configure events from the NNM's web interface. However, the web-based Alarm Browser displays the alarms resulting from your event configurations.

To display the `Event Configuration` window:

- From any Alarm Browser window, select `Actions:Configure Event`.
- From any submap, select `Options:Event Configuration`.

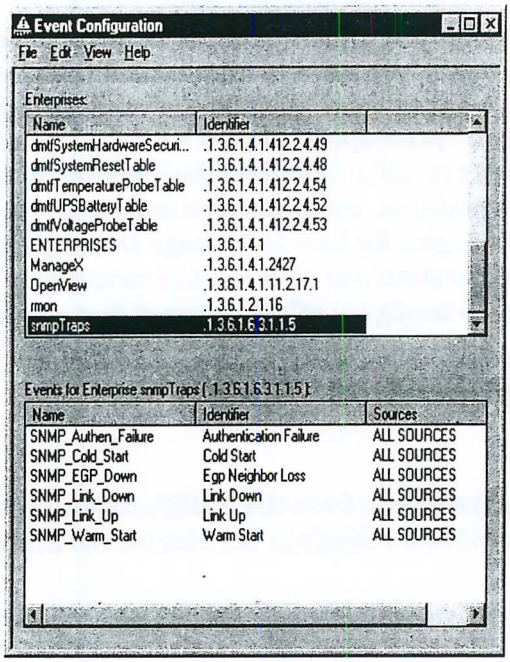
The `Event Configuration` window contains an `Enterprise Identification` section, an `Event Identification` section, and a menu bar.

To close the `Event Configuration` window, select `File:Close`. Be sure to save your changes as you exit. Event configurations are stored in the `trapd.conf` file.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0171
3740
Doc:

Figure 12-5 shows the `Event Configuration` window.

Figure 12-5 Event Configuration Window



Enterprise Identification List

The MIB files that define specific events are supplied by a number of vendors (enterprises). The list in the top half of the `Event Configuration` window identifies the enterprise that supplied the MIB whose event you wish to configure. For example, if you are configuring NNM to communicate with a Cisco Router's SNMP agent, then the event configuration should be defined under the corresponding Cisco enterprise identification (`.1.3.6.1.4.1.9.`).

Events generated by NNM processes (such as `netmon` or `snmpCollect`) will use the HP OpenView enterprise identifier.

NOTE If you are configuring a threshold event created by the HP OpenView SNMP Data Collector, you should configure it under the `OpenView` enterprise name (`.1.3.6.1.4.1.11.2.17.1`), regardless of which node the Data Collector is polling. Even if the event is for a Cisco device

exceeding a threshold, the enterprise ID of the event will be `OpenView`, not Cisco, since the event is coming from the HP OpenView SNMP Data Collector.

Select the enterprise associated with the events you want to configure. Each item in the list contains:

`Enterprise Name`

A convenient and meaningful representation of the Enterprise ID used by the Event Configuration application. This label usually corresponds to the enterprise name as defined by the enterprise-specific MIB.

`Enterprise ID`

The system object ID in dotted notation. The ID corresponds to the value supplied with the trap. If no traps are defined for an enterprise, the application will generate a generic message using the `ENTERPRISES` enterprise. `ENTERPRISES` acts as a default.

You can add or delete enterprises using:

- *Windows:* The `Edit:Events` menu item.
- *UNIX:* The `Edit:Configure` menu item.

Event Identification

The list in the bottom half of the `Event Configuration` window identifies events associated with the enterprise selected in the top half. By default, NNM configures all standard SNMP trap definitions and automatically supplies a generic configuration of all traps present in any MIB that you load into the MIB database. You may configure any event (trap, GET, SET, or custom data collection event). If no enterprise is selected, the list will be blank.

`Event Name`

The name used to reference the event (can be anything meaningful to you).

`Event Identifier`

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0172
Doc: 3740

The event identifiers may be shown as generic and specific traps or as object identifiers, depending on how you have the `View:Event Identifiers` menu set up.

If the menu is set up to display the events as SNMP traps, then the generic traps 0 through 5 are defined by SNMP and assume a specific trap of 0. The generic trap 6 is the enterprise-specific trap. `EnterpriseDefault` provides default trap handling for all traps for an enterprise. The specific traps are defined for this enterprise. The vendor defines what the specific trap numbers mean.

The object identifier for an event is in dotted decimal format. For enterprise-specific events, this identifier is the concatenation of an enterprise object ID, 0, and the specific number (for example, `1.3.6.1.4.1.11.2.17.1.0.58916872`). For SNMP generic traps (0-5), this identifier is the concatenation of the `snmpTraps` enterprise object ID and the generic trap number incremented by one (for example, `1.3.6.1.6.3.1.1.5.5` for the `SNMP_Authen_Failure` generic trap).

The default is to view the events as object identifiers.

`Sources`

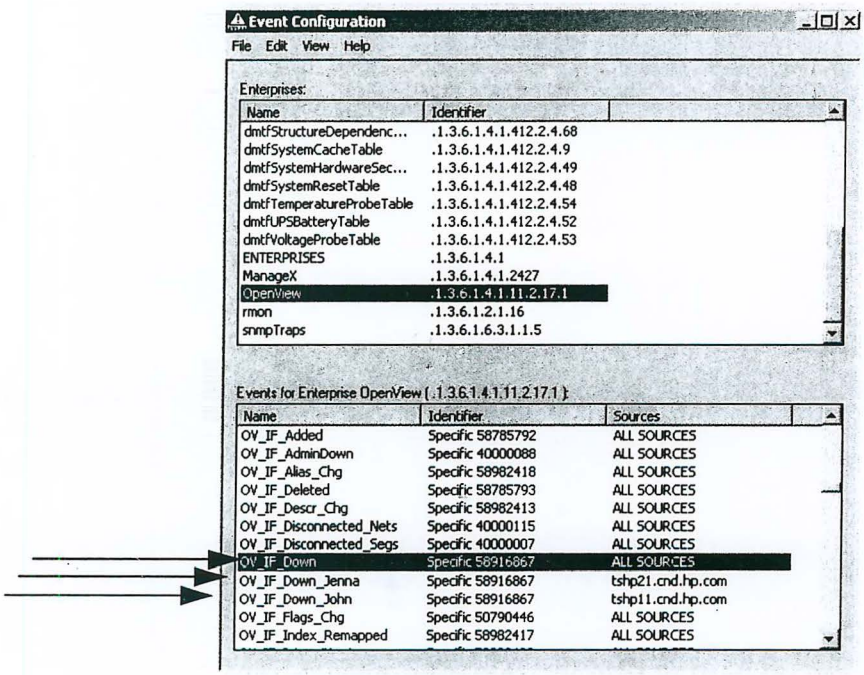
The potential sources for the event (such as nodes), or `ALL SOURCES` if this event is to be used regardless of the source of the event.

NNM allows you to configure events in a number of ways and even add new events. The preconfigured event definitions provide a starting point for your use.

For example, you can use the `OV_IF_Down` MIB object to monitor your most critical routers. For this example, assume that John is in charge of the routers at site A, and Jenna is in charge of the routers at site B. You can copy the preconfigured `OV_IF_Down` and rename it to `OV_IF_Down_John`; change the source field to indicate router interfaces for which John is responsible; then configure NNM to page John whenever a router for which he is responsible goes down. Now repeat the procedure and create another event configuration that you name

OV_IF_Down_Jenna; change the source field to indicate router interfaces for which Jenna is responsible; then configure NNM to page Jenna whenever a router for which she is responsible goes down.

Figure 12-6 Copying Preconfigured Events to Create New Ones



Vendors provide MIB objects that allow you to take this concept a step further and proactively monitor performance on your critical devices. You can configure events to alert you to potential trouble, rather than waiting for a device to fail and send a trap to the management station.

You can add, modify, copy, or delete events using:

- *Windows:* Select the event, then select the `Edit:Events` menu item.
- *UNIX:* Select the event, then use the `Edit` menu.

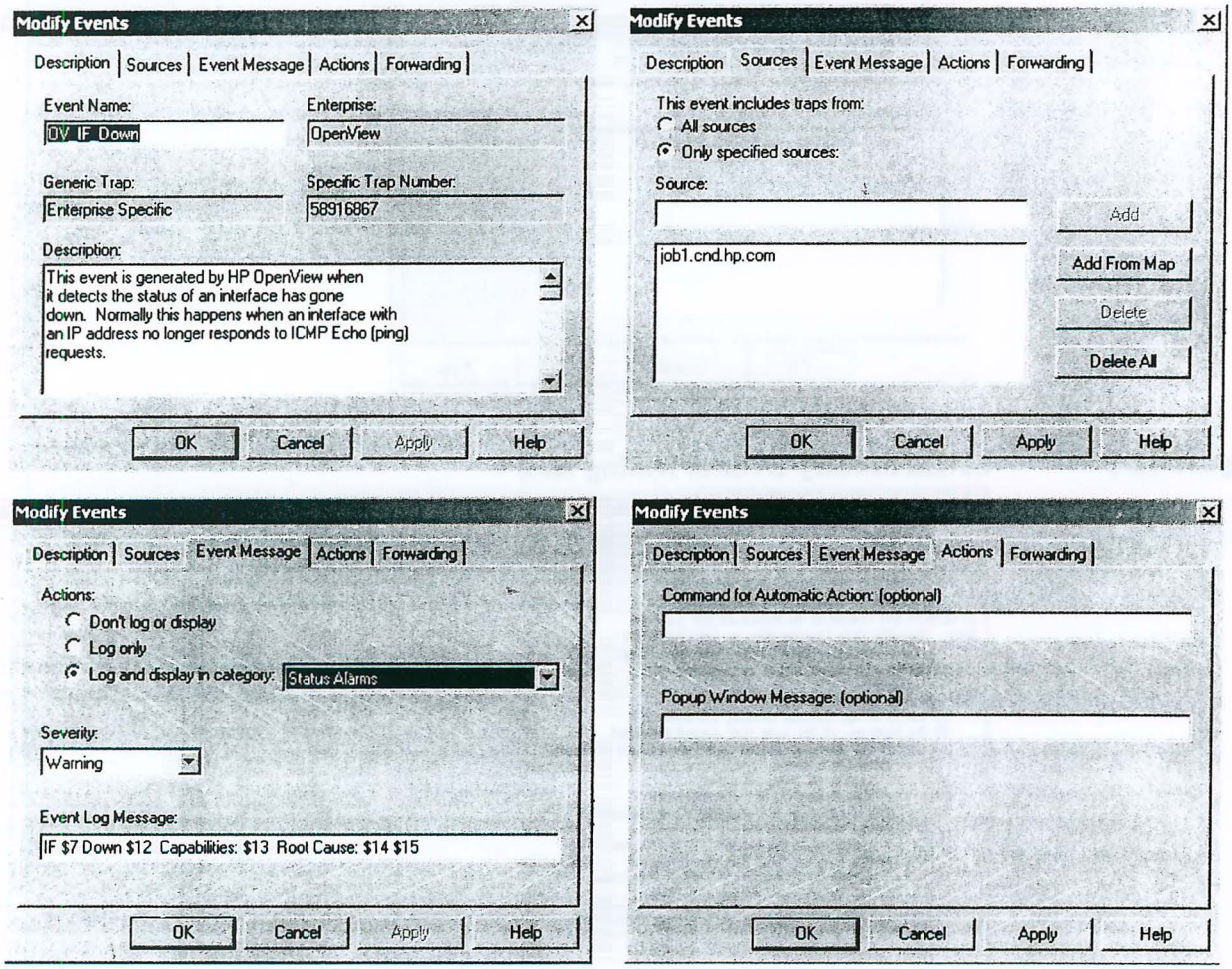
Events can be customized in a wide variety of ways to meet your team's needs. Review the choices in the `Event Configuration` window and refer to NNM's online help available from within this window for more information and ideas.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0173
3740
Doc:

The customizations that you make to event configurations are written to the `trapd.conf` file. Refer to the *trapd.conf* reference page in NNM's online help (or the UNIX manpage) for more information.

This section covers *only a few* of the possibilities for configuring events.

Figure 12-7 Windows: Modify Events Property Sheet (5 tabs)



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0174
3740
Doc:

Figure 12-8 Windows: Modify Events Property Sheet, continued

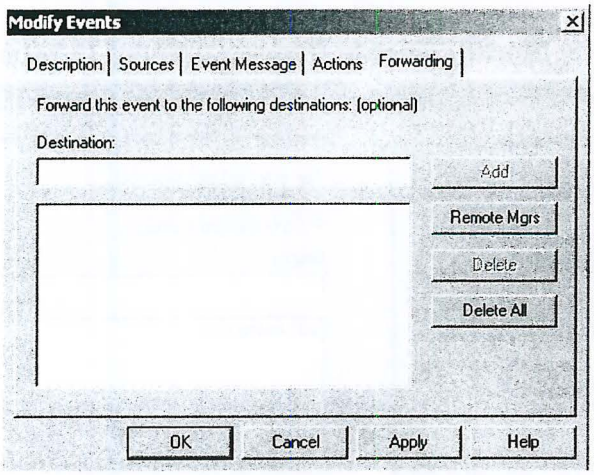
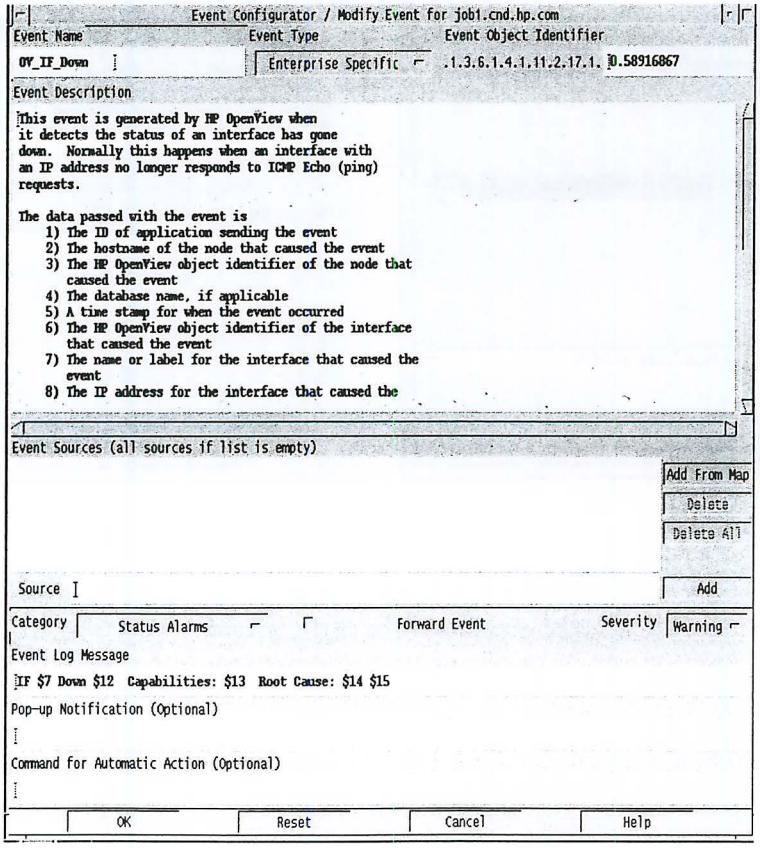


Figure 12-9 UNIX: Modify Events Dialog Box



Controlling Alarm Message Posting and Text

You can control how NNM handles specific alarms, such as:

- Control which alarms are posted into NNM's Alarm Browser and which alarms are ignored.
- Assign an Alarm Browser category for the event's alarm.
- Customize alarm messages to make them more meaningful or to provide specific troubleshooting information to your team.

Selecting Events to Post in the Alarm Browser

1. Ensure that the prerequisites have been met (see "Prerequisites" on page 422). Then, open the `Event Configuration` window:
   - From any Alarm Browser window, select `Actions:Configure Event`.
   - From any submap, select `Options:Event Configuration`.
2. In the top half of the window, select the enterprise that supplied the MIB file that defines the SNMP event that you wish to configure. In the bottom half of the window, select the specific SNMP event:
   - *Windows:* Select `Edit:Events->Modify`, then select the `Event Message` tab.
   - *UNIX:* Select `Edit:Modify Event`.
3. To ensure that NNM posts the alarm in the Alarm Browser, make a selection in the `Category` field. Also make a selection in the `Severity` field to control the severity rating that NNM assigns to this alarm.

TIP See "Creating a New Alarm Category" on page 349 for information about creating your own custom categories.

Changing Event Configurations

1. Ensure that the prerequisites have been met (see "Prerequisites" on page 422). Then open the `Event Configuration` window:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0175
3740
Doc:

- From any Alarm Browser window, select `Actions:Configure Event`.
- From any submap, select `Options:Event Configuration`.

2. In the top half of the window, select the enterprise that supplied the MIB file that defines the SNMP event that you wish to configure. In the bottom half of the window, select the specific SNMP event:
   - *Windows:* Select `Edit:Events->Copy`, then select the `Event Message` tab.
   - *UNIX:* Select `Edit:Copy Event`.
3. Type in a name for the new configuration that is meaningful to you.

TIP Copy the original name and add a meaningful extension so that both events remain together in the event list.

4. Change the source so that your customization only applies to specific host names or IP addresses.
5. To ensure that NNM posts the alarm in the Alarm Browser, make a selection in the `Category` field. Also make a selection in the `Severity` field to control the severity rating that NNM assigns to this alarm.

TIP See "Creating a New Alarm Category" on page 349 for information about creating your own custom categories.

6. To enhance the text of the alarm message so that it is more meaningful to your team, in the `Event Log Message` field, type in the new information. Follow the guidelines in "Variables and Special Characters Allowed" on page 436.

   For more information, see NNM's online help from within the `Event Configuration` window.

The customizations that you make to event configurations are written to the `trapd.conf` file. Refer to the *trapd.conf* reference page in NNM's online help (or the UNIX manpage) for more information.

Example Custom Alarm Message To configure an event to post the following entry in the Alarm Browser:

```
Inconsistent subnet mask 255.0.0.0 on interface lan0,should
be 255.255.248.0
```

The entry in the `Event Log Message` field would be:

```
Inconsistent subnet mask $9 on interface $7,should be $10
```

Defining Automatic Actions for Events

You can define actions for NNM to perform automatically whenever a specific trap (event) is received. Follow the directions in NNM's online help available from within the `Event Configuration` window.

NOTE

By default, NNM only performs commands that are trusted commands. If the command you specify is not in the `trustedCmds.conf` directory, then NNM generates an event and the action is not executed. See the *ovactiond* reference page (or the UNIX manpage) for more information. Trusted commands are listed in the following directory.

- *Windows:* *install_dir*`\conf\trustedCmds.conf`
- *UNIX:* `$OV_CONF/trustedCmds.conf`

1. Ensure that the prerequisites have been met (see "Prerequisites" on page 422). Then open the `Event Configuration` window:
   - From any Alarm Browser window, select `Actions:Configure Event`.
   - From any submap, select `Options:Event Configuration`.
2. In the top half of the window, select the enterprise that supplied the MIB file that establishes the SNMP trap that you wish to configure. In the bottom half of the window, select the specific SNMP trap:
   - *Windows:* Select `Edit:Events->Copy` (or `Modify`), then select the `Additional Actions` tab.
   - *UNIX:* Select `Edit:Copy Event` (or `Modify Event`).
3. Type in a name for the new configuration that is meaningful to you.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0176
3740
Doc:

TIP

Copy the original name and add a meaningful extension so that both events remain together in the event list.

4. Change the source so that your customization only applies to specific host names or IP addresses.
5. To configure NNM to take action automatically whenever this event is received by the Alarm Browser, in the `Command for Automatic Action` field, type in your instructions using "Variables and Special Characters Allowed" on page 436.

   For more information, see NNM's online help from within the Event Configuration windows.

The customizations that you make to event configurations are written to the `trapd.conf` file. Refer to the *trapd.conf* reference page in NNM's online help (or the UNIX manpage) for more information.

Example Commands for Automatic Action

Any program invoked from the Automatic Actions field must run to completion with no user input.

NOTE

By default, the following examples are not in the `trustedCmds.conf` directory. As root or administrator, you must add to the `trustedCmds.conf` directory any commands that you want to execute as automatic actions. You cannot use special characters such as & and | in your automatic action commands. See the *ovactiond* reference page (or the UNIX manpage) for more information. Trusted commands are listed in the following directory.

- *Windows:* *install_dir*`\conf\trustedCmds.conf`
- *UNIX:* `$OV_CONF/trustedCmds.conf`

Example 1: Send a message to a pager You can specify a paging command as an automatic action. Refer to the "Configuration: Recommended Paging Software" section of the NNM Release Notes for specific information about HP's recommended paging software.

The following is general information about scripting an automatic action to launch pager software.

1. Install and test the pager software.
2. Create a batch file that invokes the pager software and place it in the following directory. The program invoked by the batch file must run to completion with no user input:

   Windows: `install_dir\bin`

   UNIX: `$OV_BIN/`
3. Identify the event that should initiate a pager action, as follows: Select `Options:Event Configuration`. The `Event Configuration` dialog box appears. Select `Edit:Events->New` to define a new event for the selected node.
4. In the `Command for Automatic Actions (optional)` field, enter the name of the batch file.

NOTE

Windows only: If you need to use the backslash character (for example in the batch file's path), use "\\" (double backslash).

5. You can generate a test event using `SNMPNOTIFY` on another system to trigger this event and verify that the pager message was successfully sent.

Example 2: Pop-up Window Message This example pops up a message on the management station's monitor.

Specify the following in the `Popup Window Message` field:

```
An authentication failure at IPaddress:$3, community:$4
```

The output will be:

```
Authentication failure at IPaddress:15.2.77.99,
community:admin
```

Example 3: Set an Object's Status Color This example assumes that you have installed the `contrib` files (see "The contrib Directory" on page 74). Type the following command, all on one line, in the `Command for Automatic Action` field. This event status color change will be overwritten by the `ipmap` process if the object is managed by HP

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0177
3740
Doc:

OpenView. It is suggested that a symbol in the object's submap be modified instead. See the *trapd.conf* reference page (or the UNIX manpage) for a discussion of the parameters used in an `snmptrap` command to change the status color of an object on the map.

Windows: If you need to use the backslash character (for example in the batch file's path), use "`\\`" (double backslash). Note the path statement is case-sensitive.

```
\\install_dir\\contrib\\NNM\\setStatus\\setStatus $A Testing
```

UNIX:

```
/usr/OV/contrib/NNM/setStatus/setStatus $A Testing
```

Example 4: Send an Audible Alert This example assumes that you have installed the `contrib` files (see "The contrib Directory" on page 74). Type the following command, all on one line, in the `Command for Automatic Action` field. This event will only be heard if an `xnmevents` process is running. See the *trapd.conf* reference page (or the UNIX manpage) for more information.

Windows: If you need to use the backslash character (for example in the batch file's path), use "`\\`" (double backslash).

```
\\install_dir\\contrib\\NNM\\ringBell\\ringBell $A "User
Alert"
```

UNIX:

```
/usr/OV/contrib/NNM/ringBell/ringBell $A "User Alert"
```

Variables and Special Characters Allowed

When customizing event configuration's `Event Log Message`, Popup Window Message (in UNIX called Pop-up Notification), and `Command for Automatic Action` fields, use special "`$` variables" to present data that was received with the event. You may enter several special characters to give you control of the formatted output. The format can include the following standard C `printf` formats, which will be converted to their ASCII equivalent. (See also NNM's online help available from the `Event Configuration` window for more information.)

Note that nonprintable characters are converted to their `\`*ooo* equivalent for display in the event browser or when passed to the operator-initiated (manual) actions. The two exceptions are that a tab is displayed as `\t` in the event browser and as spaces in pop-up messages. A newline is

displayed as `\n` in the event browser and as a new line in pop-up messages. All nonprintable characters are passed unconverted to automatic actions executed by `ovactiond`.

Special Characters

`\a`	Alert (bell) character
`\b`	Backspace
`\f`	Formfeed
`\n`	Newline
`\r`	Carriage return
`\t`	Horizontal tab
`\v`	Vertical tab
`\\`	Backslash
`\`*ooo*	Octal number, first character must be 0 or 1 and second and third numbers must be 0-7
`\x`*hh*	Hex number, both *hh* characters must be [0-9][a-f][A-F]

You can also include information from the incoming event by using the `$[`*arg*`]` format specification.

Special Information Variables

You can also include information from the incoming event by using the `$[`*arg*`]` format specification. The following `$` variables are valid regardless of the type of event (`SNMPv1`, `SNMPv2C`, `CMIP`, `GENERIC`):

`$[`*arg*`]`

`$x`	Print the date the event was received using the local date representation (*UNIX only:* see the `%x` option in the *strftime* manpage).
`$X`	Print the time the event was received using the local time representation (*UNIX only:* see the `%X` option in *strftime* manpage).
`$@`	Print the time the event was received as a number of seconds since the Epoch (Jan 1, 1970) using the `time_t` representation.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0178
Doc: 3740

`$O`	Print the name (object identifier) of the received event.
`$o`	Print the name (object identifier) of the received event as a string of numbers.
`$V`	Print the event type, based on the transport the event was received. Currently supported types are `SNMPv1`, `SNMPv2C`, `CMIP`, and `GENERIC`.
`$r`	Print the implied source of the event in textual form. This may not be the true source of the event if the true source is proxying for another source, such as when a monitoring application running locally is reporting information about a remote node.
`$ar`	Same as `$r` except print the IP address instead of the name.
`$R`	Print the true source of the event in textual form. This value is inferred via the transport mechanism which delivered the event. If the event was forwarded, this will display the address of the remote event framework (that is, remote `pmd`'s system).
`$aR`	Same as `$R` except print the IP address instead of the name.
`$c`	Print the category in which the event belongs.
`$s`	Print the severity of the event.
`$N`	Print the name (textual alias) of the event format specification used to format the event, as defined in `trapd.conf`.
`$F`	Print the textual name of the remote event framework's system (that is, remote `pmd`'s system) if this event was forwarded; otherwise, print the local system's name.
`$U`	Universally Unique Identifier (UUID) of the current event in the form of a long string of alphanumeric characters.
`$$`	Print the `$` character.

Sequential Attribute Variables

The following $ variables are used to access the sequential attributes that were received with the event. Each event has attributes associated with it (possibly none). They are accessed using the $*n* notation, where *n* is the positional attribute, with 1 being the first possible attribute. The printing format is based on the ASN.1 type of the attribute. These attributes are equivalent to the variable bindings in an SNMP trap.

$[*arg*]

$#
Print the number of attributes in the event.

$*
Print all the attributes as [*seq*] *name* (*type*): *value* strings, where *seq* is the attribute sequence number.

$*n*
Print the *n*th attribute as a *value* string.

$-*n*
Print the *n*th attribute as a *name* (*type*): *value* string.

$+*n*
Print the *n*th attribute as a *name*:*value* string.

$>*n*
Print all attributes greater than *n* as *value* strings; useful for printing a variable number of arguments. $>0 is equivalent to $* without sequence numbers, names, or types.

$>-*n*
Print all attributes greater than *n* as [*seq*] *name* (*type*): *value* strings.

$>+*n*
Print all variables greater than *n* as *name*: *value* strings.

SNMP-Specific Variables for Traps

The following variables are valid only for events created from SNMPv1 or SNMPv2 traps:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0179
3740
Doc:

`$[arg]`	
`$C`	Print the trap community string.
`$E`	Print the trap enterprise as a text string, if possible; otherwise, as in the `$e` arg below.
`$e`	Print the trap enterprise as an object ID string of numbers.
`$A`	Print the trap agent address as defined in the trap protocol data unit (PDU). Note that this may be different from the agent that actually sent the event. If the name server knows about this node, the node name will be printed; otherwise, the IP address will be printed.
`$aA`	Same as $a except print the IP address instead of the name.
`$G`	Print the trap's generic-trap number.
`$S`	Print the trap's specific-trap number.
`$T`	Print the trap's `sysUpTime` time-stamp. This is the remote machine's time in hundredths of a second between the last reinitialization of the device and the generation of the trap; it is *not* the time the event was received.

Obsoleted/Reserved Variables

The following variables are reserved or obsoleted. Their use may cause unpredictable results, and should not be used:

`$[arg]`	
`$L`	Obsolete, do not use.
`$i`	Do not use.
`$I`	Do not use.
`$t`	Do not use.
`$=`	Do not use.

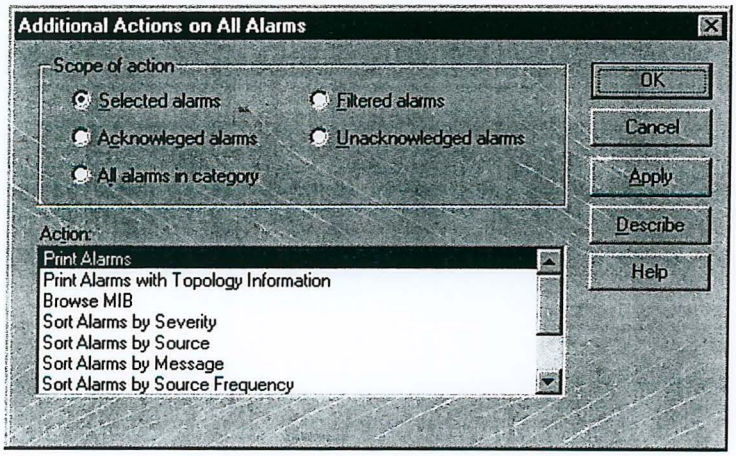
Defining Additional Actions

NOTE This feature is not available through NNM's web interface. It is available on the management station and from remote consoles.

You can configure NNM to provide easy access to batch files or executable files that your team commonly uses. An example might be to forward the event to a trouble ticket system, to send email regarding the event, or to archive the event. You provide the programs for the additional action.

The `Additional Actions` window is accessed from any Alarm Browser window under `Actions:Additional Actions`.

Figure 12-10 Additional Actions



Additional Actions are not the same as *Automatic Actions* for events. The difference between an Additional Action and an Automatic Action is that the Automatic Action automatically runs when the event is received; whereas the Additional Action is run only at the operator's choosing. The Automatic Action is tied to a particular event, whereas an Additional Action can be run on any event.

Although the additional actions list is accessed through any Alarm Browser window, you modify the list of possible additional actions through the `Event Configuration` window.

To display the `Event Configuration` window:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0180
Doc: 3740

- From any Alarm Browser window, select `Actions:Configure Event`.
- From any submap, select `Options:Event Configuration`.

To configure an additional action:

- *Windows:* Select `Edit:Additional Actions`.
- *UNIX:* Select `Edit:Configure->Additional Actions`.

See NNM's online help available within the `Additional Actions` dialog box for more information. For an explanation of how to write an additional action, see the *trapd.conf* reference page in NNM's online help (or the UNIX manpage).

Using the MIB Application Builder

The MIB Application Builder application of Network Node Manager enables you to set up easy access to MIB objects that your team commonly uses. The application that you create displays real-time gathered MIB instances. You select the manner in which the information should be presented: form, table, or graph. You set up access to your application through NNM's map menu structure.

For examples of what is possible, see the standard applications provided in the map menu structure under:

- `Configuration:System Information`

  This example shows real-time instances of six MIB objects in *form* format.

- `Fault:Test IP/TCP/SNMP`

  This example shows real-time instances of four MIB objects in *table* format.

- `Performance:Network Polling Statistics`

  This example shows real-time instances of six MIB objects in *graph* format. You specify the interval between polling instances.

The MIB Application Builder is helpful when you want to monitor specific MIB objects on an as-needed basis. By integrating your MIB application in the menu bar, you have a convenient way to monitor multivendor network devices. For example, you could create multiple MIB applications under NNM's Performance menu that access the vendor-specific MIBs supplied by each router vendor:

```
Performance:Routers->HP
Performance:Routers->Cisco
Performance:Routers->Wellfleet
Performance:Routers->Proteon
```

TIP Use NNM's Data Collection & Thresholds application (see page 447) if you want to automate the collection, rather than use it on an as-needed basis.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0181
3740
Doc:

Prerequisites

- Make sure the enterprise-specific MIB you will use to build your MIB application is loaded in the MIB database on the management station and the same version is on the device itself. (The `Options:Load/Unload MIBs:SNMP` dialog box lists all MIB modules currently loaded in the MIB database.) If the enterprise-specific MIB is not loaded, see "Loading MIBs in the MIB Database" earlier in this chapter.
- Make sure you understand the enterprise-specific MIB. To build useful applications, you need to understand the definitions of the MIB objects and what they do.

  Most device vendors include documentation about their enterprise-specific MIB with their product. This documentation typically describes the MIB objects and what the objects do. In addition, some vendors include overview information describing strategies for managing their specific devices. The vendor documentation can give you the conceptual understanding that you need to build an effective application.

  Note that enterprise-specific MIBs are device-specific. For example, if you build an application for a Cisco router using a Cisco MIB, you probably cannot use that application on a Wellfleet router.

NOTE Familiarize yourself with the MIBs by using the `Tools:SNMP MIB Browser` operation.

- Design your application. Consider the following:
  - — Which objects do you want to include in your application?
  - — Which objects make sense to group?
- Should you graph this information or put it in a table or form? You can choose from one of three presentation styles -- Form, Table, or Graph.
  - — `Form`. Use this option to display MIB information that is not part of a table and does not change very often (for example, system description).

The information associated with each MIB object is displayed one MIB object per line with the MIB value to the right of the MIB label. Any type of MIB object is allowed.

— `Table`. Use this option to display MIB information that constructs a logical table in the MIB (for example, a routing table).

The MIB objects are laid out horizontally, making up the columns of the table. Each entry in the MIB table makes up the rows of the application table. Any type of MIB object is allowed.

NOTE You cannot create table applications which consist of MIB fields from multiple MIB tables.

— `Graph`. Use this option to display numeric MIB information that fluctuates over time (for example, interface statistics). Only numeric MIB values are allowed.

- Plan the menu structure. For example, if you have multiple devices from different vendors, you may want to organize the menu structure such that you have all MIB applications for routers grouped under one menu.

Procedure Tips

Refer to NNM's online help available within the `MIB Application Builder` window for information about how to add, modify, or delete applications.

When you build your applications, keep the following in mind:

- You must provide a unique name for the MIB application.
- You can perform MIB operations on one or more MIB objects at a time.
- Menu path. Decide which NNM menu your application belongs under, such as Performance, Fault, Configuration, or Tools. Use the character sequence -> to separate menu items in the menu path field.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0182
Fls. Nº
3740
Doc:

If the menu path field is blank, the application is created and automatically registered; however, the application will not appear in the menu bar. This is useful for creating applications to be used as the action for an executable symbol.

- You can specify selection rules for your application. Selection rules determine when a menu item is unavailable and when it is available. They are based upon defined capabilities of the nodes for which this application is compatible. If the application is registered in the menu bar, the menu item for this application is only accessible if the capabilities of the selected nodes match those defined in this selection rule; for example, `isSNMPSupported`. See NNM's online help within the `MIB Application Builder` window for more information.
- You can enter help text for your application. For example, you may want to give a general description of the MIB operation and how to interpret the information that is obtained. When you create the MIB operation menu item, the program automatically adds an entry under:
  - *Windows:* `Help:On Application`.
  - *UNIX:* `Help:Misc->Function` and in the dialog box help.

Data Collection & Thresholds

This section describes how to use NNM's Data Collections & Thresholds application to do the following:

- Collect MIB data from network nodes automatically at regularly scheduled intervals.
- Store the collected MIB data in a file.
- Set threshold monitoring on critical devices.

See page 469 for information about viewing the data after it is collected.

TIP You cannot configure Data Collections & Thresholds from NNM's web interface. However, the web-based Alarm Browser displays the alarms resulting from your configurations.

Prerequisites

- The node for which you want to collect data must support SNMP version 1 or version 2c.
- Make sure the correct version of the enterprise-specific MIB that you want to use to collect data is loaded into the MIB database on the management station. (The `Options:Load/Unload MIBs:SNMP` menu item lists all MIB modules currently in the MIB description file.) If the enterprise-specific MIB is not loaded, see "Loading MIBs in the MIB Database" on page 413.
- You can collect data or monitor thresholds on numeric MIB objects; that is, the MIB objects defined as `Counter`, `Gauge`, `INTEGER`, `IpAddress`, `Counter64`, or `TimeTicks`.
- You can collect data on MIB objects with a `String` data type; that is, monitor MIB objects such as `sysContact`.
- To configure your system to collect MIB data, you need to understand the definitions of the MIB objects and what they do.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0183
3740
Doc:

Most device vendors include documentation about their enterprise-specific MIB with their product. This documentation typically describes the MIB object and what the object means. In addition, some vendors include overview information describing strategies for how to manage their specific device. The vendor documentation can give you the conceptual understanding you need to configure your system to collect MIB data.

- Decide if it would be useful to collect the results of a MIB expression (MIB objects combined into a mathematical formula) rather than individual MIB objects. If you want to use a MIB expression, see "Creating and Using MIB Expressions" on page 460 for information about writing and using MIB expressions.
- Identify the nodes on which you will collect data. For example, for a network segment, you may want to collect data on the router, the hubs, and the key file server.
- Identify how often you want to collect data.
- Ensure the management station has enough room to store the data. NNM automatically collects data by default (select `Options: Data Collection and Thresholds` to see the list of current data collections). The amount of disk space required depends upon how much data you collect. For an example, say that you want to collect data for 10 MIB objects on 50 nodes, each with an average of 8 instances of these objects. If you choose a collection interval of half an hour, the collection rate will be 10x50x8x2 = 8000 values/hour. Since each value collected consumes 24 bytes of disk space, the disk consumption rate is 8000x24 = 192,000 bytes/hour.

  Windows: Data is stored in the *`install_dir`*`\databases\snmpCollect` directory.

  UNIX: Data is stored in the `$OV_DB/snmpCollect` directory. If you need more disk space, symbolically link to another file system.

TIP

For HP-UX systems only: You can expand the file system with Logical Volume Manager. Extend the logical volume, then use `extendfs` (hfs) or `fsadm` (vxfs).

Procedure Tips

To access NNM's Data Collection & Thresholds application, from any submap, select `Options:Data Collection & Thresholds:SNMP`. Refer to NNM's online help available from the Data Collection & Thresholds window for directions and additional information.

Select the MIB object or expression to be used for data collection. The `Label` field (circled in the following figure) in the MIB selection window determines the file name where the collected data will be stored. (Make

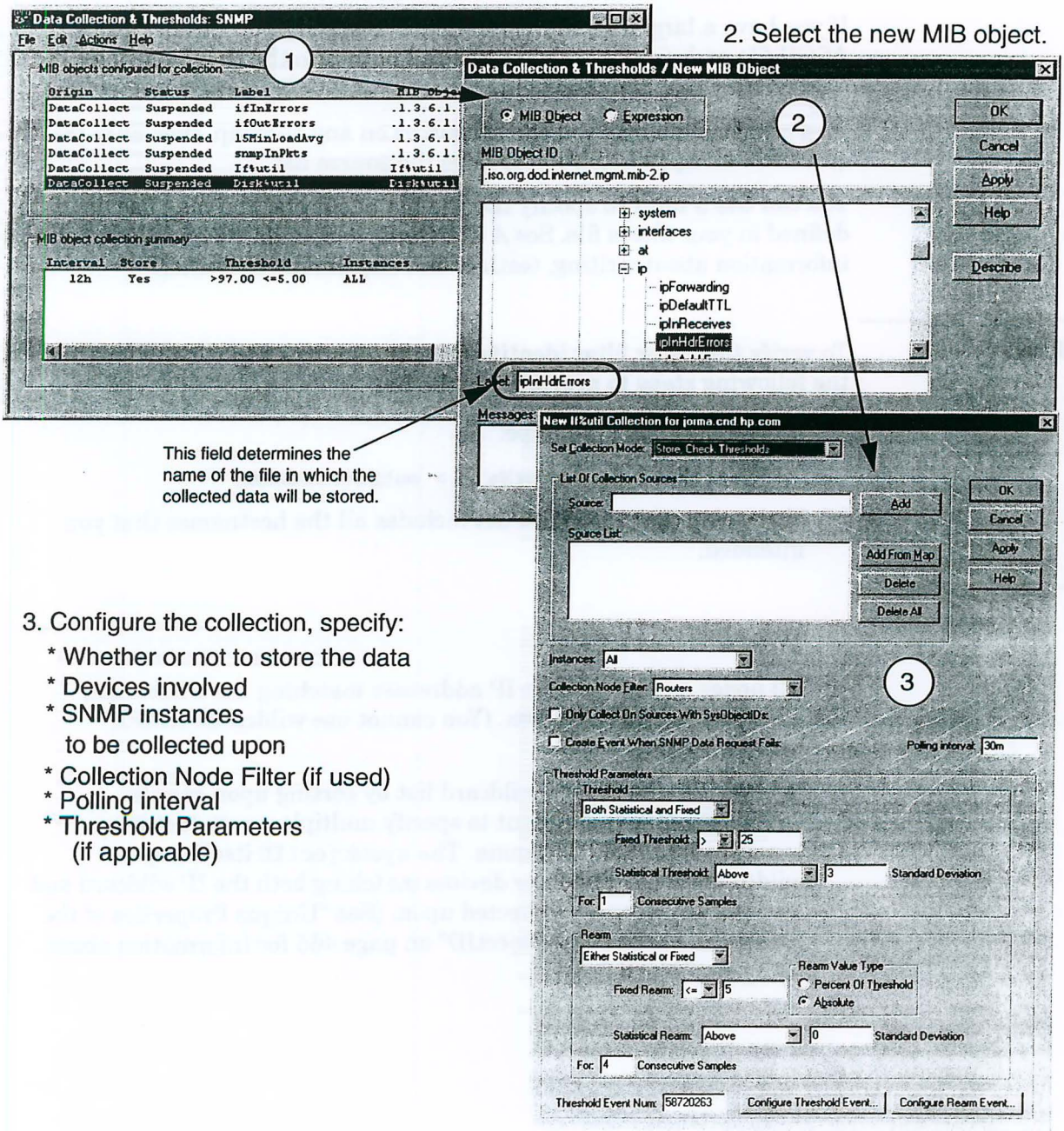
RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0184
Doc: 3740

sure the label conforms with file naming conventions for your operating system.) The label defaults to the last component of the MIB mnemonic name.

1506
A

Figure 12-11 Data Collection Configuration

1. Use Edit:Modify to reconfigure an existing MIB Object or MIB expression for collection.
   or use Edit:New to specify a New MIB Object or expression to collect upon (GET).



3. Configure the collection, specify:
   * Whether or not to store the data
   * Devices involved
   * SNMP instances
     to be collected upon
   * Collection Node Filter (if used)
   * Polling interval
   * Threshold Parameters
     (if applicable)

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0185
3740
Doc:

Then, configure the collection and designate the devices to be monitored.

You specify the devices to be monitored by IP host name, `sysObjectID`, IP address, IP address wildcard (such as `15.21.*.*`), and/or (*NNM for Windows only*) IPX address.

If you have a large number of nodes to specify, you can list them in an ASCII file and simply place the full path name to the file in the `List of Collection Sources` field.

As a convenience, you can select sources on any submap, then click the `[Add From Map]` button to populate the source list.

You can use a filter to specify the list of objects. You may use any filter defined in your filters file. See *A Guide to Scalability and Distribution* for information about writing, testing, and implementing a filter.

TIP

To verify that your filter identifies the sources you wish to monitor, use the following steps to preview the list:

1. At the command line, type:

   ```
   ovfiltertest -f filterName > outputFileName
   ```

2. Verify that the generated list includes all the hostnames that you intended.

With wildcard IP addresses:

- All nodes or devices with IP addresses matching the wildcarded address are collected upon. (You cannot use wildcards on IPX addresses.)
- You can further limit a wildcard list by sorting upon specific `sysObjectIDs`. If you want to specify multiple `sysObjectIDs`, separate them with a comma. The `sysObjectID` itself may be wildcarded. Only nodes or devices matching both the IP wildcard and the `sysObjectID` are collected upon. (See "Unique Properties of the SNMP MIB Object sysObjectID" on page 465 for information about using sysObjectID.)

1.504
A.

NOTE

You *must* save *any* changes for the new configuration to take effect. For example, if you suspend collection on a MIB object by selecting `Actions:Suspend Collection`, the `Status` column in the selection list indicates `Suspended`. However, even though the `Status` column displays a `Suspended` status, this change does not take effect until you select `File:Save`.

The data collection configuration is reanalyzed by `snmpCollect` each time you select `File:Save`. If you used IP wildcards, and you have a large number of managed nodes, there may be a significant delay before collections resume.

Counters are computed by calculating the change per second in the sampled values. Gauges and integers store the actual sampled value.

To view the collected data, open the Data Collection & Thresholds window, highlight the specific collection configuration in the list, and then select `Actions:Show Data`.

TIP

SNMP polling requests using the `Options:Data Collection & Thresholds:SNMP` menu item increase the amount of network traffic. If this becomes a problem:

- Change the status for particular collections to `Suspended` from within the Data Collection & Thresholds dialog box.
- Modify the details of your custom data collection by either deleting nodes, deleting instances, excluding nodes, or changing polling intervals.

Defining Thresholds for Monitored MIB Objects

Thresholds let you take a proactive approach to network management. You can manually define thresholds for specific MIB objects that you are monitoring, or have NNM calculate statistical thresholds for you. You can configure events to be posted in the Alarm Browser and/or automatic actions to be taken when the specified thresholds are exceeded. Once you have established a threshold and configured a threshold event, you can

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0186
3740
Doc:

use the web Reporting interface to create threshold violation reports. See NNM's online help for more information about the web Reporting interface.

If setting fixed thresholds, first determine what would constitute reasonable thresholds. To decide on a threshold value, you need to know what is normal and what is out of range. Only you can decide what is normal behavior for a device on your network. Generally, HP recommends that you collect information about a device throughout one complete business cycle before determining the normal high/low range. Consider collecting values such as error rates, retry limits, collisions, throughput, relation rates, and many more. Explore the MIB being used to determine which information to collect.

As soon as you install NNM, data collections on certain MIB objects are started. (You can see which objects are being collected from which devices by selecting `Options:Data Collection and Thresholds`.) This data is available for automatically setting thresholds based upon deviation from normal values. NNM uses the following process to establish statistical thresholds based upon the data being collected:

1. NNM gathers data as configured in Data Collection & Thresholds (the `snmpCollect` background process collects, compares, and stores requested SNMP MIB values).
2. NNM exports the collected *trend* data to the data warehouse every hour. See the *request_list* reference page in NNM's online help (or the UNIX manpage) for information about when NNM runs export tasks.
3. The data warehouse computes, for each instance of each configured collection:
   - The number of data points gathered in the past four days
   - The data summary
   - The sum of the squares for each collection

   This information, from the previous four days, is written to the `snmpColStats.txt` file. This file is recreated each time data is exported to the data warehouse. A notification event is sent to `snmpCollect`.

   These data points are sorted into three time periods, 8 p.m.-5 p.m., 5 p.m.-8 a.m., and weekends. See the *statTimeRanges.conf* reference page in NNM's online help (or the UNIX manpage) for information about controlling the definitions of the time periods.

1.502
A.

4. When using automatic statistical threshold generation for a data collection configuration, `snmpCollect` reads `snmpColStats.txt` and calculates, one threshold standard deviation for each time period (bucket) for each data collection instance. Every time the `snmpColStats.txt` file is read, NNM compares the standard deviation calculations to the standard deviation that you specified. An alarm is generated if the current standard deviation exceeds the threshold standard deviation. See the *snmpCollect* reference page in NNM's online help (or the UNIX manpage) for more information.

   Multiple thresholds are allowed per node, one for each instance; for example, one threshold set for a primary hard drive, and a different threshold set for the secondary hard drive.

CAUTION If you are using `ovdwtrend -trim` or `-delete` options to manage the volume of your collected data, ensure that your schedule allows sufficient data history for the statistical threshold feature. See the *ovdwtrend* reference page in NNM's online help (or the UNIX manpage) for information.

Prerequisites

- Configure the data collection to which the threshold applies (see "Data Collection & Thresholds" on page 447).
- You can monitor thresholds on numeric MIB objects; that is, the MIB objects defined as `Counter`, `Gauge`, `INTEGER`, `IpAddress`, `Counter64`, or `TimeTicks`. You can also set thresholds on MIB expressions (see "Creating and Using MIB Expressions" on page 460).

Procedure Tips

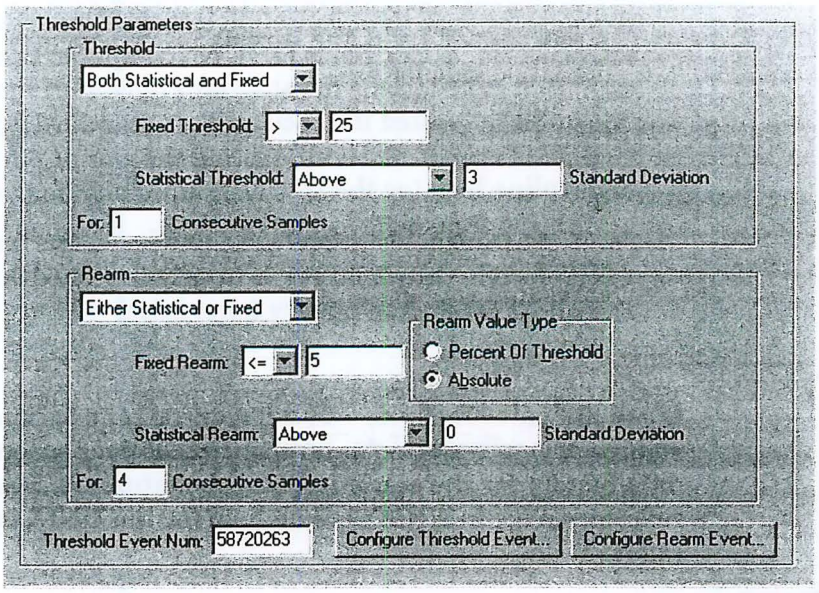
Access the collection configuration dialog box of the configured Data Collection you have been using to establish the normal operating range of your device. Select *one* of the following menu items from the `Option` menu next to the `Collection Mode` label:

- `Don't Store, Check Thresholds`
- `Store, Check Thresholds`
  (required if you want to use the statistical threshold feature)

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0187
3740
Doc:

The `Threshold` and `Rearm` fields are now available.

Figure 12-12 Threshold Area of Data Collection Window



To set up fixed-value threshold monitoring, select "Fixed" or "Both Statistical and Fixed" mode, specify a threshold value, and specify the number of consecutive samples required to violate the threshold. To set up fixed-value rearm monitoring, specify a fixed rearm value or percent, and the number of consecutive samples required to rearm the threshold.

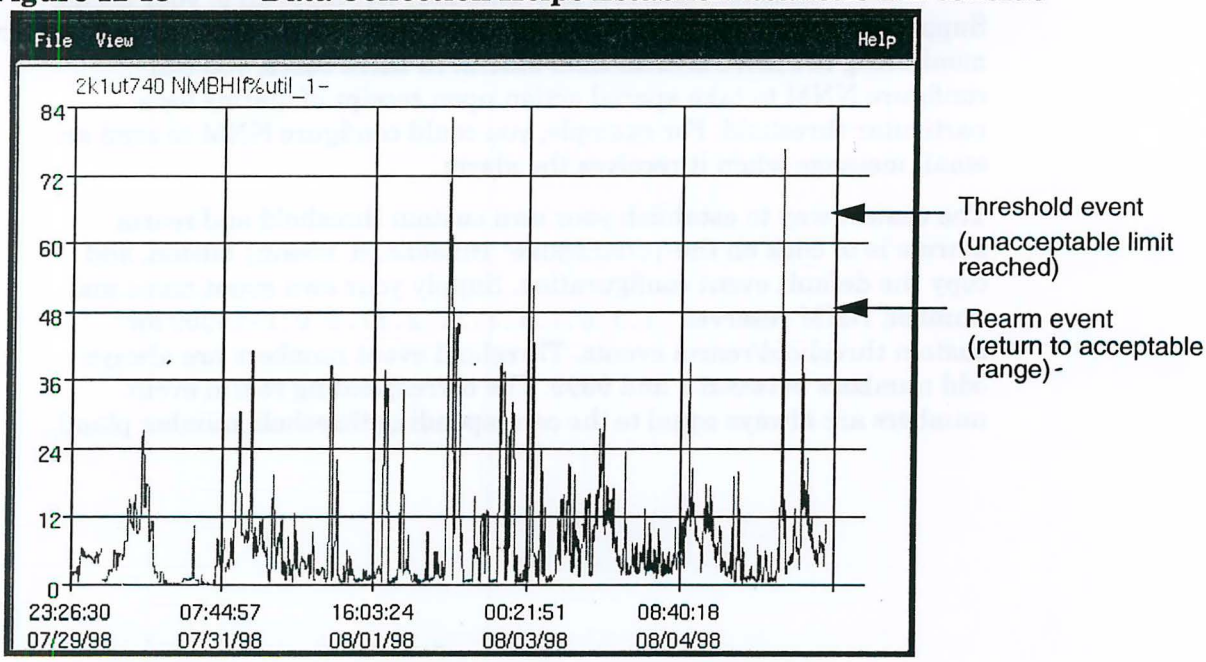
To set up automatic statistical threshold monitoring, select "Statistical" or "Both Statistical and Fixed" mode, specify the standard deviation, and specify the number of consecutive samples required to violate the threshold. To set up automatic statistical rearm monitoring, select "Both Statistical and Fixed" or "Either Statistical and Fixed" mode, specify standard deviation, and specify the number of consecutive samples required to violate the threshold. NNM automatically calculates the standard deviation according to the data warehouse's schedule for exporting trend data.

When the threshold setting is exceeded, a threshold-exceeded alarm is posted in the Alarm Browser, and any automatic actions (such as dialing a pager) that you specify in the Event Configuration are executed.

The *rearm value* controls how frequently a threshold event is generated. The *rearm* indicates that the device has returned to a non-critical state. A *rearm alarm* is posted in the Alarm Browser and any automatic

actions that you specified in the Event Configuration are executed. Another threshold event is not generated until the rearm event occurs and the collected value again reaches the threshold setting.

Figure 12-13 Data Collection Helps Establish Realistic Thresholds



For example, suppose you want to monitor interface percent-utilization. You can set a `Threshold` of 70% and a `Rearm` value of 50%. When the data collector detects a value above 70%, a threshold alarm is generated. Another threshold alarm will be generated only if the reading drops below 50% (sending a rearm alarm) and then goes above 70% again. Note that you can also specify absolute values rather than percentages.

Optionally, specify a value for the `Consecutive Samples` field. This value specifies the number of consecutive times the `Threshold` or `Rearm` expression must be satisfied before a corresponding alarm is generated. This field lets you distinguish sustained abnormality from a brief spike in behavior.

NNM uses two preconfigured events under the `OpenView` enterprise name (`.1.3.6.1.4.1.11.2.17.1.0`.) as the default events for thresholds and rearms:

```
OV_DataCollectThres (58720263)
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0188
3740
Doc:

`OV_DataCollect_Rearm (58720264)`

The default alarm is posted in the Alarm Browser's Threshold Alarms category.

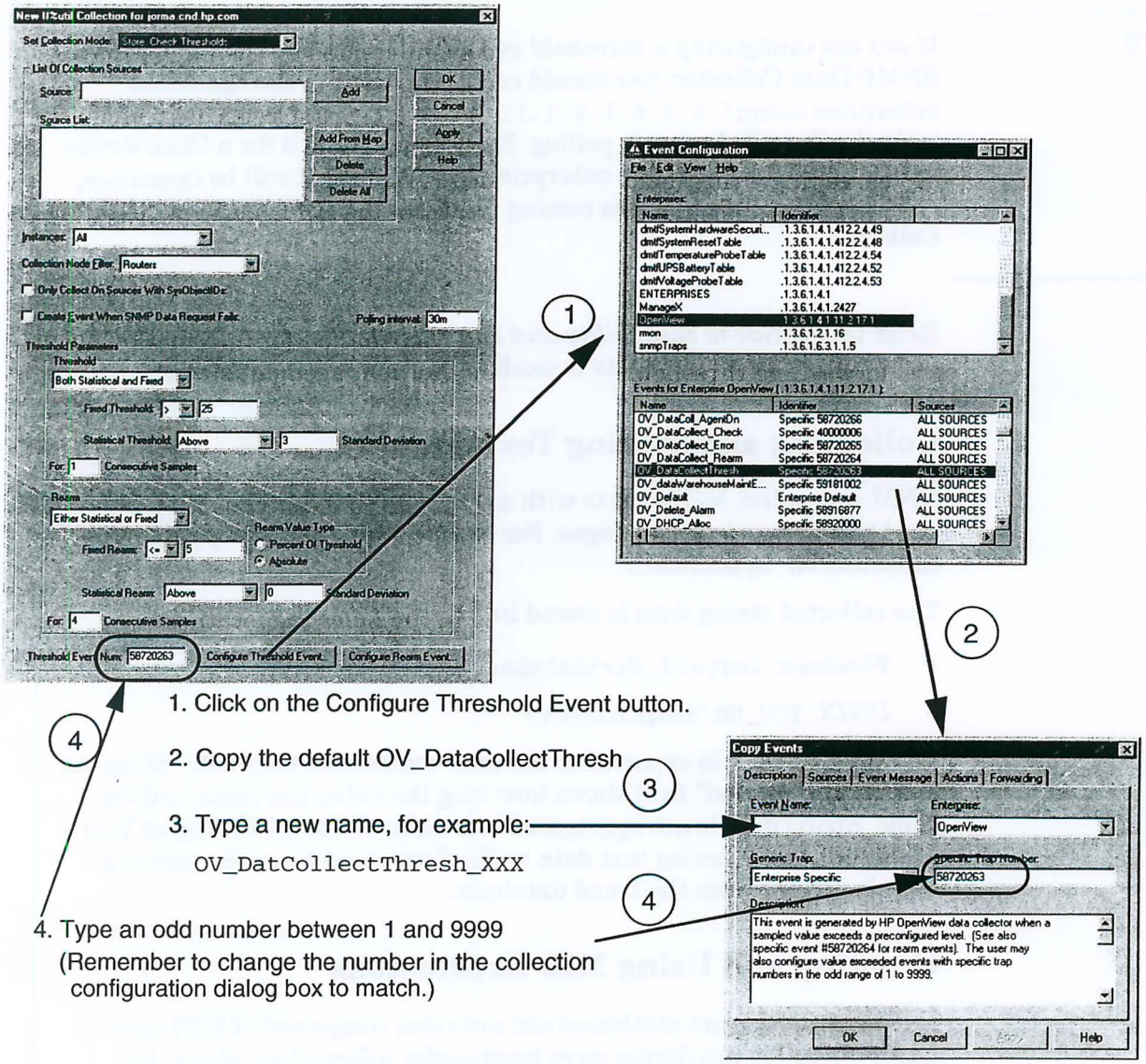
The default threshold and rearm events may not meet all of your needs. Suppose, for example, that some of the threshold values you are monitoring are more critical than others. In these cases, you can configure NNM to take special action upon receipt of alarms for a particular threshold. For example, you could configure NNM to send an email message when it receives the alarm.

The easiest way to establish your own custom threshold and rearm alarms is to click on the `[Configure Threshold Event]` button, and copy the default event configuration. Supply your own event name and number. NNM reserves `.1.3.6.1.4.1.11.2.17.1.0.1-10000` for custom threshold/rearm events. Threshold event numbers are always odd numbers between 1 and 9999. The corresponding rearm event numbers are always equal to the corresponding threshold number plus 1.

1.498
A.

NOTE If you create a custom threshold event, you must also create a matching rearm event.

Figure 12-14 Customizing the Threshold Event



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0189
3740
Doc:

For example, the threshold event ID 1005 will have a rearm event ID of 1006. These rearm event IDs are automatically assigned but *not* automatically configured in NNM. If you use one of the optional threshold event numbers, you must configure events for both the threshold and rearm event IDs (use the `[Configure Threshold Event]` and `[Configure Rearm Event]` buttons).

NOTE

If you are configuring a threshold event created by the HP OpenView SNMP Data Collector, you should configure it under the `OpenView` enterprise name (`.1.3.6.1.4.1.11.2.17.1.0`), regardless of which node the Data Collector is polling. Even if the event is for a Cisco device exceeding a threshold, the enterprise ID of the event will be `OpenView`, not Cisco, since the event is coming from the HP OpenView SNMP Data Collector.

Refer to *A Guide to Scalability and Distribution* for information about forwarding threshold events to another management station.

Collecting and Storing Textual Data

NNM can collect MIB objects with a `String` data type. This data can be used to monitor device changes. For example, you can set up data collection on `SysContact`.

The collected string data is stored in the following locations.

- *Windows:* *`install_dir`*`\databases\snmpCollect\`
- *UNIX:* `$OV_DB/snmpCollect/`

When string data is exported to the data warehouse, only new values are stored. The "period" field shows how long the value has remained the same. String data is not aggregated into daily, Weekly, Monthly, or Yearly tables. When exporting text data to the data warehouse, the existing data is deleted from the trend database.

Creating and Using MIB Expressions

MIB expressions are mathematical formulas comprised of MIB objects. Expressions let you derive more meaningful information about the health of your network than you could gather using individual MIB objects. MIB expressions are used by several NNM components, and are

1.496
A.

available for your use through the Data Collection & Thresholds window. You can also create your own and add them to the list by making additions to the `mibExpr.conf` file and the `mibExpr.conf` file.

Default MIB Expressions

NNM includes many default MIB expressions for your convenience. To explore the default MIB expressions, from any submap, select `Options:Data collection & Thresholds`, then select the following menu item:

Windows: `Edit:MIB Object->New`

UNIX: `Edit:Add->MIB Objects...`

Select the `Expressions` radio button. The list of predefined MIB expressions is displayed for your use. The following are a small sampling of the MIB expressions provided:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0190
Doc: 3740

Equation 12-1 **If%deferred (MIB II)**
The percent of packets on an interface which were deferred:

(packets deferred rate ÷ packets transmitted rate) × 100

Equation 12-2 **If%collision (MIB II)**
Percent of packets on an interface which collided:

(collision rate ÷ packets transmitted rate) × 100

Equation 12-3 **If%inErrors (MIB II)**
Percent of input packets on an interface which had an error:

$$\left(\frac{\text{input error rate}}{\text{received unicast packet rate} + \text{received non-unicast packet rate}}\right) \times 100$$

Equation 12-4 **If%outErrors (MIB II)**
Percent of output packets on an interface which had an error:

$$\left(\frac{\text{output error rate}}{\text{transmitted unicast packet rate} + \text{transmitted non-unicast packet rate}}\right) \times 100$$

Equation 12-5 **If%util (MIB II)**
Percent of available bandwidth utilized on an interface:

$$\left(\frac{(\text{received byte rate} + \text{transmitted byte rate}) \times 8}{\text{interface link speed}}\right) \times 100$$

Equation 12-6 **IfInOutOctets (MIB II)**
Total absolute traffic on an interface or the summation of octets (bytes) sent and received on an interface:

received byte rate + transmitted byte rate

Equation 12-7 **IfInOutPackets (MIB II)**
Total absolute traffic on an interface or summation of packets sent and received on an interface:

$$\left(\frac{\text{received unicast packet rate}}{\text{received non-unicast packet rate}} + \frac{\text{transmitted unicast packet rate}}{\text{transmitted non-unicast packet rate}}\right)$$

1494
A.

Equation 12-8 **Disk%util (HP-UX MIB)**

Percentage of disk utilization:

$$\left(\frac{\text{blocks} - \text{free blocks}}{\text{blocks} - \text{free blocks} + \text{available blocks}}\right) \times 100$$

Simply select one from the list and configure it for data collection and/or threshold monitoring on your network's devices.

TIP

There are seven additional MIB expressions defined specifically for use with the HP-extensible agent. They are located in:

- *Windows:* `install_dir\conf\extExpr.conf`
- *UNIX:* `$OV_CONF/extExpr.conf`

Open the file to read about them.

The mibExpr.conf File

The expressions are stored in an ASCII file:

- *Windows:* `install_dir\conf\mibExpr.conf`
- *UNIX:* `$OV_CONF/mibExpr.conf`

You can modify this file or create your own expressions using the `xnmcollect -loadExpr` utility. Best practice is to create a separate file with your new or revised MIB expressions, and then merge the expressions into the `mibExpr.conf file` using the following utility from the command prompt:

```
xnmcollect -loadExpr filename
```

The `-loadExpr` checks syntax, removes duplicate expressions, and rewrites the file.

See the *mibExpr.conf* reference page in NNM's online help (or the UNIX manpage) for information about writing your own MIB expressions; and see the *xnmcollect* reference page in NNM's online help (or the UNIX manpage) for information about updating the `mibExpr.conf` file.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 191
3740
Doc:

J.493

The mib.coerce File

The `mibExpr.conf` file works in partnership with the `mib.coerce` file. Entries in the `mib.coerce` file instruct NNM to convert (coerce) a received MIB value from one data type to another (for example, from a gauge or counter to an integer) for use in the mathematical formula defined in the `mibExpr.conf` file. The `mib.coerce` file is an editable ASCII file:

- *Windows:* `install_dir\conf\mib.coerce`
- *UNIX:* `$OV_CONF/mib.coerce`

After making changes to the `mib.coerce` file, you must force NNM to acknowledge the changes; from the command line, type:

```
xnmloadmib -event
```

See the *mib.coerce* reference page in NNM's online help (or the UNIX manpage) for more information about converting MIB values from one data type to another for use in your MIB expression.

1.492
A.

Unique Properties of the SNMP MIB Object sysObjectID

The sysObjectID is an important SNMP MIB object to NNM operations. This section describes:

- What the sysObjectID is
- How network management operations use the sysObjectID

The sysObjectID is registered in the Internet-standard MIB-II module as iso.org.dod.internet.mgmt.mib-2.system.sysObjectID (1.3.6.1.2.1.1.2). The sysObjectID is used for administrative purposes to uniquely identify the type of SNMP agent software that is running on a given vendor's hardware. This object is different from most other MIB objects; when you query it, you get back an object identifier that describes the product. For example, when you query the iso.org.dod.internet.mgmt.mib-2.system.sysObjectID using the MIB Browser on an HP OpenView SNMP Agent that is running on an HP 9000 Series 700 or Sun SPARCstation, SNMP returns one of the following object identifiers:

```
iso.org.dod.internet.private.enterprises.hp.nm.system.hpsun.sparc.sun4
iso.org.dod.internet.private.enterprises.hp.nm.system.hpsun.sparc.sun5
iso.org.dod.internet.private.enterprises.hp.nm.system.hpux.hp9000s700
```

This result tells you how the HP 9000 Series 700 or Solaris agent is registered in the MIB. The numeric identifier for Solaris is 1.3.6.1.4.1.11.2.3.10.1.2

Note that there is no value associated with the object ID returned in sysObjectID. It is a unique identifier.

The sysObjectID includes both hardware and software information, and varies depending on the type of hardware and agent software. Some vendors have a different sysObjectID for every version of their agents. For example, Hewlett-Packard sells several SNMP agents, each uniquely identified. To distinguish the HP 9000 Series 800 agent from the HP 9000 Series 700 or Solaris agent, HP registered the HP 9000 Series 800 agent as:

```
iso.org.dod.internet.private.enterprises.hp.nm.system.hpux.hp9000s800
```


IRQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: Nº 0192
3740
Doc:

netmon, a service (background process) that automatically discovers the nodes on your network, obtains the sysObjectID when it queries SNMP nodes. NNM operations take advantage of this special object in the following ways:

- To identify the vendor; that is, the manufacturer of the hardware.
- To identify the source of the SNMP agent, which is the type of agent software running on the hardware. For example, if you do a GetRequest to a Sun SPARCstation, the vendor is Sun, but the SNMP agent may be
  - An HP OpenView SNMP Agent for SunOS
  - An SCO UNIX for SunOS agent
  - Other SNMP agent software
- To determine IP topology behavior. An agent's sysObjectID provides hints about what type of node the agent is; for example, a gateway, a bridge, or a host.
- To determine symbol type when putting symbols for newly discovered nodes on the map; for example, a bridge, a gateway, or a hub.
- To identify the source of an event. A sysObjectID is sent in every event. You can use the sysObjectID when you configure events and data collections. The reference in the Event Configuration dialog box to enterprise ID is generally synonymous with the sysObjectID of the agent that generated the event.

Like NNM, you can take advantage of the sysObjectID in many ways, such as:

- From any submap, select Find:Object By Attribute to locate quickly all of a certain manufacturer's model-X when they require a software upgrade.
- If you are writing a rules-based application or script, use the sysObjectID as a rule index.
- On any submap, select a node and use Edit:Object Properties to quickly determine which SNMP agent is running on that node.
- Use the sysObjectID in your filter definitions: discovery, topology, map, etc.

1490
A.

- Use the `sysObjectID` when using the `ovtopodump` command to generate useful lists.
- Customize NNM to display a symbol that you created for a specific type of object (see Appendix D, "Changing All the Symbols for a Particular Device," on page 661).
- If NNM displays an object on the map with a generic symbol (just the outside shape, no vendor-specific icon within the shape), you can specify the icon of your choice to be mapped to that device's `sysObjectID` (see Appendix D, "Changing All the Symbols for a Particular Device," on page 661).
- Specify nodes for which data should be collected, as described in the previous section.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0193
3740
Doc:



1.488
A

13 Using Event Data

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0194
3740 - 0
Doc.

NNM provides several features that can assist you in analyzing the network data that has been collected:

- *Graph SNMP Data* (page 471)

  Display collected SNMP data in graphs. This can be SNMP data that has been collected over time and stored in a file, or real-time values that are graphed as they are collected, or both at the same time.

- *Data Warehouse* (page 476)

  Allows you to export collected historical data for use with other statistical analysis tools. Command line functions allow you to maintain the data warehouse database.

- *Web Reporting Interface*

  Allows you to use data from the data warehouse to create reports using a set of predefined templates. See the *Reporting and Data Analysis* online manual and the online help for more information.

NOTE For information about how to merge data from multiple NNM collection stations into a single database, see *A Guide to Scalability and Distribution*.

Ideas for utilizing your collected data:

- Anticipate the need for more network and computer resources, such as gateways and disk space.
- Detect deviations in normal activity.
- Isolate network faults and performance problems.
- Generate inventory reports.

1486
A.

Graphing SNMP Data

The NNM Grapher tool allows you to graph collected MIB data from within the SNMP MIB Browser. Once the Grapher window is displayed, you can set time intervals to continue the collection and even automatically establish a configuration for continuous monitoring by selecting `File:Configure in Data Collector`.

The NNM Grapher tool also enables you to organize MIB data that was collected by the Data Collections & Thresholds feature and view it in graph form. You can graph combinations of data values in the same graph. The data values can be different instances of MIB variables or different variables for different nodes. For example, you can graph instance 1 and instance 3 of a MIB variable for one system, or you could graph instance 3 of a MIB variable for one system, and a completely different variable for another system. You can also normalize the data over configurable time periods to identify trends in the historical data.

This section describes the following:

- Graphing collected data, which includes graphing all data or graphing selected data only, and updating data that has been graphed.
- Graphing historical and real-time data in the same graph.
- Zooming in and out of a specific period of time to view the data in greater or less detail.
- Modifying line attributes in a graph.
- Printing a graph.

NOTE The Grapher tool is available in NNM on a Windows or UNIX operating system. If you are using NNM on the Web, there is a Grapher tool available in the `contrib` directory. (See page 74 for information about using programs from the `contrib` directory.)

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0195
3740
Doc:

J.485 A.

Graphing Collected Data

You can graph the data collected in the Data Collector's database by using the `Performance:Graph SNMP Data->All` and `Performance:Graph SNMP Data->Selected Nodes` menu items. You can also access the Grapher tool from within the SNMP MIB Browser or by using the `xnmgraph` command. Refer to the *xnmgraph* reference page in NNM's online help (or the UNIX manpage) for more information.

Behavior

The Graph Selected Nodes dialog box consists of a line graph. The legend across the top of the graph identifies the currently graphed data. Time is shown on the X-axis.

The menu bar has functions that enable you to manipulate the data. The menu bar also has help entries explaining how to use the different menu options to manipulate the data.

The Graph SNMP Data operation does not update the graph with new information as the data is collected. To update the graph with the most current MIB data, select `File:Update Data` from the Grapher menu bar.

Refer to the online help within the graph window for additional information.

Graphing All Data

The `Performance:Graph SNMP Data->All` operation enables you to view collected data in graph form without first having to build an application. This is useful when you want to browse all the data in the Data Collector's database:

- *Windows:* Data is stored in the *`install_dir`*`\databases\snmpCollect` directory.
- *UNIX:* Data is stored in the `$OV_DB/snmpCollect` directory. (If you need more disk space, symbolically link to another file system.)

TIP

For HP-UX systems only: You can expand the file system with Logical Volume Manager. Extend the logical volume, then use `extendfs` (hfs) or `fsadm` (vxfs).

1.484
A

Use this operation when you want to graph some data points just once, or when you want to compare different variables across different systems. For example, let's say you want to compare the load averages to the number of packets, but had not used the Application Builder (see page 443) to set up your own application for this purpose. You can easily use the Graph All operation to graph these two variables together.

CAUTION

This operation reads in *all* the collected data from the Data Collector database into its memory. Depending on the amount of data stored in the database, displaying the Graph All dialog box may take a long time.

Graphing Data on Selected Nodes

The `Performance:Graph SNMP Data->Selected Nodes` operation enables you to view collected data on the nodes that are currently selected on the map, without having to use the Application Builder (see page 443) to set up your own application for this purpose. This is useful when you want to browse the collected data for these nodes. Use this operation when you want to graph some data points just once, or when you want to compare different variables across different systems.

For example, let's say you want to compare the load averages to the number of packets on the selected systems, but had not used the Application Builder (see page 443) to set up your own application for this purpose. You can use the Graph Selected Nodes operation to easily graph these variables together.

Graphing Historical and Real-Time Data in the Same Graph

When you use the Grapher tool via an NNM-provided menu item, the Grapher displays both the collected data and real-time data in the same graph (for example, `Performance:Network Activity`).

When Grapher starts up, it does the following:

1. Reads in the data from the Data Collector's database.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0196
Doc 3740

When the Grapher tool first comes up, it loads all the collected data from the Data Collector database and seeds its memory with the information in the database. The resolution of the collected data is determined by what the Data Collector was configured to collect.

Once the Grapher tool is running, the tool does not interact with the data in the Data Collector database again (unless you select `File:Update Data`). The Data Collector operates in the background and continues to collect data. This data is available for you to use in future operations.

2. Starts to graph the real-time data.

   The real-time data displayed is independent of the Data Collector. The Grapher tool processes SNMP requests based on the interval specified under `View:Time Intervals` and displays the data in the graph. Unless you save the graphed data to a file using the `File:Save As` menu item, the real-time data is lost as soon as you exit the Grapher.

Stopping Real-Time Data Graphing

To stop real-time data graphing, from the Graph window:

- *Windows:*

  Select `Options:Time Intervals->SNMP Polling Off`.

- *UNIX:*

  Select `View:Time Intervals->SNMP Polling Off`.

Grapher Operations

This section describes some common operations for manipulating a graph.

Selecting Time Intervals

To select time intervals, using the left mouse button:

- Click on the left edge of the graph to page back one screen.
- Click on the right edge of the graph to page forward one screen.
- Click within the graph to center the graph around the selected point in time. Holding the mouse button down and dragging enables you to fine tune the point that you want centered.

1.482
A

Zooming In and Out of a Graph

The Grapher allows you to zoom in and out of a specific period of time in order to view data in greater or lesser detail. To do so, using the right mouse button, click anywhere within the graph. An option menu appears. You can zoom in and out to different amounts of detail. You can also use the menu to page forward, page backward, or show different data points.

Modifying a Line Attribute

To access the `Line Configuration` dialog box, from the Graph window:

- *Windows:* Select `Options:Line Configuration`.

  Option buttons are arranged in rows and columns. Each item in the list controls the attributes for a particular line on the graph.

- *UNIX:* Select `View:Line Configuration`.

  Option buttons are arranged in rows and columns. Each row in the list controls the attributes for a particular line on the graph.

Printing a Graph

To Print a graph, from the Graph window:

- *Windows:* Select `File:Print`. The standard `Print` dialog box appears. Make your selections and click `[OK]`.
- *UNIX:* An `xwd`-compatible file is produced by the Grapher. The default `Print` command is configured in the Grapher print resource. The commands shown in the Print Command window are used to print that file. If the default command does not meet your needs, you can change it. Before you configure the default `Print` command, determine which command options will give you the best printouts. See NNM's online help for more information.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0197
Doc: 3740

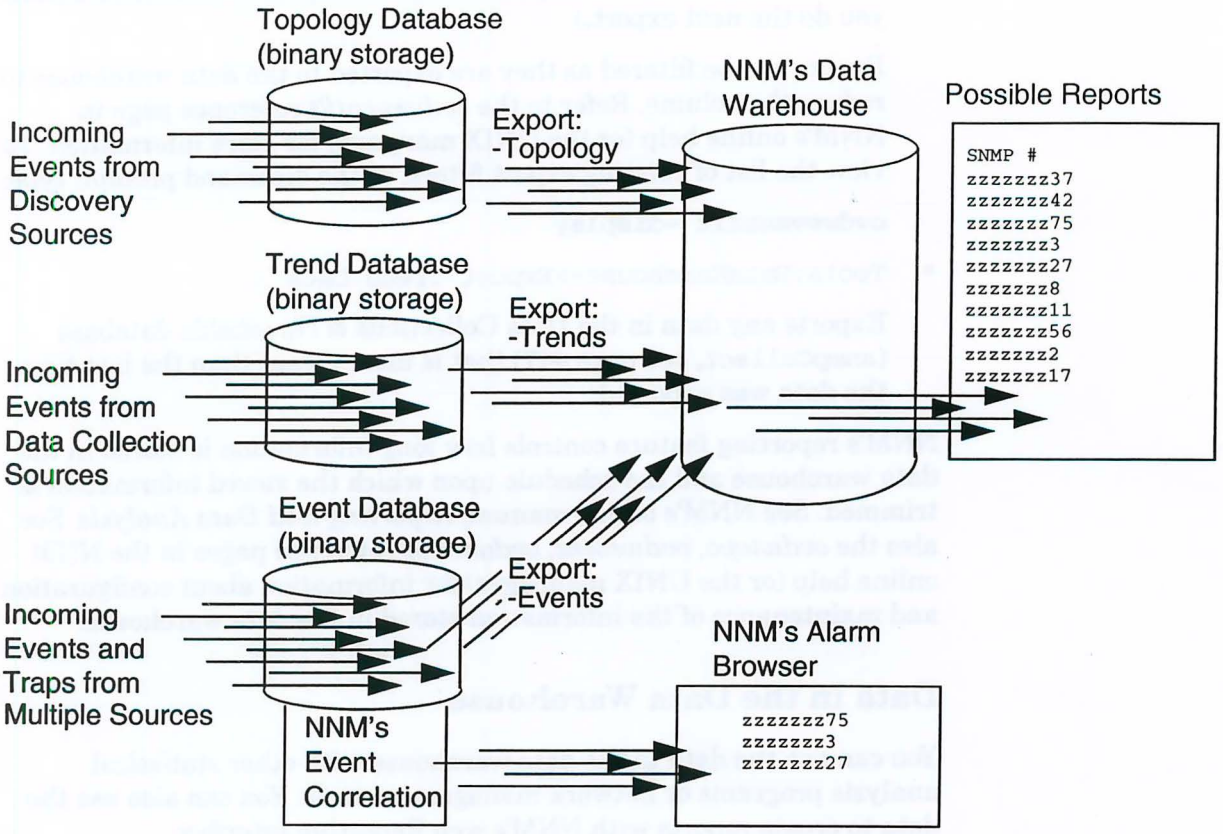
Data Warehouse

The NNM data warehouse is a relational database (RDBMS) provided with NNM. NNM stores a *copy* of the information from the NNM operational databases into the data warehouse so you can gain an historical perspective of your network information. The data warehouse information is accessible with standard SQL statements using ODBC tools. You can also create reports from the data using the NNM web Reporting interface.

By contrast, the information in the NNM *event database* is discarded when a certain volume is reached (see page 343). Information copied to the *data warehouse* is retained for as long as you need it. You can derive reports from hourly, daily, weekly, monthly, or even yearly information. The limit to the size of the data warehouse is up to you and the allotted hard drive space for the data warehouse.

1.480

Figure 13-1 NNM's Event Flow



NNM periodically populates the data warehouse according to a schedule. See the *ovrequestd* and *request_list* reference page in NNM's online help (or the UNIX manpage) for more information. To view the current schedule, at the command prompt, type:

```
request_list schedule
```

You can also manually populate the data warehouse using the following pull-down menu items:

- `Tools:DataWarehouse->Export Topology`

  Exports the current network topology information, replacing any topology information previously sent to the data warehouse.

- `Tools:DataWarehouse->Export Events`

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0198
3740
Doc:

Exports any event database information that is more current than the last time the events database was exported. (Remember: NNM's event database is automatically trimmed when it reaches maximum size, see page 343, so it *is possible* that events will be deleted before you do the next export.)

Events can be filtered as they are exported to the data warehouse to reduce the volume. Refer to the *ovdweventflt* reference page in NNM's online help (or the UNIX manpage) for more information. To view the list of existing export filters, at the command prompt, type:

```
ovdweventflt -display
```

- `Tools:DataWarehouse->Export Trend Data`

  Exports any data in the Data Collections &Thresholds database (`snmpCollect`, see page 447) that is more recent than the last time the data was exported.

NNM's reporting feature controls how long information is stored in the data warehouse and the schedule upon which the stored information is trimmed. See NNM's online manual, *Reporting and Data Analysis*. See also the *ovdwtopo*, *ovdwevent*, *ovdwtrend* reference pages in the NNM online help (or the UNIX manpages) for information about configuration and maintenance of the information stored in the data warehouse.

Data in the Data Warehouse

You can use the data in the data warehouse with other statistical analysis programs or network management tools. You can also use the data to create reports with NNM's web Reporting interface.

See the NNM online manual, *Reporting and Data Analysis*. See also the NNM online help.

Reporting

Reporting is enabled by default when NNM is installed. Once the report data is collected, daily and month-to-date reports for general availability, threshold violation exceptions, and network performance are available from the `Tools:Report Presenter` command or from the HP OpenView Launcher. Daily Inventory reports are available as soon as the report data is collected. For more information about reporting see page 45 in this manual.

For more information about the Reporting feature, see the section labeled "Reporting Interface" on page 516 in this manual.

For more information about the NNM databases and the data warehouse, consult the online manual *Reporting and Data Analysis*.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0199
Doc: 3740

J.477
A

1.476
A

14 NNM on the Web

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0200
Doc: 3740

This chapter describes HP OpenView's Java™-based web interface, and tells you how to set up, configure, and administer NNM's web applications.

This chapter will not attempt to teach you how to use all the features of HP OpenView's web interface. You should consult the NNM online help within the web interface for usage instructions. For an introduction, explore the *Get Acquainted with HP OpenView Network Node Manager: Training for NNM Operators* CD provided with NNM.

This chapter refers to HP OpenView Application Registration Files (ARF) in several places. If you are not familiar with that file, review its functionality in the online manual *Creating and Using Registration Files*.

TIP

If you make changes or additions to the web registration files ensure that your new files are properly backed up. They are *not* included in NNM's backup scripts. See "Backup/Restore to Protect Your Investment of Time" on page 165 for more information.

This chapter includes:

- An overview of the HP OpenView web applications, including setting up the web applications and security for the web applications (page 484).
- A description of the HP OpenView Launcher, the UI integration point for the web applications, including configuration details (page 492).
- A description of the Network Presenter, the web application that displays maps and map data (page 501).
- A description of the SNMP Data Presenter, which displays the results of operations that gather data from managed SNMP nodes (page 509).
- A description of the web-based Alarm Browser, a graphical interface that presents network alarm data, including a comparison of the web-based Alarm Browser and the Alarm Browser running on the management station (page 512).
- A description of Event Correlation Services, NNM's multi-protocol event correlator (page 515).

- A description of the Reporting interface, the web application that allows you to configure and view reports (page 516).
- A description of several supplemental views of discovered nodes (page 518).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0201
Doc: 13740

Overview

HP OpenView's Java-based web interface further expands NNM's network management capabilities. A part of NNM's base product, the web interface and its applications present the same information about your network that is available from the NNM management station. This information is now presented in a familiar, operator-friendly format that you can access from a remote workstation running a web browser. From your web browser on any PC or UNIX operating system workstation, you can log onto the web and access NNM on the management station to display maps and alarm information. You can easily monitor the status of your network from any place at any time, a real advantage when your pager goes off in the middle of the night!

The HP OpenView Web lets you:

- Inquire about the status of your network and troubleshoot problems from anywhere via the World Wide Web.
- Obtain dynamic updates on map information.
- Share management data with others.
- Present both a graphical and tabular view of the network.
- Access and configure security for web applications.
- Launch NNM and other web-based applications.
- Interact with a familiar web interface.
- Configure and view reports.

The HP OpenView Web includes the following applications:

- HP OpenView Launcher
- HP OpenView Network Presenter
- HP OpenView SNMP Data Presenter
- HP OpenView Alarm Browser
- HP OpenView ECS Configuration
- HP OpenView Correlation Composer
- HP OpenView Reporting interface

An overview and the administration of each of these applications is discussed in the following sections of this chapter.

Setting Up the HP OpenView Web

When you install NNM on the management station the files and applications necessary to run the web interface are also installed. The management station must also have a web server running.

When you install NNM on a management station running Windows, a web server is not installed, since the Windows operating system comes with its own web server. The web server on the Windows operating system is automatically configured for NNM's use during the NNM installation.

When you install NNM on a management station with a UNIX operating system, a web server *is* installed. This server is fully configured to access scripting aliases and documentation aliases used by NNM. The web server uses port 3443 for communication.

If you want to set up your own web server, configure the port number and set up the aliases `OvCgi`, `OvDocs`, and `OvBackgrounds`, see NNM's release notes for additional information about installing a web server.

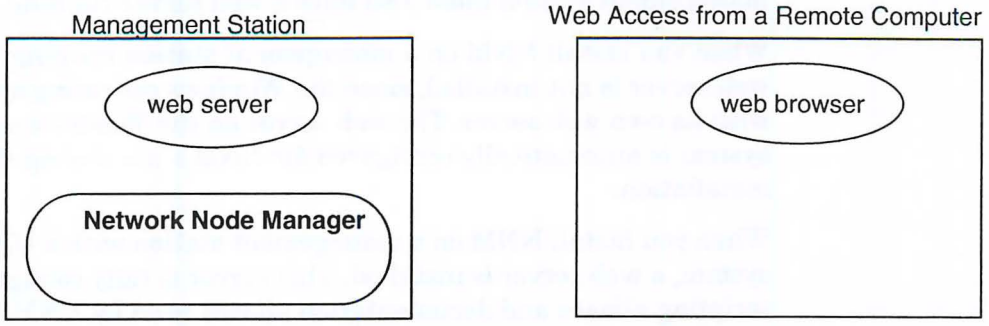
The client station only needs to have a web browser running. Supported web browsers are:

- Netscape
- Microsoft Internet Explorer

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0202
Doc. 3740

NOTE Refer to the "Supported Configurations: Supported Web Browsers" section of the NNM Release Notes for specific information about supported web browsers.

Figure 14-1 Management Station and Remote Web Access



See Figure A-4, "Services and Files for the Web Components," on page 551 for more detailed information about the files and services (processes) on the management station and remote computer at installation time.

On the management station, there must be a non-web based version of NNM running for each map that will be accessible through remote web access. For example, if you want your team to be able to access the Home Office map and the map showing your operations in Germany, you must start NNM on the management station with your Home Office map displayed and start another instance of NNM on the management station with the Germany map displayed. See page 508 for more information.

From remote sites you can now use your web browser and NNM's Network Presenter to display the Home Office map or the Germany map.

Role Configuration Files for the HP OpenView Web

Since the HP OpenView Web can be accessed from virtually any system, security measures are in place to ensure that only authorized users log in to your NNM management station. The way the HP OpenView Launcher and the web applications use these mechanisms varies. The security mechanisms are:

- User authentication (password) file.
- User authorization (roles) file.
- Session configuration file.
- Audit log files.
- `ovw.auth` and `ovwdb.auth` files (used by the Network Presenter and discussed in the section "Configuring Security for the Network Presenter" on page 506).

Since the Launcher is the access point for all other web applications, it provides the first level of security. When security is enabled via the session configuration file, the user password file and user roles file are read to ensure that the user is authorized to access NNM on the management station. The user roles file ensures that only those applications approved for that user role are made available via the Launcher.

User Authentication (Password) File

User authentication is accomplished through a user name and user password. Users should not use the same password as their operating system password. Since the passwords are passed in cleartext format at the beginning of a session, it is possible that they may be intercepted. The Launcher uses the user password file when the user attempts to log on.

The user password file is located on the management station at:

Windows: `install_dir\www\etc\htpasswd`

UNIX: `/etc/opt/OV/share/www/etc/htpasswd`

Entries in the file appear as:

```
john: FXSD198sdfADS
sue: PO12ADFpoiuS
```

The file is installed with administrator-only (Windows operating system) or root-only (UNIX operating system) permission.

Set passwords as follows:

`ovhtpasswd` *username*

The command prompts you for the password for that user.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: Nº 0203
3740
Doc:

See the *ovhtpasswd* reference page in NNM's online help (or UNIX manpage) for more information about this command.

User Authorization File

Users may be assigned to any number of groups for authorization purposes. These user groups are called user roles in NNM. A **user role** is a designation given to individuals who perform specific tasks with NNM. Users are assigned roles, and then those roles are given access to specific URLs. The Launcher uses the user roles file to define what list items are visible from the Launcher window. When a user logs in, his or her role is verified, and then he or she can access the URLs assigned to that specific role. User roles are valid only when a user accesses NNM via the web interface; they are not valid when a user accesses NNM directly on a management station.

Predefined user roles and their functions are listed below. You can change these roles, or add new roles.

- NetworkAdmin

  The role of NetworkAdmin is intended for individuals who have a higher level of knowledge of networks. Capabilities for configuration of the network and connecting devices, and advanced troubleshooting should be associated with this user role.

- NetworkOper

  The role of NetworkOper is intended for individuals who do routine troubleshooting and maintenance tasks associated with the network. Capabilities for monitoring the network, and routine troubleshooting and maintenance of the network and network devices should be associated with this user role.

- NTAdmin

  The role of NTAdmin is intended for individuals who have a higher level of knowledge of the Windows operating system. Capabilities for configuration of the Windows operating system and advanced troubleshooting should be associated with this role.

- NTOper

1468
A.

The role of NTOper is intended for individuals who do routine troubleshooting and maintenance tasks associated with Windows operating system. Capabilities for monitoring the system, and routine troubleshooting and maintenance of the Windows operating system should be associated with this user role.

- UNIXAdmin

  The role of UNIXAdmin is intended for individuals who have a higher level of knowledge of UNIX operating systems. Capabilities for configuration of UNIX operating systems and advanced troubleshooting should be associated with this user role.

- UNIXOper

  The role of UNIXOper is intended for individuals who do routine troubleshooting and maintenance tasks associated with UNIX operating systems. Capabilities for monitoring the system, and routine troubleshooting and maintenance of UNIX operating system should be associated with this user role.

- OVAdmin

  The role of OVAdmin is intended for individuals who do configuration and customization of the HP OpenView environment and management applications. Capabilities for configuring and customizing management applications should be associated with this role.

The user roles file is located on the management station at:

Windows: *install_dir*\www\etc\htgroup

UNIX: /etc/opt/OV/share/www/etc/htgroup

The format of the user roles file is:

```
NetworkAdmin: user1 user2

NetworkOper: user4 user5

NTAdmin:user1 user3

UNIXOper: user6
```

You can also use a plus sign (+) instead of specific user names. This allows any user access to the capabilities of that user role.

User roles work in conjunction with the Access specification in the Launcher Registration Files (WLRF). See "Action Block" on page 496.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0204
Doc: 3740

Session Configuration File

The session configuration file is used by the Launcher. A **session** is a group of applications associated with a particular user on a particular display. When a user logs in, all the applications started (directly or indirectly) from the Launcher are part of that session. The applications that are part of a session can share information, such as locale.

A session is terminated when the user exits the web browser, when the session has been inactive for some configurable period of time (the default is 9 hours), or when the management station is shut down.

The session configuration file allows you to enable or disable security for NNM's web applications (default is disabled). If you specify `Off` in the `UserLogin` field of this file, NNM's web applications open directly. If you specify `On` in the `UserLogin` field of this file, NNM's web applications display a login dialog box upon opening.

WARNING **The default is for the session configuration file to disable security. If the security mechanisms are disabled in this file, users will not be presented with a login screen, and will have access to all registered actions.**

The session configuration file is located on the management station at:

Windows: *`install_dir`*`\www\conf\session.conf`

UNIX: `/etc/opt/OV/share/www/conf/session.conf`

The session configuration file has the following format:

```
UserLogin: on|off
LoginLogging: on|off
AccessLogging: on|off
SessionTimeout: hours
```

The default values are `off` for the first three items, and 9 hours for the session timeout. Time should be specified in integer values. Open the editable ASCII `session.conf` file for more information.

If you modify this file while you have the Launcher running, you need to exit the web browser and restart the Launcher for the new information to take effect.

1.466
A

Audit Log Files

There are two audit log files — one for logging logins and one for logging URL access from the Launcher. These are useful for security auditing purposes, as you can check on which users are accessing the Launcher by monitoring these files.

There is no log file management; the files continue to grow. You should periodically check these files and when they get large, you should save them or trim them.

The files are located on the management station at:

Windows: *install_dir*\www\logs\login_log (login log)

install_dir\www\logs\access_log (access log)

UNIX: /var/opt/OV/www/logs/launch/login_log (login log)

/var/opt/OV/www/logs/launcher/access_log (access log)

Each log entry is a single line of text. If the session configuration file is set to LoginLogging:on, the following information is recorded:

- Host
- User name
- Date
- Session number
- Access permitted; either Allowed or DENIED
- URL accessed (for the access_log file only)

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0205
Doc: 3740

J.465

The HP OpenView Launcher

The HP OpenView Launcher is the user interface integration point for the HP OpenView web applications. Just as with management station-based NNM, developers can tie their applications into NNM's web interface. Then users access those applications through the Launcher interface.

You can also create your own application that you access from the Launcher. If you create your own application, you can integrate it with the Launcher by creating a registration file for that application.

The Launcher provides functionality in three areas:

- Launching of management functionality and applications via a URL or via the web interface.
- User login and user roles.
- Maintenance of session information shared by all web interfaces.

Launcher User Interface

The Launcher interface is started from a web browser. The URL for the Launcher is:

`http://`*`hostname`*`:`*`[port]`*`/OvCgi/ovlaunch.exe`

For example, if the host system is a management station named `UX-manage1` running a UNIX operating system, you would enter:

`http://ux-manage1:3443/OvCgi/ovlaunch.exe`

A web server is automatically installed on UNIX management stations and configured to use port number 3443 for communication.

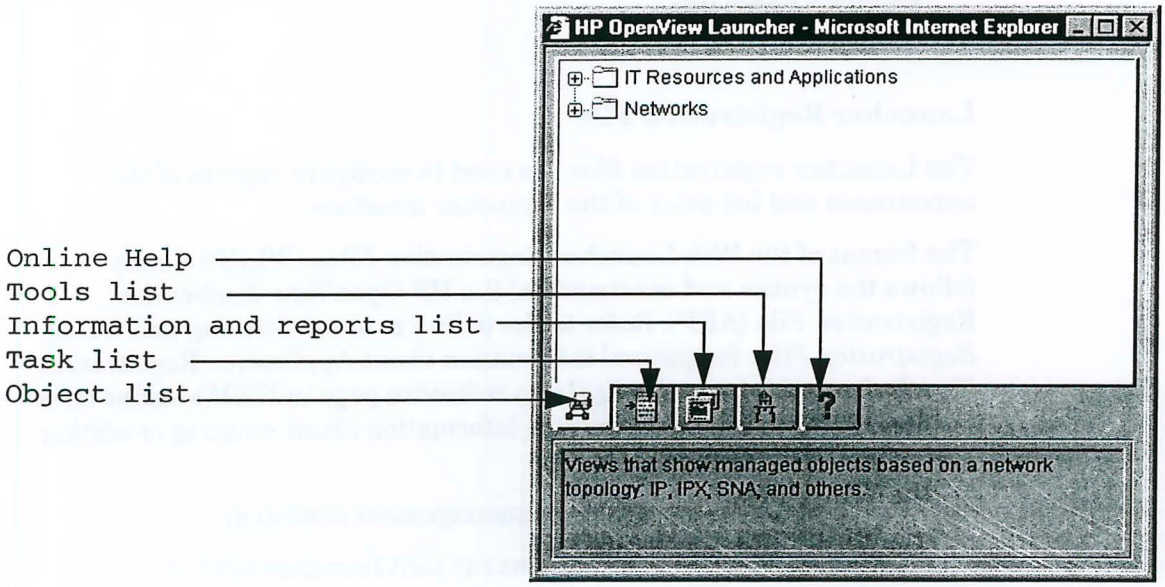
If the host system is a workstation named `nt-mgmt` running Windows, you would enter:

`http://nt-mgmt/OvCgi/ovlaunch.exe`

No port number is required for management stations running a Windows operating system.

If the management station has been configured for security, a login screen appears where the user enters his or her name and password. If no security has been configured, the Launcher window comes up without asking for login and password.

Figure 14-2 The Launcher Window



The Launcher window displays a tabular view of the capabilities available through the Launcher. The bottom tabs of the Launcher window contain the Task, Tool, Object Views, Management Areas, and Help categories. These categories correspond to the basic functionality of NNM on a management station. These are also the categories where other HP OpenView web applications will be linked.

Click on a category to expand it, or click on the expanded category to contract it. You can also click on the +/- indicator.

If you double-click on a list item, you execute the URL associated with that item.

The categories that are displayed in the tabular section of the Launcher window are determined by the user roles file and the Launcher Registration Files (WLRF), described next.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0206
Doc: 3740

J.463 A.

Configuring the Launcher

There are several files you can use to customize the Launcher.

- Launcher registration files.
- Error log file.
- Installed locale file.
- Java parameters file.

Launcher Registration File

The Launcher registration files are used to configure aspects of the appearance and behavior of the Launcher interface.

The format of the Web Launcher Registration Files (WLRF) closely follows the syntax and constructs of the HP OpenView Application Registration File (ARF). Refer to the online manual *Creating and Using Registration Files* for general information about Application Registration files. Refer to the *LauncherRegIntro* reference page in NNM's online help (or the UNIX manpage) for specific information about creating or editing the WLRF files.

The WLRF files are located on the management station at:

Windows: *install_dir*\www\registration\launcher\C*.*

UNIX: /etc/opt/OV/share/www/registration/launcher/$LANG

The bitmaps referenced in the WLRF are located in:

Windows: *install_dir*\www\htdocs\C\images*.*

UNIX: /opt/OV/share/www/htdocs/$LANG/bitmaps

Components of the WLRF There are several sections of a WRLF that you might need to modify. Only those sections will be discussed here.

Once you have modified a WLRF file, you can check it for errors with the command `regverify`. See the *regverify* reference page in NNM's online help (or the UNIX manpage) for more information.This command is located on the management station at:

Windows: *install_dir*\bin\regverify

UNIX: /opt/OV/bin/regverify

Tab Block

1.462

The Launcher has several tabs at the bottom of its window. The tab block indicates under which of the tabs an application will appear.

The tab block allows an optional icon file name to display on the tab. If one is not specified, a default will be used. The icon appears in front of the name of the application in the Launcher content area. The format for icons is 16x16 GIF. The file name is relative to:

Windows: *install_dir*\www\htdocs\bitmaps

UNIX: $OV_WWW/htdocs/bitmaps

The tab block also contains optional active help text. This active help is presented when the mouse pointer is over the tab.

The tab block contains List Item entries instead of Menu Items (for the menu bar). Following is a sample of the tab block.

```
Tab <60> "Tools" Icon "launcher/toolsfold.20.gif"
        ActiveHelp { "tools" }
{
        <70> "Session"
                Icon "launcher/toolsfold.16.gif"
                ActiveHelp {"Session Info" }
                f.list "SESSION";
}
```

List Block

The list block of the WLRF corresponds to the menu block in the ARF.

The following statements are allowed in the list block:

- Precedence value

  This has the same definition as in the ARF.

- List Item Label

  This is the label that is displayed for the entry.

- Icon

  This is a locale-dependent icon that is displayed for the list item. The format for icons is 16x16 GIF.

- ActiveHelp

  This is the active help text that is displayed when the mouse pointer is placed over the entry.

- Functions

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0207
Doc: 3740

Two functions are supported:

— `f.action`

This indicates a terminal list item. It points to an Action block that has the action definition.

— `f.list`

This indicates a component list item. It points to a list block to allow the definition of a hierarchical tree list.

Following is a sample of the list block.

```
List "SESSION"{
    <80> "Session Info Viewer"
            Icon "launcher/tools.16.gif"
            ActiveHelp { "Session Info Viewer" }
            f.action "printsession";
}
```

Action Block

The action block of the WLRF serves the same function as in the ARF. The following statements are allowed in the action block:

- URL

  This is the URL to launch for the action. The URL may contain the special variable `$OVwWebServer`. This variable will be substituted with the name of the system from which the Launcher was loaded.

- Access

  This is a list of user roles that have access to this action. If a user does not belong to a group that has access, the user will not see the list item that invokes this action in their Launcher window. If the access statement is not present, all valid users can access this action. The user roles values correspond to entries in the user roles file. For example, `NetworkAdmin`. See "User Authorization File" on page 488.

- Window

  The Window statement specifies the characteristics of the window into which the URL will be loaded. If the WebWindow statement is not present, the URL will be loaded into an unnamed full web browser window.

  The Window definition has the following components:

1460
A.

— Window name

This is a name for the window to allow window reuse by targeting a named window. The window name is a string of alphanumeric characters and underscores; it may not include blanks. If a new window is desired every time the URL is loaded, a blank window name (" ") may be given.

— Type (full, intermediate, or limited)

Type specifies the type of the window and determines which features it supports. If no type field is present in a window block, `full` is assumed. The values are:

— `full`, all window elements present and user configurable.

— `intermediate`, directories and menubar off, all other window elements present and user configurable.

— `limited`, all window elements off but user configurable.

— Toolbar (on or off)

— Location (on or off)

— Status (on or off)

— Scrollbars (on or off)

— Resizable (on or off)

— Width (integer value)

— Height (integer value)

Following is a sample of the action block.

```
Action printsession
{
     URL "/OvCgi/printsession.exe";
     WebWindow "OvPrintSession" {
          Type full;
          Toolbar off;
          Status off;
     }
}
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0208
3740
Doc:

Error Log File

The Launcher error log records internal errors from the Launcher. You can use the output from this file when discussing a problem with the HP Response Center or HP support personnel.

The Launcher error log file is located in:

Windows: `install_dir\www\logs\launcher\error_log`

UNIX: `$OV_WWW/launcher/error_log`

The error log contains the following information:

- Date
- Host
- User
- Session
- Reason or error

The error log file continues to grow without bounds. You need to watch the size of this file and truncate it as needed.

If the error log file does not give you sufficient information for troubleshooting, you can set a parameter in the URL for **ovlaunch.exe** that will enable more in-depth error logging on a session level. See "Troubleshooting Web Components" on page 613 for more information. The parameter is:

```
http://sysname:3443/OvCgi/ovlaunch.exe?Debug=/tmp/file
```

Language Selection

The Launcher and the Web applications started from the Launcher execute under a particular language, such as English or Japanese. The language used by the Launcher and the Web applications is based on the following:

- The language specified by the user when the security is enabled.
- The language specified by the user through the URL.
- The language specified by the browser.

Once a session is started, the language selection cannot be changed without restarting the browser with a different language.

J.458
A

Language Selection When Security is Enabled Security is enabled via the session configuration file. When security is enabled, the user is presented with a login page listing the languages available for the session under the `[Options]` button. This list represents the languages supported by the Launcher and other installed products that integrate into the Launcher. The languages presented in `[Options]` is based on the contents of the `locales.installed` file. This file is located in:

Windows: *`install_dir`*`\www\conf\locales.installed`

UNIX: `/etc/opt/OV/share/www/conf/locales.installed`

This file contains a list of locales for which the Web applications have been localized. For instance, if the Japanese NNM has been installed, this file will contain an entry for English and for Japanese, for example:

```
en

ja
```

This file can be modified by a developer or administrator. When an HP OpenView web application has been localized to a language not listed in this file, a locale entry should be added to this file. Refer to the *HP OpenView Windows Developer's Guide* for details on syntax.

Language Specified Through the URL The language for a session can be specified when the `ovlaunch.exe` URL is specified. This is done through the CGI parameter `AcceptLang`. This language specification will take precedence over the browser language specification, but can be overridden if security is on and the user chooses a different language on the login page. If security is not on, the login page will come up in the language specified by the `AcceptLang` parameter. For example:

`http://`*`mysystem`*`:3443/OvCgi/ovlaunch.exe?AcceptLang=ja`

Language Specified Through the Browser When security is not enabled, the Launcher uses language specified through the browser. For instance, if the browser has been configured to run in English, the Launcher will execute in English.

Java Parameters File

There are some Java parameters that you can modify to control Launcher appearance. You change these parameters by modifying the APPLET block in the following file, located on the management station at:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0209
Doc. 3740

Windows: *install_dir*\www\htdocs\C\nnm\launcher\browser.html

UNIX: $OV_WWW/htdocs/$LANG/nnm/launcher/browser.html

The Java parameters that you can modify are:

- background
- foreground
- activeTabColor
- inactiveTabColor
- treeBackground
- treeForeground
- treeConnectingLineColor
- displayActiveHelp
- activeHelpLines
- fontName
- fontStyle
- fontSize
- displayInFrame

1.456
A

HP OpenView Network Presenter

The HP OpenView Network Presenter is a Java-based applet that connects to NNM for the purpose of displaying maps. It provides multiple views of map data on a management station from any system with a web browser that supports Internet Explorer or Netscape Navigator.

NOTE Refer to the "Supported Configurations: Supported Web Browsers" section of the NNM Release Notes for specific information about supported web browsers.

The Network Presenter communicates with the management station to get registration information, map data, and map object data. It provides read-only access to the map data and has dynamic updates to reflect the changes that occur on the management station. You can navigate through the map views, select and obtain status on symbols, and launch other web applications on the selected objects via the Network Presenter.

Starting the Network Presenter

You must start an NNM session on the management station for each map that you want available through the web, as described on page 485.

You can invoke the Network Presenter through the Launcher using either of the following tabs:

`Objects` tab, then choose `Networks:IP Network`

`Tools` tab, then choose `NNM:Network Presenter`

Alternatively, you can enter the URL for the Network Presenter:

`http://`*`hostname`*`[:`*`port`*`]/OvCgi/jovw.exe?[MapName=`*`mapname`*`&ObjectName=`*`selectionname`*`]`

On UNIX operating systems, you must specify port number `3443`. Ona Windows operating system, no port number is required. The `MapName` and `ObjectName` fields are optional.

The `MapName` field specifies which map to open. The `ObjectName` field specifies what object to show initially. Refer to the *OvWebURLIntro* reference page in NNM's online help (or UNIX manpage) for more information.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0210
3740
Doc:

NOTE When starting the Network Presenter directly from the URL, you lose the session information that the Network Presenter would have if it were started from the Launcher, including language information.

If a *mapname* is not specified in the URL used to start the Launcher, Network Presenter attempts to connect to an NNM session running with the default map. If there is no NNM session running with the default map, the Network Presenter displays an error message that says the map was not found.

If a *mapname* is specified in the URL, the Network Presenter attempts to connect to an NNM session on the management station with an open map called *mapname*. If there is no NNM session running on the management station with this map open, the Network Presenter displays an error message that says the map was not found.

If you close the NNM session or open a new map, the Network Presenter session attached to that NNM session is ended. The Network Presenter displays a dialog box informing the users that NNM is closing its map.

By default, the Launcher will start the Network Presenter with the `default` map displayed. To make a map other than `default` available to the Network Presenter, modify the `jovw` Web Launcher Registration File (WLRF) that specifies in the URL portion which map to open. See "Listing Multiple Maps in the Launcher" on page 508 and "Launcher Registration File" on page 494 for information.

The Network Presenter Window

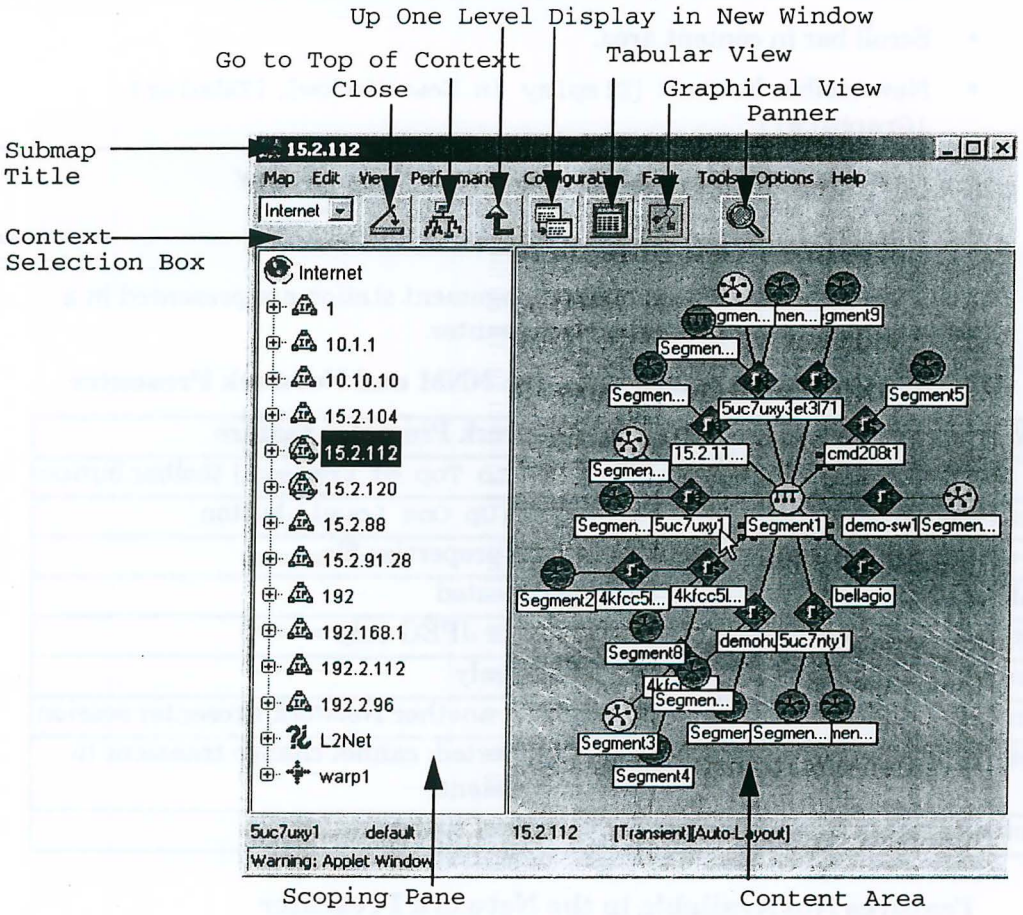
The Network Presenter window has the following components:

- Submap title
- Menu bar
- Context selection box
- Toolbar
- Content area
- Scoping pane

1.454
A.

- Status bar

Figure 14-3 **Network Presenter Window**



Network Presenter versus NNM on a Management Station

There are some differences in the functionality and presentation of information between the Network Presenter and NNM on a management station.

Features in the Network Presenter

Following are features in the Network Presenter that are not available in NNM on a management station.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0211
3740
Doc:

- Context selection box to choose among the highest-level views.
- Scoping pane.
- Tabular view of data.
- Scroll bar in content area.
- New toolbar buttons: `[Display in New Window]`, `[Tabular]`, `[Graphical]`
- New menu items: `Up One Level`, `Top of Hierarchy`

Features That Differ in the Network Presenter

Some features from NNM on a management station are presented in a different format in the Network Presenter.

Table 14-1 Differences in Features Between NNM and Network Presenter

NNM Management Station Feature	Network Presenter Feature
`[Go to Root]` toolbar button	`[Go to Top of Context]` toolbar button
Parent toolbar	Use `[Up One Level]` button
App-defaults file	Java properties file
Symbol labels	Truncated
Background graphics	GIF or JPEG only
Inner shapes	GIF only
Open map	Start another Network Presenter session
Persistent and transient submaps	Supported; cannot change transient to persistent
Automatic layout	Cannot turn on or off

Features Not Available in the Network Presenter

The following features in NNM on a management station that are not available in the Network Presenter.

- `Map Description` dialog box.
- `Submap Properties` dialog box.
- `Locate Submap` dialog box.
- Home submap.
- `Symbol Properties` dialog box.
- Snapshots.

1.452
A

- Symbol enhancements (flashing, transparent, alerts, etc.).
- Menu collapsing.
- Symbol, submap editing.
- Invoking executable symbols.

Interaction Between NNM on the Management Station and the Network Presenter

Since the Network Presenter cannot do editing, the Network Presenter does not influence what happens to NNM on the management station; however, changes in the current session on the management station are dynamically reflected in the content area and scoping pane of the Network Presenter as appropriate. You will see changes in the content area if the submap that is displayed on the management station changes. You will see changes in the scoping pane if that level of hierarchy is displayed. Changes are not dynamically reflected in open dialog boxes.

Configuring the Network Presenter

You can modify the Network Presenter Registration Files (NPRF) to configure certain aspects of the Network Presenter.

The NPRFs are located on the management station at:

Windows: *install_dir*\www\registration\jovw\c*.*

UNIX: /etc/opt/OV/share/www/registration/jovw/$LANG

The format of the Network Presenter Registration Files (NPRF) closely follows the syntax and constructs of the HP OpenView Application Registration File (ARF). Refer to the online manual *Creating and Using Registration Files* for general information about Application Registration files. Refer to the *NetworkPresenterRegIntro* reference page in NNM's online help (or the UNIX manpage) for specific information about creating or editing the NPRF files.

You can add entries to the Action block to specify your own applications to be called when the Network Presenter is launched. You can also change the WebWindow properties in the Action block to control some aspects of the appearance of the Network Presenter (see "Components of the WLRF" on page 494 for sample contents of a registration file). You can add pull-down menus, toolbar buttons, and popup menus that operate on selected objects.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0212
3740
Doc:

Configuring Security for the Network Presenter

There are two levels of security for the Network Presenter.

- The `session.conf` file, described earlier in this chapter.
- The `ovw.auth` and `ovwdb.auth` files, described next.

The Network Presenter allows role-based, restricted access to menu items that have action blocks that contain access statements. See the *Action Block* description on page 496 for more information.

Authorization Files The `ovw.auth` and `ovwdb.auth` files specify which users are allowed access to which management stations. These files are located on the management station at:

Windows: *`install_dir`*`\conf\ovw.auth`

`install_dir``\conf\ovwdb.auth`

UNIX: `$OV_CONF/ovw.auth`

`$OV_CONF/ovwdb.auth`

Each of these files contain instructions for their use.

Using Symbol Registration Files and Bitmaps

Symbol registration files used by the Network Presenter are the same as those used by NNM on a management station. Therefore, if a symbol definition is added for NNM on a management station, it also appears in the Network Presenter. Symbol registration files are located in:

Windows: *`install_dir`*`\symbols\%LANG%`

UNIX: `$OV_SYMBOLS/$LANG`

See the *OVwRegIntro* reference page in NNM's online help (or the UNIX manpage) for more information about creating or editing symbol registration files.

The graphic files for the symbols, themselves, are stored in two places. One directory used by NNM on the management station (see page 664), and one directory used by NNM's web-based interface. The web-based interface requires GIF files. Other additional graphic file formats are supported on the management station. If you create your own GIF files, place a copy in each location.

1.450
A.

The Network Presenter loads its bitmaps in GIF format from the directory:

Windows: *install_dir*\www\htdocs\bitmaps

UNIX: $OV_WWW/bitmaps

TIP

If you can see a symbol on the management station, but cannot see it over the web interface, check the Contrib directory (see page 74) for the convertBitmaps.ovpl script which walks through each graphic in the management station's symbol graphic directory and ensures that a corresponding GIF file exists or is created in the web interfaces's symbol directory.

Symbols in the web-based interface have the same appearance as in NNM on a management station; however, the symbol labels do not scale based upon the size of the label. Instead, a long label is truncated to fit the space available.

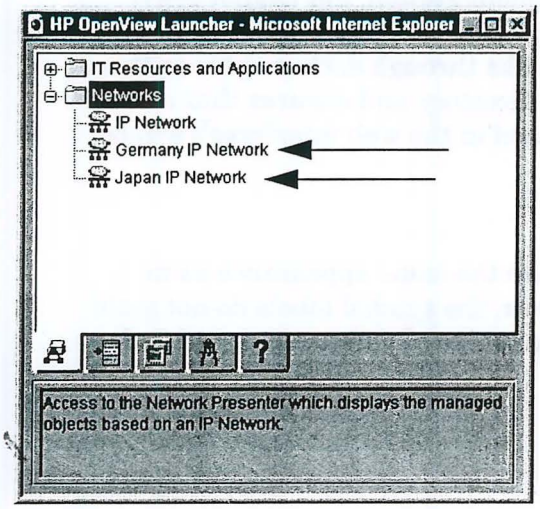
RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0213
3740

Listing Multiple Maps in the Launcher

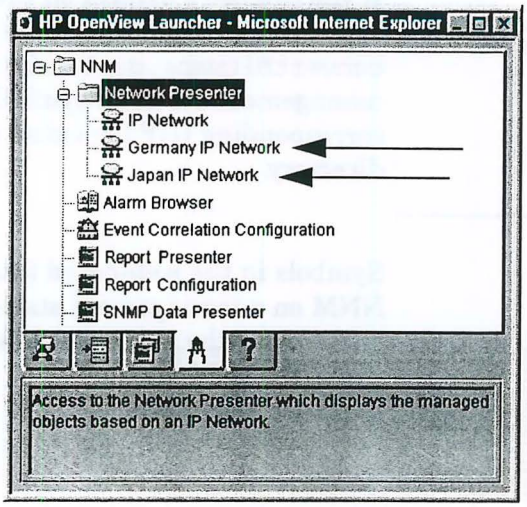
You can modify the Launcher registration file for the Network Presenter so that each of your custom maps is listed.

Figure 14-4 Listing Multiple Maps in the Launcher Window

Custom Maps Added to Object View Tab



Custom Maps Added to Tools Tab



For each map, you must make additions to the `List` and `Action` blocks of the following file:

- Windows: *`install_dir`*`\www\registration\launcher\C\jovw`
- *UNIX:* `$OV_WWW_REG/launcher/$LANG/jovw`

Open this file and read the instructions provided for more information. See also the *LauncherRegIntro* reference page in NNM's online help (or the UNIX manpage) for specific information about creating or editing the WLRF files.

On the management station, there must be a non-web based version of NNM running for each map that will be accessible from the Network Presenter. For example, if you want your team to be able to access the Germany map and the map showing your operations in Japan, you must start NNM on the management station with your Germany map displayed and start another instance of NNM on the management station with the Japan map displayed.

1448
A.

SNMP Data Presenter

The SNMP Data Presenter displays results of operations that present tabular or textual data for managed SNMP nodes selected from the map.

You can use the SNMP Data Presenter even if there is no NNM session running on the management station. The SNMP Data Presenter accesses NNM's Application Registration Files (ARFs) to retrieve information about menu structure and actions, executes the command on the management station, and displays the results in the web browser.

The SNMP Data Presenter displays configuration, performance and fault information. Here are a few examples:

- Interface status.
- SNMP authentication failures.
- TCP connections.
- IP Network addresses.
- IP Routing tables.
- IP ARP cache table.
- System information.
- SNMP trap recipients.

To start the SNMP Data Presenter, select the target node in the content area of Network Presenter and then select one of the following:

- `Performance:SNMP Data Presenter`
- `Configuration:SNMP Data Presenter`
- `Fault:SNMP Data Presenter`

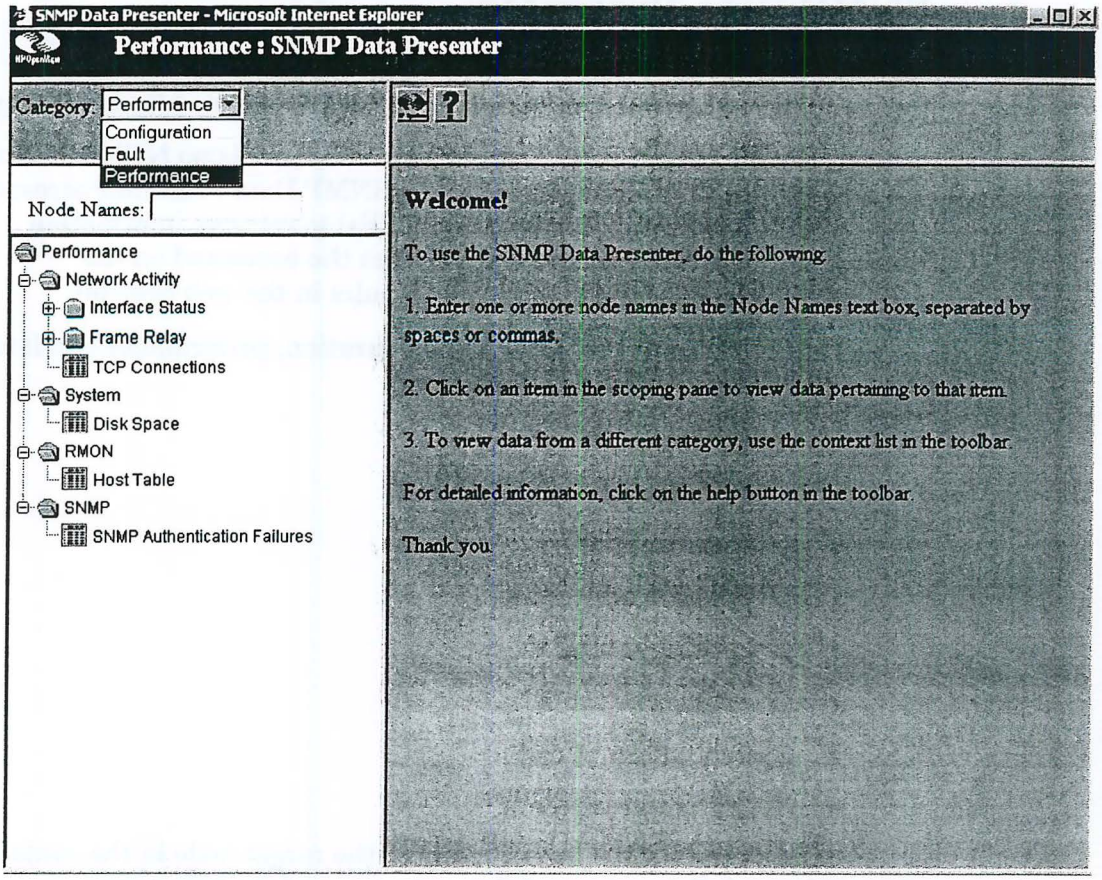
To start the SNMP Data Presenter from the Launcher, select:

- `Tools` tab, then `NNM:SNMP Data Presenter`

RQS nº 03/2005 - C.
CPMI - CORREIO
Fls. Nº 0214
3740
Doc:

The SNMP Data Presenter window is shown in Figure 14-5.

Figure 14-5 SNMP Data Presenter Window



Scoping Pane Content Pane

When accessed from the `Tools` tab, the scoping pane contains categories and actions in a tree format. You can click on the category items to expand them and then click on an action to execute that action. You can also use the Category pull-down.

The results of an action are shown in the content area. A link at the bottom of this area allows you to display a new web browser window with the currently displayed information. This allows for easy comparing of data.

1.446
A.

Configuring the SNMP Data Presenter

The SNMP Data Presenter uses NNM's Application Registration Files (ARFs) and the Application Builder. Because of this, you can execute the same SNMP monitoring operations as you do in NNM, and add new operation commands to the menu structure with Application Builder.

See NNM's online manual, *Creating and Using Registration Files,* for details about editing application registration files (ARFs). See "Using the MIB Application Builder" on page 443 for more information about the Application Builder feature.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0215
3740
Doc:

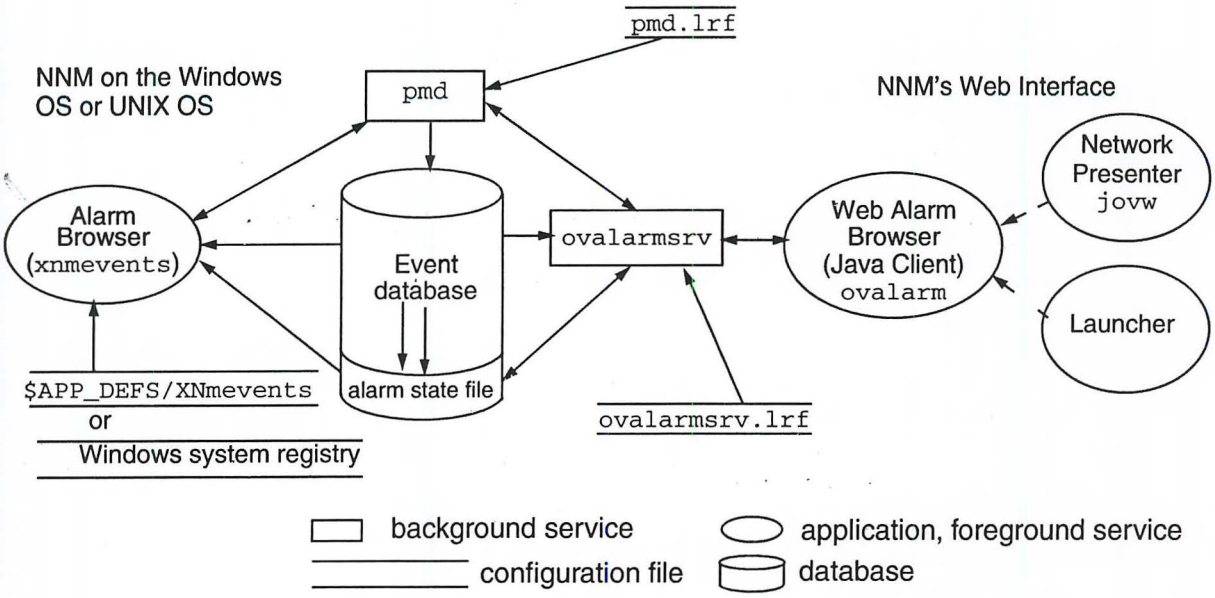
Alarm Browser

The Alarm Browser presents alarm data via the web interface. Through the Alarm Browser, you can filter alarms and take actions on specific alarms. All alarms are global to all web users, as are the acknowledge, delete, change category, and change severity functions.

The web-based Alarm Browser service, `ovalarmsrv`, is started by `ovstart` when you start an NNM session on the management station.

Figure 14-6 illustrates the relationship and data flow between the Alarm Browser application on a management station and the web-based Alarm Browser.

Figure 14-6 Relationship Between the Two Alarm Browsers



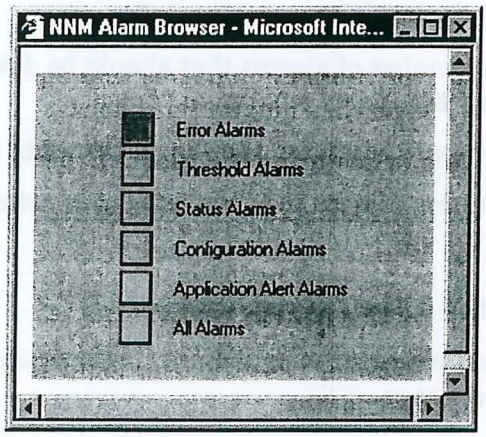
You access the Alarm Browser using one of the following methods:

- In the Launcher, select the `Tools` tab, then select `NNM:Alarm Browser`

1444

- In Network Presenter, select the `Fault` menu, then select `Alarm Browser`.

Figure 14-7 Web-Based Alarm Browser's Category Window



Using and Configuring the Alarm Browser

You can use the Alarm Browser to perform the following:

- Acknowledge/Unacknowledge alarms.
- Move alarms to a different category.
- Assign alarm severities.
- Filter alarms.
- Delete alarms.
- Examine alarm details to find correlated events.

To move an existing alarm message to a different category. Select the alarm that you want to recategorize. Then select `Actions:Change Category` from the menu bar. Refer to the online help if you need more information.

This change affects only the selected alarms. Future alarms of the same type will continue to be posted in the old category's list.

You can configure an alarm to activate your web browser to a specific URL. See "Launching Specific Views or URLs from Alarms" on page 340 for more information.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0216
3740
Doc:

See Chapter 12, Customizing Events: Doing It Your Way, for configuration options:

- Setting the maximum size of the event database (default 16 MB).
- Setting the maximum number of alarms in the Alarm Browser's state file (default 3500).
- Setting the number of alarms that should be deleted each time the state file reaches maximum capacity.
- Copying or restoring the Alarm Browser's state file.
- Assigning alarms to other categories and creating new alarm categories.

Security for the Alarm Browser

The Alarm Browser uses the user login security mechanisms, described earlier in this chapter.

1-442
A.

Event Reduction

Event reduction is the process by which the relationship between events is identified. Once identified, a smaller number of new events providing higher information content can be generated. This simplifies the task of diagnosing network faults. There are three event reduction strategies that are configured and working within NNM. You can access the configuration windows for two of them over the web:

- "ECS Correlations" on page 360
- "Correlation Composer Correlators" on page 386

There are several ways to access these event correlation features. For more information, from any submap:

- Select `Toos:HP OpenView Launcher`.
- Select the `[?]` tab.
- Click `Tasks`, `Event Correlation Management`.

  Read the information under *Accessing the Event Correlation Configuration Windows*

For information about the NNM event reduction strategies, see Chapter 11, "Event Reduction Capabilities: Getting to the Root Cause," on page 351.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0217
3740
Doc:

Reporting Interface

The web Reporting interface is a graphical user interface that is available through a web browser. The Reporting interface consists of:

- Report Configuration-- create, modify, and view report schedules.
- Report Presenter-- view reports.

You can access the Report Configuration in one of the following ways:

- From NNM on a management station, select the `Options:Report Configuration` menu item.
- From Network Presenter, select the `Options:Report Configuration` menu item.
- From the Launcher, select the `Tools` tab, and expand the NNM category. Double-click on `Report Configuration`.
- From your browser, specify the following URL:

  `http://`*`hostname`* `[:`*`port`*`]/OvCgi/RptConfig.exe`

  You need to specify a port if you are running NNM on a UNIX machine.

You can access the Report Presenter in one of the following ways:

- From NNM on a management station, select the `Tools:Report Presenter` menu item.
- From Network Presenter, select the `Tools:Report Presenter` menu item.
- From the Launcher, select the `Tools` tab, and expand the NNM category. Double-click on `Report Presenter`.
- From your browser, specify the following URL:

  `http://`*`hostname`* `[:`*`port`*`]/OvCgi/RptPresenter.exe`

  You need to specify a port if you are running NNM on a UNIX machine.

The NNM Analysis and Reporting interface will be displayed in your browser window.

3.440
A-

Refer to the online manual *Reporting and Data Analysis with HP OpenView NNM* and the web online help for more information.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0218
Doc: 3740

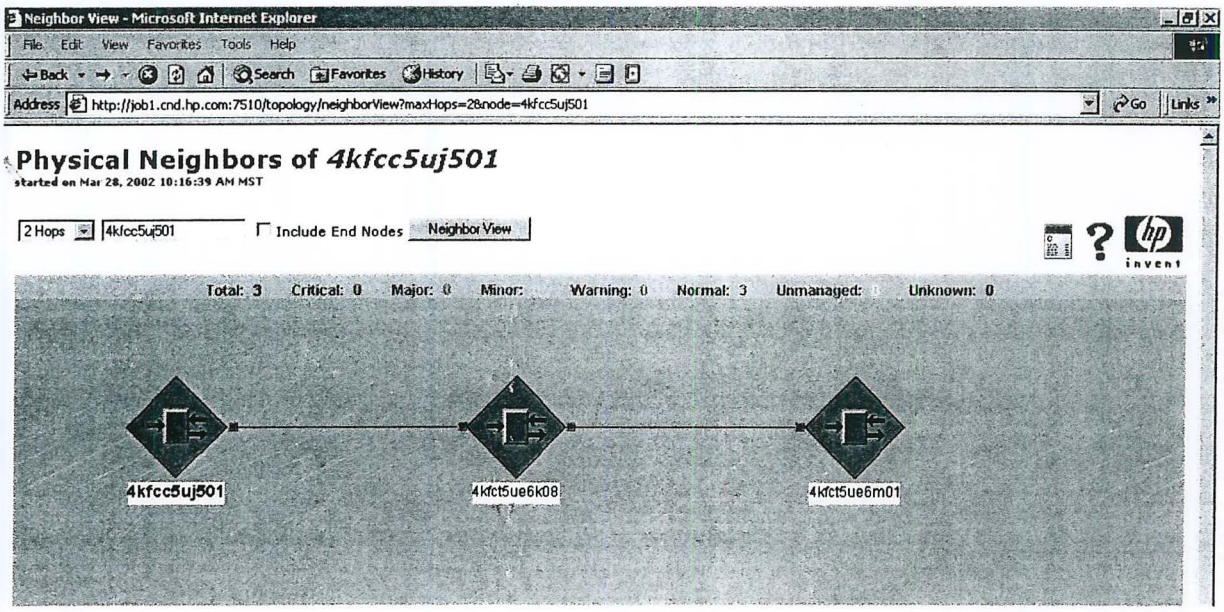
Additional Views

NNM presents several different views of discovered nodes. NNM's Neighbor view, Path view, Node view, Cisco Discovery Protocol view (CDP view), Station view, Internet view, and Port-Address Mapping capabilities show topology views that supplement NNM's map views.

Neighbor View

The Neighbor view shows you a graphical representation of the selected device and the connector devices related to it, within a specified number of hops of the selected device.

Figure 14-8 Neighbor View Example

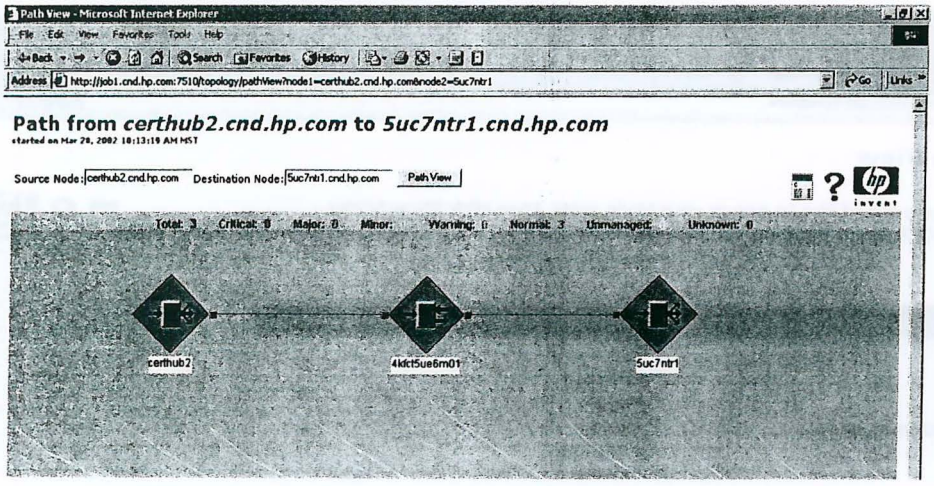


1438
A

Path View

The Path view shows you a graphical representation of the path between two nodes. NNM calculates the shortest path between the source and destination nodes from information contained in the topology database.

Figure 14-9 Path View Example

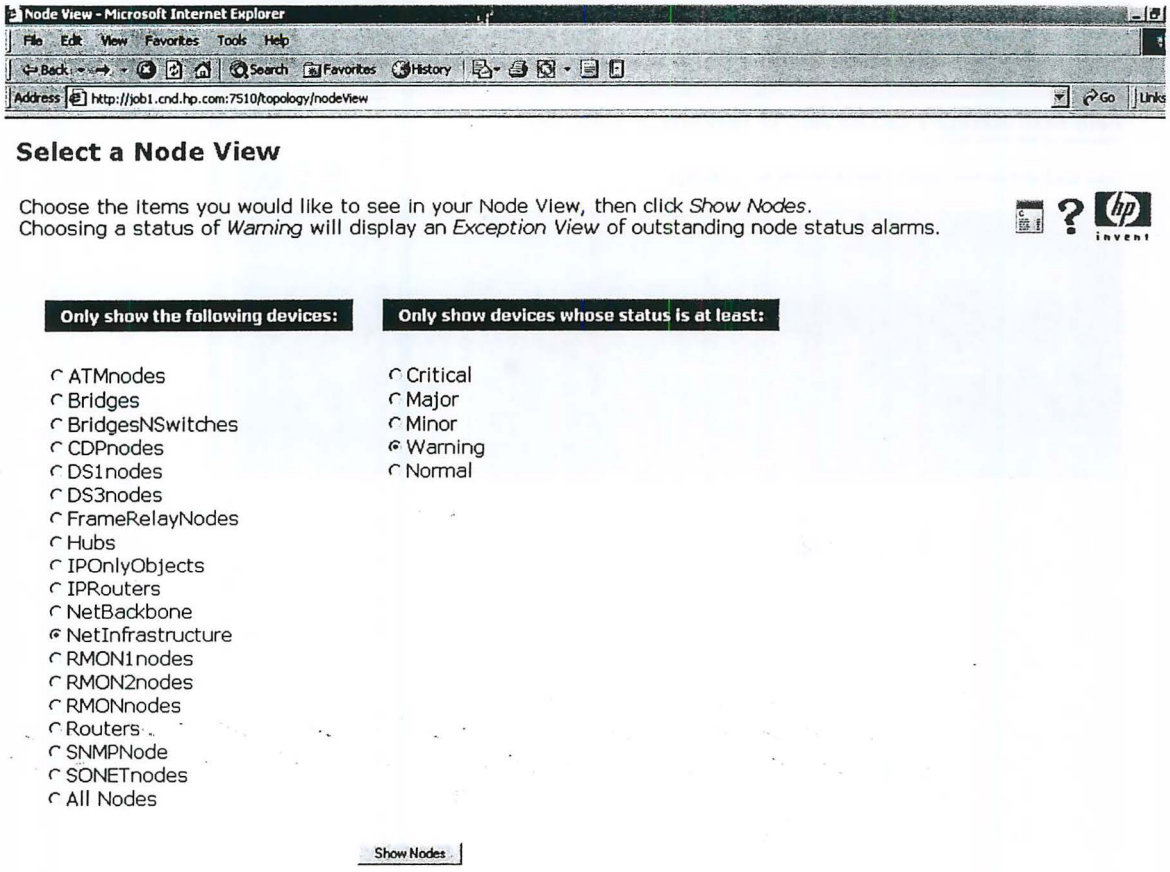


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0219
3740
Doc:

Node View

The Node view creates a visualization of a set of nodes and shows how they are connected. To create a visualization, use the NNM `Tools:Views->Node` menu item. The `Node View` interface contains device types and device status selections as shown in Figure 14-10.

Figure 14-10 Selecting a Node View



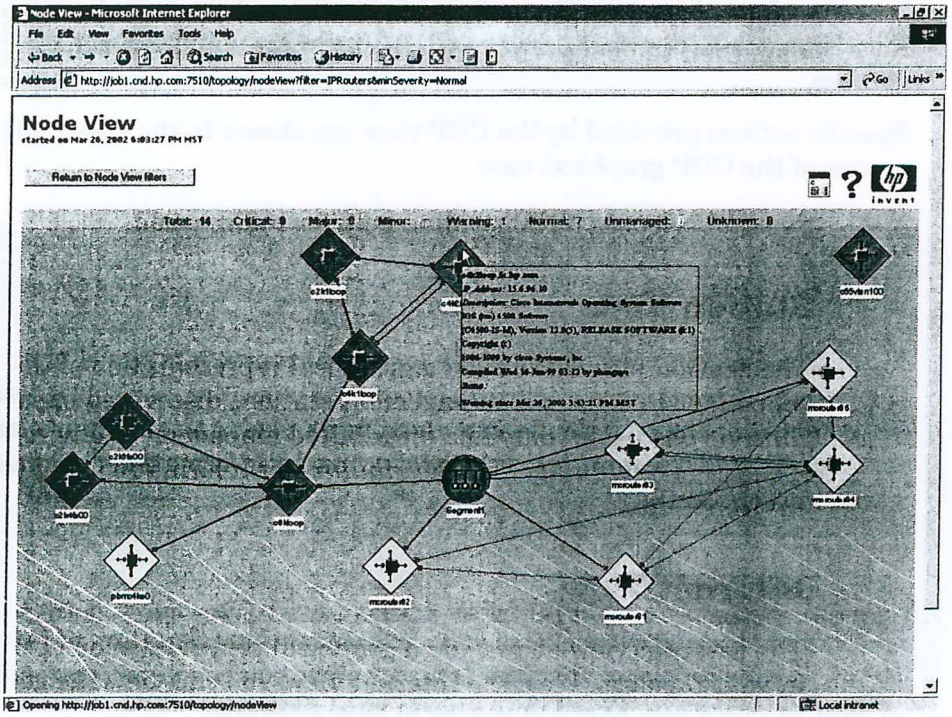
Device selection relies on filters contained within the `filters` file. This is the same file that contains filters such as discovery filters and DHCP filters. The filters file is found in the following locations:

- Windows: *`install_dir`*`\conf\C\filters`
- *UNIX:* `$OV_CONF/C/filters`

J.436
A.

For detailed information about how to develop a filter, refer to *A Guide to Scalability and Distribution*.

Figure 14-11 Node View Example



When working with Node view, placing your mouse over a node displays additional information about the node, such as the hostname, IP address, model number and version, system location, and system contact, subject to availability. Single-clicking allows you to zoom in and zoom out on the display. Double-clicking a node shows the node's attributes from the `ovtopodump` command.

CDP View

Cisco Discovery Protocol (CDP) is a Cisco-proprietary protocol that enables the gathering of information about the types of devices in the network, the links between those devices, and the number of interfaces within each device. It runs on Cisco-manufactured devices, including routers, bridges, access servers, and switches.

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0220
Doc: 3740

You can view the CDP connectivity of your network by selecting `Tools:Views->CDP` from NNM, the HP OpenView Launcher, or from the Network Presenter. The `Tools:Views->CDP` menu item presents a graphical view of all the CDP nodes in the NNM topology. If a CDP node is currently selected on the map, then the discovery of CDP nodes branches from this node. If you do not have any nodes selected on the map, then the nodes that pass the CDP filter will start the discovery process.

Specific actions provided by the CDP view are shown in the upper left corner of the CDP graphical view.

See *CDP View* in NNM's online help for information.

Station View

The Station view shows you a graphical representation of the NNM collection stations and management stations discovered in your topology. This view is useful only in a distributed management environment. See *A Guide to Scalability and Distribution* for information about distributed environments.

Internet View

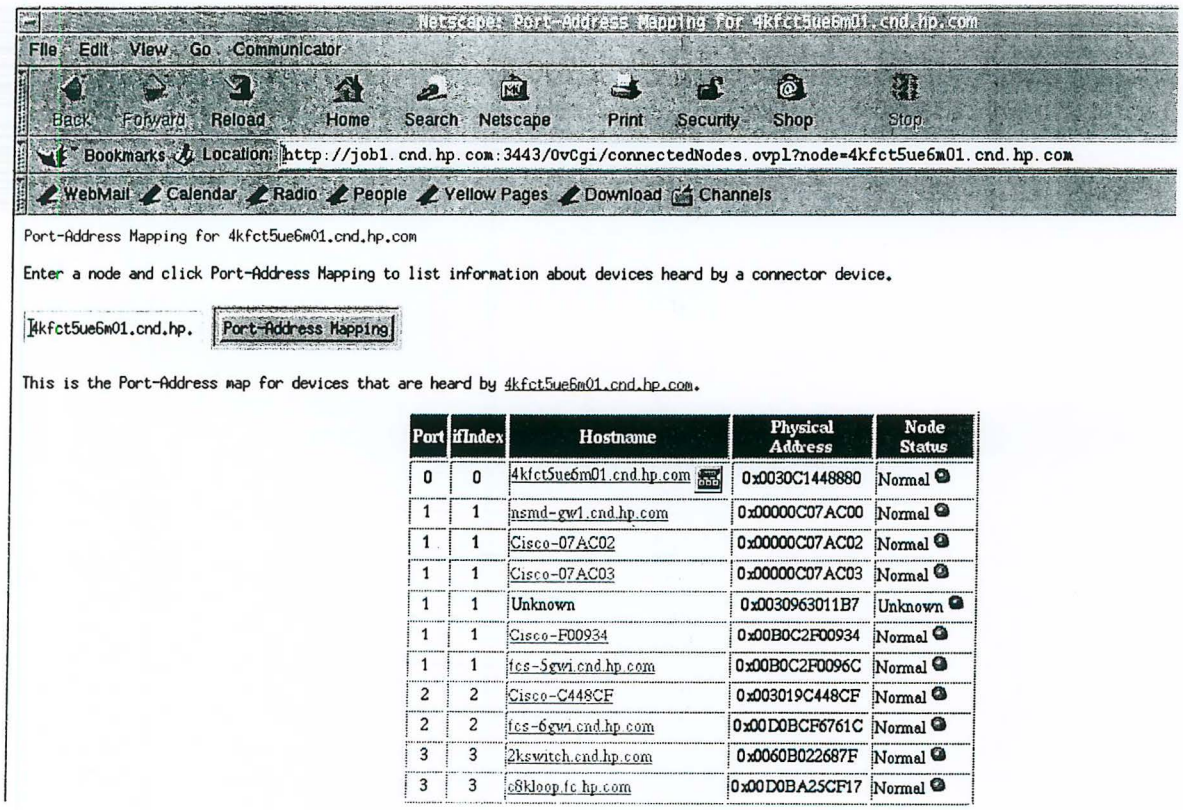
The Internet view shows you a graphical representation of the networks in your topology. With the Internet view, you can view the general status of your network and locate problems in your network.

Port-Address Mapping

By selecting a node and using the `Tools:Port-Address Mapping` menu item you'll see a table of all devices connected to the selected node. The menu item works for most devices that support the *Transparent Forwarding Database MIB* or the *Bridge MIB*.

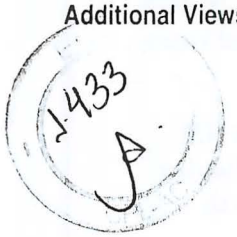
In Figure 14-12 the user selected device `4kfct5ue6m01` from the NNM map, then used the `Tools:Port-Address Mapping` command to display a table of all of the devices connected to the selected node along with information associated with these connected devices.

Figure 14-12 Example of Port-Address Mapping Table



Port	ifIndex	Hostname	Physical Address	Node Status
0	0	4kfct5ue6m01.cnd.hp.com	0x0030C1448880	Normal
1	1	nsmd-gw1.cnd.hp.com	0x00000C07AC00	Normal
1	1	Cisco-07AC02	0x00000C07AC02	Normal
1	1	Cisco-07AC03	0x00000C07AC03	Normal
1	1	Unknown	0x0030963011B7	Unknown
1	1	Cisco-F00934	0x00B0C2F00934	Normal
1	1	fcs-5gw1.cnd.hp.com	0x00B0C2F0096C	Normal
2	2	Cisco-C448CF	0x003019C448CF	Normal
2	2	fcs-6gw1.cnd.hp.com	0x00D0BCF6761C	Normal
3	3	2kswitch.cnd.hp.com	0x0060B022687F	Normal
3	3	c8kloop.fc.hp.com	0x00D0BA25CF17	Normal

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0221
3740
Doc:


J.433

1.432
A.

15 Maintaining NNM

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0222
3740
Doc:

1.431
A

This chapter gives you ideas and suggestions for maintenance tasks that, when performed on a regular basis, can help keep Network Node Manager running more smoothly and without errors.

Included are tasks for:

- Daily maintenance, including checking running services, checking disk space, and trimming files (page 527).
- Weekly tasks, including backing up NNM, cleaning up databases, and monitoring polling performance (page 531).
- Monthly tasks, including obtaining the latest patch releases and updating licensing requirements (page 533).
- Yearly tasks, including evaluating the latest product release (page 534).
- Other maintenance tasks that will help your NNM installation run smoothly (page 535).

For information about maintaining NNM's data warehouse, see the online manual *Reporting and Data Analysis with HP OpenView Network Node Manager*.

1.430

Daily Tasks

You may wish to perform the following tasks on a daily basis.

Check Running Services

Each day you should check to see that all the required services (processes) are running. It is possible that a service has gotten "hung" or did not restart after a backup.

To check on the status of services use the `ovstatus` command. See the *ovstatus* reference page in NNM's online help (or the UNIX manpage) for command options.

If you encounter a service that fails on a regular basis and you cannot find a cause, refer to the service's reference page in NNM's online help (or the UNIX manpage) for more information. You can also use the Event Configuration feature to automatically restart the service whenever it fails. In the `Event Configuration` dialog box, open the `OpenView: OV_DaemonTerminated(.1.3.6.1.4.1.11.2.17.1.59180100)` event configuration and make the following entry in the `Command for Automatic Actions` field: `ovstart $4`.

Check Disk Space

You should check the available disk space on a daily basis. This will ensure that you have enough space to store collected data and to perform a backup.

To check available disk space:

- Use the `Performance:System->Disk Space` menu item.

  Since this information is generated by an HP enterprise-specific MIB, it is available only from an HP 9000 or Sun SPARCstation running the HP OpenView SNMP Agent software.

  If this menu item is not available, you can use the following:

  Windows: Use Windows Disk Administrator

  UNIX: Use the `df` or `bdf` command. See the appropriate manpage for more information.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0223
3760
Doc:

To regain disk space, you can trim certain files, described next.

Trim Files

Some files can grow large very quickly. This slows the discovery and map generation processes and affects overall system performance.

The NNM Data Warehouse and snmpCollect

NNM pre-configures several data collections for you. NNM exports data from pre-configured data collections as well as collections you have manually configured, to the data warehouse. NNM uses data from the data warehouse to generate pre-configured `General Availability`, `Threshold Violations`, `General Inventory`, and `Ping Response Time/Ping Retries` reports. NNM automatically trims data from the following directories as well as from the data warehouse on a regular basis.

- *Windows:* *`install_dir`*`\databases\snmpCollect\`
- *UNIX:* `$OV_DB/snmpCollect/`

NOTE

Select `Options: Data Collection and Thresholds` to see the list of current data collections. Event information is also exported to the data warehouse and trimmed from the Binary Event Store regularly. NNM automatically trims both collected data and event information to reduce disk usage.

TIP

HP uses trimming options that will satisfy a majority of your requirements. If you need to keep collected data and/or Data Warehouse data for longer time periods, you may need to manually complete the export and trimming functions using the `ovdwtrend` command. See the bulleted items on page 526.

To reduce the rate at which the `snmpCollect` directory fills up all available disk space, do the following:

J.429
A-

- Reduce the polling intervals by using the `Options:Data Collection & Thresholds` operation. This slows the rate at which `snmpCollect` fills up available disk space. In addition, if you want to check fixed thresholds only, do not store the data.
- You can use the `ovdwtrend` command to reduce the size of files residing in the `snmpCollect` directory. For example, you can use the `ovdwtrend -export -delpriorto "2001-12-31 00:00:00"` command to export all new data collected since the last export while trimming snmpCollect data file information dated prior to December 31, 2001. Review the *ovdwtrend* reference page in NNM's online help (or the UNIX manpage) to plan your strategy for trimming files in the `snmpCollect` directory.
- You can use the `ovdwtrend -trim` command to delete SNMP trend data from the NNM data warehouse. For example, you can use the `ovdwtrend -trimpriorto [240]` command to trim data older than 240 hours from the *snmp_reduced_trend* table of NNM's data warehouse. Review the *ovdwtrend* reference page in NNM's online help (or the UNIX manpage) and the online manual *Reporting and Data Analysis with HP OpenView Network Node Manager* to plan your strategy for managing data in NNM's data warehouse.

Removing Reports

NNM automatically generates `General Availability`, `Threshold Violations`, `General Inventory`, and `Ping Response Time/Ping Retries` reports. You should review these reports and remove those reports that are no longer of use. See the online manual *Reporting and Data Analysis with HP OpenView Network Node Manager* for instructions on how to delete reports.

Trace and Log Files

Trace and log files can grow quite large, and should be periodically checked for size.

Tracing, especially in the case of `netmon`, can cause the trace file to grow extremely large (multiple megabytes in size) fairly quickly. If you use tracing, remember to monitor the size of the trace file frequently, and turn tracing off as soon as you are finished. The `netmon` trace file is *install_dir*`\log\netmon.trace ($OV_LOG/netmon.trace)`.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0224
3740
Doc:

J.428 P.

Windows: Run **netmon -MO** to disable polling. Use Notepad to edit the *netmon.trace* file, deleting all lines. Save the file. Then run **netmon -M** to enable polling.

UNIX: **cat /dev/null > $OV_LOG/netmon.trace**

Default Log Files

The log files in *install_dir*\analysis\default\log ($OV_DATABASE/analysis/default/log) are an audit trail of successful transactions since your last backup. These files are required for recovering the database at a point *other than* when the last backup was performed. These default log files are normally present with all relational databases.

If you are not performing backups on a regular basis, these log files could grow without bounds. If you are not concerned about recovering your database, you can remove these files at any time. New log files are constantly generated by your relational database software.

J.427
A.

Weekly Tasks

You may wish to perform the following tasks on a weekly basis.

Back Up NNM

It is a good idea to do a full backup weekly (or as often as required at your site), so that you can restore to a relatively current state in the event of a system failure or a corrupted database. This will also ensure that you have all of the databases and configuration files together.

If you perform backups on a regular basis, you can restore to a relatively current state in the event of a system failure or a corrupted database.

There are a number of other situations when you should back up your NNM files. At a minimum, always do a full backup before starting any of the following tasks:

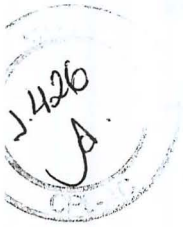
- Upgrading to a new version of NNM.
- Extensively editing or customizing your map.
- After performing initial or expanded discovery, once you think your map accurately reflects your network.

Refer to Chapter 6, "Preserve Your Sanity: Backup and Polling Configuration."

Check Polling Performance

You should periodically check to see how well `netmon` is keeping up with the changes in your network. Use `Performance:Network Polling Performance` to gauge how effectively netmon is collecting network data. If `netmon` is not keeping up with the network changes, you can adjust polling intervals and/or queue sizes (see "Fine-Tuning the Polling Services" on page 193 for more information). You can also consider reducing the size of the managed environment (see "Automatically Limit Your Management Domain" on page 124 for more information).

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0225
3740
Doc:



Check Web Launcher Log Files

The Web Launcher log files record errors and messages from the Launcher. These files will grow without bounds, and should be truncated as needed. The Launcher log files are:

Windows:

```
install_dir\www\logs\launcher\error_log
install_dir\www\logs\login_log
install_dir\www\logs\access_log
```

UNIX:

```
/var/opt/OV/www/logs/launcher/error_log
/var/opt/OV/www/logs/launcher/login_log
/var/opt/OV/www/logs/launcher/access_log
```

1.425
A

Monthly Maintenance Tasks

You should perform the following tasks on a monthly basis.

Check Patch Releases

Check the HP OpenView Web site for the latest patch releases or support updates. These can usually be downloaded at no charge. The HP OpenView Web site is:

`http://openview.hp.com`

Check License Requirements

When running NNM 250, it is a good idea to check to see if you are going to need more licenses. If your network is growing quickly and you have added many nodes, you could run out of available licenses. When the system gets within 25 nodes of the licensed nodes limit, an application alert will be generated. However, you can also check the number of nodes being managed and the number of nodes licensed before this alert is generated. To check the status of licenses:

1. In the NNM main window, right-click on the `Internet` object.
2. Select `Object Properties` from the pop-up menu.
3. Select `IP Map` and click `Edit:Attributes`. This will display the number of nodes that you are licensed for and the number of nodes that are currently being managed.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls.: Nº 0226
3740
Doc:

D.424
A.

Yearly Maintenance Tasks

You should perform the following tasks on a yearly basis.

Evaluate Latest Release

When new releases of Network Node Manager are announced, you should evaluate the new features that are included. If your network management needs have changed, the newest release may have new tools and features that will help you manage your network more effectively.

1.423
A.

Other Maintenance Tasks

There are other maintenance tasks that you may want to perform occasionally to improve the performance of the system, or just to make routine tasks easier.

Enabling/Disabling Automatic Startup

The NNM installation service creates the appropriate files such that the host operating system automatically starts NNM when the management station boots. Occasionally you may want to disable automatic NNM startup, such as during system maintenance when the system is going to be rebooted several times.

On a Windows Operating System:

1. From the Windows `Start` menu, select `Settings:Control Panel`.
2. In the `Control Panel`, click on `Services`.
3. Select `HP OpenView Process Monitor` and choose `Manual Startup`.

On a HP-UX Operating System:

Edit the startup file `/etc/rc.config.d/ov500` and set the variable `START_OV500` to either 1, to start NNM at boot up or to 0, to disable NNM boot at startup. You do not need to reboot the system after making this change.

On a Solaris Operating System:

To disable NNM from starting at boot time, rename the filename `S98netmgt` within the sequencing link `/etc/r3.d/S98netmgt` to a name that begins with a letter other than "S" or "K". To re-enable NNM starting at boot time, change the filename back to `S98netmgt` and reboot.

Customizing the Startup Configuration

The service `ovspmd` starts each service according to instructions it finds in the startup file *`install_dir`*`\conf\ovsuf ($OV_CONF/ovsuf)`. Depending on which services are configured to start, system response

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0227
3740
Doc:

time can be impaired, performance may be slower, and disk space can be rapidly consumed. If you encounter these problems, consider modifying the startup configuration.

Do not edit the `ovsuf` file directly. Instead, configure startup options in the local registration file (LRF) for the individual services. LRF files are then submitted to `ovsuf` through the `ovaddobj` command. Conversely, service startup instructions are disabled from `ovsuf` using the `ovdelobj` command.

Table 15-1 describes each LRF and any options applied as defaults in the LRF. The table does not contain a complete list of options. To learn about all the available options, see the reference page in NNM's online help (or the UNIX manpage) with the particular service's name.

The steps for customizing the startup configuration follow Table 15-1.

Table 15-1 Local Registration Files (LRFs)

LRF	Description
`netmon.lrf`	The LRF for `netmon`, the background service that polls agents to initially discover your network. Default option: `-P` which means that it is started through `ovstart`. You may want to use the following options. Be aware, however, that using these options can affect performance. `-b` *`burstcount`* — Add if you have an unreliable network. This allows you to do multiple pings on a node. `-s` *`seedfile`* — Add when you want the initial map to include specific networks in your administrative domain. `-J` — Add if you have few SNMP agents on your network to accelerate initial discovery.
`ovactiond.lrf`	The LRF for `ovactiond`, the background service that executes configured commands when an event is received. Default option: none.

1.421
A.

Table 15-1 Local Registration Files (LRFs) (Continued)

LRF	Description
ovcapsd.lrf	The LRF for ovcapsd, the background service that discovers Remote DMI nodes, Web-manageable nodes, and Web servers. Default option: none.
ovrepld.lrf	The LRF for ovrepld, the background service that replicates objects.
ovtopmd.lrf	The LRF for ovtopmd, the background service that controls the topology database. Default option: -O which means that it is started through ovstart. Use the -f *filter* option to specify a topology filter and make use of NNM's scalability and distribution feature.
ovtrapd.lrf	The LRF for ovtrapd, the background service that executes configured commands when an event is received. Default option: none.
ovuispmd.lrf	The LRF for ovuispmd, the background service that manages user interface services and distributes relevant ovspmd requests to OVW. Default option: none Use the -t option to change the time period that ovuispmd will wait for commands to complete.
ovwdb.lrf	The LRF for ovwdb, the background service that controls the object database. Default option: -O which means that is started by ovstart. You may want to use the *-n number of objects* option to reduce the amount of memory used by ovwdb when managing large numbers of nodes.
pmd.lrf	The LRF for pmd, the background service that multiplexes and logs events. Default option: none.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0228
Fls. Nº
3740
Doc:

1420

Table 15-1 Local Registration Files (LRFs) (Continued)

LRF	Description
`snmpCollect.lrf`	The LRF for `snmpCollect`, the background service that collects MIB data. Default option: none.

Steps for Customizing the Startup Configuration

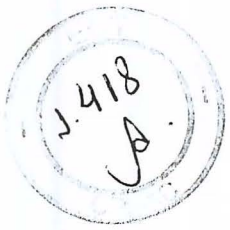
1. Stop NNM.
   a. Exit any currently-running `ovw` sessions.
   b. Run **`ovstop -c`**
2. Create a back-up copy of the service's LRF file.
3. Open the selected service's LRF file in a text editor:
4. Edit the lines that control the behavior you want to change. Save and close the file.
5. Submit the new LRF file with the `ovaddobj` command:

   `ovaddobj $OV_LRF/netmon.lrf`
6. Restart NNM. Run **`ovstart -c`**

1.419
A.

A NNM Services and Files

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0229
3740
Doc:



This appendix describes key services (processes) and files in the operation of Network Node Manager.

Topics covered include:

- Differences between background services and foreground services (page 541).
- How the services interact at NNM startup and during operation (page 547).
- The web application services and how they interact (page 545).

1.417
A.

Services and Files

There are two types of services:

- Background services that run continuously independent of whether ovw is running.
- Foreground services that run while ovw is running.

The interaction among these services are shown in the figures in this appendix. A brief description of each service and file follows. For more information on these services and files, see the reference page in NNM's online help (or UNIX manpage) having the same name as the service you wish to learn about.

Background Services

The following services and files are involved with the startup of NNM.

ovstart	Starts the various services that make up the HP OpenView Network Node Manager product.
ovspmd	Launches and manages all background services. ovspmd interacts with the user commands ovstart, ovstop, ovstatus, ovpause, and ovresume, and performs the appropriate actions on the background services.
ovsuf	Contains the configuration information for ovspmd. Each entry in ovsuf is created by ovaddobj from information in the LRF (Local Registration File).

The following services run in the background during regular operation. All of the following files reside in *install_dir*\bin\ (%OV_BIN%).

httpd	Handles http requests. This is a web server that is provided on the UNIX operating system only.
netmon	Polls SNMP agents to discover your network, and then detects topology, configuration, and status changes in the network.
ovactiond	Receives events from pmd and executes commands.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0230
Doc: 3740

1.416 A

ovalarmsrv	Provides event information to Java-based Alarm Browsers.
ovcapsd	Listens for new nodes and checks them for remote DMI capabilities, web-manageability, and web server capabilities.
ovas	Maintains topology and node status information for NNM Dynamic views.
ovrepld	Responsible for object replication. ovrepld is started only when monitoring remote collection stations in a DIDM environment.
ovrequestd	Executes the reports and data warehouse exports according to a predefined schedule. Once a report is configured, ovrequestd starts executing the exports and the reports.
ovsessionmgr.exe	Manages users' web sessions. ovsessionmgr.exe is started by ovstart.
ovtopmd	Maintains the network topology database. The topology database is a set of files that stores netmon polling status and information about network objects, including their relationships and status. ovtopmd reads the topology database at start-up.
ovtrapd	Receives SNMP traps and forwards them to pmd. ovtrapd also responds to SNMPv2 requests.
ovuispmd	Manages the NNM user interface services and distributes relevant ovspmd requests to each instance of ovw that is running. ovuispmd must be running for ovw to be started, and should be running whenever ovspmd is running.
ovwdb	Controls the object database. The object database stores semantic information about objects.
pmd	Receives and forwards events, and logs events to the event database. pmd also forwards events from the network to other applications that have connected to pmd using the SNMP API.

1.415
A-

snmpCollect	Collects MIB data and performs threshold monitoring. snmpCollect stores the data it collects in the *install_dir*\databases\snmpcollect ($OV_DB/snmpcollect) directory and sends threshold events to pmd.

Foreground Services

This section describes the NNM foreground services that may be running after you execute ovw. All of these files reside in *install_dir*\bin\ ($OV_BIN):

ipmap	Runs under ovw to automatically draw IPX and IP topology maps representing your network.
mibform, mibtable, rnetstat, findroute, rbdf, rnetstat, rping	Commands executed by xnmappmon that enable you to monitor and diagnose problems in your TCP/IP network.
ovw	The service that provides map drawing, map editing, and menu management. When you start the OVW services by executing the ovw command, ovw automatically invokes ipmap, xnmevents, and the other applications, which register to be started by ovw.
xnmappmon	The Application Encapsulator that displays textual results of monitoring operations for managed SNMP objects selected from the map.
xnmbrowser	The Tools:SNMP MIB Browser menu item that enables you to get and set MIB values for Internet-standard and enterprise-specific MIB objects.
xnmbuilder	The Options:MIB Application Builder:SNMP menu item that enables you to build custom screens to manage multivendor MIB objects. The information you define using the MIB Application Builder is stored in registration files and help files using mibform, mibtable, and xnmgraph.
xnmcollect	The Options:Data Collection & Thresholds:SNMP menu item that enables you to configure snmpCollect to collect MIB data from network objects at regular, configurable intervals. The configuration information

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0231
3740
Doc:



	is stored in the *install_dir*\conf\snmpCol.conf ($OV_CONF/snmpCol.conf) and snmpRep.conf configuration files. The collected data are stored in files in the *install_dir*\databases\snmpCollect ($OV_DB/ snmpCollect) directory.
xnmevents	The alarm browser that is automatically invoked by ovw to display events that are being received by pmd. xnmevents reads the *install_dir*\log\xnmevents ($OV_LOG/xnmevents).*username.map* file only at start-up for events that occurred since the last time xnmevents was run. xnmevents reads the event database only at start-up to obtain those pending events. xnmevents also reads trapd.conf to obtain information about how to customize event messages.
xnmgraph	The tool that enables you to graph the results of monitoring operations for managed SNMP objects selected from the map. The results may be real-time or collected historical data.
xnmloadmib	The Options:Load/Unload MIBs:SNMP menu item used to load new Internet-standard or enterprise-specific MIBs into the loaded MIB database.
xnmpolling	The Options:Network Polling Configuration->IP/IPX menu item that updates the polling configuration.
xnmsnmpconf	The Options:SNMP Configuration menu item that enables you to add, delete, and modify SNMP configuration parameters and the netmon status polling interval. The SNMP configuration parameters include community name, set community name, timeout interval, number of retries, and proxy information.
xnmtrap	The event configurator invoked by the Options:Event Configuration menu item that enables you to define enterprise-specific events (traps). You can customize the alarm message displayed through xnmevents when a particular event arrives. You can also specify a command or a batch file that should be executed when

2.413
A.

a particular event arrives. Event configuration changes are stored in the *install_dir*\conf\C\trapd.conf ($OV_CONF/$LANG/trapd.conf) configuration file.

Web CGI Programs

The following programs are CGIs, which access HP OpenView's web applications. See the *OVWebURLIntro* reference page in NNM's online help (or the UNIX manpage) for more information about (*) only. The others are used internally by NNM and listed only for your information.

`jovw.exe` * Starts the Network Presenter.

`jovwreg.exe` Called by the Network Presenter to parse menu information from application registration files registered with the Network Presenter. Also parses symbol and enroll information from registration files registered with ovw.

`nnmRptConfig.exe`* Launches the Report Configuration interface.

`nnmRptPresenter.exe`* Launches the Report Presenter.

`ovalarm.exe`* Launches the Alarm Browser user interface.

`ovlaunchreg.exe` Reads the Launcher registration files (WLRFs), passing input to the Launcher window for display.

`ovlaunch.exe`* Launches the HP OpenView Launcher and opens the user login screen, when `UserLogin` is set.

`ovlogin.exe` Processes the user login screen. Should not be called as a standalone URL.

`ovsessioninfo.exe` Collects session information from the ongoing session.

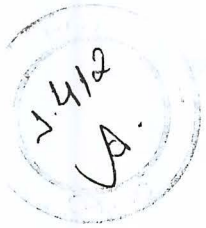
`ovwebdata.exe` Tool for accessing NNM data stores via read-only http queries.

`OvHelp` The NNM 5.0 help CGIs.

`OvWebHelp.exe` The NNM 6.0 help CGIs.

`printsession.exe` Browser-callable URL to present user session information.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0232
3740
Doc:



`snmpviewer.exe` * Launches the SNMP Data Presenter, or displays textual or graphical results of SNMP monitoring operations on your browser.

`webappmon.exe` Application encapsulator used by SNMP Data Presenter.

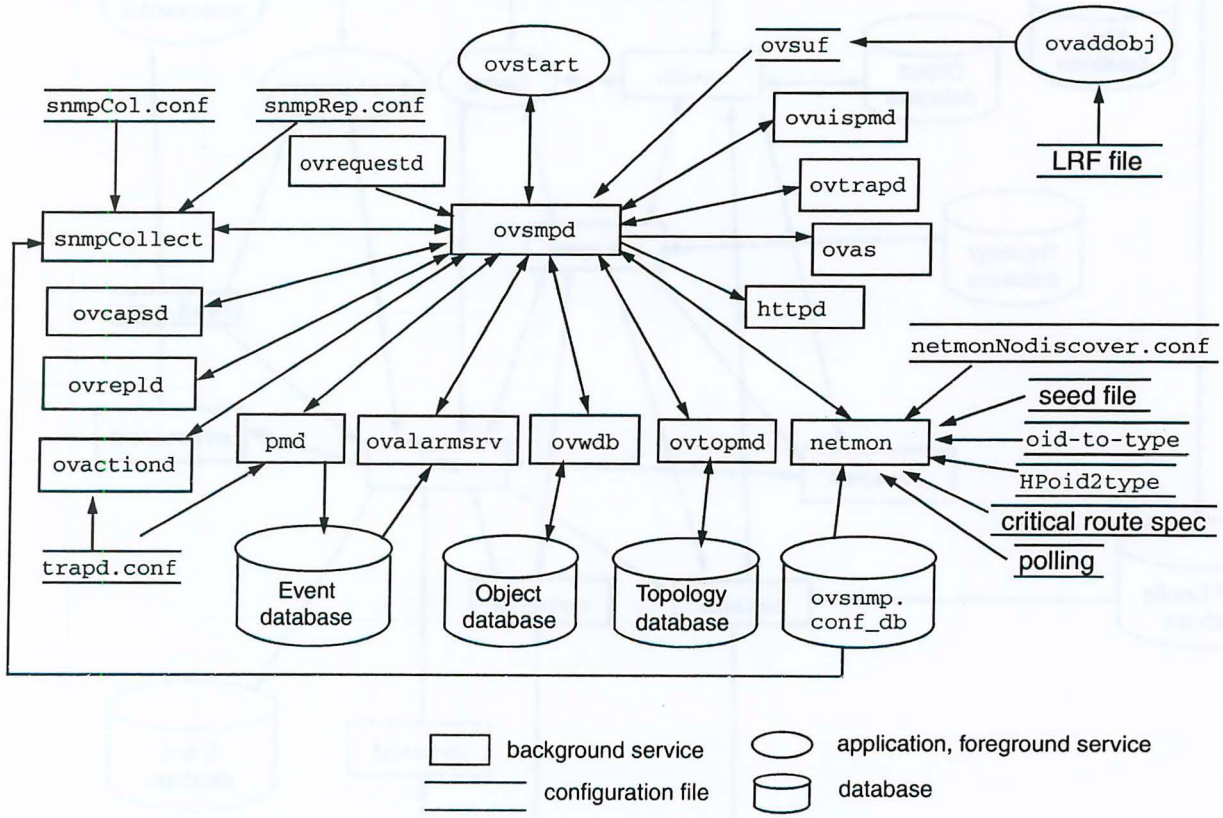
Figure A-4 on page 551 illustrates how the CGI programs interact with NNM's other services.

1.911
A

Behavior of the Services and Files

Figure A-1 shows the interactions and relationships among background services and files at start-up time. The arrows indicate the direction that communication flows.

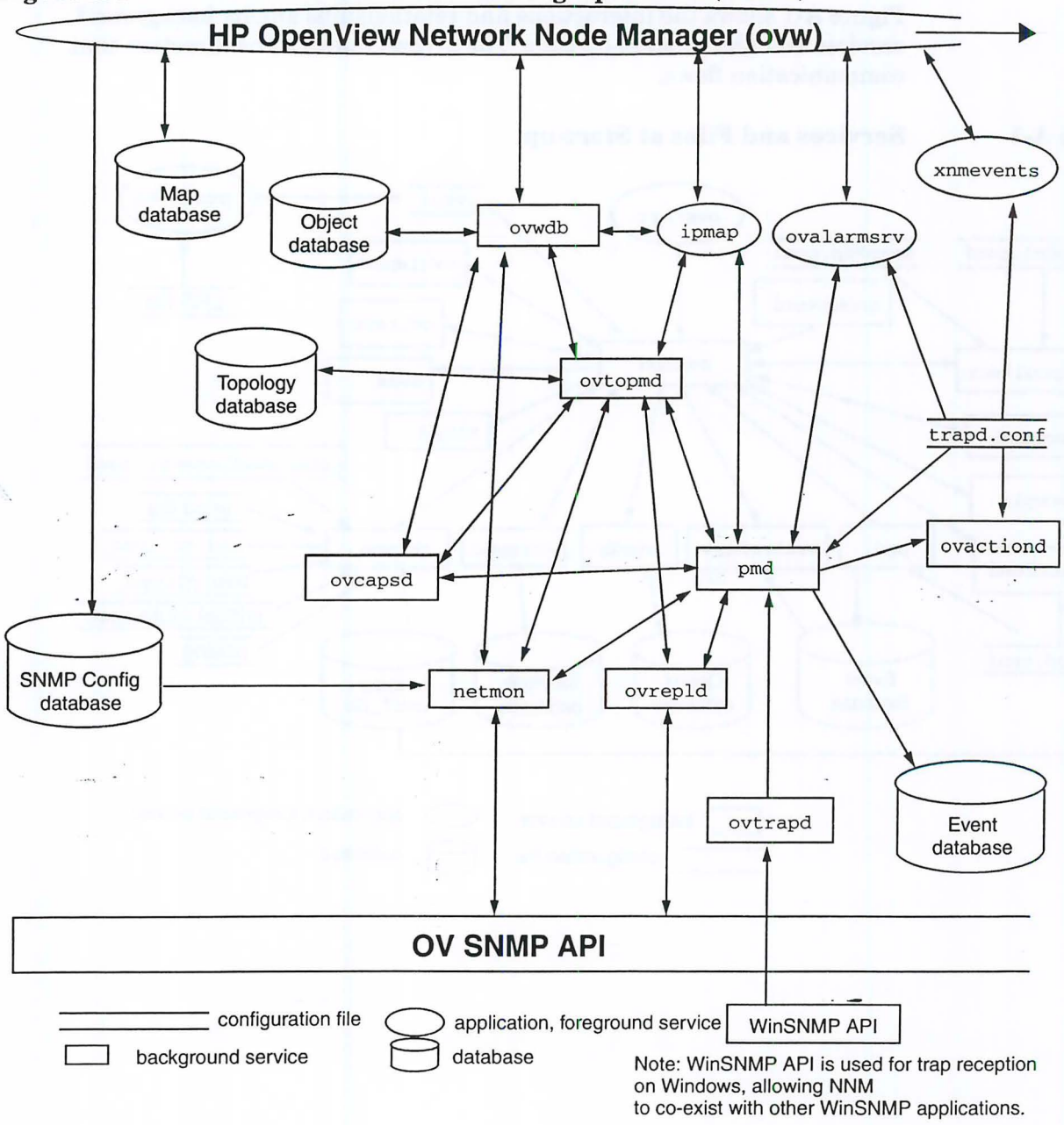
Figure A-1 Services and Files at Start-up



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0233
3740
Doc:

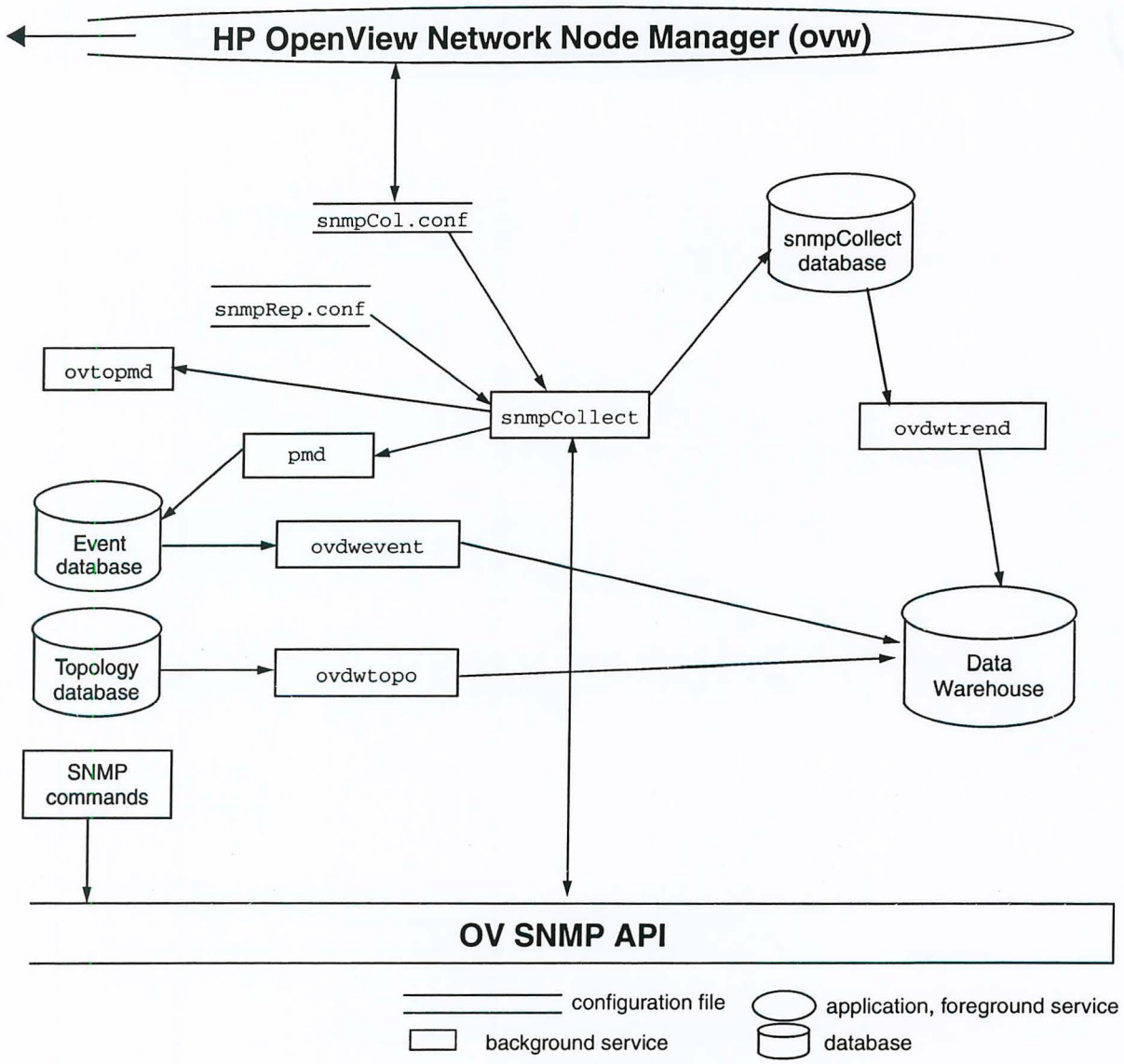
Figure A-2 and Figure A-3 show the interactions and relationships of background services and files during operation. The arrows indicate the direction that information flows.

Figure A-2 Services and Files During Operation (Part 1)



1.409
A

Figure A-3 Services and Files During Operation (Part 2)



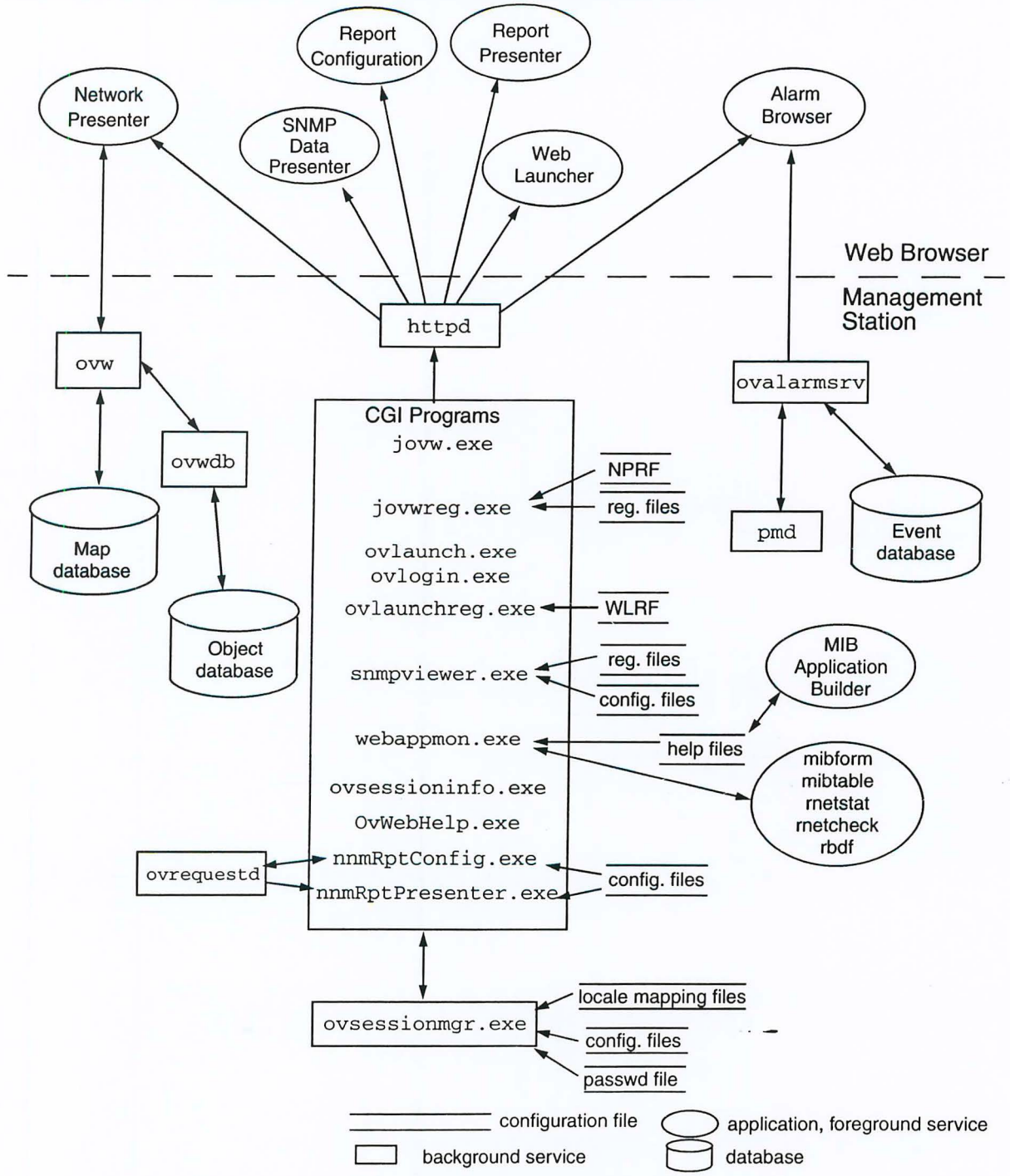
RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0234
3740
Doc:



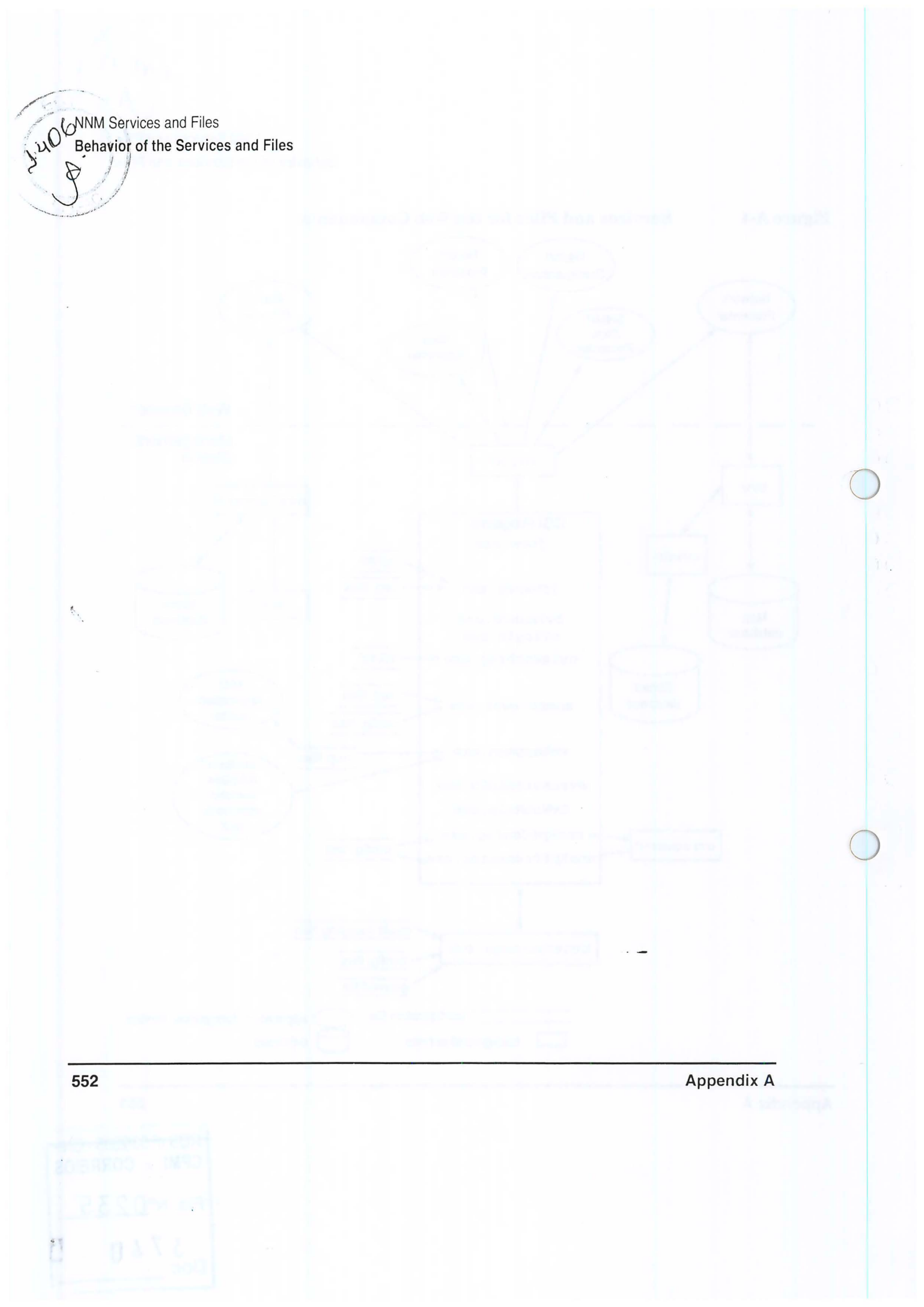
Figure A-4 shows the interactions and relationships among the services and files of the web components.

1407
A

Figure A-4 Services and Files for the Web Components



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0235
3740
Doc:



1.405
A.

B Network Troubleshooting Tools

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0236
3740
Doc:

J 404 A.

Network Node Manager includes many tools for your convenience. This appendix includes brief descriptions of the tools available for your use. For more information about each tool, access the online help within NNM, and search the index for the tool name.

To find out about easily creating your own custom SNMP tools and adding them to the pull-down menu choices, see "Using the MIB Application Builder" on page 443.

The tools in this appendix are organized as follows:

- Tools in NNM on a management station:
  - — Performance tools (page 556).
  - — Configuration tools (page 562).
  - — Fault management tools (page 566).
  - — Miscellaneous tools (page 569).
- Tools in NNM's web applications (page 575).

You can also run a variety of Microsoft diagnostic tools on a management station with a Windows operating system from the NNM menus. These tools will appear depending on whether your computer is a workstation or a server, and whether you have installed the tools on your computer.

The Windows operating system tools are:

- Registry Editor
- Performance Monitor
- Event Viewer
- Windows Diagnostics
- Server Manager
- User Manager
- SMS Properties
- Run SMS

NOTE The Microsoft System Management Server (SMS) does not come with the Windows operating system and must be purchased separately from Microsoft. Consult your Windows operating system documentation for details on using these tools.

1.403
A.

Tools in NNM on a Management Station

The tools discussed in this section are located in the menu structure in NNM on a management station under the `Performance`, `Configuration`, `Fault`, and `Tools` pull-down menus. You simply highlight the node or nodes for which you want to gather information, then select the menu choice. NNM sends the MIB request and displays the responses for you in an easy to read graph, chart, or table.

Map Snapshots

Use `Map:Snapshot` to create a snapshot of a particular map frozen in time. A snapshot displays all persistent submaps showing the state of your network at the time you took the snapshot, including the status and location of all symbols. This may be useful to:

- Compare versions of your network and system map before and after a department is moved to a new building. You can use the snapshot as a reference to ensure that all connections are re-established correctly.
- Troubleshoot a network breakdown by reviewing multiple snapshots of a map showing the progression of the problem. This may give your team clues about the initial cause.

The map must be open with read-write access when the snapshot is created. Snapshots are read-only. You cannot edit a snapshot. However, you can traverse the submaps by double-clicking on symbols, locate objects, and keep an updated selection list for each submap. Only one snapshot may be open at a time. If a snapshot is already opened when you choose to open another snapshot, the previously opened snapshot is closed.

Use the `Map:Snapshot->Delete` command to remove old snapshots in order to free up memory and improve system performance.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0237
3740
Doc:

Performance Tools

Network Activity

Interface Status->Overview Select any node symbol on the map, then use this command to display a variety of information such as interface numbers, name, status, and last status change.

Select any interface symbol on the map, then select this command to display a wealth of information about the interface board.

Interface Status->DS1/E1 Serial Line Status Select a node that supports SNMP and the DS1 MIB, then use this command to list all interface status attributes for the interfaces on the selected node. This command is useful for determining the status of each selected node or interface on the map, which can be used in troubleshooting.

Interface Status->DS3/E3 Serial Line Status Select a node that supports SNMP and the DS3 MIB, then use this command to list all interface status attributes for the interfaces on the selected node. This command is useful for determining the status of each selected node or interface on the map, which can be used in troubleshooting.

Interface Errors->Error Rate Select any number of node or interface symbols on the map, then select this command to display a graph showing the number of bad packets dropped over time on each interface. This command is useful for troubleshooting data transmission problems.

Interface Errors->Error Percentage Select any number of node or interface symbols on the map, then select this command to display a graph comparing the percentage of bad packets dropped to the total number of packets received over time on each interface. This command is useful for troubleshooting data transmissions problems.

Interface Errors->Discard Rate Select any number of node or interface symbols on the map, then use this command to display a graph of the number of packets dropped by the selected node or interfaces for reasons other than errors in the packet over a period of time. This command is useful for troubleshooting data transmission problems.

1401
A.

Interface Errors->Discard Percentage Select any number of node or interface symbols on the map, then use this command to determine the percentage of packets dropped by the selected node or interfaces for reasons other than errors in the packet over a period of time. This command is useful for troubleshooting data transmission problems.

Interface Traffic->Packet Rate Select any number of node or interface symbols on the map, then use this command to display a graph showing the average number of packets successfully sent and received over time on each interface. For example, if you suspect network performance problems, you could monitor SNMP nodes to analyze interface traffic patterns over a period of time.

Interface Traffic->Utilization Select any number of node or interface symbols on the map, then use this command to display a graph that compares the percentage of traffic flowing on each interface as it relates to the overall capacity of the interface over a period of time. This command is useful for troubleshooting interface traffic problems.

Interface Traffic->Throughput Select any number of node or interface symbols on the map, then use this command to display a graph of the number of successful packets sent and received over each interface over a period of time. This command is useful for troubleshooting data transmission problems.

Interface Traffic->Data Rate Select any number of node or interface symbols on the map, then use this command to display a graph of the average number of bytes that are received or transmitted over the node or interface over a period of time. This command is useful for troubleshooting data transmission problems.

Interface Traffic->Avg. Packet Size Select any number of node or interface symbols on the map, then use this command to display a graph of the average size of packets sent or received on the node or interfaces over a period of time. This command is useful for troubleshooting data transmission problems

TCP Connections You can use the `TCP Connections` command to list the TCP Connections table for the remote SNMP nodes you select.

Ethernet (802.3)->Ethernet Errors Use the Ethernet Errors graph to monitor interface error statistics for a node running HP SNMP agent software. The graph is useful for viewing and tracking patterns. For

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0238
Fls. Nº
3740
Doc:

example, if you suspect performance problems, you could monitor HP SNMP agent nodes to analyze the pattern of interface card CRC errors versus frames received over a period of time.

Ethernet (802.3)->Ethernet Traffic Use the Ethernet Traffic graph to monitor interface statistics for a node running HP SNMP agent software.

Frame Relay->Circuit Traffic->Data Rate Select a node or interface that supports SNMP and the Frame Relay MIB, then use this command to display a graph of the average number of bytes that are received and transmitted on the virtual circuit over some period of time. This command is useful for troubleshooting problems with the interface and for assessing the performance of the interface.

Frame Relay->Circuit Traffic->Frame Rate Select a node or interface that supports SNMP and the Frame Relay MIB, then use this command to display a graph of the average number of frames sent and received on the Frame Relay virtual circuit. This command is useful for troubleshooting problems with the interface and for assessing the performance of the interface.

Frame Relay->Circuit Traffic->Avg. Frame Size Select a node or interface that supports SNMP and the Frame Relay MIB, then use this command to list the average frame size of packets sent and received on the Frame Relay virtual circuit. This command is useful for characterizing the type of traffic flowing on the interface.

Frame Relay->Circuit Congestion Select a node or interface that supports SNMP and the Frame Relay MIB, then use this command to display a graph that shows the percentage of Frame Relay Virtual Circuits that indicate forward and backward congestion in the Frame Relay network. This command is useful for characterizing the amount of traffic flowing through the Frame Relay network.

Frame Relay->Circuit Errors Select a node or interface that supports SNMP and the Frame Relay MIB, then use this command to display a graph that shows the percentage of received frames that are dropped, either because of format errors or because the circuit is not active. Data is expressed as a percentage of all received frames. This command is useful for troubleshooting data transmission problems.

1399
A

Frame Relay->Data Link Errors Select a node or interface that supports SNMP and the Frame Relay MIB, then use this command to display a table that shows the data link errors for the selected interface. This command is useful for troubleshooting data transmission problems.

System

CPU Load Use this command to monitor and graph the average number of jobs in the run queue for each of the selected SNMP agent nodes. (Jobs are processes that are running on a system.) The graph is useful for viewing and tracking CPU utilization patterns. For example, you could monitor SNMP agent nodes to analyze the pattern of jobs performed over a period of time. By graphing the CPU load of several nodes, you may discover that some nodes are overworked, while others are underutilized. This information might be useful in determining how to distribute tasks among several nodes.

Since this information is generated by an HP enterprise-specific MIB, it is available only from an HP 9000 or Sun SPARCstation running the HP OpenView SNMP Agent software.

Disk Space You can list the disk space used and available for a remote SNMP agent node.

Since this information is generated by an HP enterprise-specific MIB, it is available only from an HP 9000 or Sun SPARCstation running the HP OpenView SNMP Agent software.

RMON

Segment Utilization Select one or more nodes that support SNMP and the RMON MIB, then use this command to monitor and graph the percent of the segment bandwidth that is currently being utilized. This graph is useful for finding segments that are being overutilized.

Segment Errors Select one or more nodes that support SNMP and the RMON MIB, then use this command to monitor and graph the rate of errors on the segment.

Segment Octets Select one or more nodes that support SNMP and the RMON MIB, then use this command to monitor and graph the rate of 8 byte octets in the segment. This graph is a good indication of the amount of traffic on the segment.

~~RQS nº 03/2005 - CN -~~
CPMI - CORREIOS
Fls. Nº 0239
3740
Doc:

Segment Packet Sizes Select one or more nodes that support SNMP and the RMON MIB, then use this command to monitor and graph the number of packets in six different predefined octet size ranges. This data can give you a breakdown of the packet sizes being transmitted and received on a network segment.

Segment Packet Types Select one or more nodes that support SNMP and the RMON MIB, then use this command to monitor and graph the rate of multicast packets versus broadcast packets.

Host Table Select one or more nodes that support SNMP and the RMON MIB, then use this command to show a table of the traffic patterns per physical address on the segment.

SNMP

SNMP Authentication Failures Select one or more nodes that are HP9000 or Sun SPARCstation systems running the HP OpenView Extensible SNMP Agent software. Then use this command to list the management stations that caused an authentication failure on the selected nodes. Authentication failures occur when a management station sends an SNMP request with an incorrect community name. This command is useful for troubleshooting SNMP authentication failures.

SNMP Traffic Select one or more nodes that support SNMP. Then use this command to monitor and graph the SNMP network traffic to and from selected nodes. This command is useful for comparing the SNMP traffic graph to interface traffic: packet rate graph to determine the percentage of traffic to and from the selected node that is attributed to the SNMP management of the selected node.

SNMP Operations Select one or more nodes that support SNMP. Then use this command to display a summary of the SNMP operations requested of and performed by the SNMP agent on the nodes you select. This command is useful for reporting the total number of operations for the given category that have occurred since the SNMP agent on the selected node was last started.

SNMP Errors Select one or more nodes that support SNMP. Then use this command to display a summary of the SNMP protocol errors detected by the SNMP agent on the nodes you select. This command is

1.397
A-

useful for determining the total number of errors for the given category that have occurred since the SNMP agent on the selected node was last started.

Network Polling Statistics

This command graphs data based on interface status polling and SNMP node polling. This data can tell you how busy the management stations and collection stations are. Refer to A *Guide to Scalability and Distribution for Network Node Manager* for information on management stations and collection stations. The data being graphed is the data collected from the netmon service. The polling activities from the data Collector and other SNMP applications are not being shown in this graph. The polling activity that this graph displays is configured in the `Options:Network Polling Configuration` dialog box and in the `Options: Status Polling` field of the `SNMP Configuration` dialog box.

Graph SNMP Data

Selected Nodes This command graphs data that was previously collected with the MIB Data Collector and allows you to manipulate that data.

Use this command to view collected data on the selected nodes without having to first build an application to do so. This approach is useful when you want to browse the collected data for these nodes. Use this command when you want to graph some data points just once, or when you want to compare different variables across different systems.

For example, if you want to compare load averages to the number of packets on the selected systems and you have not built an application to do so, you can use this command to graph these two variables together.

All This command reads in ALL the collected data from the Data Collector database into its memory. Depending on how much data is stored in the database, displaying the Graph All Collected Data window may take a long time.

Windows Performance Monitor

On Windows operating systems only, use this command to run the Windows performance monitor. If NNM does not recognize the target node as one with a Windows operating system, the `Windows Performance Monitor` item is unavailable on your menu.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0240
3740
Doc:

J.396 A.

Configuration

Network Configuration

Interface Properties Use this command to generate the list of attributes of all the interfaces within a selected node. The list includes information such as name, type, alias, and status.

IP Addresses Use this command to list the IP and link addresses for the selected remote SNMP nodes. This command is useful for determining IP and interface addresses associated with a node without looking through configuration files.

IP Routing Table You can list the routing table information for the remote SNMP nodes you select. This information determines how IP packets are routed on the nodes. Use the `IP Routing Table` command for diagnosing connectivity problems (for example, one node cannot communicate with another).

On UNIX operating systems, this information can be used to determine more efficient routes on the network, to assess the need for explicit routes, and to diagnose connectivity problems. The information you see is real-time data from the node rather than static information from a database.

On UNIX operating systems, if you want to reroute traffic on the network, you can either temporarily change the routing using the `route` command, or permanently change the routing by editing the `netlinkrc` file and rebooting the system. (Routing commands may vary across vendor systems.)

IP ARP Cache You can list the ARP (Address Resolution Protocol) cache table for the remote SNMP nodes you select. The `IP ARP Cache` command is useful for diagnosing connectivity problems because it indicates whether two nodes have a different link address for a third node. The information is real-time data taken from the node rather than static information from the database.

IP Services You can list the services that the remote SNMP-supported nodes you select are configured to support. This information tells you which configured services a node is currently running. The information is real-time data from the node rather than static information from the database.

1.395
A.

For example, if you wanted to know if a node is executing the Telnet server, you could use the `IP Services` command to see if the node is listening with Telnet TCP port number 23.

Cisco Discovery Protocol->Interface Table Select one or more nodes that support SNMP and the CISCO-CDP MIB, then use this command to display device interface information contained in the Cisco Discovery Protocol Interface Table (cdpif). Refer to the `rnetstat` reference page in NNM's online help (or the UNIX manpage) for specific information about information contained in the Cisco Discovery Protocol Interface Table.

Cisco Discovery Protocol->Cache Table Select one or more nodes that support SNMP and the CISCO-CDP MIB, then use this command to display device interface information contained in the Cisco Discovery Protocol Cache Table (cdpcache). Refer to the `rnetstat` reference page in NNM's online help (or the UNIX manpage) for specific information about information contained in the Cisco Discovery Protocol Cache Table.

Cisco Discovery Protocol->Global Table Select one or more nodes that support SNMP and the CISCO-CDP MIB, then use this command to display device interface information contained in the Cisco Discovery Protocol Global Table (cdpglobal).Refer to the `rnetstat` reference page in NNM's online help (or the UNIX manpage) for specific information about information contained in the Cisco Discovery Protocol Global Table.

Cisco VLAN Membership Table Select one or more nodes that support SNMP and the CISCO-VTP MIB, then use this command to view the Cisco VLAN port membership table. There is one row for each bridge port that is assigned to at most one VLAN. Ports with more than one VLAN are not represented. An entry may be created and deleted when ports are created or deleted via SNMP or the management console on a device.

Bridge MIB->Base Table Select one or more nodes that support SNMP and the BRIDGE MIB, then use this command to view a table that contains information describing the basic bridging functionality provided by this device, regardless of the bridging protocol the device supports.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0241
3740
Doc:

Bridge MIB->Base Port Table Select one or more nodes that support SNMP and the BRIDGE MIB, then use this command to list all the ports on the device and basic information about each port.

Bridge MIB->Spanning Tree Table Select one or more nodes that support SNMP and the BRIDGE MIB, then use this command to view a table that contains configuration information about the Spanning Tree Protocol implementation.

Bridge MIB->Spanning Tree Port Table Select one or more nodes that support SNMP and the BRIDGE MIB, then use this command to view a table that contains information maintained by every port about the Spanning Tree Protocol state for that port.

Bridge MIB->Transparent Forwarding Table Select one or more nodes that support SNMP and the BRIDGE MIB, then use this command to view a table that contains information about unicast entries for which the bridge has forwarding and/or filtering information. This information is used by the transparent bridging function in determining how to propagate a received frame.

Bridge MIB->Transparent Port Table Select one or more nodes that support SNMP and the BRIDGE MIB, then use this command to view a table that contains transparent bridging protocol information about each port.

Bridge MIB->Static Table Select one or more nodes that support SNMP and the BRIDGE MIB, then use this command to view a table that contains filtering information configured into the bridge by (local or network) management, specifying the set of ports to which frames received from a specific port and containing a specific destination address are allowed to be forwarded.

Frame Relay-> Properties Select one or more nodes, then use this command to list information for all selected nodes or interfaces on a selected node.

Frame Relay->Virtual Circuits Select one or more nodes, then use this command to list the virtual circuit properties for all interfaces on the selected node. You can use this information for verifying the information related to each interface on the selected node.

1.393
A.

ATM Properties Select one or more nodes, then use this command to list the common attributes for the selected nodes or for all interfaces on a selected node.

DS1/E1 Serial Line: Properties Select a node or interface, then use this command to list the attributes for the selected nodes or for all interfaces on a selected node.

DS3/E3 Serial Line: Properties Select a node or interface, then use this command to list the attributes for the selected nodes or for all interfaces on a selected node.

SONET/SDH: Properties Select a node or interface, then use this command to list the attributes for all interfaces on the selected node. You can use this list to verify the information about each interface on the selected node.

System: Information

Choose this command to display information about the selected system, such as system location and system contact.

System->HP-UX SAM

On HP-UX systems only, this command starts up a tool — System Administration Manager (SAM) — that enables you to administer and configure HP-UX systems. Although SAM is started on the remote HP-UX node that you selected, it appears in a window on your local node.

SNMP: Trap Recipients

Choose this command to list the management stations (by IP address) that are configured to receive events (traps) from the selected node.

Windows Registry Editor

Use this command to run the Windows operating system Registry Editor. If NNM does not recognize the target node as one with the Windows operating system, the `Windows Registry Editor` item is not on your menu.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0242
3740
Doc:

Fault Resolution Tools

Alarms

Choose this command to list all the undeleted alarms for a selected node. The `Alarms` command is particularly useful when you know that a specific node is at least partially responsible for certain problems (for example, connectivity or performance problems). Use this command to:

- Filter the selected alarms based on severity, time, source, message, or event type.
- Browse incoming alarms and alarms contained in the event database.

You must have a read-write Alarm Browser window to perform the following: Acknowledge, Unacknowledge, Delete, Assign Category, and Assign Severity.

Network Connectivity

Poll Node Choose this command to update the open map and database with information about selected objects. It is useful for diagnosing communication problems between NNM and the node. This command performs the following operations on node objects that are selected and managed:

- Provides information about the node.
- Updates the status of the selected node objects.
- Checks for exceeded thresholds and logs any events into the event log.

Status Poll Use this command to update the open map and database with status information about selected objects. This command performs a status poll on IP and IPX node objects that are selected and managed. It is useful for diagnosing communication problems between NNM and the node.

Capability Poll Use this command to check nodes for remote DMI devices, and web management and web server capabilities. If the node supports DMI, `ovcapsd` will register with that node for NNM to receive DMI events.

ECT 1.391 A

Ping Choose this command to send one ICMP Echo packet per second from the local management station to a remote node. (The transmitted packet size is 64 bytes.) The output displays the number of packets sent and lost, and the round-trip times.

Remote Ping Choose this command to check connectivity between two remote nodes by transmitting packets between the nodes. You must first select a source and destination node. The source node selected must be an HP 9000 or Sun SPARCstation running the HP OpenView SNMP Agent software.

Trace Route Select a node or interface, then use this command to track the route that packets follow from the NNM management station to the selected node. Trace Route utilizes the IP protocol time to live field and attempts to elicit an ICMP `time exceeded` response from each gateway along the path to the selected node or interface.

Locate Route via SNMP Choose this command to locate specific IP routes between selected nodes. The command does two things:

- Lists all the intermediate nodes in the dialog box.
- Highlights the route on the network map.

The `Locate Route` command is useful for diagnosing connectivity problems (for example, cases where one node cannot communicate with another).

Path View Select 2 nodes, then use this command to display a description of the path between the two selected nodes. If you select only one node, NNM uses the local node as the source node. Show Path lists the node name or interface name, the IP address, the physical address and the status of each node or interface along the path. This command is useful for diagnosing connectivity problems.

Test IP/TCP/SNMP

Choose this command to check the connection between the local management station and another node or nodes. This command is useful for diagnosing network connection problems by testing networking protocols.

The TCP test uses a telnet port to check TCP connectivity. This test may fail since some workstations with the Windows operating system may not have a telnet server installed.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0243
3740
Doc:

Interface Status

Interface Status->Overview Select any node symbol on the map, then use this command to display a variety of information such as interface numbers, name, status, and last status change.

Select any interface symbol on the map, then select this command to display a wealth of information about the interface board.

Interface Status->DS1/E1 Serial Line Status Select a node that supports SNMP and the DS1 MIB, then use this command to list all interface status attributes for the interfaces on the selected node. This command is useful for determining the status of each selected node or interface on the map, which can be used in troubleshooting.

Interface Status->DS3/E3 Serial Line Status Select a node that supports SNMP and the DS3 MIB, then use this command to list all interface status attributes for the interfaces on the selected node. This command is useful for determining the status of each selected node or interface on the map, which can be used in troubleshooting.

Interface Errors

Interface Errors->Error Rate Select any number of node or interface symbols on the map, then select this command to display a graph showing the number of bad packets dropped over time on each interface. This command is useful for troubleshooting data transmission problems.

Interface Errors->Error Percentage Select any number of node or interface symbols on the map, then select this command to display a graph comparing the percentage of bad packets dropped to the total number of packets received over time on each interface. This command is useful for troubleshooting data transmissions problems.

Interface Errors->Discard Rate Select any number of node or interface symbols on the map, then use this command to display a graph of the number of packets dropped by the selected node or interfaces for reasons other than errors in the packet over a period of time. This command is useful for troubleshooting data transmission problems.

Interface Errors->Discard Percentage Select any number of node or interface symbols on the map, then use this command to determine the percentage of packets dropped by the selected node or interfaces for reasons other than errors in the packet over a period of time. This command is useful for troubleshooting data transmission problems.

Frame Relay Circuits Select a node or interface that supports SNMP and the Frame Relay MIB, then use this command to display a graph that shows the percentage of received frames that are dropped, either because of format errors or because the circuit is not active. Data is expressed as a percentage of all received frames. This command is useful for troubleshooting data transmission problems.

Frame Relay Data Link Select a node or interface that supports SNMP and the Frame Relay MIB, then use this command to display a graph that shows the data link errors for the selected interface. This command is useful for troubleshooting data transmission problems.

Windows Event Viewer

Use this command to run the Windows operating system Event Viewer. If NNM does not recognize the target node as a one with the Windows operating system, the `Windows Event Viewer` item is not on your menu.

Windows Diagnostics

Use this command to run the Windows operating system diagnostics tools. If NNM does not recognize the target node as a one with the Windows operating system, the `Windows Diagnostics` item is not on your menu.

Miscellaneous Tools

Report Presenter

Use the `Report Presenter` command to access the NNM Report Presenter. The NNM Report Presenter is a presentation interface for viewing reports. Available report categories include device inventory, availability, performance, and exceptions.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0244
3740
Doc:

Remote Power On

New computers may have an energy-saving feature that automatically reduces the power after a specific idle time limit is reached. Some computers include a hardware-based feature in their network interface card that can be accessed to restart the computer remotely. Use `Remote Power On` to revive computers that respond to AMD Corporation's MagicPacket (`remotepoweron`) utility.

Highlight network devices on your map and select `Tools:Remote Power`. Then select one of the following.

Power On This command broadcasts the `remotepoweron` command for the highlighted device or devices. If the network interface card is capable of responding to the `remotepoweron` command, the computer will begin the power up process.

Power On and Ping This command broadcasts the `remotepoweron` command for the highlighted device or devices. NNM then waits a specified amount of time to allow for the power up process to complete, then issues a `ping` command to determine if the power-up was successful.

Note that this tool generates a lot of network traffic due to the broadcast.

TIP

Create a batch file that you can use to issue the `remotepoweron` command for all IP/IPX addresses of all devices on your network that contain hardware capable of responding to the `remotepoweron` command. Currently there is no way for NNM to detect which devices do or do not have this capability. You need to compile the list yourself.

For more information, refer to the *remotepoweron* reference page in NNM's online help (or UNIX manpage).

Terminal Connect

Choose this command to create a terminal emulator on a local system that is connected to a remote system using a network virtual terminal protocol.

Telnet (hpterm) On UNIX operating systems only, you can use this command to open an HP terminal window to telnet to other systems.

1.387
A.

Telnet (xterm) On UNIX operating systems only, you can use this command to open an X terminal window to telnet to other systems.

Unused IP Addresses

The `Unused IP Addresses` command will display a list of IP addresses from networks NNM is managing that have not been recently heard from. You can configure the time in which a node must be heard from using the `Options:Network Polling Configuration:IP` command. In the Status Polling configuration area, check the `Delete nodes if down for` check box and specify a value.

HP OpenView Launcher

This command enables you to use the HP OpenView Launcher. The `HP OpenView Launcher` is an integration point with the HP OpenView web applications. It provides login security for HP OpenView applications and a central point from which you can launch all of the applications that have been integrated into the HP OpenView Web.

Port-Address Mapping

Select a node. Then use this command to display a table of the nodes that are connected to the node that you selected.

Data Warehouse

Export Topology This commands exports information from topology database to the data warehouse.

Export Events This command exports information from the event database to the data warehouse.

Export Trend Data This commands exports information from the trend database to the data warehouse.

Web Browser

Management Page Some servers can provide an alternative to their Home Page that is called the Management Page. The Management Page is semi-private, in that an individual wanting to browse it must know its URL.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0245
3740
Doc:

Choose this command to launch your web browser on the Management Page of the target node, provided that NNM recognizes the target node as an HTTP server that provides an alternative to its Home Page (`Attribute isHTTPmanaged = true`). If the target node is not recognized as such a server, this command remains grayed out.

Server Home Page Choose this command to launch your web browser on the Home Page of the target node, provided that NNM recognizes the target node as an HTTP server (`Attribute isHTTPsupported = true`).

If you choose the `Home Page` command with no node selected on the map, then it will open the default home page of your own web browser. If a target node is selected, then the command will open the target node's default home page.

SNMP MIB Browser

Use the MIB Browser as a general-purpose diagnostic tool to access the Management Information Base (MIB) on agents. The MIB is a collection of objects (management information) that encompasses configuration and status values.

Use the SNMP MIB Browser to:

- Learn what MIBs are available for building diagnostic applications that monitor MIB values.
- Query and display MIB objects that you use infrequently.
- Troubleshoot problems with other MIB commands.

For more information, refer to "SNMP MIB Browser" on page 412.

Views

Neighbor Select a node, then use this command to display a graphical representation of the selected device and the nodes connected to it, within a specified number of hops. The number of hops defaulted to two, however you can use the drop down list to modify the number of hops.This command is useful for understanding relative device connectivity and for diagnosing the root cause of abnormal device status alarms.

Path Select two nodes, then use this command to display a graphical representation of the path between the two selected nodes. If you select only one node, NNM uses the local node as the source node. The

1.385

`Views:Path` command lists the node name or interface name, the IP address, the physical address and the status of each node or interface along the path. This command is useful for diagnosing connectivity problems.

Node The `Views:Node` command opens a menu that you can use to configure a topology view based upon the various filters available. A second selection criteria is the status of the managed devices that pass the selected filter.

CDP The `Views:CDP` command presents a graphical view of all the managed nodes supporting the CDP (Cisco Discovery Protocol) MIB. If a CDP node is currently selected on the map, then the discovery of CDP nodes will branch from this node. If you do not have any nodes selected on the map, then the nodes that pass the CDP filter will start the discovery process.

Station The `Views:Station` command shows you a graphical representation of the NNM collection stations and management stations discovered in your topology. This command is useful in a distributed management environment.

Internet The `Views:Internet` command shows you a graphical representation of the networks in your topology. This command lets you see the general status of your network, locate problems in your network, or proactively monitor all of your networks.

NOTE If you have not purchased and enabled the HP OpenView NNM Extended Topology product for UNIX operating systems, the OSPF Backbone, All HSRP Groups, All VLANs, and IPv6 Network views described below do not function as shown, but instead open a view that tells you how to purchase, install and enable Extended Topology.

OSPF Backbone For UNIX operating systems, the `Views:OSPF Backbone` command shows you a graphical and tabular representation of an OSPF area. By default, Extended Topology launches your web browser to the OSPF backbone (area 0.0.0.0).

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0246
3740
Doc:

All HSRP Groups For UNIX operating systems, the `Views:All HSRP Groups` view presents both a graphical display and a table of HSRP groups. From the All HSRP Groups view you can open two other view, the HSRP Group Detail view and the HSRP Node Detail view.

All VLANs For UNIX operating systems, the `Views:All VLANs` command presents a table that lists all the VLANs in your network. From this table, you can link to two other VLAN views: a VLAN membership view and a switch centric view. You can use the VLAN membership view to observe the switches whose ports participate in a specific VLAN. You can use the switch centric view to observe a selected switch and the VLANs that it participates in.

IPv6 Network For UNIX operating sytems, the `Views:IPv6 Network` command shows you a graphical representation of an IPv6 network, including routers and end nodes that support IPv6. Lines connect IPv6 nodes to the prefix group or groups they logically connect to. From the IPv6 Network view, you can open two other views, the IPv6 Node Detail view and the IPv6 Prefix Groups view.

DMI Browser (Desktop Management Interface)

Some HP personal computers have a Desktop Management Interface (DMI) that you can query to determine the computer's status, configuration, and available resources. You can create queries for a single device, or a group of devices, using the DMI commands.

NOTE

Make sure the computers you select support Remote DMI. Select the `isRDMISupported` attribute from the `Find By Attribute` dialog box to see a list of HP PCs that support Remote DMI. For more information, see "DMI Events (Indications)" on page 327 and "DMI Browser" on page 417.

NNM uses Intel's DMI Explorer to browse DMI information. Refer to the DMI Explorer's online help for more information.

1383
A

Tools in NNM's Web Applications

NNM's web applications also contain tools for managing your network. Some of the tools are accessed from tabs, while others are accessed through commands. For details about any of the following tools or commands, see the HP OpenView web online help.

HP OpenView Launcher

There are several tabs at the bottom of the `HP OpenView Launcher` window that can help you troubleshoot the network. The tabs listed below contain tools to help you manage your network.

Object Views

The Object Views tab provides access to applications that provide views. From the Object Views tab you can use the SNMP MIB Browser to retrieve and view SNMP data or you can view your network topology using the Network Presenter.

Tasks

The `Tasks` tab provides access to task presentation managers, wizards, and tabbed dialog boxes that perform tasks.

Information and Reports

The `Information and Reports` tab displays the containers for Accounting and Assets, Configuration Information, Faults and Alarms, and Resources and Performance. You can generate reports from these containers. This information can be instrumental in helping you diagnose network problems.

Tools

The pane associated with the `Tools` tab displays the container for NNM. Under the NNM container are the leaf nodes for the Network Presenter, Unused IP Addresses, Alarm Browser, Event Correlation Configuration, Report Presenter, Report Configuration, SNMP Data Presenter, SNMP MIB Browser, and Views. Accessing any of these tools will present additional useful network information.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0247
3740
Doc:

1.382

1.381
A.

C Troubleshooting NNM Itself

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0248
3740
Doc:

This appendix describes measures that you can use to identify and troubleshoot system and software problems that may occur during Network Node Manager operations. These measures include the following:

- General network management troubleshooting considerations (page 579).
- Characterizing various types of problems (page 582).
- Troubleshooting background services (processes), such as `netmon` and `ovtopmd` (page 584).
- Troubleshooting the Web applications (page 613).
- Troubleshooting various operations, such as MIBs and runtime components (page 623).
- Troubleshooting Windows operating system applications (page 637).
- Recommended practices for logging and tracing (page 639).
- Improving performance and traffic management (page 654).

These measures are not intended to be used for troubleshooting your network problems, but are only for system and software problems related to NNM operations.

Most of the steps you will take in troubleshooting NNM are the same for NNM on either a Windows or UNIX operating system; however, some files and services are different. In addition, there are considerations to NNM on Windows operating systems that do not apply to NNM on UNIX operating systems, and vice versa.

NOTE For troubleshooting NNM's databases and the data warehouse, refer to the online manual *Reporting and Data Analysis with HP OpenView Network Node Manager*.

1.379
A.

General Troubleshooting Considerations

Consider the following when troubleshooting NNM:

- Network Node Manager is memory and page-file (swap-space) intensive. Problems may be due to resource exhaustion. Refer to "Performance" on page 656 for memory conservation tips.
- If you are using the Berkeley Internet Name Domain (BIND) Service on your network, each `gethostbyaddr` request for the hostname of a host with multiple IP addresses could return a different hostname.

When You Need More Information

Other information that may assist your troubleshooting is available in the following locations:

- The release note files (see page 71).
- The NNM online help.
- The Request for Comment (RFC) documents referenced in the introduction to this book (see page 33).

If a problem does not appear to be with the network management products themselves, see the following:

- Networking documentation for general network troubleshooting procedures.
- System documentation for system troubleshooting procedures.
- On UNIX operating systems only, X Windows documentation for X Windows troubleshooting procedures.

Preventive Practices

Following these recommended practices can help you prevent problems:

- Ensure that the management station meets the hardware, software and configuration prerequisites and recommendations.
- Maintain the system by regularly editing and deleting files. See Chapter 15 for maintenance tasks.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0249
3740
Doc:

- Ensure that *install_dir*\bin\ ($OV_BIN) is in your path.
- On a UNIX operating system, source /opt/OV/bin/ov.envvars.sh into your environment.
- On a Windows operating system, source *install_dir*\bin\ov.envvars.bat into your environment.
- Do not modify Network Node Manager product files without retaining the original files. The original files provide a way of restoring a known good operational configuration. If you correct a problem by restoring the original files, you can isolate the problem to one of the changes you made to these files.

  When you back up original files, do not copy the files to a new file name in the same directory. All files in the following directories are considered "live;" that is, every file in these directories will be used and you will end up with duplicate definitions.

  install_dir\registration\ ($OV_REGISTRATION)
  install_dir\fields\ ($OV_FIELDS)
  install_dir\symbols\ ($OV_SYMBOLS)
  install_dir\bitmaps\ ($OV_BITMAPS)
  install_dir\conf\ ($OV_CONF)
  install_dir\help\ ($OV_HELP)
  install_dir\tmp\ovbackup ($OV_TMP/ovbackup)

  See the backup procedure in Chapter 6 for complete guidelines and procedures for backing up your files.
- Make sure that you are not using up too much of your management station's CPU and network resources by collecting too much MIB data or setting too frequent polling intervals for the netmon service. Use Performance:Network Polling Statistics to gauge how effectively netmon is collecting network data.
- Use logging and tracing of background services to help isolate problems, but be sure to clean up log and trace files regularly. For more information see "Recommended Logging and Tracing Practices" on page 639 in this appendix.
- Use ovstatus -c -v to check the status of background services and OVW sessions.
- Use ovstart -c to track the progress of the services being started by ovspmd.

1377

- Use the `-d` option to `ovstart`, `ovstop`, `ovpause`, and `ovresume` to get additional debugging information.
- Use the `-verify` option to `ovw`. This option checks the syntax for all the installed application, symbol type, and field registration files. It also verifies the semantics of the application registration files and reports conflicts among application registration information. When started with this option, NNM does not start a normal "windowed" session; rather, it displays status messages in a text window.
- Use the `-mapcount` option to `ovw`. This option checks the consistency between the map database maintained by NNM and the object database maintained by `ovwdb`.
- Be careful when changing the permissions on files used by the management software. Restricting access could cause management services to be unable to access the file.
- On UNIX operating systems only, HP recommends that you not modify the files in `$APP_DEFS`. Instead, you can override the default X resources by modifying them in your `$HOME/.Xdefaults` file. If you are running HP VUE, modify your VUE resources. See `$APP_DEFS/XNm` for more details.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0250
3740
Doc:

Characterizing the Problem

Symptoms are visible conditions that indicate a problem. Whenever you encounter a symptom, collect the basic information described in the following subsections. The problem can usually be characterized in one or more of the following ways: scope of the problem, what changed just before the problem occurred, duration of the problem, and what action was performed when the problem occurred.

Distinguish Local versus Remote Problems

If you suspect a problem on a remote node or agent system, try to duplicate it on a local node or management station, and vice-versa. If you cannot duplicate the problem on the local node, the problem is probably associated with the remote node. If you can duplicate the problem on the local node, the problem may be in the management station or somewhere in the link, or may be a problem common to the agents.

Remote Nodes' Level of Manageability

What type of remote node are you trying to communicate with when the problem occurs?

The amount of information that NNM can collect depends on whether a remote node:

- Supports SNMP or not (or is proxied).
- Supports all the mandatory objects in MIB-II.
- Supports a partial, full, or extended (non-standard) MIB.
- Is an HP node or not.
- Is a TCP/IP node or not.
- Is an IPX node or not.
- Is an IPX router/server or not.

The management station gets the most information from an HP SNMP node, less information from other SNMP nodes, least information from non-SNMP and TCP/IP nodes, and no information from non-SNMP and non-TCP/IP nodes.

1375

Context: What Changed?

Determine what may have changed recently on your network or product configuration: hardware, software, files, security, utilization, etc. Keep a record of the software patches you install, so you can undo the changes in the order they occurred.

Also determine what is unique about a particular node that is having problems.

Duration: How Long or How Often?

Is the problem consistent (fails every time) or intermittent (fails sometimes)?

Context: What Action Was Performed?

When the problem occurred, what was happening? For instance:

- What operation was selected?
- What command was executed?
- What mouse operation was performed?
- What data was requested or sent?
- Was an alarm generated?
- Was an error or warning logged through the Windows Application Event Log (or `nettl`)?
- Was an error or warning logged through `ovconsole`, or the window from which `ovw` was started?
- Does `ovstatus -c` show all background services running?
- Does `ovstatus -v ovuispmd` list all of the OVW services that are expected to be running?

RQS nº 03/2005 - CN - CPMI - CORREIOS
0251
Fls. Nº
3740
Doc:

Troubleshooting Background Services

This section explains the background services of NNM and suggests actions to take if you have problems with one of the following background services. The background services are:

- hpptd
- netmon
- ovactiond
- ovalarmsrv
- ovcapsd
- ovrepld
- ovrequestd
- ovtopmd
- ovtrapd
- ovuispmd
- ovwdb
- pmd
- snmpCollect

In addition to explaining the background services, this section explains how to troubleshoot ovspmd, the service that monitors and controls the background services.

The background services and ovspmd should always be running whenever NNM is running. Normally, the background services are started through ovstart. See the *ovstart* reference page in NNM's online help (or the UNIX manpage) for all the options to ovstart. It may be particularly useful to use the -c or the -d options when troubleshooting.

To verify that the background services are running, enter the following:

```
ovstatus -c
```

See the *ovstatus* reference page in NNM's online help (or the UNIX manpage) for all the options to ovstatus.

The result should look similar to the following:

1373


```
Name              PID   State        Last Message(s)
OVsPMD           3676   RUNNING      -
ovsessionmgr     3677   RUNNING      Initialization complete.
ovwdb            3678   RUNNING      Initialization complete.
ovuispmd         3701   RUNNING      Initialized. 1 ovw clients registered.
ovtrapd          3698   RUNNING      Initialization complete.
ovactiond        3699   RUNNING      Initialization complete.
ovalarmsrv       3700   RUNNING      Initialization complete.
pmd              3679   RUNNING      Initialization complete.
ovdbcheck        3680   RUNNING      Connected to embedded database.
ovrequestd       3681   RUNNING      Initialization complete.
httpd               -   unknown      (Does not communicate with ovspmd.)
ovtopmd          3697   RUNNING      Connected to native database "openview".

netmon           3702   RUNNING      Initialization complete.
snmpCollect      3703   RUNNING      No values configured for collection.
```

If ovstatus indicates that an object manager was not found, the problem may be caused by one of the following:

- The ovspmd configuration has been incorrectly modified or is corrupted. If the ovspmd configuration is corrupted, see "The ovspmd Background Service" on page 592.
- The executable file has been removed or moved from its expected location. ovsuf either has a pathname to each executable or expects them to be in *install_dir*\bin\ (%OV_BIN%). Make sure they exist where they are supposed to be.

If ovstatus indicates that a service is in a paused state, it may mean that a backup is currently being performed, or that the service did not restart as expected after a backup. In that case, the state will be one of the following: PAUSED, RESUME_ERROR, or DEPENDENCY_ERROR. In this case, check the backup log in *install_dir*\tmp (%OV_TMP%) to determine the cause of the error. You can then stop all services using ovstop, and restart all the services by typing:

```
ovstart -c
```

Some of the background services depend on other services to operate properly. Table C-1 shows the dependencies.

Table C-1 Background Service Dependencies

Background Service	Dependencies
httpd	no dependencies

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0252
3740
Doc:

Table C-1 Background Service Dependencies

Background Service	Dependencies
netmon	ovwdb, pmd, ovtopmd
ovactiond	pmd
ovalarmsrv	pmd
ovcapsd	ovwdb, pmd, ovtopmd
ovdbcheck	none
ovrepld	pmd, ovtopmd
ovrequestd	none
ovtopmd	ovwdb, pmd, snmpd
ovtrapd	pmd
ovuispmd	ovwdb, ovtopmd
ovwdb	no dependencies
pmd	snmpd
snmpCollect	ovwdb, pmd, ovtopmd

For problems with individual background services, see the appropriate subsection in this appendix on how to troubleshoot a specific background service.

The httpd Background Service

The `httpd` service handles http (web) requests. It is provided only on UNIX operating system installations of NNM. Here are some problems that can be caused by `httpd` and possible solutions to those problems.

`httpd` should be running wherever NNM is running. Normally it is started by `ovstart`. To verify that it is running, type:

```
ovstatus httpd
```

ECT 1.371 A

You can also see if `httpd` is running by typing **`ps -elf | grep httpd`** on UNIX operating systems. You should see multiple copies of `httpd` running, since the parent `httpd` service spawns multiple children to improve performance in handling `httpd` requests.

If `httpd` is running, you can validate that it is running correctly by entering the following into your web browser:

`http://hostname:3443/`

You should see a short web page with the title "It Worked!"

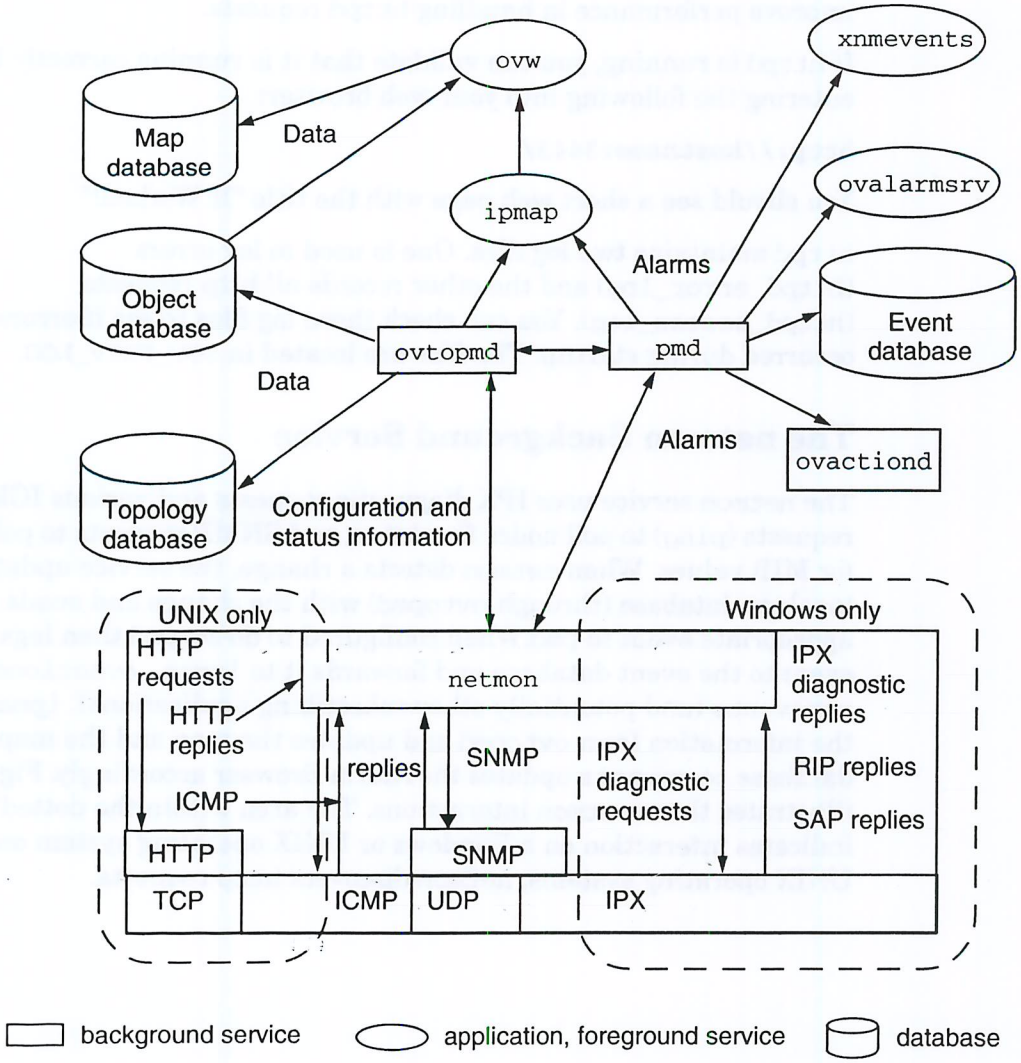
`httpd` maintains two log files. One is used to log errors (`httpd_error_log`) and the other records all http requests (`httpd_access_log`). You can check these log files to see if errors occurred during startup. The files are located in `$OV_PRIV_LOG`.

The netmon Background Service

The `netmon` service uses IPX diagnostic requests and various ICMP requests (`ping`) to poll nodes for status, and SNMP requests to poll nodes for MIB values. When `netmon` detects a change, the service updates the topology database (through `ovtopmd`) with the change and sends the appropriate event to `pmd`.When configured to do so, `pmd` then logs the event to the event database and forwards it to `ipmap`, `ovactiond`, and `xnmevents` (and potentially other subscribing applications). `ipmap` gets the information from `ovtopmd` and updates the map and the map database. `xnmevents` updates the Alarm Browser accordingly. Figure C-1 illustrates these `netmon` interactions. The area within the dotted oval indicates interaction on a Windows or UNIX operating system only. On UNIX operating systems, `netmon` discovers `http` requests.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0253
3740
Doc:

Figure C-1 netmon Interactions



You can control `netmon`'s polling through the map's `Options:SNMP Configuration` and the `Options:Network Polling Configuration:IP/IPX` menu item. The `SNMP Configuration` menu item modifies the *`install_dir`*`\conf\ovsnmp.conf_db` (`$OV_CONF/ovsnmp.conf_db`) database. The `Network Polling` menu item stores `netmon`'s polling intervals in the

1.369
A.

install_dir\conf\polling ($OV_CONF/polling) file. Do not modify this file directly; use the command line options to the program xnmpolling.

The xnmevents service checks every five minutes to see if netmon and snmpCollect are running. If either service is not running, xnmevents will display a dialog box and report the inactive service. (For information on changing the five-minute default polling interval or on disabling this polling feature, see the System Registry on Windows operating systems, or the file /usr/lib/X11/app-defaults/XNmevents on UNIX operating systems.

Status polling is scheduled on a per node basis, but is not deterministic. Therefore, polling of a node may not occur when scheduled if netmon gets behind due to its polling load for a particular time interval. Also, polling of manually added nodes and nodes changed from unmanaged to managed may not occur immediately after they are added or managed.

While you are unmanaging a network or segment during active discovery, a few managed nodes may appear on that network. To avoid this problem, do one of the following:

- Wait until the program finishes active discovery of the map.
- Turn polling off while unmanaging the network.

Only one instance of netmon may run on the management station; the *install_dir*\conf\ ($OV_CONF) netmon.lock file enforces this restriction.

The following tools can help you troubleshoot netmon problems.

- Use the Fault:Network Connectivity:Poll Node or Status Poll menu item to test or cause immediate netmon polling activity to a node.
- Use ovdumpevents to check for netmon service errors.
- Use the Performance:Network Polling Statistics menu item to determine if netmon is able to perform its polling at the configured frequency. See the online help for an explanation of the output of this menu item.
- Use netmon tracing to help isolate problems. For information see "Logging and Tracing" on page 639, or see the *ovstatus* reference page in NNM's online help (or the UNIX manpage).

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: Nº 0254
Doc: 3740

Auto-configuration of SNMP Traps

When netmon detects a node running an HP OpenView SNMP agent, it attempts to add the IP address of the NNM system to the trap destination table using an SNMP set request. In order for this to work, the NNM system must be configured with the correct SNMP set community name using Options:SNMP Configuration.

The ovactiond Background Service

The ovactiond service is started when you start NNM. It receives events from pmd that have automatic actions defined. For each of these actions, ovactiond formats the command string, then passes it on for interpretation and execution.

When you configure events using the Options:Event Configuration menu item in NNM, you are configuring ovactiond. If the result of your configuration of events is not what you expected, you can check the status of ovactiond.

Use the command ovstatus ovactiond to see if the service is running. ovactiond requires that pmd is running, so you should also check the status of pmd.

You can check the log file ovactiond.log for error messages. The file is located in:

Windows: *install_dir*\logs

UNIX: $OV_LOG

The ovalarmsrv Background Service

The ovalarmsrv service is started when you start NNM, and is the service that forwards events to xnmevents on NNM on a management station, and to NNM's web-based Alarm Browser. ovalarmsrv relies on pmd to be running; therefore, if you have problems starting xnmevents or the Alarm Browser, first check to see if pmd is running using ovstatus pmd.

You can also check the status of ovalarmsrv by using the ovstatus command. If ovstatus shows that ovalarmsrv is not running, and it will not start using ovstart ovalarmsrv, check to see if the service is running but ovstatus is not reporting it.

On UNIX operating systems, type

1.367

ps -elf | grep ovalarmsrv.

On Windows operating systems, use the Task Manager. If you find an ovalarmsrv service running, kill that service and restart ovalarmsrv using **ovstart ovalarmsrv**.

If you still have problems starting ovalarmsrv, be sure that you do not have a port conflict. ovalarmsrv uses two ports for communications. You can check those values in the /etc/services file. Make sure that another application is not using one of the ports assigned to ovalarmsrv.

ovalarmsrv reads alarms from the event database, receives new alarms from pmd, and maintains the state of all user modifications (for example, acknowledge, delete, etc.) to presented alarms. If the event database or the state file have somehow become corrupted, or if the file permissions have changed such that those file can't be read, you will not receive any data in xnmevents or the Alarm Browser.

You can also check the ovalarmsrv log file, ovalarmsrv.trace for error and tracing messages. The file is located in:

Windows: *install_dir*\logs

UNIX: $OV_LOG

The ovcapsd Background Service

The ovcapsd service checks newly-discovered nodes for Remote Desktop Management Interface (remote DMI or RDMI) and Hypertext Transfer Protocol (HTTP) capabilities. It periodically rechecks all Normal-status nodes. Capabilities are stored in the ovwdb database. ovcapsd gets IP and IPX address information for nodes from ovtopmd.

See the *ovcapsd* reference page in NNM's online help (or the UNIX manpage) for the most complete information available. Here are two important troubleshooting tips:

- ovcapsd checks nodes' capabilities after netmon has added them to the topology database. It might not have checked a node before the node appears in your ovwdb database or your map. If you search on a capability such as isHTTPSupported, ovcapsd might not yet have had a chance to check the node in which you're interested. You can run ovcapsd from the command line to check individual nodes synchronously. Also, ovcapsd can be made to check nodes faster by

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0255
3740
Doc:

increasing the number of threads it creates to check the nodes. See the *ovcapsd* reference page in NNM's online help (or the UNIX manpage) for more information.

- See the *install_dir*\log\ovcapsd.log file for ovcapsd service errors and on-exit messages.

The ovspmd Background Service

The ovspmd service monitors and controls the NNM background services. These background services are designed to run as children of ovspmd. The ovspmd service should be running whenever the background services are running. Normally, ovspmd is started by ovstart.

To verify the status of the services, type:

```
ovstatus -c
```

If ovstatus provides output indicating that all services are running, the problem is not ovspmd. If you do not receive the expected output, either ovspmd has a communication problem or the ovspmd service is not running. If the output indicates that ovsmpd is not running, start it using ovstart ovspmd.

Determining ovspmd Problems

You need to determine whether the problem is related to ovspmd or to a background service. If you determine you have an ovspmd problem, you need to determine what type of problem it is. Here are some indications of ovspmd problems:

- If the ovstatus output indicates that one of the background services is not running, type

  ```
  ovstart -v
  ```

  This should start any service that is not running. If any service fails to start, an error message will appear, indicating which service is not running. If this happens, use the Task Manager on a Windows operating system.

  On UNIX operating systems only, type **ps -ef** to list currently running services.

  Do *one* of the following:

1.365
A.

— If the output indicates a certain service is running, but ovspmd says the service is not running (using ovstatus or ovstart), ovspmd does not know that service is running. This problem can occur when ovspmd is shut down unexpectedly.

— If the output indicates that a certain service is not running, that service has a problem. See the troubleshooting section for that service.

When you run ovstart, the error message you receive about the service should provide information that will help resolve the problem.

- If you receive an ovspmd error message in the following format:

```
ovspmd:conf\ovsuf: error message
($OV_conf/ovsuf: error message)
```

you may have a corrupt ovsuf configuration file.

On UNIX operating systems only, go to the next section "Recreating the ovspmd Sockets Directory (UNIX operating systems only)".

- On UNIX operating systems only, if you receive *one* of the following error messages

```
ovstart: ovspmd is not running.It may have failed to start.
ovstart: unable to contact ovspmd: error message
```

you need to verify that the ovspmd sockets directory exists. Go to "Recreating the ovspmd Sockets Directory (UNIX operating systems only)" below.

Recreating the ovspmd Sockets Directory (UNIX operating systems only)

This section is for UNIX operating systems only. If you are using NNM on a Windows operating system, see the section "The netmon Background Service" on page 587.

Use this procedure when ovstart is unable to start or connect to the ovspmd service.

1. Verify that the $OV_SOCKETS directory still exists. ovspmd creates the OVsPMD_MGMT and OVsPMD_REQ socket files in this directory, which enable ovspmd to communicate with the other background services. If this directory no longer exists, recreate it by typing

```
mkdir $OV_SOCKETS
```


FRQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0256
3740
Doc:

2. Find out if any of the background services are running by typing

   ps -ef

3. Kill all the NNM background services that are running using the `kill` command. *Do not* use `kill -9`. For a list of the services, see "Troubleshooting Background Services" on page 584 in this appendix.

4. To restart the services and verify that they are starting properly, type

   ovstart -c

The ovrepld Background Service

`ovrepld` is a service that manages the discovery and monitoring of objects done on behalf of the local management station by remote collection stations. This remote topology information is merged with information obtained locally by `netmon` to create a more comprehensive topology database. If objects known to be present on remote collection stations are not appearing on your map, or are not being updated as expected, it is possible that `ovrepld` has stopped functioning.

Use `ovstatus ovrepld` to determine if `ovrepld` is running. If it is not, you can start it using `ovstart ovrepld`. In addition, `ovrepld` relies on `pmd` and `ovtopmd` to be running, so check to be sure that those services are also running.

`ovrepld` writes errors to a log file, `ovrepld.log`. The file is located in:

Windows: *`install_dir`*`\logs`

UNIX: `$OV_LOG`

The ovtopmd Background Service

The `ovtopmd` service is responsible for maintaining the topology database that is used by `netmon` and `ipmap`. It provides both enforcement of rules for correctness of the IP topology, and caching of the data to improve the performance of the system.

`ovtopmd` should be running whenever NNM is running. Normally it is started through `ovstart`. To verify that it is up and running, type

ovstatus ovtopmd

You should see something like this:

```
object manager name:    ovtopmd
state:                  RUNNING
PID:                    4119
last message:           Connectedto native database "openview"
exit status:            -
```

If ovstatus gives an error similar to this:

```
ovspmd:install_dir\conf\ovsuf:object manager ovtopmd not found
($OV_CONF/ovsuf:object manager ovtopmd not found)
```

The problem may be that the ovspmd configuration is corrupted. If the ovspmd configuration is corrupted, see "The ovspmd Background Service" on page 592 in this appendix.

If ovstatus reports the following message:

```
Running. Lost connection to master agent.
```

This could indicate that ovtopmd is still executing, but has lost its connection to the master SNMP agent (snmpd). Usually this is because the master agent (snmpdm) exited or has been shut down.

Restart the master agent on the Windows operating system using the Services applet in the Control Panel. Start the SNMP EMANATE Master Agent and SNMP EMANATE Adapter for NT/2000 services.

On UNIX operating systems only, restart snmpd by executing

/usr/sbin/snmpd

If the master agent is executing, try executing the following commands:

ovstop ovtopmd

ovstart ovtopmd

If ovstatus knows about ovtopmd, but indicates that it is not running, enter the following:

ovstart -c

Normally, this should start ovtopmd and all background services on which ovtopmd depends. In particular, ovtopmd depends on ovwdb and pmd being started. If ovwdb does not start, ovtopmd will not be able to execute successfully. In addition to ovwdb executing, ovtopmd relies on the field definitions being loaded into ovwdb, which normally happens through the configuration scripts at installation time.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0257
3740
Doc:

If ovtopmd gives an error indicating that it was unable to map a field name into a field ID, do the following:

- Verify that $LANG is set correctly and that the *install_dir*\fields\C ($OV_FIELDS/$LANG) directory exists and contains at least the following files: ovw_fields, ip_fields, snmp_fields, topm_fields, and misc_fields. The $LANG environment variable provides support for localizing native languages. If not otherwise defined, $LANG is assumed to be C, which means that no native language support is provided. (UNIX systems only: For more information on native language localization, see the *lang* manpage.)
- Type the following commands:

  ```
  ovstop -c
  ovstart ovwdb
  ovw -fields
  ovstart -c
  ```

  This should load any necessary field definitions into ovwdb, and then start ovtopmd and netmon (as well as any other background services).

By default, ovtopmd uses a TCP socket bound to port 2532. If ovtopmd indicates an error attempting to bind to this port number because another application is already using it, follow these steps:

1. Make sure that you do not have another ovtopmd service using port 2532.

   The most common reason for errors binding to the TCP socket is the presence of another ovtopmd service. If an ovtopmd service was started outside of ovstart, the ovstop, ovstart, and ovstatus commands will not recognize this service. To prevent this problem, always start all NNM background services with the ovstart command and stop them with the ovstop command.

   If another application is using port 2532, continue with the next step.

2. Change the port number to any unused port by changing the entry for ovtopmd in %SystemRoot%\system32\drivers\etc\services (/etc/services):

   ```
   ovtopmd 2532/tcp  # OpenView IP Topology daemon
   ```

   Choose a number other than 2532 that does not conflict with other services listed in services (/etc/services).

1361
A

3. Reconfigure NNM by typing the following commands:

   ovstop

   ovstart

4. If ovtopmd still fails to run successfully from ovstart, contact your HP support representative.

NOTE On UNIX operating systems only, if you are using the Network Information Service (NIS), make sure you update your NIS Master Server.

Once ovtopmd has been started through ovstart, you can verify that it is responding to requests by executing *install_dir*\bin\ovtopodump ($OV_BIN/ovtopodump). By default, ovtopodump will print a single line of output for each object in the topology. You can also get verbose listings and summary information. For more information see the *ovtopodump* reference page in NNM's online help (or the UNIX manpage). For example, if you type

ovtopodump -l

or, for remote collection stations

ovtopodump -c *nodename*

your result will look something like

```
TOPO OBJECT ID: 70
TIME CREATED: Fri Apr 10 14:52:02 1995
TIME MODIFIED: Fri Apr 10 14:52:02 1995
GLOBAL FLAGS:
NUMBER OF NETWORKS: 13
NUMBER OF SEGMENTS: 19
NUMBER OF NODES: 238
NUMBER OF INTERFACES: 281
NUMBER OF GATEWAYS: 21
```

This prints the summary information for the entire topology. If ovtopodump fails, this indicates some problem with ovtopmd. Try stopping all background services with ovstop, and then restarting them with ovstart.

If ovstart succeeds, but ovtopodump still fails, verify that at least one of the following is true:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0258
3740
Doc:

- The IP address of the loopback interface is `127.0.0.1`.
- There is an entry for `localhost` that has the correct address for the loopback interface.
- The IP address for the `localhost`'s hostname is correct. (That is, do an `ipconfig /all`, ping the hostname that was returned, and verify that the address returned is correct.)

  On UNIX operating systems only, do a `hostname`, and then look up that name with `nslookup`, and verify that the address returned is correct.

If `ovtopodump` still fails, contact your HP support representative.

In addition, `ovtopmd` maintains consistency with the object database maintained by `ovwdb`. You can use the `ovtopofix` command to do the following consistency checks and updates:

- Check object existence in both the topology and `ovwdb` databases.
- Ensure that the managed state is consistent.
- Remove incomplete interface objects and incomplete nodes created by the discovery process from the object database.
- Update the presentation time to force `ipmap` to update the object's status during map synchronization.
- Update the creation time of the object to force `ipmap` to add the object during map synchronization.

To run `ovtopofix` and check for problems, type

`ovtopofix -n`

To run `ovtopofix` and fix any problems found, follow these steps:

1. Exit `ovw` using the `Map:Exit` menu item.
2. Stop `netmon` by typing **`ovstop netmon`**.
3. Type **`ovtopofix`**.
4. Restart `netmon` by typing **`ovstart netmon`**.

For more information, see the *ovtopofix* reference page in NNM's online help (or the UNIX manpage).

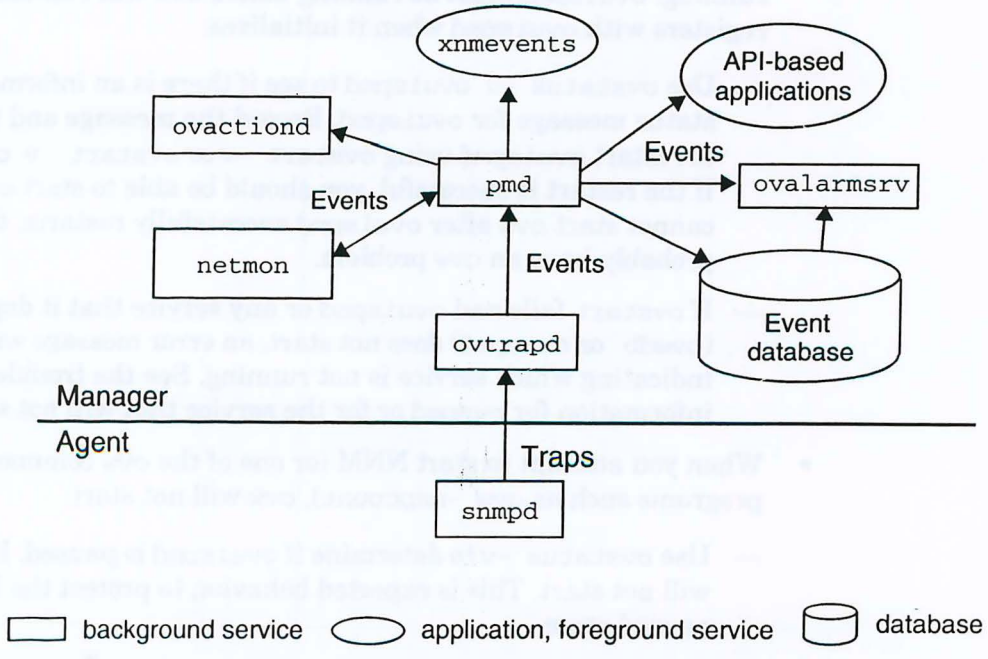
1.359
A.

A license problem could also cause ovtopmd to fail. In this situation, verify that the license in *install_dir*\conf\.license ($OV_CONF/.license) is correct.

The ovtrapd Background Service

SNMP traps generated by an agent (snmpd in the case of the HP OpenView SNMP Agent) go to ovtrapd (via UDP port 162), which forwards them to pmd. ovtrapd acts as a buffer for traps that could potentially be dropped when pmd is busy. pmd logs and forwards the traps (in the form of an event) to netmon, ovactiond, ovtopmd, ipmap, and xnmevents (and potentially other subscribing applications). Figure C-2 illustrates this interaction.

Figure C-2 ovtrapd Event Interactions with SNMP Agent



RQS nº 03/2005 - CN -
CPMI - CORREIOS
0259
Fls. Nº
3740
Doc:

The ovuispmd Background Service

You are most likely to see ovuispmd problems when you are trying to start ovw, since you cannot start ovw if ovuispmd is not running. You may also see ovuispmd problems when you use ovpause and ovresume, which are invoked when you perform a backup.

Problems that appear to be ovuispmd problems can actually be the result of:

- Problems with ovuispmd itself.
- Problems with one of the services on which ovuispmd depends.
- Problems with ovw, which depends on ovuispmd.

The easiest way to determine if the problem is with ovuispmd itself, or with another service, is to look at the symptom, as follows.

- When starting NNM, you get a dialog box saying that registration with the UI process manager failed. This is because ovuispmd is not running. ovuispmd must be running before ovw will run because ovw registers with ovuispmd when it initializes.
  - Use `ovstatus -v ovuispmd` to see if there is an informative exit status message for ovuispmd. Record the message and then try to restart ovuispmd using `ovstart -v` or `ovstart -v ovuispmd`. If the restart is successful, you should be able to start ovw. If you cannot start ovw after ovuispmd successfully restarts, then you probably have an ovw problem.
  - If `ovstart` fails and ovuispmd or any service that it depends on (ovwdb or ovtopmd) does not start, an error message will appear, indicating which service is not running. See the troubleshooting information for ovspmd or for the service that will not start.
- When you attempt to start NNM (or one of the ovw command line programs such as `ovw -mapcount`), ovw will not start.
  - Use `ovstatus -v` to determine if ovuispmd is paused. If it is, ovw will not start. This is expected behavior, to protect the NNM's paused state.

    It should not take long for ovpause to complete. If the pause was initiated by the automated backup program, you can determine how long the system has been paused from the log file, *install_dir*`\tmp\ovbackup.log` (`$OV_TMP/ovbackup.log`).

1.357
A-

If the paused state persists and there is no ovbackup in progress you can attempt to ovresume the system. Do not do this if a backup is in progress because it can result in corruption of the data store copies that are being created.

- You attempt an ovpause or ovbackup.ovpl when an ovw command line client is running, and ovuispmd denies the pause. This is expected behavior. Under these conditions the command ovstatus ovuispmd tells you that ovuispmd's state is PAUSE_ERROR and ovuispmd's last message field indicates that it denied the pause because a command line client is running.

  To prevent database inconsistency or inaccurate reporting, ovuispmd denies a pause request if the pause request is received when one of ovuispmd's registered ovw services is an ovw that was invoked with the -mapcount, -deleteMap, or -copyMap option.

  — To resolve this problem, issue a new pause request after the ovw service terminates. These ovw command line services are designed to do specific, short tasks and then exit.

- There are ovw sessions that seem to be stuck pausing. If you have run ovbackup.ovpl and you find ovw sessions still paused after the background services have resumed, ovuispmd may have exited or been killed during the pause.

  If a resume request is issued when ovuispmd is not running, then ovw sessions will not be notified of the resume and will remain paused, even when the background services have resumed. When ovuispmd terminates ungracefully it leaves a state file containing information about the registered ovw sessions. You can examine this file in *install_dir*\conf\ovuispmd.state ($OV_CONF/ovuispmd.state). *Do not modify this file!* It is used by ovuispmd when it is restarted.

  — Use ovstatus to determine if ovuispmd is still running. If it is not running, restart it. When it initializes, it will automatically attempt to resume all of the ovw sessions that were registered with it when it terminated ungracefully.

- The ovw session information reported by ovuispmd is not correct. When you run ovstatus -v ovuispmd, it includes ovw sessions that are no longer running.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0260
Doc: 3740

Under some termination conditions, ovw sessions are unable to unregister with ovuispmd before they terminate. In those cases, ovuispmd's list of ovw sessions will not be corrected until ovuispmd attempts to communicate with the registered sessions.

  - If no ovw sessions are running locally or remotely then it is safe to stop ovuispmd and restart it. Its ovw session information will be updated when it is restarted.

- ovuispmd exits ungracefully. This may be due to a termination signal from ovspmd.

  - See the *ovuispmd* reference page in NNM's online help (or the UNIX manpage) for information about forced termination. Also refer to the file *install_dir*\lrf\ovuispmd.lrf ($OV_LRF/ovuispmd.lrf) for useful comments about configuring the timeout field to prevent this occurrence.

- When you try to start ovw, ovw will not start or ovuispmd exits.

  - If ovuispmd is running but ovw does not start, or if ovw startup causes ovuispmd to abort, there may be useful information in the ovuispmd logging messages. The log messages may help you characterize the problem as an ovw problem, an ovuispmd problem, or an application problem.

    Detailed instructions for using the Windows Application Event Log and the UNIX operating tracing and logging facilities, nettl and netfmt, are found in this appendix in the section "Logging and Tracing" on page 639. Examine the logging output for ovuispmd errors in the OVEXTERNAL subsystem section. Also refer to the diagnostics in the *ovuispmd* reference page in NNM's online help (or the UNIX manpage).

The ovwdb Background Service

The ovwdb service controls the object database. Here are some problems that can be caused by ovwdb and possible solutions to the problems.

ovwdb should be running whenever NNM is running. Normally it is started through ovstart. To verify that it is up and running, type:

```
ovstatus ovwdb
```

You should see something like this:

```
object manager name:    ovwdb
state:                  RUNNING
PID:                    4115
last message:           Initialization complete.
exit status:            -
```

By default, ovwdb uses a TCP socket bound to port 9999. If ovwdb indicates an error attempting to bind to this port number because another application is already using it, follow these steps:

1. Make sure that you do not have another ovwdb service using port 9999. Check the `/etc/services` file for a listing of ports being used.

   The most common reason for errors binding to the TCP socket is the presence of another ovwdb service. If an ovwdb service was started outside of ovstart, the ovstop, ovstart, and ovstatus commands will not recognize this service. To prevent this problem, always start all NNM background services with the ovstart command and stop them with the ovstop command.

   If another application is using port 9999, continue with the next step.

2. Change the port number to any unused port by changing the entry for ovwdb in `%SystemRoot%\system 32\drivers\etc\services` (`/etc/services`).

   ```
   ovwdb    9999/tcp      # OpenView Object Database daemon
   ```

3. Reconfigure NNM by typing the following commands:

   ovstop

   ovstart

4. If ovwdb still fails to run successfully from ovstart, contact your HP support representative.

NOTE If you are using the Network Information Service (NIS), make sure you update your NIS Master Server.

If you notice a great deal of swapping and the system performance does not meet your expectations, you can do one of two things:

- Edit the *install_dir*`\lrf\ovwdb.lrf` (`$OV_LRF/ovwdb.lrf`) file to configure the maximum number of objects that will be in the ovwdb cache.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0261
3740
Doc:

- Change the system parameters (kernel parameters and regenerate the kernel). For more information, see "Improving Traffic Management and Performance" on page 654 in this appendix.

To verify the status of ovwdb, first run the `ovstatus -v` command to determine if everything is working correctly. If ovwdb stops running, netmon and ovtopmd will also stop running because these services are dependent on ovwdb. On UNIX operating systems only, if ovwdb is no longer running, check the `nettl` log using `netfmt`. Note that this assumes `nettl` was running when the problem occurred. To verify that `nettl` is running, execute the `nettl -status` command. See "Using nettl and netfmt (UNIX operating systems only)" on page 643 for more information on using `nettl`.

If you exhaust all available memory, the ovwdb service will stop running. To solve this problem, follow the suggestions described above for solving problems with excessive swapping; that is, either edit the `ovwdb.lrf` file or change the system (kernel) parameters.

If ovwdb stopped running due to memory problems, a disaster message will be logged into the Application Event Log (through `nettl`).

If the object database gets corrupted in any way, for example, by removing the files in the *`install_dir`*`\databases\ovwdb` (`$OV_DB/ovwdb`) directory, you need to restart the automatic map generation from the beginning.

The pmd Background Service

The pmd service is the postmaster background service. It provides event (trap) forwarding and message passing between services. When pmd receives an event, it forwards it to all the services that are registered to receive the event. Events are generated by these services:

- ipmap and ovtopmd when you edit the map or when nodes' status propagates to segments and networks.
- netmon, when it detects a change as a result of polling nodes or as a result of receiving a trap forwarded by pmd.
- ovtrapd, when ovtrapd receives a trap from agent services.
- ovtopmd, when topology changes occur.
- snmpCollect, when a threshold is exceeded or reset.
- ovevent, when this command is called from a batch file (shell script).

1353
A.

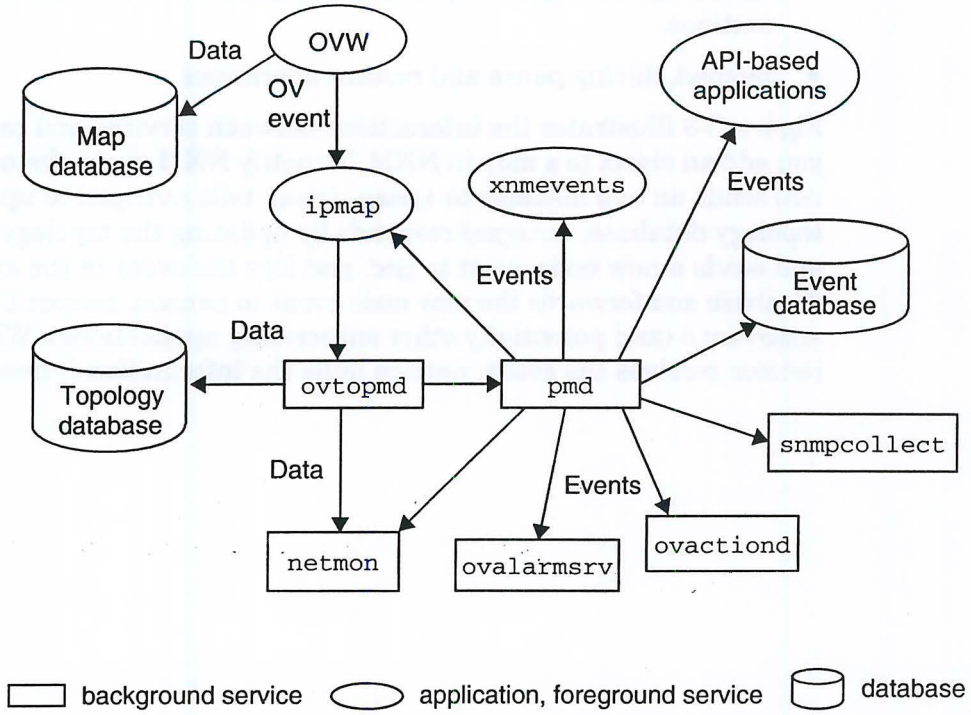
- Configuration operations such as `xnmloadmib`, `xnmtrap`, `xnmsnmpconf`, and `xnmcollect` when you edit configuration files.
- `ovrepld` as a result of a change detected on a remote collection station. Refer to *A Guide to Scalability and Distribution* for information on the `ovrepld` background service and collection stations.
- `ovspmd`, during pause and resume operations.

Figure C-3 illustrates the interactions between services and `pmd` when you add an object to a map in NNM. To notify NNM about the new object, `ovw` sends an `ovw` message to `ipmap`. `ipmap` tells `ovtopmd` to update the topology database. `ovtopmd` responds by updating the topology database and sends a new node event to `pmd`. `pmd` logs the event in the event database and forwards the new node event to `netmon`, `snmpcollect`, and `xnmevents` (and potentially other subscribing applications). When `netmon` receives the event, `netmon` pulls the information it needs from

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0262
3740
Doc:

the topology database through ovtopmd. When snmpCollect receives the event, it checks to see if the new node should be collected from (that is, whether it matches any configured IP wildcards).

Figure C-3 pmd Event Interactions



For a discussion of pmd's interactions and operation concerning events generated by netmon, see "The netmon Background Service" on page 587.

If you suspect a problem with the pmd background service, try the following actions to further isolate the problem:

- If pmd is not configured to write to eventdb, you'll first need to execute ovdumpevents to write the contents of the event database to a log file.
- Look for events logged to the event database, using xnmevents or the Alarm Browser.

1.351
A

- Add a node to the map and then check to see if the event was recorded in the event database, using `xnmevents` on a management station or the Alarm Browser through the Web UI.
- Run `ovstatus` and check the status of `pmd`. If the `pmd` service appears to be hung, stop the service using `ovstop` and restart all background services with `ovstart`.
- Check `pmd.log0` to see any messages related to the `pmd` service.
- Turn on tracing as described in the "Recommended Logging and Tracing Practices" on page 639 in this chapter. Your HP support representative can help you interpret the trace results.
- Verify that events can be generated. Use the `popupMsg` contributed script in `$OV_CONTRIB/NNM/popupMsg` to generate an event.

The ovrequestd Background Service

The `ovrequestd` service executes reports and data warehouse exports according to a predefined schedule. Once a report is configured, `ovrequestd` starts executing the exports and the reports.

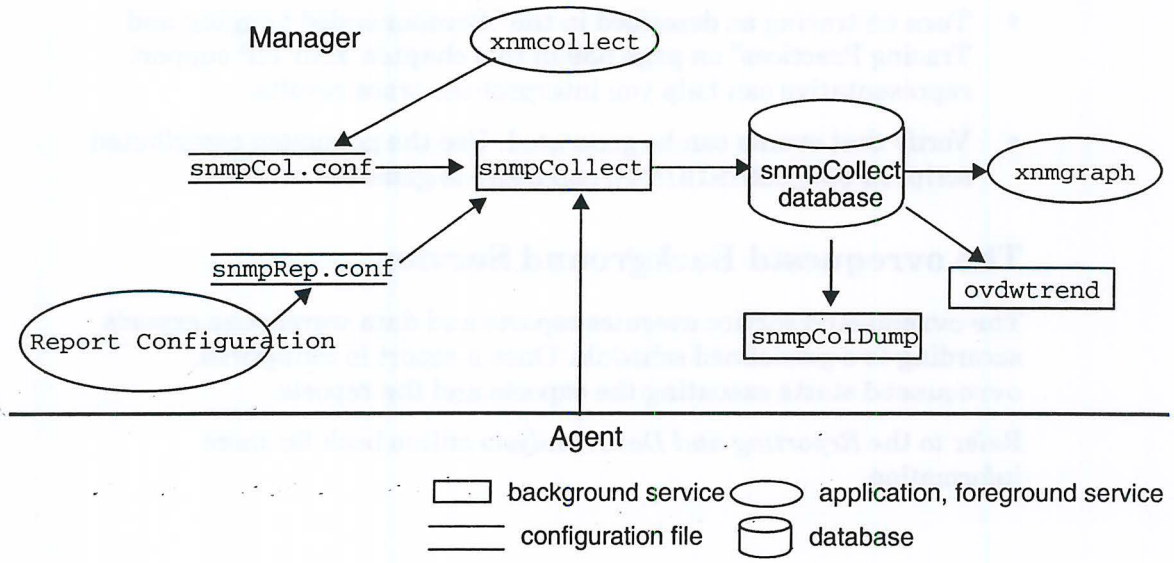
Refer to the *Reporting and Data Analysis* online book for more information.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0263
3740
Doc:

Troubleshooting Data Collector Problems

Figure C-4 shows the interactions among the services xnmcollect, xnmgraph, snmpCollect, snmpColDump, and an SNMP agent.

Figure C-4 snmpCollect Interactions with SNMP Agents



If you have problems collecting MIB data, check for these problems:

- The service for the data collector, snmpCollect, may not be running on the management station.
  - — Make sure that you are not out of disk space. The data collector stops running when the disk is full. See page 610 for information about what to do if the disk is full.
  - — Verify the snmpCollect service is running by executing the ovstatus snmpCollect command. If the snmpCollect service is not running, restart the data collector using the ovstart command.
- Data is not being collected from the node it should be or thresholds are not being generated.
  - — Make sure the target node supports SNMP.

j. 349
A.

- Make sure the node is managed, or that the `-u` option to `snmpCollect` is used.
- Verify that the MIB object is configured for collection. Use the `Options:Data Collection & Thresholds:SNMP` menu item to verify the configuration.
- Verify that the target node is configured to collect data or generate threshold events. You can configure the node to collect data by explicitly specifying the node name, by specifying a wildcard, or by specifying the name of an ASCII file that contains the node name. Also, verify that the target node has not been excluded for collection. Use the `Options:Data Collection & Thresholds:SNMP` menu item to verify the configuration.
- Ensure that collections for the MIB object are not in `Suspended` state.
- Ensure that the desired instances are specified for the MIB object and node combination.
- Perform `Fault:Test IP/TCP/SNMP` on the collection in question. This checks the connection between the local management station and other SNMP nodes.
- If `sysObjectID` filtering is being used, make sure the correct `sysObjectID` is being used.
- See if other collections or thresholds from that node are working. If none are working, the problem is probably with the node. From the `Options:Data Collection & Thresholds:SNMP` window, select the MIB object, and then select `Actions:Show Data` to see if data is being collected from the node.
- Try to access the MIB object using the `Tools:SNMP MIB Browser` dialog box.
- Run `snmpCollect -S` and look at the *`install_dir`*`\log\($OV_LOG)snmpCol.trace` file. This command lists the configuration of the data collection.
- Try turning on verbose tracing. Execute `ovstop snmpCollect`. Then execute `ovstart snmpcollect -V`. Check the output in the `snmpCol.trace` file.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0264
3740
Doc:

— If you expect threshold events to occur, but they do not, start a data collection on the MIB variable. The problem may be that the threshold value is not set correctly. For example, if the normal value for this variable is 20 and you set the threshold value to 100, you will probably never see a threshold event.

— If you can't resolve the problem, use the tracing command. To use the tracing command, try restarting the data collector with the same command as in the *install_dir*\lrf\snmpCollect.lrf (`$OV_LRF/snmpCollect.lrf`) file, but add the `-t` *filename* option. The `-t` option is a tracing option that logs the results to the *filename*. Run `snmpCollect -T` to toggle the tracing. To determine whether or not tracing is on, look at the trace file. See the *snmpCollect* reference page in NNM's online help (or the UNIX manpage) for more information.

— For more information about troubleshooting threshold events, see the section "Configuring Events" on page 631 in this appendix.

- The disk is full. The data collector stops running when the disk is full. To solve this problem and to prevent this problem from happening again, do the following:

  - Use `ovdwtrend -delpriorto` *date/time*. This command will export `snmpCollect` data to the data warehouse and then delete the `snmpCollect` data after it has been exported. See the *ovdwtrend* reference page in NNM's online help (or the UNIX manpage) for more information on using this command.

  - Free up disk space by removing files in the *install_dir*\databases\snmpCollect (`$OV_DB/snmpCollect`) directory. Note, however, when you remove files you lose the data you have saved. If you don't want to remove the whole file, you can edit the file and keep only the most recent data by deleting older entries in the file. Once you have freed up disk space, as `root` restart the data collector with the `ovstart` command.

  - Edit files in the *install_dir*\databases\snmpCollect (`$OV_DB/snmpCollect`) directory using the `snmpColDump` command. For example, to retain the last 100 entries of a file, use the following commands (available in the MKS Toolkit on a Windows operating system):

```
snmpColDump -tTI snmpCollect\filename\
awk -F\t '{printf("%d\t%d\t%s\t%1g\n", $4, $5, $6, $3)}' | \
  tail -100 > \tmp\save
snmpColDump -r \tmp\save install_dir\databases\snmpCollect/
```

On UNIX operating systems only:

```
snmpColDump -tTI $OV_DB/databases/snmpCollect/filename\
awk -F\t '{printf("%d\t%d\t%s\t%1g\n", $4, $5, $6, $3)}' | \
  tail -100 > /tmp/save
snmpColDump -r /tmp/save $OV_DB/databases/snmpCollect/
```

- If you want to stop all data collection, kill the `snmpCollect` service with the `ovstop snmpCollect` command, or suspend all data collections using the `Options:Data Collection & Thresholds:SNMP` menu item.

To prevent the problem in the future:

— Lengthen the polling intervals. Using the `Options:Data Collection & Thresholds:SNMP` menu item and set the polling interval to not collect as often. In addition, if you only want to check thresholds, don't store the data.

— Reduce the number of MIB objects you are collecting on.

— Reduce the number of nodes you are collecting on.

— Reduce the number of instances you are collecting for some or all nodes.

— Set up programs (`cron`) to periodically either remove files in the *install_dir*`\databases\snmpCollect` (`$OV_DB/snmpCollect`) directory or export and trim them with `ovdwtrend`.

- There is no response when querying DMI devices.

— Make sure that DMI is configured correctly on the remote device.

— The Data Collector supports only SNMP devices. Install an SNMP agent and a DMI-to-SNMP mapping agent on the DMI system.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0265
3740
Doc:

Set-community Name and Trap-dest Loss Upon Re-Installation

The emanate SNMP agent uses the following two configuration files in the *install_dir*\conf\SnmpAgent ($OV_CONF/SnmpAgent) directory:

- snmpd.cnf — the SNMPR-format emanate configuration file.
- snmpd.conf — the HP-format SNMPD configuration file.

emanate uses the union of configuration information from both files. However, some of the information is in both—sysDescr, sysName, sysContact, and sysLocation. When emanate starts up, it uses the snmpd.conf values (if defined) and copies them to snmpd.cnf; otherwise, it uses the values in snmpd.cnf.

The get-community, set-community, and trap-dest fields in snmpd.conf are not replicated in snmpd.cnf, so they are appended (in emanate run-time memory) to the set of configurations in snmpd.cnf because it is allowable to have more than one value for each.

Thus, upon installation, the default snmpd.cnf file is conditionally installed by Setup (only if one doesn't already exist)—but the default snmpd.conf file is always installed. After uninstallation and re-installation, the result is that sysContact and sysLocation get taken from the existing snmpd.cnf file, but the set-community and trap-dest are taken from the new/default snmpd.conf file (in which they are not defined).

The solution is to conditionally install snmpd.conf only when it does not already exist.

1.345
A.

Troubleshooting Web Components

If you experience problems starting any of the web components, you should first check the following before doing further troubleshooting.

- Make sure that NNM is installed on the host specified in the URL, and that the host is running.
- Make sure that you are using a supported web server, and that it is configured properly and is running. Supported web servers include Microsoft Peer Web Services, Microsoft Internet Information Server, and Apache (shipped with NNM for UNIX operating systems.) Try entering the simplest URL (`http://hostname[:port]`) in the web browser and see if the server is accepting connections.
- Make sure that you are using a web browser that supports NNM. Supported web browsers include Netscape 4.6 or greater and Microsoft Internet Explorer 5.0 or greater.
- If starting the web component directly from a URL, make sure the full URL was entered correctly. If NNM is running on a UNIX operating system, check that port 3443 is specified in the URL.
- Make sure that the hostname in the URL is fully qualified. Do not use the short version of the hostname. For example, use `mysystem.home.com` instead of just `mysystem`.
- Exit and restart the browser, and then re-enter the URL.
- Clear the memory and disc caches for the browser, and restart the browser.

  In Netscape Navigator, select the `Edit:Preferences` menu item. In the dialog box, click on `Advanced`, then click on `Cache`. In the next dialog box, click on `Clear Disk Cache` and `Clear Memory Cache`.

  In Internet Explorer, select the `View:Internet Options` menu item. On the `General` page, select the `Temporary Internet Files` field. Then click on the `Delete Files` button.
- Check the contents of all of the web log files for possible errors.

  Windows:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0266
3740
Doc:

```
install_dir\www\logs\launcher\error_log
install_dir\www\logs\launcher\login_log
install_dir\www\logs\launcher\access_log
```

UNIX:

```
/var/opt/OV/www/logs/launcher/error_log
/var/opt/OV/www/logs/launcher/login_log
/var/opt/OV/www/logs/launcher/access_log
```

- If an http proxy server is in use, try disabling the web browser from using it.

  In Netscape, select the `Edit:Preferences` menu item. In the dialog box, click on `Advanced`, then click on `Proxies`. In the dialog box, select `Direct connection to the Internet`.

  In Internet Explorer, from the `General` page select the `View:Internet Options` menu item. On the Connection page, deselect `Access the Internet using a proxy server`.

- For errors in the Reporting interface, refer to the *Reporting and Data Analysis* online manual.

Language Selection Problems

NNM's web applications are available in English and Japanese. However, it is possible to integrate and use other web applications that have been translated into other languages while NNM's web applications remain in English. If you expect the web applications to be in a language other than English and they are not, it could be due to one of the following problems:

- If the strings are appearing in English, check the browser's language configuration.

  In Netscape, `Languages` is configured through the `Netscape:Preferences` menu item.

  In Internet Explorer, `Languages` is configured through the `Internet:Options` menu item.

  In both cases, the language that you expect to see should be listed at the top of the `Languages` window. To see NNM's web applications in Japanese, be sure that the Japanese entry (`ja`) is listed before the English entry (`en` or `en-us`). Restart the browser after making changes.

J.343
A.

- If the non-English strings appear garbled in the window, check the following:

  — The browser's encoding or font configuration may be incorrect.

  In Netscape, the encoding is specified through the `View:Encoding` menu item.

  In Internet Explorer, the font is specified through the `View:Font` menu item.

  To choose Japanese, one of the Japanese fonts or encodings should be selected.

  — On UNIX systems only, the browser was not started with the correct environment variable settings.

  The browser process should be started with the correct `$LANG` setting. For Japanese, `XMODIFIERS` must also be set. These variables are usually set by the desktop environment.

  — On Japanese on UNIX systems only, the default codeset in use by the server may be incompatible with the Web applications.

  By default, NNM's web applications expect the data from the servers to be in Shift-JIS codeset for HP-UX and Windows operating systems. On Solaris, EUC is the default. Use the `ovchange_locale_mapping` command to switch the default configuration. See the *ovchange_locale_mapping* manpage for details.

HP OpenView Launcher

User Login Problems

If you expected to get a user login screen when the Launcher starts, but you did not, then the file `session.conf` probably has not been set up for user logins. See Chapter 14, NNM on the Web, for information on setting up users and logins.

If you get the user login screen and the Launcher does not accept the login, check the following:

- Make sure you typed the user name and password correctly.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0267
Fls.-Nº
3740
Doc:

- Make sure the password file, `htpasswd`, includes the user name and password. See Chapter 14, NNM on the Web, for information on setting up the `htpasswd` file.
- If running NNM in a non-English language, be sure that the environment variable `XMODIFIERS` is set correctly.

Starting the Launcher

If you have problems starting the Launcher, check the error log file for potential errors. The Launcher error log records internal errors from the Launcher. You can use the output from this file when discussing a problem with the HP Response Center or support personnel.

If the error log file does not give you sufficient information for troubleshooting, you can set a parameter in the URL for `ovlaunch.exe` that will enable more in-depth error logging on a session level.

The parameter is:
`http://`*`hostname`*`:[`*`port`*`]/OvCgi/ovlaunch.exe?Debug=/tmp/`*`file`*

The output of this file is less "friendly" than other error log files, but it contains valuable information that may be useful to a support person who is trying to assess the problem.

If the Launcher does not start and you get an error message indicating that there is a CGI problem, then the problem could be with one of the Launcher's CGI programs. Try executing each of the following programs from the command line. These programs are located in:

Windows: *`install_dir`*`\www\cgi-bin`

UNIX: `/opt/OV/www/cgi-bin`

- `ovlaunch.exe`
- `ovlogin.exe`
- `ovsessioninfo.exe`
- `ovlaunchreg.exe`

You can tell if these programs are running if they output ASCII text to the screen. If one of these programs is not running, contact HP Support.

Launcher Window Problems

If the Launcher window comes up with no content (blank), it could be one of the following problems:

- The correct patches have not been installed on the system. Check the system requirements section of the Installation Guide.
- You could have a conflict if you had an older version of Netscape installed on your system. If you have set the `CLASSPATH` environment variable when running an older version of Netscape, it will cause Java access problems when you run the recommended version of Netscape. If you have set this variable, you should unset it before running the newer version of Netscape.
- You could have a Java applet problem. Check the Java log as follows:
  - In your web browser, check to see that the items Java and Java script are enabled. In Netscape Navigator, check this by using `Edit:Preferences->Advanced`. In Internet Explorer, check this by using `View:Advanced`.
  - Bring up a Java console and view the messages it contains. In Netscape Navigator, use `Window:Java Console`. In Internet Explorer, use `View:Java Console`.
  - Try starting the Launcher without going through a proxy.

    In Internet Explorer, select the `View:Internet Options` menu item. Choose the `Connection` tab, then turn off the proxy server.

    In Netscape Navigator, select the `Edit:Preferences` menu item, choose `Advanced`, and disable the proxy server.
  - The Java console also provides a method of logging information about the Java virtual machine interpretation of the Java code that is executing. Both of the supported web browsers allow you to turn on Java error logging from the browser menu. In Netscape Navigator, look under the `Window` menu item. In Internet Explorer, select the `View:Internet Options` menu item under the `Advanced` tab.

If you encounter errors when reading in registration files, run the `regverify` command in *`install_dir`*`\bin\` (`$OV_BIN`) against the Launcher Registration File (WLRF) in the following directory:

Windows: *`install_dir`*`\www\registration\launcher\%LANG%`

UNIX: `/etc/opt/OV/share/www/registration/launcher/$LANG`

You can also hold down the **Shift** key and press the `[Reload]` button on your browser to force the registration files to reload.

RQS nº 08705 - CN -
CPMI - CORREIOS
FIS. Nº 0268
Doc: 3740

Other Sources of Information

Web server log files are available that provide you with information about server-related problems. The error log is located at:

Windows: `\WINNT\System32\Logfiles`

UNIX: `/opt/OV/httpd/logs`

This is the default location, but it may vary depending on where your web service is set to log errors. Check your web server properties to verify the location.

Network Presenter

If the Network Presenter does not start, check the items on page 613, and the following:

- If the Network Presenter progress bar does not appear, it could indicate web server problems. Try connecting to the web server from your browser without starting Network Presenter. For example:

`http://`*`hostname`*`:3443`

- Make sure the Network Presenter is registered with NNM. In NNM on a management station, use the `Help:About HP OpenView` menu. In the dialog box, click `Applications`. Verify that the Network Presenter appears in the list. Alternatively, check the registration directory to ensure that the file `netpresenter` appears. The location is:

  Windows: *`install_dir`*`\share\registration\%LANG%`

  UNIX: `/etc/opt/OV/share/registration/$LANG`

- Make sure that NNM is running on the management station, with the map opened to which the Network Presenter is trying to connect.
- If you tried starting the Network Presenter from the `Tools` or the `Objects` selection in the Launcher, try starting it directly from the URL instead.

If there are missing menu bar or toolbar items, do the following:

- Check the permissions on the registration files registered with Network Presenter. The permissions need to be read by all, and the owner and the group should be set to `bin`. The registration files are located in:

1339
A.

Windows: `install_dir\www\registration\jovw\%LANG%`

UNIX: `/etc/opt/OV/share/www/registration/jovw/$LANG`

- Set the `QUERY_STRING` environment variable to `menus`. Then run `jovwreg.exe` from the command line on the system running NNM. Alternatively, from the browser, use the URL `http://hostname:[port]/OvCgi/jovwreg.exe?menus`
- Run the `regverify` command `install_dir\bin\ ($OV_BIN)` against the Network Presenter Registration Files (NPRF).

If symbols are missing from the Network Presenter, do the following.

- Set the `QUERY_STRING` environment variable to `symbols`. Then run `jovwreg.exe` from the command line on the system running NNM. Alternatively, from the browser, use the URL `http://hostname:[port]/OvCgi/jovwreg.exe?symbols`

If the Network Presenter connected to an `ovw` session that you think you should not be connected to:

- In the Network Presenter, bring up the `Help:About HP OpenView` dialog box. Verify that the session ID is the session ID in the `ovw` session to which you wanted to connect.

If you are not getting dynamic updates to your map:

- Verify that you are connected to a read/write version of the map. To do this, compare session IDs in the Network Presenter and in NNM on the management station. If both a read/write and read-only version of a map are running on the same system, and you want to connect to the read/write version, ensure that the read/write version of the map is started in NNM before the read-only version.

Alarm Browser

If the Alarm Browser does not start when requested, check the items on page 613, and the following:

- Run `ovstatus ovalarmsrv` on the command line. This will tell you if the `ovalarmsrv` service is running. If it is not, execute `ovstart ovalarmsrv`.
- If `ovalarmsrv` is running, stop it using `ovstop ovalarmsrv`, then restart it using `ovstart ovalarmsrv`. This usually clears up the problem.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0269
Fls. Nº
3740
Doc:

- `ovalarmsrv` reads from the event database. Make sure that there is not a problem with this database. Make sure that the `eventdb` directory in *`install_dir`*`\databases\` (`$OV_DB`) and all the files in that directory have read permissions.
- `ovalarmsrv` depends on the `pmd` service to be running. Check to be sure that `pmd` is running.
- Make sure that the specification file *`install_dir`*`\www\conf\NNM.spec` (`$OV_WWW/NNM.spec`) is present and that it has read/write permissions.

If you have trouble running the Alarm Browser:

- Clear the cache in your browser. See the procedure on page 615.
- Use the options to the `ovalarmsrv` command to change the parameters to the command. See the *ovalarmsrv* reference page in NNM's online help (or the UNIX manpage) for more information.

SNMP Data Presenter

If the SNMP Data Presenter does not start, check the items on page 613, and the following.

SNMP Data Presenter is Empty

If the SNMP Data Presenter does not show any data, check the following:

- Make sure JavaScript is enabled in your browser. In Netscape Navigator, select `Edit:Preferences->Advanced`. In Internet Explorer, Java is always enabled.
- Make sure `ovsessionmgr` is running on the server. To check:

  Windows: Use the Task Manager.

  UNIX: Type **`ps -ef | grep ovsessionmgr`**

  If it is not running, then start it by entering the URL for `ovlaunch.exe`.

Access Denied

If you receive an error message indicating that access is denied, that a violation occurred, or that data was not found, check the following:

1337
A

- Check your web server configuration. Verify the port number, alias names, directory names, and permissions. For more information, consult your web server documentation.

If you receive a message that you have a CGI Error or an Internal Server Error, please contact HP Support.

If No Data or Wrong Tree Structure Appears

If no data or the wrong tree structure is shown on the scoping pane:

- Verify the application registration files (ARFs) on the management station. Type:

  Windows: ***install_dir*\bin\regverify**

  UNIX: **$OV_BIN/regverify**

  (Set the LANG environment if necessary.)

  Alternatively, you can enter **http://*hostname*:*[port]*/OvCgi/snmpviewer.exe?ins=check** in your browser.

  If there are errors, fix the errors by editing the ARFs.

New Applications Not Displayed

If you added new applications with Application Builder, but they are not displayed on the scoping pane, clear the cache on your browser following the instructions on page 615, then launch SNMP Data Presenter again.

Results Not Shown, or are Incorrect

If the scoping pane is blank after resizing the browser window or frames:

- Click with the right mouse button on the scoping pane and select `Frame Reload`.

If you click an item in the scoping pane, but the results are not shown in the results pane:

- Check if the target nodes are healthy. Try `ping` or SNMP commands on the management station to the target nodes. See "Network Management Operations" on page 626 for more information.

If results are shown, but errors are indicated:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0270
3740

- All the operations in SNMP Data Presenter are defined in ARFs on the management station. NNM on the management station has the same menu items as in SNMP Data Presenter. Try the operation on the management station. If you still encounter errors, see the sections "Network Management Operations" on page 626 and "Executing MIB Applications" on page 629.

If the format in the results pane is unappealing:

- Make sure a fixed font is specified in the fixed width font setting. In Internet Explorer, select the `View:Internet Options->Fonts` menu item to change fonts. In Netscape Navigator, select the `Edit:Preferences->Appearance->Fonts` menu item.

1.335

Troubleshooting NNM Operations

This section suggests actions to take if you suspect a problem with one of the operations of NNM. This section also discusses the sequence of interactions and/or the flow of data associated with an operation when such information may help you to isolate the problem. This section covers the following:

- Runtime components.
- Network management operations.
- Browsing MIBs.
- Building MIB applications and executing MIB applications built by the MIB Application Builder.
- Collecting MIB information from network nodes at regular intervals.
- Configuring events.
- Event Reduction Capabilities
- Loading MIBs.
- X Windows components.
- Online help.

For detailed information on a command or service mentioned in this section, see its associated reference page in NNM's online help (or the UNIX manpage).

Runtime Components

If you are having problems running NNM, you should check file permissions, start-up scripts, and error log. These topics are discussed below.

Manager File Permissions

By default, the `ovw` (graphical network map) program is executable by anyone; the `ovwdb`, `pmd`, `snmpCollect`, `ovactiond`, `ovtopmd`, and `netmon` background services are executable only by `root`.

The remainder of this section is for UNIX operating systems only.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0271
3740

You may restrict the permissions on the map files using the `$OV_BIN/ovwchmod`, `$OV_BIN/ovwchgrp`, and `$OV_BIN/ovwchown` commands. These commands, along with the `ovwls` command, are explained in the *ovwperms* reference page in NNM's online help (or the UNIX manpage). These commands change all of the map data files associated with a map. You use the commands the same way as the operating system `chmod`, `chgrp`, and `chown` commands, except that you follow them with a map name instead of a file name. Note that these commands do not change permissions on the product's directories or executable files, nor on other configuration and data files.

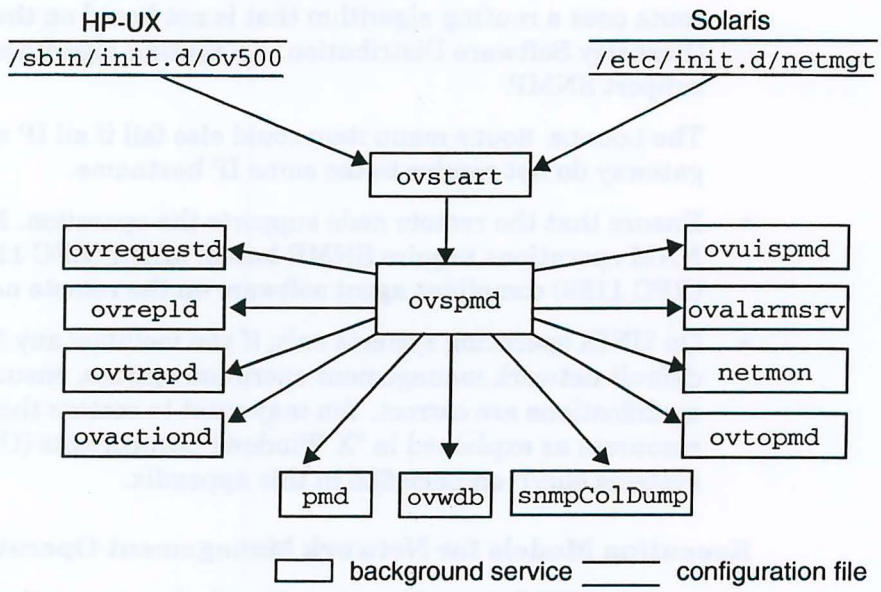
NOTE Do not change map permissions when NNM is running.

If you are having problems running NNM, try restoring the map file permissions to their default using the `ovwchmod` command with mode 0777.

Start-Up Scripts (UNIX operating systems only)

Check to see if some component in the execution sequence is "broken," such as a syntax error in one of the product's start-up scripts. Figure C-5 shows the start-up execution sequence for NNM. All files are in the `$OV_BIN` directory.

Figure C-5 Manager Startup



A script file automatically executes `ovstart` when you reboot the system. The script file has the following name:

- *HP-UX*: `/sbin/init.d/ov500`
- *Solaris 2.X*: `/etc/init.d/netmgt`

If `ovstart` does not execute, the problem may be with the start-up script. The script file is created during installation. If the file already exists, the existing file is moved to another file, and the new one is copied to the original file name. For example, on HP-UX systems the existing file would be moved to `/sbin/init.d/#ov500`, and the new file would be copied to `/sbin/init.d/ov500`.

RQS nº 03/2005 - CN - CPMI - CORREIOS Fls. Nº 0272 3740 Doc:

Network Management Operations

If you are having problems running an operation to a remote node, check the following items.

- If you configured agent community names, verify that the node's community name listed in the `Options:SNMP Configuration` dialog box matches the community name configured on that node.
- The `Locate Route` operation could fail if one of the nodes in the route uses a routing algorithm that is not based on the BSD (Berkeley Software Distribution) 4.2 routing algorithm or does not support SNMP.

  The `Locate Route` menu item could also fail if all IP addresses for a gateway do not resolve to the same IP hostname.
- Ensure that the remote node supports the operation. Most of the NNM operations require SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC 1158) compliant agent software on the remote node.
- On UNIX operating systems only, if you modified any X resources for default network management operation options, ensure that the modifications are correct. You may want to restore the default X resources as explained in "X Windows Components (UNIX operating systems only)" on page 635 in this appendix.

Execution Models for Network Management Operations

Some of the NNM operations start directly from `ovw`; others are started by an integrating service, `xnmappmon`.

1331
A.

Figure C-6 shows some of the network management operations started (or startable) directly by ovw.

Figure C-6 Applications Started Directly by the ovw Service

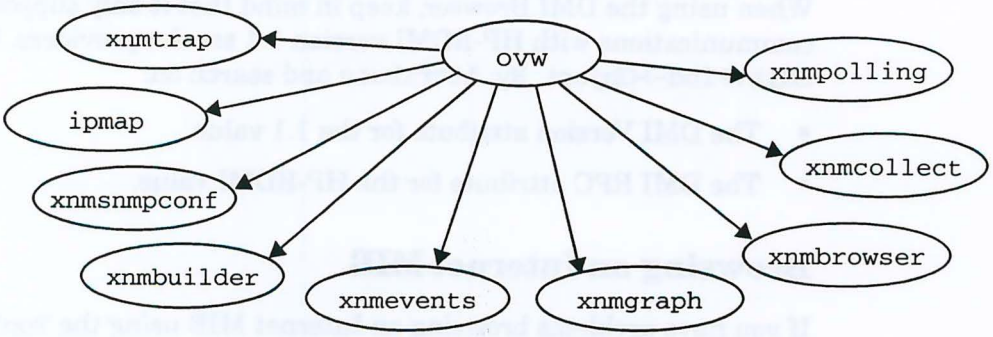
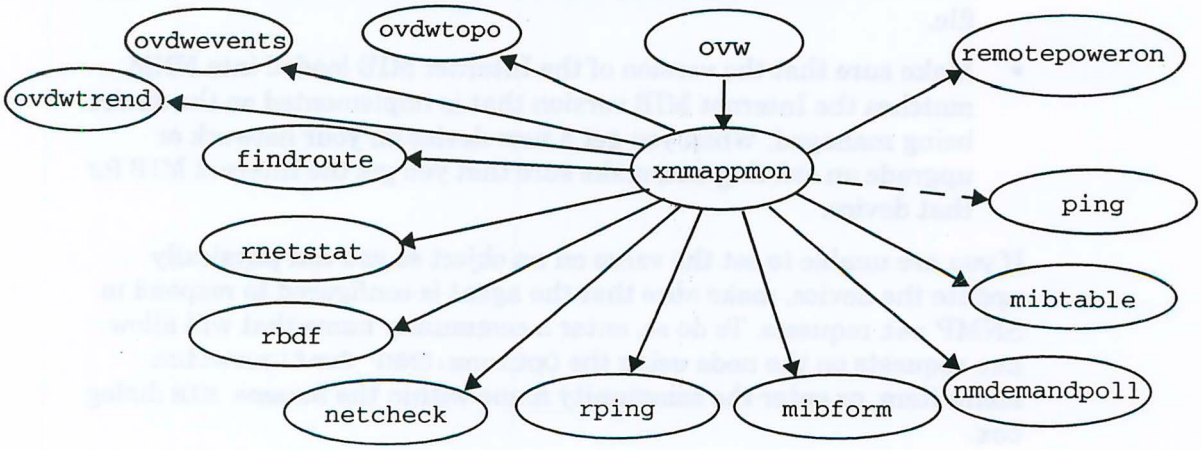


Figure C-7 shows those operations started by xnmappmon.

Figure C-7 Applications Started by xnmappmon



Many of the services shown in the previous two figures may be run as commands for remote troubleshooting. For information about which commands are executed for the different services, see each service's reference page in NNM's online help (or the UNIX manpage). ping is shown as a dotted line because it is a system command.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0273
3740
Doc:

Managing DMI Devices

NNM supports SNMP communications. In order to access DMI devices, you must install a DMI-to-SNMP mapping agent on the DMI system. Then SNMP requests will get processed.

When using the DMI Browser, keep in mind that it only supports DMI communications with HP-RDMI version 1.1 service providers. Use `Edit:Find->Object By Attribute` and search on:

- The DMI Version attribute for the 1.1 value.
- The DMI RPC attribute for the HP-RDMI value.

Browsing an Internet MIB

If you have problems browsing an Internet MIB using the `Tools:SNMP MIB Browser` menu item, check the following:

- Make sure the Internet MIB is loaded. Use the `Options:Load/Unload MIBs:SNMP` menu item to see what modules are currently loaded. If the MIB is not listed, use the `Load/Unload MIBs` menu item to load the Internet MIB into the MIB description file.
- Make sure that the version of the Internet MIB loaded into NNM matches the Internet MIB version that is implemented on the device being managed. When you get a new device on your network or upgrade an existing one, make sure that you get the Internet MIB for that device.

If you are unable to set the value on an object so you can physically update the device, make sure that the agent is configured to respond to SNMP `set` requests. To do so, enter a community name that will allow `set` requests on the node using the `Options:SNMP Configuration` menu item, or enter the community name within the `Browse MIB` dialog box.

Building and Executing MIB Applications

The problems you may encounter while building MIB applications and executing MIB applications built by the MIB Application Builder are closely related.

1.329
(A.

For example, some errors made while building an application may not show up until you actually execute the application. If the problem is an incorrectly built application, you need to modify your application.

This section is organized as follows:

- Things to check when you have problems building an application.
- Things to check when you have problems executing an application. Problems executing applications can be caused by either an error in the way the application was built, or by independent things such as the community name not being configured correctly.

Building MIB Applications

If you have problems building MIB applications using the `Options:MIB Application Builder:SNMP` menu item, check the following:

- Make sure to read the instructions in online help about adding MIB applications.
- Make sure you have the enterprise-specific MIB loaded. Use the `Options:Load/Unload MIBs:SNMP` menu item to see what modules are currently defined. If the MIB is not listed, use the `Load/Unload MIBs` menu item to include the MIB in the loaded MIB database.
- Make sure the MIB object ID you select is supported by the device you are trying to monitor. To verify this, use the `Tools:SNMP MIB Browser` menu item.
- When you create a Table application, you can only select fields from a single table in the MIB tree.
- Make sure that the version of the MIB loaded into NNM matches the MIB version that is implemented on the device being managed. When you get a new device on your network or upgrade an existing one, make sure that you get the MIB for that device.

Executing MIB Applications

If you have problems executing applications built using the `Options:MIB Application Builder:SNMP` menu item, check the following:

- Make sure you have the enterprise-specific MIB loaded. The application does not come up when the MIB for that particular application is not loaded. Use the `Options:Load/Unload MIBs:SNMP`

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0274
3740
Doc:



menu item to see what modules are currently defined. If the MIB is not listed, use the `Load/Unload MIBs` menu item to load the MIB into the MIB description file.

The MIB may be missing; for example, if you load a MIB, build an application, and then unload the MIB or if you copy the application to a new machine and the MIB is not on that machine. Make sure that if you copy the MIB application to another system, you also load the enterprise-specific MIB on that system.

- Make sure the MIB object ID you select is supported by the device you are trying to monitor. To verify this, use the `Tools:SNMP MIB Browser` menu item.
- Make sure the application was built to monitor the device you have selected. The problem may be that the application was built to monitor a different device than the one you are trying to monitor. For example, the application was built for an HP-UX agent, and you are trying to run that application on a Fred Router from Flintstones Company.
- Verify that the management station can talk to the agent. Use the `Tools:SNMP MIB Browser` menu item to verify that the manager station can actually talk to the agent and that the agent is responding with the values. Also, use the `Fault:Test IP/TCP/SNMP` menu item.
- Verify that the community name is set up properly in the `Options:SNMP Configuration` menu item. If you get a message indicating no response from the device, the management station may not have the proper community name defined for that device.
- Make sure that the version of the MIB loaded into NNM matches the MIB version that is implemented on the device being managed. When you get a new device on your network or upgrade an existing one, make sure that you get the MIB for that device.
- Verify that the following three files created by the MIB Application Builder are intact:

  — The registration file in *`install_dir`*`\registration\C\ovmib` (`$OV_REGISTRATION/$LANG/ovmib`, where `$LANG` is the language NNM is set to use). Make sure the registration file name for the application is the same as the application name that was specified when the application was created.

— The help file name is the same as the application name that was specified when the application was created.

The help file is:

Windows: `install_dir\help\C\ovmib\OVW\Functions`

UNIX: `$OV_HELP/$LANG/ovmib/OVW/Functions`

— On UNIX operating systems only, the line entry in the help index file in the `$OV_HELP/$LANG/OVW/functions/INDEX` directory corresponds to your specific MIB application.

- If you typed the object identifier in the MIB selection field, make sure you enter a full object identifier. For example, you cannot create a form application for `.iso.org.dod.internet`. The object ID must correspond to an object supported by the selected device.
- If you configured your Application Builder program to query DMI devices using the corresponding mapped MIB values, and there is no response from the DMI devices, do one of the following:

  — Use the DMI Browser feature of NNM.

  — Install an SNMP agent along with a DMI-to-SNMP mapping agent on the DMI device.

Configuring Events

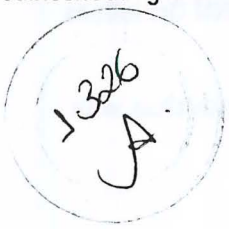
If you have problems configuring events using the `Options:Event Configuration` menu item, first see the vendor documentation that describes the traps generated by that specific device to make sure the enterprise and trap number correspond to what you have indicated.

To get a description of the NNM events shipped with the product, use the `Options:Event Configuration` menu item. From the `Event Configuration` dialog box, select `OpenView` as the `Enterprise Name`, then select an event name and select `Edit:Events->Describe (Describe Event)`.

If you have defined an action for an event, but the action is never taken or it is not executed the way it was intended to, check the following:

- Verify the configuration. When you save the configuration for a new event, the entire `trapd.conf` file is rewritten, and an event is sent to `xnmevents`, `ovactiond`, and `pmd`. Common configuration problems are:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0275
3740
Doc:



  - The command is typed wrong.
  - The arguments are not specified properly.
- Make sure the format message for a particular trap is intact. For example, if the format message for the `coldStart` trap has been erased, you will not see that trap in the event log file or the Alarm Browser window.
- Make sure you do not edit the `trapd.conf` file. The `trapd.conf` file contains the logging and action definitions. If this file is corrupted, the events you have configured may not be logged.
- Use `ovdumpevents` to see if the trap was decoded properly. Each time NNM receives an event, the `pmd` service logs an entry in the event database. For example, the event database identifies ASN.1 coding problems in enterprise-specific traps.
- Verify that the event is logged to the expected category. For example, if you selected `log only`, you will not see the event in the event browser window. If you selected `ignore`, you will not see the event.
- On UNIX operating systems only, compare your `$OV_CONF/C/trapd.conf` file with the default configuration file, `/usr/OV/newconfig/OVEVENT-MIN/conf/C/trapd.conf`.

Event Reduction Capabilities

Event reduction is the process by which you can identify relationships between events. Once identified, a smaller number of new events with the same or higher information content can be generated.

Two event reduction strategies that NNM uses are ECS correlations and Correlation Composer correlators. For more information about these strategies, see "ECS Correlations" on page 360 or "Correlation Composer Correlators" on page 386.

Troubleshooting ECS Correlations

If you are having problems with any of the ECS correlations, see "Troubleshooting" on page 381 for more information.

Troubleshooting Correlation Composer Correlators

If you are having problems with any of the Correlation Composer correlators, see "Troubleshooting" on page 397 for more information.

1.325
4.

Loading Internet MIBs

When you load an Internet MIB, the `Options:Load/Unload MIBs:SNMP` menu item takes all vendors' Internet MIBs and puts them into one single loaded MIB database, *`install_dir`*`\conf\(SOV_CONF) snmpmib`. The `Load/Unload MIBs` menu item creates a binary file, *`install_dir`*`\conf\snmpmib.bin (SOV_CONF/snmpmib.bin)`. The SNMP MIB Browser, MIB Data Collection, MIB Application Builder, and the MIB applications built using the MIB Application Builder access the loaded MIB database for their routines.

NOTE Always use the `Options:Load/Unload MIBs:SNMP` menu item to modify the loaded MIB database; do *not* edit the loaded MIB database directly.

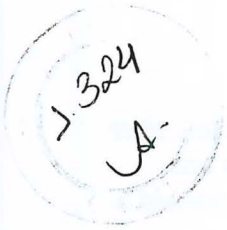
If you have problems including Internet MIBs in the MIB description file using the `Options:Load/Unload MIBs:SNMP` menu item, check the following:

- Make sure that the format of the MIB definition is correct. For example, it must have an ASN.1 module `DEFINITIONS` clause. The enterprise-specific files should only contain modules that are unique to that vendor.

  The format must conform to *RFC 1155*, *RFC 1212*, *RFC 1902*, *RFC 1903* or *RFC 1904*. *RFC 1155* and *RFC 1212* apply to the SNMPv1 SMI, while *RFC 1902*, *RFC 1903*, and *RFC 1904* apply to the SNMPv2 SMI.

- Make sure that the syntax is correct. Hewlett-Packard has verified that the syntax of the MIB modules included with the NNM product is correct. However, if you get the MIB module directly from the vendor, you may have to correct syntax errors. The `Options:Load/Unload MIBs:SNMP` menu item checks for syntax errors and displays an error that tells you where the error is and how to fix it. The most common syntax errors are typing errors and non-conformance to the RFCs.
- Compare the MIB with the Hewlett-Packard MIB to look for errors. By comparing the MIB that does not load with the Hewlett-Packard MIB, you may be able to troubleshoot the problem. The Hewlett-Packard MIB loads correctly.

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0276
3740
Doc:



Known Limitations

The object label in a MIB module must be unique. Due to lack of standards this is not clearly identified by SNMP. If you have mnemonic names for an object ID component that is used elsewhere in the module, the second object shows up in the MIB tree under the first object that has the common component name. Furthermore, the translation from the mnemonic object name to the numeric object ID will be incorrect, causing SNMP queries to fail.

For example, suppose the xyzCorp has the enterprise MIB `device` object defined in a module XYZCORP-MIB under `.iso.org.dod.internet.private.` as

```
enterprises.xyzCorp.bridge.device.name
                                  .number
                                  .ROMid
```

and another `device` object defined as

```
enterprises.xyzCorp.hub.device.model
                                  .serialNumber
                                  .otherInfo
```

The MIB parser cannot distinguish between the two `device` objects. As a result, the xyzCorp fields `model`, `serialNumber`, and `otherInfo` will appear incorrectly in the Internet MIB tree as

```
enterprises.xyzCorp.bridge.device.model
                                  .serialNumber
                                  .otherInfo
```

To circumvent the problem, patch the enterprise-specific MIB to use a unique component name. For this example, change `.hub.device` to `.hub.hubdevice`. When the object name is translated to the numeric object ID used in the SNMP query, the proper object ID will be used and the SNMP query should work.

A second (and more contrived) alternative is to put the second and any subsequent occurrences of duplicate object labels (and any objects based on them) in a separate ASN.1 module with a fully-qualified reference as to their proper position in the global Internet MIB tree.

For example, the first occurrence of `device` could be defined in a module as

```
XYZCORP1-MIB DEFINITIONS ::= BEGIN
xyzCorp OBJECT IDENTIFIER ::= { iso org(3) dod(6) internet(1) private(4)
                                  enterprises(1) 999 }
```

1.323
A.


```
    bridge  OBJECT IDENTIFIER ::= { xyzCorp 1 }
    device  OBJECT IDENTIFIER ::= { bridge  1 }
     -- all subsequent children...
        .
        .
        .
END
```

and the second in a module as

```
XYZCORP2-MIB DEFINITIONS ::= BEGIN
hub OBJECT IDENTIFIER ::= { iso org(3) dod(6) internet(1) private(4)
                                              enterprises(1) xyzCorp(999) }
   device  OBJECT IDENTIFIER ::= { hub  1 }
    -- all subsequent children...
        .
        .
        .
END
```

X Windows Components (UNIX operating systems only)

This section discusses X Windows-related files for NNM only. If the problem does not appear to be with this product, refer to your X Windows documentation for further troubleshooting information.

To verify the status of the background services, run the `ovstatus` command. For more information about `ovstatus` and how to troubleshoot the background services, see "Troubleshooting Background Services" on page 584 in this appendix.

To determine whether there is a problem with the X Windows component of NNM, try restoring the default X resources for this product, and see if this solves the problem.

1. Ensure that the files in the `$APP_DEFS` directory contain the installed X resource defaults for the product: `XNm`, `OVw`, `XNmevents`, `XNmgraph`, `OVHelp`, etc.

   The X resource defaults are listed in the *ovw* and *ovhelp* manpages. The `XNm` resource defaults are listed in the `XNm` resource file itself.

2. Ensure that the `XENVIRONMENT` shell variable is not set.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0277
Doc: 3740



3. Remove resources starting with `XNm`, `XNmevents`, `XNmgraph`, `OVw`, or `ovhelp` from your `$HOME/.Xdefaults` file. Or, temporarily rename this file.
4. Restart X Windows.
5. Restart `ovw` (`$OV_BIN/ovw`) without any X resources specified as arguments.

Online Help

The text files used for the NNM Help operations (not including reference pages or UNIX manpages) are below the directory *`install_dir`*`\help\C\help\C` (`$OV_HELP/help/C`). On UNIX operating systems only, you can also use the `man` command on the manpage name.

1-321
A.

Troubleshooting Windows Applications

This section discusses troubleshooting applications on Windows operating system.

Problems Launching Applications

If you experience problems launching the Event Viewer, Performance Monitor, Registry Editor, or Windows Diagnostics, and an error message like `Permission denied` or `Access denied` appears after launching the application, it may be that you do not have enough privileges to be able to administer or view the remote computer's properties.

Windows Operating System Tools

The Windows operating system tools, listed below, can assist you in troubleshooting Windows applications. These tools appear on NNM's menus, depending on the applications on your system. There can be up to eight Windows tools menu items:

- `Fault:Windows Event Viewer` — always present
- `Performance:Windows Performance Monitor` — always present
- `Configuration:Windows Registry Editor` — present only if the currently logged-on user has Administrative privileges
- `Fault:Windows Diagnostics`
- `Server Manager` and `User Manager` — present only if running on a Windows server (as opposed to a Windows workstation)
- `SMS Properties` and `Run SMS` — present only if SMS Administrator software has been installed

  If you launch SMS and do not see an OpenView icon when viewing the properties on a node, verify that NNM is running.

  If you have installed SMS Administrator software on your system and the two SMS-related menu items are missing, ensure that you installed SMS version 1.2 — only version 1.2 is supported.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0278
3740
Doc:

In order to be able to view SMS properties for a node selected on the NNM map, you must copy the `machview.exe` utility from your SMS CD-ROM to the `smsadmin\x86.bin` directory where SMS Administrator software is installed.

1·319
A.

Recommended Logging and Tracing Practices

The following sections discuss the logging and tracing practices of Network Node Manager.

Logging and Tracing

Table C-2 lists the two logging and tracing facilities used by NNM.

Table C-2 Logging and Tracing Facilities

For this service	Use this facility

`pmd`
`netmon`
`ovactiond`
`ovalarmsrv`
`ovcapsd`
`ovrepld`
`ovrequestd`
`snmpCollect`
	Command line options.
	See the reference pages in NNM's online help (or the UNIX manpages) for the command options for these background services.

`ipmap`
`ovspmd`
`ovtopmd`
`ovuispmd`
`ovwdb`
	Windows Event Viewer. Also see the *ovtracelog* reference page in NNM's online help (or the UNIX manpage).
	`nettl` for logging and tracing.
	`netfmt` to format and view the logged data.

NOTE Tracing is normally used only by support personnel. Tracing, especially in the case of `netmon`, can cause the trace file to grow extremely large (multiple megabytes in size) fairly quickly. If you use tracing, remember to monitor the size of the trace file frequently, and turn tracing off as soon as you are finished.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0279
Fls. Nº
3740
Doc:

Using Command Line Options

The following section describes logging and tracing options for the NNM background services pmd, netmon, ovactiond, snmpCollect, and ovalarmsrv.

The *install_dir*\bin\pmd (`$OV_BIN/pmd`) event logging facility has the following characteristics:

- The default logging is set to ON. Specify the `n` option in the `pmd.lrf` to prevent event logging.
- The event log database is, by default, set to 16 MB. When this space is used up, the oldest log is truncated, and new events are written into the reclaimed space. Refer to the *ov_event* reference page in NNM's online help (or the UNIX manpage) for more information.

The *install_dir*\bin `$OV_BIN/pmd` background service logging facility has the following characteristics:

- The default logging is set to log WARNING, ERROR, and DISASTER.
- The log file is *install_dir*\log\pmd.log0 (`$OV_LOG/pmd.log0`). When this log file is filled to a user-configurable size, its contents are automatically moved to the file *install_dir*\log\pmd.log1 (`$OV_LOG/pmd.log1`).

The *install_dir*\bin\pmd (`$OV_BIN/pmd`) event and service tracing facility has the following characteristics:

- The default tracing is set to OFF. Specify the `T` option in the `pmd.lrf` file to enable tracing.
- The trace file is *install_dir*\log\pmd.trc0 (`$OV_LOG/pmd.trc0`). When this trace file is filled to a user configurable size, its contents are automatically moved to the file *install_dir*\log\pmd.trc1 (`$OV_LOG/pmd.trc1`).
- When tracing is turned on, event traces are also found in the trace file.

The *install_dir*\bin\netmon (`$OV_BIN/netmon`) tracing facility has the following characteristics:

- The default tracing is set to OFF.

- The default trace and hexdump file is *install_dir*\log\netmon.trace ($OV_LOG/netmon.trace).
- To turn tracing on, run netmon -M *tracemask* at the command line, or add the -m *tracemask* option to netmon.lrf.
- To turn tracing off, specify netmon -M 0 (zero).

The following information explains the variable *tracemask* discussed in the netmon tracing facility. Trace masks specify the type of output listed in netmon's trace file. To select multiple output types, add the individual *tracemask* values together and enter the sum. netmon has the following tracing options:

0	Turn off tracing.
1	Trace ICMP echo requests.
2	Trace ICMP echo replies and timeouts.
4	Trace SNMP requests.
8	Trace SNMP replies and timeouts.
16	Trace traps generated.
32	Trace traps received.

Some examples follow. These assume netmon is already running.

To trace ICMP echo replies and timeouts, enter the following command:

```
netmon -M 2
```

To trace ICMP echo replies and timeouts, as well as SNMP replies and timeouts, add their *tracemask* values (2 + 8) to determine the *tracemask* value to enter:

```
netmon -M 10
```

The *install_dir*\bin\ovactiond ($OV_BIN/ovactiond) tracing facility has the following characteristics:

- The default tracing is set to ON.
- The default tracing file is *install_dir*\log\ovactiond.log ($OV_LOG/ovactiond.log) and *install_dir*\log\ovactiond.log.old ($OV_LOG/ovactiond.log.old).
- To turn verbose tracing on and off when tracing is on, specify ovactiond -V (toggle ON/OFF).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0280
Doc: 3740

- The `-t` option must have a value greater than 0 (zero) to see the return value of the event actions.

The *install_dir*`\bin\ovalarmsrv` (`$OV_BIN/ovalarmsrv`) tracing facility has the following characteristics:

- By default, logs only errors.
- Logs errors to *install_dir*`\log` (`$OV_LOG`) `ovalarmsrv.trace`.

  To change the level of logging that is performed, edit the LRF file and add `-D2` as a parameter. This will increase the logging information (for example, add tracing information as well).

The *install_dir*`\bin\snmpCollect` (`$OV_BIN/snmpCollect`) logging facility has the following characteristics:

- The default logging is set to ON.
- The data that is collected is stored in the file *install_dir*`\log\snmpCol.trace` (`$OV_LOG/snmpCol.trace`).

The *install_dir*`\bin\snmpCollect` (`$OV_BIN/snmpCollect`) tracing facility has the following characteristics:

- The default tracing is set to OFF.
- The default tracing is limited.
- The default trace file is *install_dir*`\log` (`$OV_LOG`) `snmpCol.trace` and *install_dir*`\log` (`$OV_LOG`) `snmpCol.trace.old`.
- To turn the tracing on and off, specify `snmpCollect -T` (toggle ON/OFF) while `snmpCollect` is running.
- To turn verbose tracing on and off when tracing is on, specify `snmpCollect -V` (toggle ON/OFF) while `snmpCollect` is running.
- To trace `snmpCollect` initialization, add the options `-T -V` to *install_dir*`\lrf\snmpCollect.lrf` (`$OV_LRF/snmpCollect.lrf`). This turns off verbose tracing from the moment `snmpCollect` starts up.

Using the Windows Application Event Log

NNM services perform logging (to capture network activities such as state changes, errors and connections) and tracing (to capture inbound and outbound packets going though the network, as well as loopback or header information). All tracing and logging is directed to the Windows

1.315
4

Event Log and can be accessed through the Windows Event Viewer application. See the *ovtracelog* reference page in NNM's online help (or the UNIX manpage) for further details. You can use the following troubleshooting tools:

- **tracing**, which records a detailed record of internal events taking place within the software. Tracing of the NNM background services is generally only used on the advice of HP Support to diagnose difficult problems, with the aid of the source code. API tracing is used by developers to determine whether they are using the HP OpenView APIs correctly.
- **logging**, which records externally-observable events such as connection establishment or termination of child services, and errors, which background services ordinarily have no other way of reporting.

Users should run tracing only when something is seriously wrong, and only on the advice of your HP support representative when it is necessary to reconstruct in detail the sequence of events that caused the problem. The trace output is intended to be interpreted by the developers of the NNM product, with the source code at hand. It is not intended to be meaningful to the ordinary user.

Using nettl and netfmt (UNIX operating systems only)

`nettl` and `netfmt` enable system administrators and developers to gather and view data about the operation of NNM software. `nettl` is the administrative interface to the tracing and logging facilities discussed previously.

It is recommended that you run the `nettl` logging facility at all times. This way, you can view the constantly updated log file to help you determine what happened when something goes wrong. Also, paradoxically, performance is better when logging is turned *on*.

`netfmt` formats the log and trace output into human-readable form.

Services use `nettl` to log or trace in particular subsystems. To examine the log or trace output of a service, you need to know the name of the subsystem the service uses. Table C-3 shows the subsystems and services.

NOTE The `nettl` and `netfmt` commands are in `$OV_BIN`. For example, to run the `nettl -status` command, you would type:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0281
3740
Doc:

```
$OV_BIN/nettl -status
```

Table C-3 Subsystem Services

Subsystem	Services Using this Subsystem	Purpose of Service
OVS	ovspmd	Starts and stops NNM background services.
OVW	ovwdb, ipmap	Provides access to object database. Automatically draws IP topology maps.
OVEXTERNAL	ovuispmd; ovtopmd; also any third-party-developed software using the OVuTL facility.	Maintains the topology database.
OVWAPI	Any software using the OVw (HP OpenView Windows) API.	Provides programmatic application integration points.

Capturing Logging and Tracing Output with nettl (UNIX operating systems only)

1. To determine whether the logging/tracing facilities are currently running, type the following command as root:

   nettl -status

   The output includes the log and trace status for each active subsystem.

2. If necessary, use the nettl command to start the logging/tracing facilities. As root, type the following command:

   nettl -start

   This command initializes the logging/tracing facilities and starts the default logging. By default, the OVS, OVW, OVWAPI, and OVEXTERNAL subsystems log error and disaster messages; the OVS subsystem also logs informative messages.

1.313
A

3. Once nettl is running, you can use command options to customize the kind of data you want to capture for any of the nettl subsystems shown in the previous table. The next section contains examples of various nettl commands.

Examples of nettl Commands Use the following examples to get started. After you have captured the data you want, go to "Formatting Network Data with netfmt" on page 649 in this section.

- **Logging Facility** - Turning it on.

  There are four classes of logging messages: informative (i), warning (w), error (e), and disaster (d). Default logging always includes disaster-class messages; you can turn on any of the other three classes by typing a nettl command for a specific subsystem.

  The command syntax is:

```
nettl -log class -entity subsystem OVEXTERNAL
```

`-log class`

Specifies the classes of logging to be turned on for the specified subsystems.

`-entity subsystem`

Specifies the subsystems for which logging is to be modified. *For logging done by HP OpenView products,* OVEXTERNAL *must always be in the list.*

Example 1:

Turn on logging of informative messages for the ovw subsystem. As root, type the following command:

```
nettl -log i -entity OVW OVEXTERNAL
```

Note that this command will turn off any log classes not listed in the command (in this example, the warning and error messages would be turned off). The one exception is disaster logging, which cannot be turned off.

Example 2:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0282
3740
Doc:

Turn on logging of informative, warning, and error messages for the OVS subsystem. As root, type the following command:

```
nettl -log i w e -entity OVS OVEXTERNAL
```

- **Tracing Facility** - Turning it on.

  There are eight kinds of tracing that nettl can turn on, as shown in the following table.

Table C-4 Tracing Facilities Activated by nettl

Type of Tracing	Keyword	Mask Number
inbound header tracing	hdrin	0x80000000
outbound header tracing	hdrout	0x40000000
inbound PDU tracing	pduin	0x20000000
outbound PDU tracing	pduout	0x10000000
procedure entry/exit tracing	proc	0x08000000
state machine tracing	state	0x04000000
error tracing	error	0x02000000
log call tracing	logging	0x01000000

The command syntax is:

nettl -traceon *kind* -entity *subsystem* OVEXTERNAL -file *filename*

-traceon *kind*

Specifies the kinds of tracing to be turned on for the specified subsystems.

-entity *subsystem*

Specifies the subsystems for which tracing is to be turned on. *For tracing done by HP OpenView products,* OVEXTERNAL *must always be in the list.*

-file *filename*

1.311

Specifies the prefix of the trace file you want to create. Trace output will be written to *file*.TRC0 and *file*.TRC1. (See "How nettl Generates the Binary Data Files" on page 648 for a description of these two trace files.)

Example 1:

Do error tracing for the OVW subsystem, putting the data in the trace files, /tmp/nettl.TRC0 and /tmp/nettl.TRC1. As root, type the following all on one line:

```
nettl -traceon error -entity OVW OVEXTERNAL -file /tmp/nettl
```

Example 2:

Do both inbound and outbound PDU tracing for the ovw subsystem, putting the data in the trace files, /tmp/nettl.TRC0 and /tmp/nettl.TRC1. To enable more than one kind of tracing, either specify all the appropriate keywords, all the appropriate mask numbers, or the logical OR of the mask numbers. As root, type one of the following command variations:

```
nettl -traceon pduin pduout -entity OVW OVEXTERNAL -file /tmp/nettl
```

or

```
nettl -traceon 0x20000000 0x10000000 -entity OVW OVEXTERNAL -file /tmp/nettl
```

or

```
nettl -traceon 0x30000000 -entity OVW OVEXTERNAL -file /tmp/nettl
```

NOTE Do not leave off the -file argument to nettl -trace on! If you do, unformatted trace output will be sent to your screen.

- **Tracing Facility** - Turning it off.

  While logging should always remain on, you should run the tracing facility only when a serious problem occurs, and it is necessary to reconstruct in detail the sequence of events that caused the problem. After you have completed a trace, you should turn tracing off.

  The command syntax is:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0283
3740
Doc:

```
nettl -traceoff -entity subsystem
```

`-traceoff` Specifies that tracing is to be turned off for the specified subsystems.

`-entity subsystem`

Specifies the subsystems for which tracing is to be turned off. To turn tracing off completely, specify all subsystems for which tracing is currently on.

Note that you cannot turn off trace kinds individually. To change the trace kinds enabled for a subsystem, turn tracing off for that subsystem, then turn tracing back on for the particular kinds in which you are interested.

Example 1:

Disable tracing for the `OVEXTERNAL` subsystem. As `root`, type the following command:

```
nettl -traceoff -entity OVEXTERNAL
```

- **Logging and Tracing Facilities** - Turning both off.

  To stop the logging/tracing facilities, as `root`, type the following command:

  ```
  nettl -stop
  ```

How nettl Generates the Binary Data Files The first time you run a `nettl` command for capturing logging data, the log file `nettl.LOG00` is generated. Binary data captured from each successive `nettl` logging command is appended to this file, until it is filled. Then a second log file with the suffix `.LOG01` is created in which new data is stored. When this second file fills up, the `.LOG00` file is overwritten.

When you run a `nettl` command for capturing trace data, you specify a filename prefix, to which the suffix `.TRC0` is added. For each successive `nettl` tracing command, you can have the binary data appended to this file, or you can specify a new file in which to store the data. If you append binary data from successive traces to the same file, it will eventually fill up. A new file with the same prefix and the suffix `.TRC1` will then be created for storing new data. If this second file fills up, then a new trace file with the same prefix and the `.TRC0` suffix is created.

If you need to check the name of a log file before formatting it with `netfmt`, use a `nettl -status` command.

1.309

Formatting Network Data with netfmt The command syntax is:

`netfmt -f binary_file`

`-f binary_file`

Specifies the log or trace file containing the binary data

It is possible to do elaborate filtering of the output, as `netfmt` has many other options that cannot be described here. Some of these options, for example, let you specify the output of a log or trace file to be filtered by timestamp, subsystem, or message class. UNIX only: for more information, see the *netfmt* manpage.

Examples of netfmt Commands The following example will help you start using the `netfmt` command.

To format the log file, `$NETFMT_LOG_FILE`, type

`$NETFMT/netfmt -f $NETMFT_LOG_FILE | more`

The next section shows what the output of `netfmt` looks like.

Log and Trace File Output Below are two complete examples of using the `nettl` and `netfmt` commands, and the final output you might see.

Example 1:

1. You ran a `nettl` logging command for informative messages in the OVW subsystem, in order to observe the startup of the `ovspmd` service, by typing:

   `nettl -log i e d -entity OVS OVEXTERNAL`

   The binary data was stored in the `$NETFMT_LOG_FILE` log file.

2. You formatted and displayed the binary log file by typing:

   `netfmt -f $NETFMT_LOG_FILE | more`

   The output would be similar to the following:

```
**********OpenView**********@#%

Timestamp        : Wed Nov 17 1995 17:28:58.441517
Process ID       : 22756          Subsystem     : OVS
User ID ( UID )  : 0              Log Class     : INFORMATIVE
Device ID        : -1             Path ID       : -1
Connection ID    : -1             Log Instance  : 0
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0284
3740
Doc:

```
Software          : ovspmd
Hostname          : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Initialized successfully:
ovspmd

**********OpenView**********@#%

Timestamp         : Wed Nov 17 1995 17:28:59.352086
Process ID        : 22756          Subsystem      : OVS
User ID ( UID )   : 0              Log Class      : INFORMATIVE
Device ID         : -1             Path ID        : -1
Connection ID     : -1             Log Instance   : 0
Software          : ovspmd
Hostname          : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Accepted request connection (fd 5)

**********OpenView**********@#%

Timestamp         : Wed Nov 17 1995 17:28:59.355761
Process ID        : 22756          Subsystem      : OVS
User ID ( UID )   : 0              Log Class      : INFORMATIVE
Device ID         : -1             Path ID        : -1
Connection ID     : -1             Log Instance   : 0
Software          : ovspmd
Hostname          : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Received request,  fd 5
[9]  [START] ""

**********OpenView**********@#%

Timestamp         : Wed Nov 17 1995 17:28:59.358398
Process ID        : 22756          Subsystem      : OVS
User ID ( UID )   : 0              Log Class      : INFORMATIVE
Device ID         : -1             Path ID        : -1
Connection ID     : -1             Log Instance   : 0
Software          : ovspmd
Hostname          : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Building master M table from $OV_CONF/ovsuf

**********OpenView**********@#%

Timestamp         : Wed Nov 17 1995 17:28:59.366810
Process ID        : 22756          Subsystem      : OVS
User ID ( UID )   : 0              Log Class      : INFORMATIVE
Device ID         : -1             Path ID        : -1
Connection ID     : -1             Log Instance   : 0
```

1.307
A.


```
Software          : ovspmd
Hostname          : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Reporting M status,  code = SUCCESS
    object manager name:  OVsPMD
    behavior:             OVs_PMD
    state:                RUNNING
    PID:                  22756
    exit status:          -
```

Example 2:

1. You ran a `nettl` tracing command for procedure tracing in the `OVEXTERNAL` subsystem, in order to observe some procedure calls in `ipmap`, by typing:

```
nettl -traceon proc -entity OVEXTERNAL -file $NETFMT_LOG_FILE
```

The binary data was stored in the trace file `$NETTL_TRC_FILE`.

2. You formatted the binary trace file by typing:

```
netfmt -f $NETTL_TRC_FILE > outfile
```

A brief fragment of the output appears below:

```
*********************OpenView*********************************@#%

Timestamp         : Wed Nov 17 1993  18048:44.443027
Process ID        : 23059          Subsystem      : OVW
User ID ( UID )   : 214           Trace Kind      : Proc. Entry/Exit
Device ID         : -1               Path ID       :  -1
Connection ID     : -1
Software          : $OV_BIN/ipmap
Hostname          : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

FieldBinding::FieldBinding(OVwFieldBinding) entered

*********************OpenView*********************************@#%

Timestamp         : Wed Nov 17 1993  18:04:44.444646
Process ID        : 23059          Subsystem      : OVW
User ID ( UID )   : 214            Trace Kind     : Proc. Entry/Exit
Device ID         : -1             Path ID        : -1
Connection ID     : -1
Software          : $OV_BIN/ipmap
Hostname          : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

FieldBinding::init() entered

*********************OpenView*********************************@#%
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0285
3740
Doc:

```
Timestamp          : Wed Nov 17 1993  18:04:44.446053
Process ID         : 23059          Subsystem      : OVW
User ID ( UID )    : 214            Trace Kind     : Proc. Entry/Exit
Device ID          : -1             Path ID        : -1
Connection ID      : -1
Software           : $OV_BIN/ipmap
Hostname           : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

FieldBinding::init() exit

**********OpenView**********@#%

Timestamp          : Wed Nov 17 1993  18:04:44.447404
Process ID         : 23059          Subsystem      : OVW
User ID ( UID )    : 214            Trace Kind     : Proc. Entry/Exit
Device ID          : -1             Path ID        : -1
Connection ID      : -1
Software           : $OV_BIN/ipmap
Hostname           : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

FieldBinding::copyFieldValue() entered

**********OpenView**********@#%

Timestamp          : Wed Nov 17 1993  18:04:44.448754
Process ID         : 23059          Subsystem      : OVW
User ID ( UID )    : 214            Trace Kind     : Proc. Entry/Exit
Device ID          : -1             Path ID        : -1
Connection ID      : -1
Software           : $OV_BIN/ipmap
Hostname           : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

FieldBinding::copyFieldValue() exit

**********OpenView**********@#%

Timestamp          : Wed Nov 17 1993  18:04:44.450233
Process ID         : 23059          Subsystem      : OVW
User ID ( UID )    : 214            Trace Kind     : Proc. Entry/Exit
Device ID          : -1             Path ID        : -1
Connection ID      : -1
Software           : $OV_BIN/ipmap
Hostname           : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

FieldBinding::FieldBinding(OVwFieldBinding) exit
```

1.305
A.

Web Launcher Error Log

The Launcher error log records internal errors from the Launcher. You can use the output from this file when discussing a problem with HP support personnel.

The Launcher error log file is located in:

Windows: `install_dir\www\logs\launcher\error_log`

UNIX: `/var/opt/OV/www/launcher/error_log`

The error log contains the following information:

- Date
- Host
- User
- Session
- Reason or error

The error log file continues to grow without bounds. You need to watch the size of this file and truncate it as needed.

If the error log file does not give you sufficient information for troubleshooting, you can set a parameter in the URL for `ovlaunch.exe` that will enable more in-depth error logging on a session level.

The parameter is:

`http://hostname:[port]/OvCgi/ovlaunch.exe?Debug=/tmp/file`

The output of this file is less "friendly" than other error log files, but it contains valuable information that may be useful to an HP support person who is trying to assess the problem.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0286
3740
Doc:

Improving Traffic Management and Performance

Traffic Management

Status polling generates the most network traffic. You can monitor the traffic generated by NNM by using the `netstat -s` command. Run the `netstat -s` command several times and observe the differences in the number of packets sent and received. Be sure that the management station is not generating any other outbound traffic. Note that the command used to show the number of packets sent and received may be different depending on the operating system you use. Make sure that you are using the appropriate command.

You can regulate the traffic generated by NNM through the following methods:

- Adjust polling intervals through the `Options:SNMP Configuration` or `Options:Network Polling Configuration` menu item. Reducing the amount of polling traffic by lengthening polling intervals may delay real-time map updates, resulting in a less accurate map.
- Apply a discovery filter to ensure that you are monitoring only what needs to be monitored.
- Unmanage nodes with the `Edit:Unmanage Objects` menu item such that you are monitoring only what really needs to be monitored. Note that this tactic decreases the amount of available management information for unmanaged nodes.
- Adjust the amount of MIB data that is collected through the `Options:Data Collection & Thresholds:SNMP` menu item. You can:
  - Stop collecting MIB data on some of the MIB objects that are configured to collect data by changing the status to `Suspend`.
  - Modify the details of the configured MIB objects by either deleting nodes, deleting instances, excluding nodes, or changing polling intervals.

1.303
A

If NNM starts to use excessive swap space, performance may decrease. To check the size of ovw (and other services), use `Help:About HP OpenView`, and click `More Info`. If the service grows too large, exit NNM and restart it. (The program automatically saves the map between invocations.)

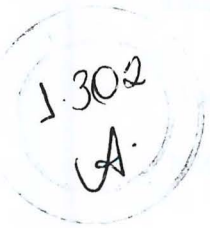
netmon will generate some network broadcast traffic; how much traffic depends on several factors.

- If you use netmon without the -J option, netmon generates, if necessary, just an ARP Request. There are several factors that determine whether netmon needs to generate an ARP Request.
  - For nodes that are up, but not on the same subnet where the management station is, netmon generates just one ICMP echo request packet and gets back one response. In this case, no ARP Request is generated.

    Because the management station is on a different subnet, a request will go through a gateway. Gateways always have large ARP caches. netmon knows the gateway's link-level address and does not have to broadcast an ARP Request to that gateway. netmon only has to send one ICMP echo request through the gateway and gets back one response.
  - For devices that are on the same subnet as the management station, netmon may generate just one ICMP echo request, or it may also generate one ARP Request as well. Because the nodes are on the same subnet, netmon does not have to go through a gateway. Broadcasting an ARP Request will depend on whether or not netmon has in its own ARP cache in the device's link-level address.
  - netmon will generate an ARP Request based on whether the address that is being polled for status is still in the ARP cache of that system.

    The presence of the address in the ARP cache is affected by how many nodes are on the subnet, and by how much physical memory is in the system (some systems will automatically adjust the size of their ARP table).
- If invoked with the -J option, netmon may cause up to three broadcast ICMP echo requests to be broadcast on each subnet it discovers. These broadcasts will only be issued on a subnet if:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0287
3740
Doc:



  - — No broadcast ICMP echo request has ever been issued on this subnet on behalf of this management station.
  - — An agent capable of issuing a broadcast ICMP echo request on `netmon`'s behalf has been discovered on this subnet. All HP-UX SNMP agents have this capability.
- The amount of `netmon`'s broadcast traffic also depends on your network's configuration, including:
  - — How many nodes are up and how many are down.
  - — How many nodes are on the same subnet.
  - — How many nodes are on other subnets.
  - — How large the permanent ARP cache is.
  - — How probable it is that a particular IP address can be found in the permanent ARP cache.
- For IPX discovery, `netmon` uses broadcast IPX packets as the basis of its discovery. The following broadcasts occur for each discovery interval:
  - — A single broadcast RIP request.
  - — A single broadcast SAP request.
  - — Two broadcast IPX diagnostic requests for each known IPX network, 10 seconds apart.
  - — You can change or schedule the IPX discovery interval using `Options:Network Polling Configuration` operation

Performance

The performance of NNM is limited primarily by three factors:

- The amount of memory installed in the manager system.
- The management station's processor (CPU) speed.
- The performance of the graphical display adapter (X Windows).

Minimum system requirements and memory recommendations are detailed in the *Performance and Configuration* guides for NNM.

1301
A.

One good way to find out if your management station has sufficient memory is to select the icon for your management station on the map. Then select the `Performance:Network Polling Statistics` menu item. If the graph shows negative numbers, the polling queue has fallen behind because of resource shortage.

Following are some tips to conserve memory and increase performance:

- You may want to install additional memory and/or upgrade your CPU.
- Reduce the number of devices that need to be monitored, thus decreasing the polling load. Refer to "Controlling the Amount of Traffic Generated by NNM" on page 178 for more information.
- Change the polling interval setting to a less frequent interval. Refer to "Controlling the Amount of Traffic Generated by NNM" on page 178 for more information.
- If you are currently running OVW sessions directly on a management station, you can improve system performance by running OVW sessions on an NNM remote console instead.
- You can reduce NNM's memory usage by changing `ipmap`'s persistence level to a higher level than `All Levels`. See *A Guide to Scalability and Distribution* for more information.
- Run `ipmap` with the `-D 2` option. This option prevents the automatic creation of node submaps for end nodes (unless an end node is a gateway). Nodes with submaps that have not been created are marked with an empty string on the label. See the *ipmap* reference page in NNM's online help (or the UNIX manpage) for information on how to use the `-l` or `-L` options to modify this empty string. Double-clicking on such a node will result in the creation of the submap. The advantage of this option is that no memory is used for end node submaps that are never viewed. The disadvantage is that the locate operation will not work for addresses for end nodes.

  The option can be set in:

  Windows: `install_dir\registration\C\ipmap`

  UNIX: `$OV_REGISTRATION/C/ipmap`
- Partition the environment into multiple maps. See "Partitioned Internet Submaps" on page 248 for more information on partitioning submaps.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0288
3740
Doc:

- Delete unwanted nodes. After the nodes on a particular network have been discovered, you may want to delete some of the nodes, for example, PCs that are not being managed directly.
- Restart the system after active discovery. Some extra memory is consumed in the source of active discovery. After active discovery is finished, it may help to stop and restart the system to recover memory used during the discovery process.
- Use the on-demand submap feature, which may greatly reduce the amount of memory required. The drawback is that when opening transient submaps, some extra processor work will be expended and some delay may be noticeable.
- NNM on a Windows operating system performs best if you use DNS. If you are going to use DNS, enable DNS for Windows Resolution and configure DNS correctly. In particular, when installing NNM, the IP hostname and Windows computer name of the intended NNM Manager must be correct and identical.

Performance on UNIX Operating Systems

On UNIX operating systems only, you can also increase performance in some cases by minimizing file system swapping. NNM performance is best when there is no file system swapping required. With no file swapping, `ovwdb` is running as efficiently as possible; all the object information it is managing is residing in physical memory. Any system swapping that must be done is affected by two factors: the number of objects maintained in physical memory, and the service size limit.

- If you have a system where NNM performance is poor due to file system swapping, you may use the `-n` option for `ovwdb` to limit the maximum number of objects that `ovwdb` can keep in physical memory, while storing the rest in a database.

  Note that this option is not always an appropriate solution for memory problems due to file swapping, and it is not a good performance enhancement because `ovwdb` database queries are often random. For example, a `locate` operation will cause a query over many objects in searching for a field value. In this operation, using the `-n` option would cause `ovwdb` to update the cache with each object involved in the search, as well as with all the field values for those objects. The best way to correct poor performance due to file system

swapping is to increase the amount of physical memory available to ovwdb. More physical memory reduces the amount of swapping needed.

If the -n option is not used (the default state), ovwdb will continue to grow as new objects are created until either:

— The maximum service size limit is reached.

— The system swap space is exhausted.

- Another factor that can limit the number of objects managed by ovwdb is the service size limit. If the maximum service size limit is reached, ovwdb will terminate. For information on increasing the service size limit, see the appropriate UNIX operating system administration guide.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0289
3740
Doc:



D Changing All the Symbols for a Particular Device

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0290
3740
Doc:

Procedure

Each of the following steps is explained in more detail in the example beginning on page 663.

NOTE Back up any files before you modify them.

1. Create a *symbol registration file* to add a new symbol subclass.
2. Copy and modify a set of GIF graphic files for your new symbol and place the new set of GIF files into two locations.
3. Map a specific `sysObjectID` to the new symbol by editing the `oid_to_sym` file.
4. Create a *field registration file* to define the appropriate capabilities for each new database field specified in the symbol registration file (step 1).
5. Force NNM to add the new field definitions to the database.
6. Ensure that the `sysObjectID` is listed in the `oid_to_type` file (or `HPoid2type` file) to provide information to NNM about the vendor and SNMP agent for the device you are mapping to the new symbol. This file can also be used to provide NNM with additional useful information about the device.
7. Force NNM to acknowledge your changes and update the map.
8. Open the NNM map and verify the changes.

Complete information about registration files is available in NNM's online manual, *Creating and Using Registration Files*.

Example

In this example, you will make NNM display customized symbols for HP 9000 Series 700 workstations, rather than the predefined HP-UX workstation symbol.

If you follow this example, be sure that you back up any files before modifying them. You will modify the following files in this example:

- *Windows:*

  install_dir\symbols\C\Computer\Computer_workstation

  install_dir\www\htdocs\bitmaps\C\computer\workst.16.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.20.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.26.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.32.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.38.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.44.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.50.gif

  install_dir\conf\oid_to_sym

  install_dir\conf\oid_to_type

- *UNIX:*

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.16.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.20.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.26.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.32.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.38.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.44.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.50.gif

  $OV_CONF/oid_to_sym

  $OV_CONF/oid_to_type

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0291
3740
Doc:

Create a Symbol Registration File

Because NNM provides a rich set of classes (shape outlines), you will rarely create an entirely new class of symbols. You almost always will be adding subclasses (graphics imposed over the shape) to an existing class.

To create a new subclass, create a new symbol registration file:

1. Copy the following file and name it **`Computer_workstation_700`**. Place the new file in the same directory as the original file:

   - *Windows:*

     `install_dir``\symbols\C\Computer\Computer_workstation`

   - *UNIX:*

     `$OV_SYMBOLS/$LANG/Computer/Computer_workstation`

2. Edit the new symbol registration file named `Computer_workstation_700`. Modify the file to look like this:

```
SymbolType "Computer" : "HP700"
{
  Filebase "HP700";
  CursorSize 38;

  Capabilities {
    isHP700 = 1;
  }
}
```

   Any file found in this directory is assumed to be a registration file. If you used a text editing program that makes an automatic backup of any file you edit, be sure to remove the backup file.

3. Change the permissions on the file to read-only.

Copy and Modify the Symbol Graphics

You need a *set* of GIF files to provide multiple sizes of the same graphic so that when you resize the map, the graphics grow and shrink. The easiest way to create custom graphics is to copy an existing set and modify each file. Open NNM and select `Help:Display Legend` to see the existing collection of symbol graphics.

Each set of GIF files contains several files by the same name with different numbers. The numbers indicate the pixel size of the square GIF image (20x20, 50x50). For this example, use:

- *Windows:*

  install_dir\www\htdocs\bitmaps\C\computer\workst.16.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.20.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.26.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.32.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.38.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.44.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.50.gif

- *UNIX:*

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.16.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.20.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.26.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.32.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.38.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.44.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.50.gif

1. Copy this set of `workst.##.gif` files and give them new meaningful names (for this example, use the name `HP700.##.gif`). Place them in the same directory as the ones you copied. Be sure to follow the naming scheme using the numbers in the file extensions
2. Change the permissions on the new GIF files so that you can modify them using the graphics program of your choice.

   Start with size 16. Because of size, this one is the hardest to modify. Write `700` inside the workstation's display screen in each GIF image.
3. Set the file permissions on the finished HP700 GIF files to read-only.
4. The graphic files for the symbols, themselves, are stored in two places: one directory used by NNM on the management station, and one directory used by the NNM web-based interface. (The web-based interface requires GIF files. Other additional graphic file formats are supported on the management station.)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0292
3740
Doc:

Place a copy of the new GIF files into the following directory for use by NNM on the management station. Don't worry if they are the only GIF files in this directory, because NNM ships with pixmaps:

Windows: `install_dir\bitmaps\C\computer`

UNIX: `$OV_BITMAPS/$LANG/computer`

TIP Symbols in the web-based interface have the same appearance as in NNM on a management station, except that the symbol labels do not scale in the web-based interface. Instead, a long label is truncated to fit the space available.

Map a sysObjectID to the New Symbol

NNM determines which symbol to draw on the map for a particular `sysObjectID` by referencing the entries in the `oid_to_sym` file. For additional information, refer to the comments at the top of the `oid_to_sym` file or the *oid_to_sym* reference page in NNM's online help (or the UNIX manpage).

NOTE While you are editing the file, note the many-to-one relationship between `sysObjectIDs` and symbols in the `oid_to_sym` file. You can specify "leaf" values of `sysObjectIDs` in the `oid_to_sym` file. For example, specify two `sysObjectIDs` separately:

```
1.3.6.1.4.1.11.2.3.2.2:Computer:HP-UX # 300
1.3.6.1.4.1.11.2.3.2.5:Computer:HP-UX # 700
```

A limited use of wildcards is allowed. Only a single * can exist as the last entry in a `sysObjectID` number sequence.

```
1.3.6.1.4.1.9.1.*:Computer:XX #Cisco devices use XX symbol
```

1. Locate the following file:
   - *Windows:* `install_dir\conf\oid_to_sym`
   - *UNIX:* `$OV_CONF/oid_to_sym`

2. Make a backup copy of the `oid_to_sym` file, if you have not already done so.
3. Edit the `oid_to_sym` file to modify the line referring to HP 9000 Series 700 workstations. Your changes map this device to the new HP700 subclass instead of the existing HP-UX workstation subclass.

   Old line:

```
1.3.6.1.4.1.11.2.3.2.5:Computer:HP-UX #700
```

   New line:

```
1.3.6.1.4.1.11.2.3.2.5:Computer:HP700 #700
```

Define the Capabilities for Computer_workstation_700

Now create a *field registration file* to define the `isHP700` capabilities field referred to in your `Computer_workstation_700` *symbol registration file*. Whenever the discovery and layout process creates a symbol of type `Computer:HP700`, it will automatically set the `isHP700` field to `TRUE`.

Complete information about field registration files is available in the NNM online manual, *Creating and Using Registration Files*.

Fields are defined in field registration files:

- *Windows:* *`install_dir`*`\fields\C\*.*`
- *UNIX:* `$OV_FIELDS/`*`$LANG`*`/*`

1. In this directory, create a new file called `HP700` and enter this information:

```
Field "isHP700" {
  Type  Boolean;
  Flags Capability;
}
```

   Any file found in this directory is assumed to be a registration file. If you used a text editing program that makes an automatic backup of any file you edit, be sure to remove the backup file.

2. *UNIX operating systems only:* Make sure the file is readable. At the command prompt, type:

```
chmod 644 HP700
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0293
3740
Doc:

NOTE You can specify directories other than the default directories by using environment variables, such as `OVwRegDir`, `OVwFieldDir`, and `OVwSymbolDir`.

For each registration file found, NNM executes the following steps:

a. Opens the file

b. Parses it for correctness

c. Prints any error information to the `Console` window when using a Windows operating system (to `stdout` on UNIX systems) indicating the file and line where the error occurred. Possible errors include:

- Duplicate entries
- Ill-formed entries

NOTE If you see error messages, verify the contents in the `HP700` file. Return to step 1 in "Define the Capabilities for Computer_workstation_700" on page 667 to correct sytax errors.

Provide Additional Information in the oid_to_type File

The `oid_to_type` file is used by `netmon` to map `sysObjectIds` to the correct vendor and SNMPAgent values for use with `ovw` and `ovwdb`. Applications integrated with NNM use the `vendor` and `SNMPAgent` values to determine which menu options are active for particular devices.

This file can also be used to provide topological information to NNM. For example, use this file to automatically set all devices with this `sysObjectId` to *unmanaged* or fine-tune the manner in which NNM identifies devices with this `sysObjectId`.

The file is located in:

- *Windows:* *`install_dir`*`\conf\oid_to_type`
- *UNIX:* `$OV_CONF/oid_to_type`

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0294
3740
Doc:

Their are four fields for each entry in the file:

sysObjectId:vendor:SNMPAgent:IP Map Topology Attributes

For information about controlling the vendor and SNMPAgent values, see Appendix E, "Changing an Object's Vendor and SNMP Agent," on page 675. For information about providing IP Map topology attributes for a specific device, refer to the comments at the top of the `oid_to_type` file and refer to the *oid_to_type* reference page in NNM's online help (or the UNIX manpage).

In general, you will not need to modify the `oid_to_type` file because extensive information by `sysObjectIds` is already included.

There are actually two files that NNM uses for this purpose: `oid_to_type` and `HPoid2type`. The `HPoid2type` file contains the HP `sysObjectId` list. The important difference between these files is:

- `oid_to_type`

  If you make changes to this file, your changes will be preserved the next time you install a patch or upgrade for NNM.

- `HPoid2type`

  If you make changes to this file, your changes will be lost the next time you install a patch or upgrade for NNM.

For this example, you do not need to make any changes. Since the HP 9000 Series 700 workstation is an HP device, the `sysObjectId: 1.3.6.1.4.1.11.2.3.2.5` is located in the `HPoid2type` file.

Update the Database

You must now ask the topology manager to update the database, so the new symbols you created appear on the map.

1. Log in as:
   - *Windows:* `Administrator`
   - *UNIX:* `root`
2. With all the NNM processes running, shut down just the `netmon` service. From the command prompt, type:

   `ovstop -c -v netmon`
3. Update the database by using the `ovtopofix` command.

The `-o` option to `ovtopofix` requires the SNMP `sysObjectID`, as returned by the agent of the object you are updating. This is the same `sysObjectID` you used in the `oid_to_sym` file. From the command prompt, type:

TIP To avoid errors, copy and paste the `sysObjectID` from the `oid_to_sym` file to the following command line entry.

- *Windows:*

```
ovtopofix -u -o 1.3.6.1.4.1.11.2.3.2.5 2>&1|more
```

- *UNIX:*

```
ovtopofix -u -o 1.3.6.1.4.1.11.2.3.2.5 2>&1|tee /tmp/ovtopofixOut
```

4. Restart the `netmon` service. From the command prompt, type:

   ```
   ovstart -v
   ```

5. Check that all services are `RUNNING`. From the command prompt, type:

   ```
   ovstatus -c
   ```

Verify Symbol Changes

1. Open NNM and check for error messages:

   - *Windows:*

     `Start:Programs:HP OpenView->Network Node Manager`

     Look carefully at any messages that are output to the `Console` pop-up window. Messages are always appended to the end of the Console file. It is a good idea to clear the contents of this file (`Edit:Clear`) each time that you see it.

   - *UNIX:* At the command prompt, open NNM and redirect any error messages to a file by typing:

     ```
     ovw 2>&1 | tee /tmp/ovwOut &
     ```

     Look carefully at any message output.

RQS nº 03/2005 - CN
CPMI - CORREIO
Fls: Nº 0295
3740
Doc:

Wait for NNM to finish synchronizing—the process by which the object and map databases are made consistent. This is indicated when the `[Synchronizing]` message is no longer displayed in the lower left of the status bar.

2. Are all HP 700 workstations using the new symbol? To verify this example, locate all HP 700 workstations. The following steps show two ways to locate the HP 700 symbols.

   - Locate the HP 700 symbol type.

     a. From the menu bar, select `Edit:Find->Object By Symbol Type`.

     b. In the `Find by Type` dialog box, select the computer class.

     c. Select the HP 700 symbol subclass.

     d. Click `[Apply]`. All HP 700 workstations should be listed. On the map, all of the HP 700 workstations should be represented by the new HP 700 symbol, and they should be highlighted.

   - Locate objects based upon the `sysObjectID` attribute:

     a. From the menu bar, select:

     `Edit:Find->Object By Attribute`

     b. Scroll through the list of object attributes until you can select:

     `SNMP sysObjectID`.

     c. For type of string search, select `Exact Match`, and then put in the `sysObjectID` for an HP 9000 Series 700 workstation at the `Complete String` field. *Note that you must include the leading dot in the sysObjectID for NNM to find the object.* To locate the HP 700 workstations, enter:

     `.1.3.6.1.4.1.11.2.3.2.5`

     d. Click `[Apply]`. All HP 700 workstations should be listed. On the map, all of the HP 700 workstations should be represented by the new HP 700 symbol, and they should be highlighted.

3. Resize a submap window that contains one of the HP 700 symbols. Does resizing the submap cause the different bitmap sizes to be used? Do the bitmaps look acceptable?

Back Up Your Efforts

The next regularly scheduled backup will save some of the files associated with your new symbols. See "Backup/Restore to Protect Your Investment of Time" on page 165.

TIP

The following *analytical data* directories are *not* included in NNM's backup scripts:

- *Windows:*

```
install_dir\backgrounds
install_dir\bitmaps
install_dir\www\htdocs\bitmaps
install_dir\www\registration
```

- *UNIX:*

```
$OV_BACKGROUNDS
$OV_BITMAPS
$OV_WWW/htdocs/bitmaps
$OV_WWW_REG
```

If you make changes or additions to map backgrounds, bitmap files, or web registration files ensure that your new files are properly backed up.

FRQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 0296
3740
Doc:

Example

1284

E Changing an Object's Vendor and SNMP Agent

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls.: Nº 0297
3740
Doc:

How NNM Discovers Vendor and SNMP Agent Values

This appendix describes how to modify the appropriate files to correctly set the vendor and SNMP agent fields for a particular device.

NNM automatically discovers all IP-addressable devices on your network (and IPX-addressable devices, if configured to do so on a management station running a Windows operating system). If the device has a responding SNMP agent (or proxy) that supports MIB II, then NNM will query the agent to find more information about the device. One of the pieces of information retrieved from the agent is the SNMP system object ID (`sysObjectID`) of the device:

```
iso.org.dod.internet.mgmt.mib-2.system.sysObjectID (1.3.6.1.2.1.1.2)
```

See "Unique Properties of the SNMP MIB Object sysObjectID" on page 465.

The discovery service then looks at the mappings defined in the `HPoid2type` and `oid_to_type` files. These ASCII files are used to set the value of the vendor and SNMP agent fields for the object.

NOTE The `HPoid2type` file contains entries that are *required* by NNM. You should *never* modify `HPoid2type`.

If no `sysObjectID` is returned by the device (that is, there is no SNMP agent running on the device) or no entry is found in these files that match the returned `sysObjectID`, the vendor and SNMP agent fields are not set. These fields are important because they can be used in the *selection rule* for certain menu items. This means that if these fields are not set, certain menu items may not be available.

These fields can also be used in `Edit:Find->Objects By Attribute`. This allows you to locate all the devices from a specific vendor. Or you can locate all the devices running a particular SNMP agent.

The vendor and SNMP agent fields for an object can be viewed from the main menu bar by selecting a symbol and `Edit:Object Properties`. Double-clicking on `General Attributes` in the `Object Attributes` list displays the `SNMPAgent` and `vendor` fields.

When the Vendor and SNMP Agent Would Not Be Set

The vendor and SNMP agent fields for a particular object are not set if:

- There is no SNMP agent running on the device; therefore the `sysObjectID` value was never passed to NNM.
- The device's `sysObjectID` does not have a corresponding entry in either the `oid_to_type` file or the `HPoid2type` file.
- The entry in the `oid_to_type` file does not contain valid values for the vendor and SNMP agent fields of the entry.

If the `oid_to_type` file contains an entry for the `sysObjectID` but the values specified for the vendor and SNMP agent are not in the corresponding field registration files, an error will be generated when NNM is started, and the fields for that object will not be set.

The vendor and SNMP agent field values are enumerated types that are defined in the following files:

- *Windows:*

  install_dir`\fields\C\ovw_fields` and

  install_dir`\fields\C\snmp_fields`

- *UNIX:*

  `$OV_FIELDS/$LANG/ovw_fields` and

  `$OV_FIELDS/$LANG/snmp_fields`

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0298
3740
Doc:

Procedure

This is the procedure for correctly modifying the appropriate files to set the vendor and SNMP agent fields for a particular device. These steps are explained in greater detail in the example that follows.

NOTE Most systems require `sysadmin` or `root` access to perform the following tasks.

During this procedure, you should not start any new sessions. If you do, the new sessions will use the partially built files and exit with errors. It is not necessary to shut down any NNM services. *You do need to* stop and restart NNM sessions, but not until the last step in the procedure. This minimizes loss of service.

1. Three files need to be examined and possibly modified:
   a. `oid_to_type`

      Add or modify the entry for the `sysObjectID`.
   b. `ovw_fields`

      Add the new vendor value.
   c. `snmp_fields`

      Add the new SNMP agent value.
2. Reinitialize the field values.
3. Force the `netmon` service to reread the `oid_to_type` file.
4. Force the `ipmap` service to use the new `oid_to_sym` mapping by closing and reopening the map.

TIP See Appendix D, "Changing All the Symbols for a Particular Device," on page 661 for information about creating and assigning your own custom symbols to a particular `sysObjectID`.

Example

The following example takes you through all the required steps in greater detail.

oid_to_type

NNM identifies each device by referencing the information contained in two configuration files:

- *Windows:*

  install_dir\conf\oid_to_type

  install_dir\conf\HPoid2type (Do *not* edit this one.)

- *UNIX:*

  $OV_CONF/oid_to_type

  $OV_CONF/HPoid2type (Do *not* edit this one.)

Although the entries in these files are already extensive, you may encounter a situation where you want to make additions or changes to the oid_to_type file.

See the instructions at the beginning of the oid_to_type ASCII file. See also the *oid_to_type* reference page in NNM's online help (or the UNIX manpage) for more information.

For this example, the sysObjectID is: 1.3.6.1.4.1.99.1.1

In the oid_to_type file, use an ASCII editor to add the following entry:

```
1.3.6.1.4.1.99.1.1:NewVendor:New SNMP Agent:B
```

ovw_fields and snmp_fields

The field registration files contain valid values for the object fields. The ovw_fields files contain the valid values for the vendor field. The snmp_fields files contains the valid values for the SNMP agent field.

ovw_fields For this example, modify the following ASCII file to add the new vendor information:

- *Windows:*
  install_dir\fields\c\ovw_fields
- *UNIX:*
  $OV_FIELDS/$LANG/ovw_fields

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0299
Fls. Nº
3740
Doc:

$LANG refers to the setting of the $LANG language shell environment variable. To check the value of $LANG on your system, from the command prompt, enter:

echo $LANG

Use the value returned. If no value is returned, then use the default, which is C.

The following example illustrates how the ovw_fields file could be modified. Note the new entry in the file.

NOTE These entries are case-sensitive and must exactly match the field in the oid_to_type file.

```
 Field "vendor" {

Type      Enumeration;
  Flags   capability, general, locate;
  Enumeration "Unset",
  "Hewlett-Packard",
  "HP/Apollo",
  "ACC",
  "Cayman",
  "cisco Systems",
    :
  "NetWare",
  "NewVendor",              <-- new entry
  "Novell",
  "NRC",
  "SGI",
  "SynOptics",
  "Ungermann-Bass",
  "Wellfleet",
  "Xyplex",
   ;
  }
```

snmp_fields For this example, modify the following ASCII file to add the new SNMP agent information:

- *Windows:*
  install_dir\fields\c\snmp_fields

- *UNIX:*
  `$OV_FIELDS/$LANG/snmp_fields`

  `$LANG` refers to the setting of the `$LANG` language shell environment variable. To check the value of `$LANG` on your system, from the command prompt, enter:

  `echo $LANG`

  Use the value returned. If no value is returned, then use the default, which is `C`.

The following example illustrates how an `snmp_fields` file could be modified. Note the new entry in the file.

NOTE These entries are case-sensitive and must exactly match the field in the `oid_to_type` file.

```
Field "SNMPAgent" {
  Type      Enumeration;
  Flags     capability, general, locate;
  Enumeration "Unset",
  "HP 3000/XL",
  "HP 386",
  "HP 700/[R]X X-Terminal",
  "HP 9000/HP-UX",
    :
  "cisco Terminal Server",
  "cisco T-Router",
  "cisco Protocal Translator",
  :
  "Netware 386 TCP/IP",
  "New SNMP Agent",       <-- new entry
  "Novell Lantern",
  "NRC Fusion Xenix agent",
  "Process Software Corp. VMS agent",
    :
  "Xyplex Remote Ethernet Bridge",
  "4BSD ISODE";
  }
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
0300
Fls. Nº
3740
Doc:

Configure the Database

It is not necessary to shut down the NNM services or to exit NNM when performing this step.

It is necessary to reinitialize the fields so that the new ones in the `snmp_fields` and `ovw_fields` files are loaded into the object database.

To reinitialize the fields, at the command prompt, type:

```
ovw -fields
```

Updating Field Values

It is not necessary to shut down the NNM services or to exit NNM when performing this step.

To force the `netmon` service to reread the `oid_to_type` file, at the command prompt type:

```
xnmpolling -event
```

Updating the Map

To update the map to reflect the changes, close and then reopen the map.

If the device has already been discovered, the vendor and SNMP agent changes will be detected during the next regularly scheduled configuration check. Those fields will be updated at that time to reflect the new values. You can set the intervals between configuration checks using `xnmpolling` or using the `Options:Network Polling Configuration->IP` menu item.

Alternately, you can delete the device's symbol from the map and let it be rediscovered. When the device is rediscovered, the new values will be used.

Backing Up Your Efforts

The following *analytical data* directories are *not* included in NNM's backup scripts:

- *Windows:*

  install_dir\backgrounds
  install_dir\bitmaps
  install_dir\fields
  install_dir\symbols

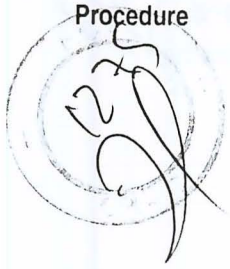
- *UNIX operating system:*

```
$OV_BACKGROUNDS
$OV_BITMAPS
$OV_FIELDS
$OV_SYMBOLS
```

When you make changes or additions to map backgrounds, bitmap files, field registration files, or symbol registration files ensure that your new files are properly backed up. See "Backup/Restore to Protect Your Investment of Time" on page 165 for more information.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0301
3740
Doc:

Procedure



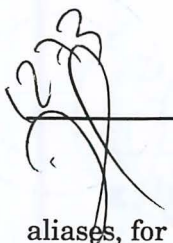
Symbols

.login file
  modifying, 101
.profile file
  modifying, 101
.vueprofile file
  modifying, 101

A

access
  no access, 293
  read-only, 292
  read-write, 292
  to maps, 292
accessing
  alarm information from the map, 339
  map information from alarms, 338
  MIB information, 52
accounting management
  components, 43
acknowledging alarms, 334
action block, WLRF, 496
adding
  background graphic, 262
  features to NNM, 278
  IP interface object, 260
  new symbols, 263, 662
  node object, 259
  segment object, 258
additional actions
  alarms, 339
  configuring, 339, 441
  See also Alarm Browser
additional views
  cdp view, 521
  internet view, 522
  neighbor view, 518
  node view, 520
  path view, 519
  Port-Address mapping command, 522
  station view, 522
address
  resolution, 579
  table poll operations in netmon, 179
  well-configured, 90
Address Resolution Protocol. See ARP/RARP
administrative symbol status, 271
agent. See SNMP agent
Alarm Browser
  acknowledging alarms, 334
  All Alarms category, 331
  assign category, 348
  configuring, 342
    automatic delete, 345
    event database, 343
    state file, 344
  correlated alarms, 352
  de-duplicated alarms, 352
  deleting alarms, 337
  features, 512
  filtering alarms, 335
  overview, 329
  starting, 513
  troubleshooting, 619
  window, 330, 332, 337
alarm categories
  configuring, 349
  window, 329, 331
alarm to map connection, 338
alarms, 323, 330, 338, 423
  accessing information, 338
  acknowledging, 334
  adding, 423
  additional actions, 339
  automatic actions, 433
  automatic delete configuration, 345
  categories, 348
  categories, new, 349
  configuration
    sources, 432
  configuring, 423
  copying, 423
  correlated
    see event reduction capabilities
  de-duplicated
    see event reduction capabilities
  definition, 323
  deleting, 337, 423
  deleting automatically, 345
  displaying, 329
  filtering, 335
  highlighting, 339
  monitoring devices, 326
  moving to a different category, 348
  using to diagnose problems, 566
  using to filter events, 566
  using to launch specific URLs, 340
  zoom to highlighted object, 338
Alarms command, 566

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0302
3740
Doc:



aliases, for web server, 485
All command, 561
All HSRP Groups command, 574
All VLANs command, 574
analytical data backup, 166
app-default files, 269
Application Builder. See MIB Application Builder
application layer
  hardware used in, 26
  in OSI model, 22
  protocols, 22
application registration files (ARF)
  control menu choices, 299
archive
  implement your plan, 170
  importance of, 165
ARF files for menu control, 299
ARP cache, viewing, 562
ARP/RARP, described, 23
attributes
  changing, 235
  locating objects by, 113
  object, 205
audit log file, 491
  format, 491
  location, 491
automatic actions, 433
  using trusted commands, 433
automatic discovery, 56
automatic thresholds, 453

B

background graphic
  adding, 262
  formats, 260
background processes
  See services
backup
  adding scripts, 176
  archive
    implement your plan, 170
    importance of, 165
  directory (staging area), 166
  disk space requirements, 168
  frequency, 167
  how it works, 166
  procedure, 167
  SOLID database, 175
  troubleshooting, 171, 174
backup routers
  missing from map, 136
Berkeley Internet Name Domain (BIND) Service, 579
Bridge MIB
  Base Port Table command, 564
  Base Table command, 563
  Spanning Tree Port Table command, 564
  Spanning Tree Table command, 564
  Static Table command, 564
  Transparent Forwarding Table command, 564
  Transparent PortTable command, 564
bridge MIB
  described, 28
  for topology polling, 184
bridges, 26
  discovery of, 103
  display of, 217
Browse MIB operation, SNMP Set requests, 628
browser
  DMI, 417
  MIB, 412
  See Alarm Browser
browsing
  alarms, 335
browsing MIBs
  problems with, 628
  See also SNMP MIB Browser
browsing MIFs. See DMI Browser
building new MIB applications, 43
bundled
  correlations, 360
  correlators, 386
bus layout, 242

C

cache, clearing from browser, 613
capabilities, 206
categories for alarms
  assigning, 348
  changing default, 348
  creating new, 349
  moving an alarm, 348
CDP command, 573
cdp view
  description, 521
CGI errors, 616
CGI programs, described, 545

change management
tools, 46
characteristics, symbol, 209
checking disk space, 527
checkpoint phases for backup, 166
child submaps
creating, 245
Cisco Discovery Protocol
Cache Table command, 563
Global Table command, 563
Interface Table command, 563
class, symbol, 207
client station, web components installed on, 485
collecting
historical MIB information, 45
MIB information, problems, 608
collecting data
See data collection
collecting SNMP data. See data collection
colors, status, 271
command
xnmevents, 341
communications problems diagnosing, 566
community names
configuring NNM, 93, 146
configuring SNMP agents, 93, 146
defined, 52
GET/SET, 93, 146
problems with, 626
requests for information, 52
testing with netmon.cmstr, 93, 147
Community-based SNMP version 2, 52
Composer, 386
compound status propagation, 275
configuration check
operations in netmon, 179
polling, 183
configuration management
components, 42
tools, 46
configuring
additional actions, 441
alarm categories, 349
alarms, 423
automatic actions, 433
correlations, 352
correlators, 352
de-duplications, 352
events, 422, 423
polling, 178, 194
print command, 475
problems with events, 631
SNMP events, 423
connection labels
defined, 223
connection symbol, 208
connections, multiple connections between symbols, 245
connectivity problems, diagnosing, 556, 557, 562, 567, 568
connector topology
polling, 184
Connector-Down correlation
behavior, 361
setting parameters, 362
important node filter, 192, 362
secondary failures, 192, 363
conserving memory, 657
container object, 248, 251
containment realm
editing guidelines, 253
example of Internet submap, 253
example of Partitioned Internet submap, 255
maintaining, 255
overview of, 252
context for menu items, 296
contrib programs
accessing, 74
controlling management traffic, 178
copying
events, 423
symbols, 257
correlating events, 352
correlation
background information, 354
command line control, 380
ConnectorDown, 361
files, 381
FrameRelay, 365
MgXServerDown, 369
new, 382
PairWise, 371
RepeatedEvent, 375
ScheduledMaintenance, 379
troubleshooting, 381
Correlation Composer, 386
correlator
background information, 354
files, 397

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0303
3740
Doc:

new, 398
OV_Chassis_Cisco, 387
OV_Connector_IntermittentStatus, 393
OV_HSRP_(group), 394
OV_MultipleReboots, 388
OV_NodeIf_(group), 390
troubleshooting, 397
CPU
load operation, problems with, 626
speed, performance impact, 656
viewing load, 559
CPU Load command, 559
CRC errors, viewing, 558
creating
child submaps, 245
correlations, 383
correlators, 398
de-duplication configurations, 358
executable symbols, 280
independent submaps, 245
Quick Navigator, 287
submaps, 244
critical status, 275
customizing
background graphic, 262
setting a user default map, 287
setting the home submap, 287
startup files, 535
cutting symbols, 257

D

data collection
configuring, 450
disk space usage, 168
graph, 472
graphing, 472, 473
reducing file size with ovdwtrend, 529
scheduling, 451
setting thresholds, 456
storing results, 448
using the data collector, 447
viewing results, 453
Data Collector, 473
data graphing, 473
data link layer
discovery of devices, 59
hardware used in, 26
in OSI model, 21
protocols, 23
Data Warehouse
Export Events command, 571
Export Topology command, 571
Export Trend Data command, 571
data warehouse, described, 63
database files
changing permissions, 295
databases
corrupted OVW object database, 604
event, 63
map, 62
NNM, 62
object, 62
topology, 63
trend, 63
de-duplicated, 358
deleting, 423
alarms, 337
nodes, 658
old snapshots, 555
description
Composer correlators, 386
de-duplication, 358
ECS correlations, 360
object, 236
Desktop Management Interface. See DMI
destination
SNMP trap, 325, 326
developing
additional actions, 441
automatic actions, 433
de-duplication configurations, 358
new correlations, 383
new correlators, 398
devices
discovery of, 104
supporting SNMP, 43
DHCP
described, 24
filter, 183
polling, 179, 181, 183
well-configured, 91
dialog boxes
General Attributes, 205
discovery, 103
automatic, 56
description of, 56
DIscover Level-2 Objects check box, 185
duplicate IP Address, 159
expanding, 117, 119

incorrect IPX node names, 157
IP and IPX, 58
IP Network 0.0.0.0, 156
IPX failure, 154
IPX node discoverd as two nodes, 159
Level 2, 59, 185
limiting, 117, 124
MAC address, 59
missing IPX routers, 156
netmon -k options, 185
no vendor translation, 159
non-IP devices, 59
non-IPX devices, 59
partial IPX, 157
problems with, 154
recommendations, 134, 153
requirements for IP, 56
requirements for IPX, 58
routing tables, 144
start again, 161
unmanaging a network, 589
verify accuracy, 109
discovery filter
procedure, 128
to improve performance, 531
disk space
checking, 527
regaining, 527, 529
viewing usage, 559
Disk Space command, 559
displaying alarms, 330
distributed event correlation, 357
DMI
configuring, 95, 417
described, 30
event, 54, 327
features, 30
MIF, 54, 327
See MIF
service provider, 54, 327
viewing status, 574
DMI Browser
accessing, 574
querying DMI values, 417
DMI devices
can't communicate with, 628
problems querying, 611, 628, 631
DNS
caching-only name server, 91
quick check, 92
secondary name server, 91
well-configured, 91, 133
documenting a map, 555
dynamic correlation parameters, 355
Dynamic Host Configuration Protocol. See DHCP

E

ECS, 360
e-mail message generation. See automatic actions
Enterprise Identification, 423
Enterprise MIB
adding, 423
correlating, 352
deleting, 423
environment variables
setting up, 101
error log file
contents, 498
Launcher, 653
using for troubleshooting, 498
Web Launcher, 616, 653
errors
monitoring SNMP, 561
viewing Ethernet, 558
Ethernet
statistics, monitoring, 558
traffic, monitoring, 558
Ethernet Errors command, 558
Ethernet Traffic command, 558
Event Browser
See Alarm Browser
Event Configuration
operation, 631
overview, 422
event correlation
bundled edition
Connector-Down, 192, 361
Frame-Relay, 365
ManageX Server-Down, 369
Pair-Wise, 371
Repeated-Event, 375
Scheduled-Maintenance, 379
developing your own, 383, 398
disabling, 354
distributed, 357
enabling, 354
settling time, 354
files, 381

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0304
3740
Doc:

general recommendations, 356
introduction, 353
parameters
dynamic, 355
static, 355
See event reduction capabilities
sources for more, 382
streams, 356, 380
event database
configuration, 343
event database, described, 63
Event Identification, 423
event log, browsing, 566
event reduction capabilities
Correlation Composer, 386
de-duplication, 358
described, 61, 352
ECS, 360
web based, 515
event storm prevention
Composer correlators, 386
Connector-Down correlation, 361
de-duplication, 358
ManageX Server-Down correlation, 369
Pair-Wise correlation, 371
Repeated-Event correlation, 375
Scheduled-Maintenance correlation, 379
events, 423
actions, 441
adding, 423
automatic actions, 433
configuration, 631
sources, 432
configuring, 423
correlating, 352
de-duplication, 358
definition, 323
deleting, 423
listing, 566
management stations receiving, 565
processes that generate, 591
propagation of, 591, 604
services that generate, 604
exact match, 114
executable symbols
adding, 280
described, 279
executing MIB applications, problems, 628
expanding maps
containment realm, 252
creating Partitioned Internet submap, 251
higher level maps, 247
IP interface object, adding, 260
node object, adding, 259
See Also containment realm
segment object, adding, 258
explodable symbols
defined, 279
export map, 256
Extended Topology, 44

F

fault management
components, 42
event reduction capabilities, 352
HP OpenView IT/Operations, 44
tools, 43
faults on network, diagnosing, 44, 45
field definitions, problems with, 595
field registration files, 667
file
backing up originals, 580
modifying default X resources, 581
original product, 580
permissions, 623
filters
alarms, 335
DHCP, 183
discovery, 128, 183
important node, 192
Connector-Down correlation, 362
OV_NodeIf_(group) correlator, 390
map, 232
persistence, 231
find
attributes, 235
entering text for exact match, 114
entering text for pattern match, 114
entering text for regular expressions, 114
objects, 113, 114
forwarding
SNMP trap from NNM, 326
SNMP trap to NNM, 325
Frame Relay
Circuit Congestion command, 558
Circuit Errors command, 558
Circuit Traffic Avg. Frame Size command, 558
Circuit Traffic Data Rate command, 558

Circuit Traffic Frame Rate command, 558
correlation of health, 365
Data Link Errors command, 559
Properties command, 564
Virtual Circuits command, 564
frequency of discovery value, in netmon, 179
FRF, 667
full restore of NNM data, 171

G

gateways
described, 26
discovery of, 103
General Attributes dialog box, 205
generating
alarms, 323
geometry of submaps, 266
get request, 53
get response, 53
getBulk request, 53
getNext request, 53
GIF graphics format, 260
graph
CPU load, 559
Ethernet errors, 558
Ethernet traffic, 558
Frame Relay circuit congestion, 558
Frame Relay circuit errors, 558
Frame Relay circuit traffic data rate, 558
Frame Relay circuit traffic frame rate, 558
interface discard percentage, 557, 569
interface discard rate, 556, 568
interface error percentage, 556, 568
interface error rate, 556, 568
interface statistics, 556, 568
interface traffic avg. packet size, 557
interface traffic data rate, 557
interface traffic packet rate, 557
interface traffic throughput, 557
interface traffic utilization, 557
printing, 475
selected data, 473
SNMP data, 561
SNMP errors, 561
SNMP operations, 560
SNMP traffic, 560
Graph All Data, 472
Graph SNMP Data command, 561
graphics
backgrounds for maps, 260
graphing
data, 472
historical data, 473
MIB data, 45
real-time data, 473
with xnmgraph, 544
greyed menu items, 206

H

help system, 67
files, viewing, 636
overview, 67
printing, 68
searching, 68
using separately from NNM, 69
using to create manuals, 68
hiding objects on map, 233
highlighting
alarms, 339
sources, 338
historical data, 473
holding area, 244
home submap
defined, 202
setting, 287
hotlist
creating, 287
HP Agent
trap recipients, 326
HP Education, 77
HP OpenView Grapher, 472
HP OpenView IT/Operations, for fault management, 44
HP OpenView Launcher. See Launcher
HP OpenView Web
applications, 484
Correlation Composer, 386
event correlation, 515
features, 484
requirements, 485
security, 486
setting up, 485
web browser, 485
web server, 485
HP-RDMI service provider, 417
hpterm, accessing, 570
HP-UX SAM command, 565
HSRP Group Detail view, 574
HSRP Node Detail view, 574
httpd service, troubleshooting, 586

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0305
3740
Doc:

hubs, 26

I

ICMP
  polling, 179, 181
ICMP, described, 23
icon symbols
  described, 207
import map, 256
important node filter
  Connector-Down correlation, 362
  OV_NodeIf_(group) correlator, 390
  setting, 192
independent submaps, creating, 245
initial discovery
  process, 107
  start again, 161
  troubleshooting
    IP, 131
  verify information, 109
instance
  query for, in MIB Browser, 412
instance, MIB, 29
interface
  status of interface, 556, 568
  status of node, 556, 568
Interface Avg. Packet Size command, 557
Interface Error Percentage command, 556, 568
Interface Error Rate command, 556, 568
Interface Errors
  Data Link Errors command, 569
  Discard Percentage command, 557, 569
  Discard Rate command, 556, 568
  Frame Relay Circuits command, 569
interface object, 112
Interface Status command, 556, 568
Interface Traffic
  Data Rate command, 557
  Throughput command, 557
  Utilization command, 557
Interface Traffic command
  uses of, 654
Interface Traffic Packet Rate command, 557
Internet command, 573
Internet Control Message Protocol. See ICMP
Internet level, 230
Internet Packet Exchange. See IPX
internet view
  description, 522
inventory network objects
  internet object properties, 111
inventory report, 107
IP
  addressing, 579
  described, 23
  discovery, 56
  forwarding, 140
  interaction with IPX, 58
  internet object, 111
  objects, discovery of, 103
  requirements for discovery, 56
  routes, locating, 567
  secondary addresses, 137
  topology behavior, 466
  well-configured, 90
ipmap
  described, 543
  managing objects, 255
  propagation of events from, 605
IPv6 Network command, 574
IPv6 Node Detail view, 574
IPv6 Prefix Groups view, 574
IPX
  described, 23
  discovery, 56, 57
  interaction with IP, 58
  layout, 57
  polling, 179, 180, 184
  requirements for discovery, 57
  transport software, 100
IPX discovery
  duplicate IP Address, 159
  failure, 154
  hop count
    expanding, 123
    limiting, 130
  incorrect node names, 157
  IP Network 0.0.0.0, 156
  missing routers, 156
  no vendor translation, 159
  node discoverd as two nodes, 159
  partial, 157

J

Java
  errors, 617
  parameters, modifying, 499
jumpstart

netmon, 152

K

keyboard, 474

L

latency time
for WANs, 182
in polling, 182
Launcher
accessing, 571
blank window, 616
CGI error, 616
configuring, 494
error log, 498, 653
features, 492
Information and Reports tab, 575
Java error, 617
Java parameters, 499
Object Views tab, 575
registration file. See WLRF
starting, 492
tabs, 575
Tasks tab, 575
Tools tab, 575
troubleshooting, 616
user interface, 492
user login error, 615
WLRF error, 617
Layer 1
hardware used in, 25, 26
in OSI model, 21
Layer 2
hardware used in, 26
in OSI model, 21
protocols, 23
Layer 3
hardware used in, 26
in OSI model, 22
protocols, 23
Layer 4
in OSI model, 22
protocols, 23
Layer 5
in OSI model, 22
Layer 6
in OSI model, 22
Layer 7
hardware used in, 26
in OSI model, 22
protocols, 22, 23
layers, in OSI model, 21
layout, 242
automatic, 56
bus, 242
description of, 56
point to point, 242
ring, 242
row/column, 242
layout algorithm
default, 241
level 2
discovery, 56, 59, 185
polling, 180, 184
license
checking number of nodes, 533
OVLicenseMgr, 599
limitations, known in loading MIBs, 634
line
attributes, 475
configuration, 475
Graph, All Data, 472
Graph, Select Data, 473
list block, in WLRF, 495
Load/Unload MIBs operation, 633
loaded MIB database, modifying, 633
loadhost program
expand management domain, 122
limit management domain, 127
loading MIBs, 413
limitations of, 634
operation, 633
problems with, 633
unique object label, 634
local host file
quick check, 92
well-configured, 91, 133
Local Registration File (LRF)
customizing for performance, 535
customizing for startup, 535
locating objects
see find
log files
audit, 491
error, 498, 653
Launcher error, 653
logging
common options, 640
correlations, 380

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0306
Fls. Nº
3740
Doc:

description of, 639
example, 645
explained, 643
log files, 648
output, 649
recommendations, 580
Web Launcher errors, 616, 653
with netfmt, 643
with nettl, 644
lp, 475
LRF. See Local Registration File

M

MAC address, using to discover devices, 59
magicpacket command, 570
maintenance
audit log file, 491
daily, 527
error log file, 498, 653
monthly, 533
weekly, 531
managed object, defined, 53
Management Information Base. See MIB
Management Information Framework. See MIF
management region
expanding, 108, 117, 119
IPX hop count, 123
loadhost program, 122
seed file, 120
limiting, 117, 124
Discovery filter, 128
IPX hop count, 130
loadhost program, 127
netmon.noDiscover file, 125
oid_to_type file, 129
troubleshooting, 131
management station
interaction with Network Presenter, 505
receiving traps, 565
web components installed on, 485
Management Web Page, accessing on remote node, 572
manager
defined, 51
manager-agent
communication through SNMP, 52
ManageX Server-Down correlation
behavior, 369
setting parameters, 370
managing
polling, 193
manpages
acessing, 72
printing, 73
viewing, 636
MANPATH statement
setting, 101
manuals, accessing online, 69
map database, described, 62
maps
access rights, 292
adding features, 278
automatic discovery and layout, 56
background graphics, 260
changes, 286
child submap, 245
compound status, 275
containment realm, 252
context, 296
copying, 215
creating symbols, 263
defined, 199
expanding, 247
file permissions, 292
filters for objects, 232
geometry, 266
hiding objects, 233
independent submap, 245
initial appearance, 103
layout
auto, 241
do-it-yourself, 242
limiting menu choices, 299
maintaining the containment realm, 255
menu control, 299
metaconnections submaps, 245
network symbol names, 221
new object holding area, 244
no access, 293
open map, 199, 215, 221
overlay, 267
partitioned internet submaps, 248
permissions, 292
persistance, 229
preferences, 287
problems with, 654
propagate most critical status, 276
propagate status at threshold value, 276

Quick Navigator, 288
read-only access, 292
read-write access, 292
remote viewing, 317
removing old snapshots, 555
See also expanding maps
See also Partitioned Internet submap
size and placement, 266
snapshot, 555
start over, 161
startup options, 289
switch/bridge display, 217
troubleshooting
IP, 131
IPX, 153
user preferences, 287
marginal status, 275
MAU MIB
described, 28
for topology polling, 184
memory
clearing from browser, 613
conservation tips, 657
not enough, 657
performance impact, 656
problems affecting ovwdb, 604
related problems, 579
memory requirements
for maps, 229
menu items
adding to Network Presenter, 505
adding to NNM, 299
greyed, 206
meshing
definition of, 59
example, 227
specifying in NNM, 228
meta-connection
submap, 246
symbol, 245
MIB, 43
accessing information, 52
Application Builder operation, 443, 628, 629
bridge, 28
for topology polling, 184
Browse operation, 46
building new applications, 43
collecting historical information, 45
data, 472
data collection
effects of, 453, 654
operation, 608
defined, 27
defining thresholds, 44
operation for, 453
DMI conversion from MIF, 95, 419
enterprise-specific objects, 43
graphing data, 45
instance, 29
loading (adding), 413
prerequisites, 414
MAU
described, 28
for topology polling, 184
numeric values, 447, 455
object, 28, 43
object identifier, 28
object label, unique, 634
obtaining MIB files, 94
organization, 28
private, 28
querying, 412
repeater, 28
for topology polling, 184
RFC (technical details), 33
RMON, 27
See Also data collection
setting MIB values, 412
setting values, 412
SNMP traps, 44
storing data for trend analysis, 45
tree, 28
troubleshooting, 572
variable bindings, 404
vendor-specific, 413
viewing, 412, 572
viewing MIB values, 412
MIB Application Builder
and DMI device, 628, 631
using, 443
MIB applications
executing, 629
problems building, 628, 629
troubleshooting, 629
MIB Browser. See SNMP MIB Browser
MIB event thresholds,defining, 44
mib.coerce file, 464
mibExpr.conf file, 463

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0307
Fls. Nº
3740
Doc:

MIB-II
described, 27
Microsoft Terminal Services, 317, 318
MIF, 54, 327
configuring for NNM, 95, 419
described, 29
loading (adding), 95, 419
with translation to MIB, 420
without translation to MIB, 420
mapping to MIB, 328
vendor-specific, 420
modifying
events, 423
Java parameters, 499
line attributes, 475
ovsuf, 536
monitoring
CPU load, 559
devices, 326
disk space, 559
Ethernet statistics, 558
Ethernet traffic, 558
Frame Relay circuit average frame size, 558
Frame Relay circuit congestion, 558
Frame Relay circuit errors, 558
Frame Relay circuit traffic data rate, 558
Frame Relay circuit traffic frame rate, 558
Frame Relay Circuits, 569
Frame Relay Data Link errors, 569
Frame Relay data link errors, 559
SNMP authentication failures, 560
SNMP errors, 561
SNMP operations, 560
SNMP traffic, 560
TCP connections, 557
mouse and keyboard
grapher, 474
moving
symbols, 257
multi-homed node, discovery of, 103

N

name resolution, 91, 92, 133
naming network symbols, 221
Neighbor command, 572
neighbor view, 518
NetBios
quick check, 92
well-configured, 91, 133
netfmt, 643
described, 643
examples of, 649
filtering options, 649
netmon, 466
address table poll operations, 179
configuration check operations, 179
configuring, 193
dependencies, 586
described, 541, 587
disabling, 195
discovery behavior, 541
enabling, 195
event generation conditions, 604
frequency of discovery values, 178
instance restrictions, 589
IP discovery, 56
IPX discovery, 57
jumpstart(-J), 152
monitoring, 194
netmon.noDiscover file, 125
performance check, 193
permissions, 623
poll operations, 179
problems with, 154
proxies, 179
queue (-q, -Q), 193
requirements for discovery, 56, 57
seed file, 119
timeout intervals, 179
trace masks, 641
tracing, 641
tracing example, 641
troubleshooting, 587
tools, 589
netmon.cmstr, 147
testing community names, 93
netmon.equivPorts, 60, 226, 228
netmon.lock file, 589
netmon.lrf, 193
described, 536
segRedux, 217
netmon.noDiscover file
effect on discovery, 126
example, 126
HSRP virtual IP address, 126
procedure, 126
netmon.snmpStatus, 274
netnmrc script
execution sequence, 625

nettl
described, 643
examples of, 645
generating log files, 648
generating trace files, 648
log file output, 649
options
-log, 645
-start, 644
-status, 644
-stop, 648
-traceoff, 647
-traceon, 646
pathnames for, 643
subsystems used with, 643
Network Activity menu, described, 556, 568
Network Configuration
ARP Cache command, 562
ATM Properties command, 565
Cisco VLAN MembershipTable command, 563
DS1/E1 Serial Line Properties command, 565
DS3/E3 Serial Line Properties command, 565
Interface Properties command, 562
IP Addresses command, 562
IP Routing Table command, 562
IP Services command, 562
SONET/SDH Properties command, 565
Network Connectivity
Locate Route via SNMP command, 567
Show Path command, 567
Trace Route command, 567
network hardware
bridge, 26
gateway, 26
hub, 26
repeater, 25
router, 26
switch, 26
network layer
hardware used in, 26
in OSI model, 22
protocols, 23
network level, 230
network management
benefits, 42
defined, 42
functions, 42
proactive, 40
network management operation
problems with, 626
remote node support for, 626
network map
using a seed file, 119
network object, 111
Network Presenter
components, 502
connecting to an NNM session, 502
features, 501
features vs. NNM, 503
interaction with management station, 505
permissions, 618
problems starting, 618
registration file. See NPRF
specifying map to open, 502
starting, 501
symbol registration file, 506
troubleshooting, 618
URL for, 501
network traffic
control, 178
viewing, 560
NetworkAdmin user role, 488
NetworkOper user role, 488
networks
naming symbols, 221
new node discovery
polling, 185
NIS
quick check, 92
well-configured, 91, 133
NNM
configuration files, changing permissions, 295
options for starting, 289
starting, 106, 121, 122, 195
status check, 106
NNM Extended Topology, 44
no access, 293
node
deleting unwanted, 658
discovery of IP, 57
discovery of IPX, 57
information obtainable from, 582
information storage, 57
listing information about, 565
multi-homed, 103

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0308
3740
Doc:

non-SNMP, 582, 626
object, 112
obtaining status, 566
polling, 566
represented as a symbol, 105, 679
testing remote, 570
turning on remote, 570
Node command, 573
node view, 520
description, 520
normal status, 275
notification, 325
defined, 52
NPRF
adding menus, 505
adding toolbar buttons, 505
format, 505
location, 505
troubleshooting, 619
NTAdmin user role, 488
NTOper user role, 488
numeric MIB values, 447, 455

O

object database
and ovwdb, 542
described, 62
object manager
ovstatus cannot find, 585
objects
adding attributes, 238
attribute

setting parameters, 393
OV_HSRP_(group) correlator, 394
behavior, 395
parameter settings, 396
OV_MultipleReboots correlator, 388
behavior, 388
parameter settings, 389
OV_NodeIf_(group) correlator, 390
behavior, 390
disabling, 392
important node filter, 390
setting parameters, 391
ovactiond
dependencies, 586
described, 541
troubleshooting, 590
trusted commands, 433
trustedCmds.conf directory, 433, 434
ovactiond.lrf, described, 536
ovaddobj command
described, 541
netmon, configuring seed file, 125
OVAdmin user role, 489
ovalarmadm, 347
ovalarmsrv
dependencies, 586
described, 542
troubleshooting, 590
ovas
described, 542
ovbackup.ovpl, 167, 170
ovcapsd, 54, 327, 420
dependencies, 586
described, 542, 591
troubleshooting, 591
ovcapsd.lrf, described, 537
overlay of submaps, 267
overview
Alarm Browser, 329
Event Configuration, 422
ovhtpasswd command, 487
ovrepld
dependencies, 586
described, 542
troubleshooting, 594
ovrepld.lrf, described, 537
ovrequestd, 542
ovrequestd background service, 607
ovrestore.ovpl, 172, 173
ovspmd
described, 541
determining problems, 592
recreating sockets directory, 593
troubleshooting, 592
ovstart command
described, 541
in starting background services, 584
ovstatus command
failure to find object manager, 585
verifying daemon services, 585
ovsuf
described, 541
modifying, 536
ovtopmd
dependencies, 586
described, 542, 594
troubleshooting, 594, 595
ovtopmd.lrf, described, 537
ovtopodump
description of, 597
troubleshooting, 597
ovtopofix command, 217
ovtrapd
dependencies, 586
described, 542, 599
operation of, 599
troubleshooting, 599
ovtrapd.lrf, described, 537
ovuispmd
dependencies, 586
described, 542, 600
troubleshooting, 600
ovuispmd.lrf, described, 537
ovw command
described, 543
options, 289
-mapcount, 289
-verify, 289, 302
ovw.auth file, location, 506
ovwchgrp, 295, 624
ovwchmod, 295, 624
ovwchown, 295, 624
ovwdb
corrupted OVW object database, 604
dependencies, 586
described, 542, 602
insufficient memory, 603
insufficient performance, 603
troubleshooting, 602
ovwdb.auth file
location, 506

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0309
3740
Doc:

ovwdb.lrf, described, 537
ovwls, 295, 624
ovwperms, 295

P

paging automatically. See automatic actions
Pair-Wise correlation
  behavior, 372
  setting parameters, 373
palette, 207
Partitioned Internet submap
  creating, 251
  example of, 255
  how it is managed, 255
  overview of, 248
  See Also containment realm
password
  in user authentication file, 487
  modifying, 487
pasting symbols, 257
patch releases, verifying, 533
Path command, 573
PATH statement
  modifying, 101
path view, 519
pause NNM services
  for back up
    analytical, 166, 168
    operational, 168
Performance
  Graph Data, 472
performance, 473
  customizing startup, 535
  diagnosing problems, 44, 45
  improving NNM, 658
  increasing, 656
  limiting factors, 656
  polling, 531
  problems with, 656
performance management
  components, 42
  reports, 45
  tools, 45
performance problems, diagnosing, 556, 557, 559, 568
Perl (HP's version)
  backup/archive/restore, 176
permissions
  change for configuration files, 295
  change for database files, 295
  changing, 624
  default, 623
  no access, 293
  read-only, 292
  read-write, 292
  restoring default, 624
persistance of submaps, 229
persistence filter, 231
physical layer
  hardware used in, 25, 26
  in OSI model, 21
ping
  remote node, 570
  using to determine connection, 567
planning, 80
  assuming responsibility, 82
  changes to the map, 286
  how to configure NNM, 83
  which devices to manage, 87
pmd, 323
  alarm gathering, 324
  dependencies, 586
  described, 542, 604
  operation of, 604
  permissions, 623
  troubleshooting, 381, 397, 591, 604
pmd.lrf, described, 537
point to point layout, 242
Poll Node command, 566
poll operations, in netmon, 179
polling
  adjusting intervals, 531
    from a remote computer, 182
  behavior, 589
  causing problems, 580
  configuration check, 180, 183
  controls, 178, 588
  delays in, 589
  disabling, 195
  during map generation, 178
  effects of reducing, 178, 179, 654
  file, 588
  initial process, 56
  latency time, 182
  new node discovery, 178, 180, 185
  non-IP devices, 59
  non-IPX devices, 59
  performance
    checking, 531
  problems with, 589

secondary failures, 180, 192
secondary IP addresses, 137
status, 178, 179, 181
to conserve memory, 657
topology check, 180, 184
traffic generated by, 654
troubleshooting
IP, 131
jumpstart netmon, 152
SNMP, 93, 145
subnet masks, 91, 149
tuning, 193, 194
values storage, 178, 543, 588
Port Address Mapping command, 522
description, 522
port number, used to start HP OpenView Web, 485
port trunking
definition of, 59
example, 225
specifying in NNM, 226
Port-Address Mapping command, 571
ports, connection problem, 596, 603
predefined symbols, 208
preferences, 287
preferences, setting a user default map, 287
presentation layer, in OSI model, 22
print command, 475
configuration, 475
printing
graph, 475
online help, 68
private MIB, 28
proactive network management, 40
problem management
components, 42
tools, 43
problems, 131
additional sources of information, 579
address resolution, 579
analyzing symptoms, 582
background services, 584
Browse MIB operation, 628
characterization, 582
diagnosing network faults, 44, 45
diagnosing performance, 44, 45
event correlation, 381, 397
failure to discover IPX nodes, 154
Launcher won't start, 616
launching applications, 637
limitations on loading MIBs, 634
loading MIBs, 633
map, 654
netmon, 154, 589
network management operation, 626
network operation, 623
ovtopmd, 595
ovtopodump, 597
ovwdb, 603
performance, 656
pmd, 606
polling, 589
resource exhaustion, 579
runtime, 623, 625
starting Launcher, 613
starting Network Presenter, 618
subnet mask, 149
unmanaging a network, 589
user logins, 615
X Windows, 635
product support
contacting, 77
propagating symbol status, 271
most critical status, 276
status at threshold value, 276
protocols, and OSI model, 24

Q

quick check
name resolution, 92
Quick Navigator, 288
creating, 287

R

read-only
access, 292
read-write
access, 292
real-time data, 473
real-time data graphing, stopping, 474
recreating map and topology databases, 161
reference pages
acessing, 72
printing, 72
viewing, 636
registering an application, 278
registration files
field, 667
Launcher. See WLRF

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0310
Fls. Nº
3740
Doc:

Network Presenter. See NPRF
symbol, 664
update/verify, 668
regverify command, 494
release notes, accessing, 71
remote access to NNM, 317
remote nodes
testing, 570
turning on, 570
Remote Ping
described, 567
problems with, 626
remoteConfAllow.conf file, 182
removing, old snapshots, 555
Repeated-Events correlation
behavior, 376
setting parameters, 376
repeater
discovery of, 103
repeater MIB
for topology polling, 184
repeater MIB, described, 28
repeaters, 25
report
configuration interface, 45
general availability, 45
general inventory, 45
inventory, 107
modification, 45
Reporting interface, 516
troubleshooting, 614
reports
removing, 529
restarting automatic map generation, 161
restore
adding scripts, 176
all NNM data, 171
some NNM data, 173
RFC documents
list of, 33
ring layout, 242
RMON
Host Table Command, 560
Segment Errors command, 559
Segment Octets command, 559
Segment Packet Sizes command, 560
Segment Packet Types command, 560
Segment Utilization command, 559
RMON menu, described, 559
RMON MIB, 27
root submap, 202
routers, 26
routes, locating IP, 567
routing tables
in IP discovery, 144
viewing, 562
row/column layout, 242
running services, checking, 527
runtime components on network
problems with, 623

S

SAM, accessing, 565
Scheduled-Maintenance correlation
behavior, 379
setting parameters, 379
searching online help, 68
secondary failures
Connector-Down correlation, 363
OV_NodeIf_(group) correlator, 390
polling, 192
security
audit log file, 491
for HP OpenView Web, 486
ovw.auth file, 506
ovwdb.auth file, 506
session configuration file, 490
user authentication file, 487
user roles file, 488
security management
components, 43
seed file
description of, 120
effect, 122
example, 120
format, 126
location, 126
name, 126
networks implied by, 126
when to use, 119
segment
object, 112
segment level, 230
Selected Nodes, 473
Selected Nodes command, 561
selecting
sources that correspond with alarms, 339
selection name, locate object by, 113
Server Web Page
accessing on remote node, 572
service provider

See DMI
services
at start-up time, 547
checking running, 527
dependencies on other services, 585
during operation, 548
logging and tracing, 639
netmon, 466
pmd, 323
starting with ovstart, 584
troubleshooting background, 584
verifying with ovstatus, 585
viewing configured, 562
web interface, 545
session configuration file, 490
defaults, 490
format, 490
location, 490
session layer, in OSI model, 22
set operation, 52
set request, 53
setting
community names, 145
filters, 335
home submap, 287
MIB values, directly, 412
MIB values, using query, 412
user default map, 287
setting your path, 101
settling time
event correlation, 354
Simple Network Management Protocol. See SNMP
Snapshot Recover operation, 135
snapshots
map, 555
removing old, 555
SNMP, 473
agents required, 134
Authentication Failures command, 560
community names, 146
configuration, 145, 146
data graph, 472
data graphing, 473
Errors command, 561
event configuration, 423
event correlation, 352
graphing data on all nodes, 561
graphing data on selected nodes, 561
nodes without, 59, 582, 626
Operations command, 560
operations for accessing MIB information, 52
polling, 178, 474
port, 146
proxie for agent, 146
RFC (technical details), 33
services, listing supported, 562
SetRequests in a Browse MIB operation, 628
Traffic command, 560
traps, 44
variable bindings, 404
version 1, described, 22
version 2
described, 23
SNMP agent
changing, 678
defined, 52
management operations exclusive to, 626
non-HP, 626
propagation of events from, 599
required for SNMP, 134
setting attribute, 676
unknown, 148
well-configured
community names, 93
MIB files, 93
trap forwarding, 93
SNMP Data Presenter
configuring, 511
features, 509
starting, 510
SNMP MIB Browser
accessing, 572
querying, 412
setting values, 412
troubleshooting SNMP, 136, 140, 147
viewing, 412
snmp notify, 325
SNMP services, 53
get request, 53
get response, 53
getBulk, 53
getNext, 53
set request, 53
SNMP Trap Recipients command, 565
SNMP traps, 326
forwarding from NNM, 326

IRQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0311
Doc: 3740

forwarding to NNM, 325
snmpCol.trace file, 609
snmpColDump, 608
snmpCollect
dependencies, 586
described, 543
tracing, 610
troubleshooting, 608
snmpCollect.lrf, described, 538
snmpd
errors, 635
propagation of events from, 599
SNMPv1
traps, 325
SNMPv1, described, 22
SNMPv2c, 325
described, 23
traps, 325
sockets
recreating ovsmpd sockets directory, 593
SOLID database
discreet backup, 175
sources that correspond with alarms, 339
sparse files (UNIX only)
backup, 171, 172, 173
special variables, 436
SRF, 664
staging area for backups, 165
standard deviation, 453
star
layout, 242
starting NNM, 106, 121, 122, 161, 173, 174, 195
redo initial discovery, 161
startup
automatic
disabling, 535
enabling, 535
customizing for performance, 535
state file
configuration, 344
static correlation parameters, 355
Station command, 573
station view
description, 522
status
categories, 271
colors, 271
compound source, 273
compound, explained, 275
conditions, 271
devices outside firewall, 184
marginal, 275
object source, 273
polling, 181
polling by object class, 182
polling with SNMP, 183, 273
propagate most critical, 276
symbol status, 271
stopping
all NNM sessions, 319
NNM to redo discovery, 161
real-time data graphing, 474
storing, MIB data for trend analysis, 45
streams and event correlation, 356, 380
subclass, symbol, 207
submaps, 245
background graphic, 202, 260, 262
creating, 244, 245
defined, 200
geometry, 266
home, 202
independent, creating, 245
layout algorithm, 241
meta-connection, 246
Node, 259
overlay, 267
Partitioned Internet, 248
persistence, 229
Quick Navigator, 288
regular vs. meta-connection, 246
root, 202
Segment, 259
setting, 287
subnet masks, 150
hierarchial, 91, 149
non-contiguous, 91, 149
problems with, 149
troubleshooting, 91, 149
subsystems used with nettl command, 643
support
obtaining, 77
programs provided, 74
swap space related problems, 579
switch centric view, 574
switches, 26
display of, 217
symbol
See node
symbol registration file, 664
for Network Presenter, 506

symbols
adding, 258
behavior, 279
changing, 662
characteristics, 209
class, 207
color
propagate, 274
status, 270
connection, 208, 246
context, 296
copying, 257
creating, 263, 662
cutting and pasting, 257
defined, 207
executable, 279
explodable, 279
hiding on map, 233
icon, 207
meta-connection, 245
moving, 257
multiple connections between, 245
naming networks, 221
predefined, 208
See node
status, 113, 271
subclass, 207
type, 114, 207
varieties, 207
synchronized data
restore all NNM data, 171
sysObjectID, 676
definition, 465
describing an SNMP agent's source, 466
determining IP topology behavior, 466
determining symbol type, 466
event reduction, 352
identifying an event's source, 466
netmon, 466
System Administration Manager, accessing, 565
System Information command, 565
system registry, 268
map access, 303
map appearance, 268

T

tab block, WLRF, 495
TCP
described, 23
viewing connections, 557
TCP Connections command, 557
TCP/IP
described, 23
telnet
accessing hpterm, 570
accessing terminal emulator, 570
accessing xterm, 571
terminal emulator, accessing, 570
terminal window, accessing, 570
thresholds
file, 588
operation for defining, 453
time intervals, 473
timeout intervals, 179
Tip of the Day
behavior, 69
toolbar buttons
adding to Network Presenter, 505
Tools
HP OpenView Launcher command, 571
Port-Address Mapping command, 571
Remote Power On command, 570
Report Presenter command, 569
Telnet (hpterm) command, 570
Telnet (xterm) command, 571
Terminal Connect command, 570
Unused IP Addresses command, 571
Views
All HSRP Groups command, 574
All VLANs command, 574
CDP command, 573
Internet command, 573
IPv6 Network command, 574
Neighbor command, 572
Node command, 573
OSPF Backbone command, 573
Path command, 573
Station command, 573
topology
polling, 184
topology database
and ovtopmd, 542
described, 63
total restore of NNM data, 171
trace file
trimming, 529
tracing
cautions for using, 639

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0312
3740
Doc:

common options, 640
data collection, 610
description of, 639
netmon, 641
recommendations, 580
trace files, 648
trimming file, 529
turning on, 647
with nettl, 646
traffic generation
measurement of polling, 654
regulation of polling, 178, 654
training
HP Education, 77
Transmission Control Protocol. See TCP
transport layer
in OSI model, 22
protocols, 23
trapd.conf, 422, 432
file, 631
trapd.log, 343
traps, 325, 422
defined, 52, 325
forwarding from NNM, 326
forwarding to NNM, 93, 325, 565
recipients, 326
SNMP, 44
trend database, described, 63
trimming
trace file, 529
troubleshooting, 131
additional sources of information, 579
Alarm Browser, 619
analyzing problems, 582
archive, 171, 174
background services, 584
backup, 171, 174
collecting too much data, 580
defaults modifications, 581
DMI communication, 628
IP, 131
Launcher, 616
Launcher error log file, 498, 653
name resolution scheme, 91, 92, 133
network operation, 623
Network Presenter, 618
OVLicenseMgr, 599
polling too much, 580
recommended practices, 579
restart initial discovery, 161
SNMP agents, 146
symptoms, 582
trustedCmds.conf directory, 433, 434

U

UDP, described, 23
universal pathnames
setting up, 101
universal pathnames for UNIX, 100
UNIXAdmin user role, 489
UNIXOper user role, 489
unknown status, 275
unmanage objects, 117
automatically, 129, 193, 669
defined, 53
effects of, 193, 654
uses of, 193, 654
Unused IP Addresses command, 571
user authentication file, 487
location, 487
modifying, 487
User Datagram Protocol. See UDP
user default map
setting, 287
user preferences, 287
user roles
described, 488
NetworkAdmin, 488
NetworkOper, 488
NTAdmin, 488
NTOper, 488
OVAdmin, 489
UNIXAdmin, 489
UNIXOper, 489
user roles file, 488
format, 489
location, 489

V

values
MIB, 412
variable binding
event reduction, 352
how to find and use, 404
variables, 436
vendor attribute, 676
viewing
connection labels, 223
events, 330
MIB values, 412

network services, 562
object descriptions, 111, 112
see find
traffic route, 562
VLAN membership view, 574

W

WANs
latency time for, 182
web browser
launching on remote node, 572
requirement on client station, 485
web interface services, 545, 550
web server
aliases, 485
included in NNM, 485
web sites
for NNM manuals, 76
HP OpenView, 78
HP Openview, 76
network management, 35
OpenView Forum, 77
product support, 77
WebWindow, 496
well-configured network
community names, 93
DHCP, 91
DMI service providers, 95
MIB files obtained, 94
name resolution, 91, 133, 141, 143
SNMP, 145
subnet masks, 91, 149
trap forwarding, 93
troubleshooting, 131
white papers,accessing, 75
wildcards
event sources, 432
netmon.noDiscover file, 126
threshold monitoring, 452
window, 331, 332
Alarm Browser, 329
Alarm Categories, 329
window geometry, 266
Windows
Diagnostics, 569
Event Viewer, 569
Performance Monitor, 561
Registry Editor, 565
system registry, 268
WLRF, 494
action block, 496
components, 494
list block, 495
location, 494
problem reading, 617
tab block, 495
verifying, 494
Web Launcher Registration File, 494
WebWindow, 496
www access, 318

X

X Windows
.Xdefaults file, 581
performance impact, 656
problems with, 635
resources, 581, 635
restoring default resources, 635
X11 monochrome bitmap format, 260
xnm program
operations started by, 626
permissions, 623
xnmappmon
described, 543
operations started by, 627
xnmbrowser, described, 543
xnmbuilder, described, 543
xnmcollect, described, 543
xnmevents
command, 341
xnmeventsExt.conf file, 340
launching views and URLs, 340
modifying, 340
xnmgraph, described, 544
xnmloadmib, described, 544
xnmpolling, 194
xnmpolling, described, 544
xnmsnmpconf, described, 544
xnmtrap, 422
xnmtrap, described, 544
xpr, 475
xterm, accessing, 571
xwd, 475

Z

zoom, 474

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0313
3740
Doc:

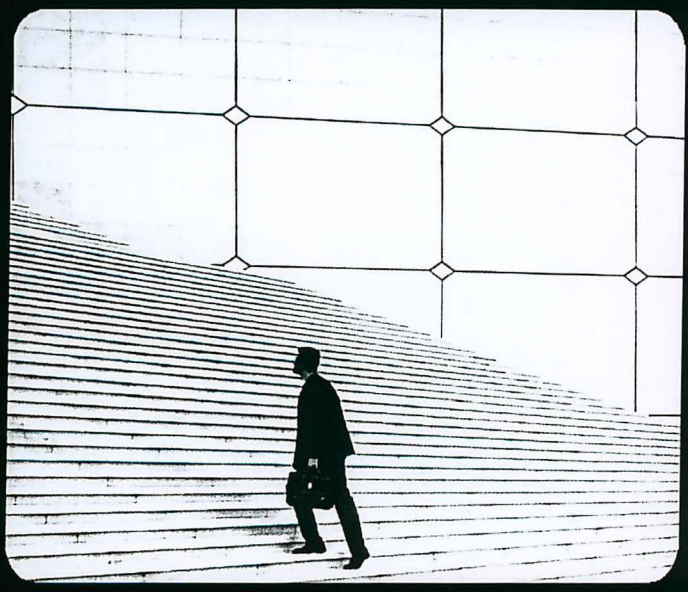


invent

Pregão nº 118/2003 – CPL/AC

Proposta

16 de dezembro de 2003

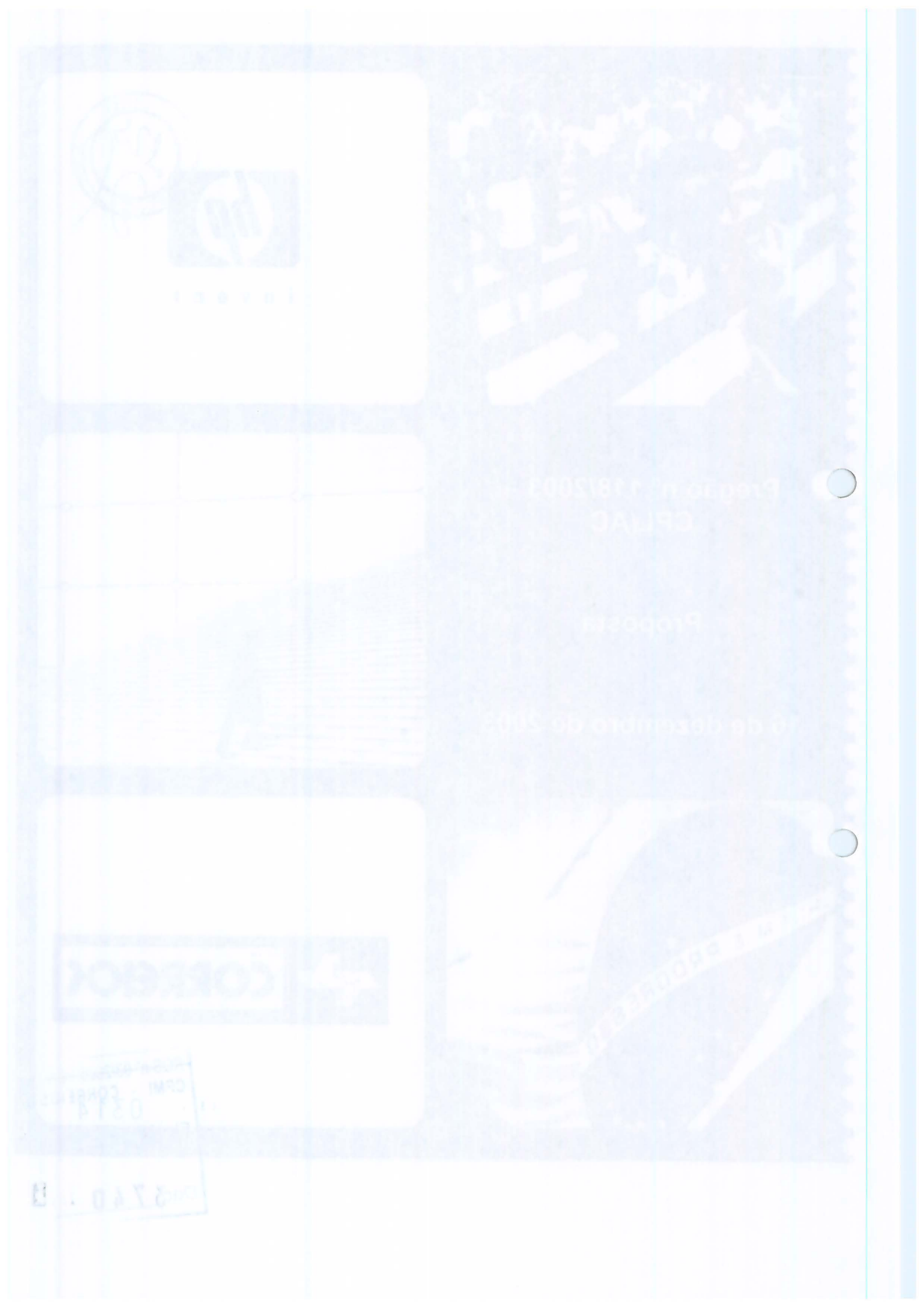




CORREIOS

RQS nº 03/2005 - CN
CPMI - CORREIOS
0314

Doc 3740



proposta

Hewlett-Packard Brasil Ltda.

CORREIOS

Pregão nº 118/2003 - CPL/AC

16 de dezembro de 2003

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0315
3740
Doc:

Hewlett-Packard Brasil Ltda.
Alameda Rio Negro, 750
Alphaville - 06454-000
Barueri - SP
Brasil

José Eduardo Ribeiro
Representante Legal
Tel.: (61) 329-6055
Cel.: (61) 9974-6565
josé-eduardo_ribeiro@hp.com

São Paulo, 16 de dezembro de 2003

Áos
CORREIOS

Ref.: Pregão nº 118/2003 – CPL/AC

Prezados Senhores,

A Hewlett-Packard Brasil Ltda. está honrada em responder sua solicitação. Estamos encaminhando para apreciação nossa proposta para Pregão nº 118/2003 - CPL/AC

Estamos confiantes que a nossa proposta atenderá suas necessidades atuais e futuras. Para maiores esclarecimentos e informações, não hesite em contatar-nos.

A Hewlett-Packard Brasil Ltda. possui pessoal, tecnologia, experiência e comprometimento que resultarão em uma parceria perfeita com vocês.

Atenciosamente,

José Eduardo Ribeiro

Representante Legal

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0316
3740
Doc.

Índice

1. Proposta Econômica
2. Características Técnicas
3. Certificação Técnica
4. Termo de Garantia Técnico

Apêndices

ECT - DOS nº 23/2005 - CN
CPMI - CORREIOS
Fls. Nº 0317
3740
Doc:

1. Proposta Econômica

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0318
3740
Doc:

PROPOSTA ECONÔMICA

PREGÃO Nº 118/2003.

1. Razão Social da Empresa: .Hewlett Packard Brasil Ltda.
2. CNPJ Nº: 61.797.924/0001-55
3. Inscrição Estadual: 206.203.572.117
4. Inscrição Municipal: .4-00.878-1
5. Endereço Completo: .Alameda Rio Negro, 750 – Alphaville – Barueri – SP – CEP: 06454-000
6. Telefone: (061).329-6055 Fax: ..(011) 4197-8432.. E-mail: .jose-eduardo.ribeiro@hp.com
7. Validade da Proposta: ..60. *(sessenta)* dias
8. Prazo de Pagamento: Em parcela única, mediante entrega das ferramentas, no prazo de 15 (quinze) dias após a emissão do Termo de Aceitação Final – TAF.
9. Banco: .341 Itaú Agência: .0912. Conta Corrente: .08067-8.
10. Representante da Empresa: .José Eduardo Pires do Rio Ribeiro
11. Cargo: ..Account Manager . RG: .15.319.247 (SSP-SP). CPF: .071.885.858-14.
12. Unidade da Federação de emissão da Nota Fiscal: .São Paulo

Apresentamos nossa Proposta para fornecimento do material do objeto do Pregão nº /2003, acatando todas as estipulações consignadas no Edital, conforme abaixo:

ITEM	DESCRIÇÃO	UNID.	QTDE.	PREÇO UNITÁRIO (R$)	PREÇO TOTAL (R$)
01	Licença do Software HP OPEN VIEW NETWORK NODE MANAGER ENTERPRISE VERSÃO 6.2 OU SUPERIOR.	UM.	05	95.000,00	475.000,00

Garantia do objeto: (01 ano)

Preço Unitário: (R$ 95.000,00) Noventa e cinco mil reais

Preço Total: (R$ 475.000,00) Quatrocentos e setenta e cinco mil reais

4

Pregão nº 118/2003 - CN -
CPMI - CORREIOS
Fls. Nº 0319
3740
Doc:

MODELO DE PLANILHA DE CUSTOS DE FORMAÇÃO DO PREÇO

ITEM	PERCENTUAL
1. MATÉRIA PRIMA/INSUMOS:	
Licenças de Software e Serviços	90%
Subtotal	90%
2. TRIBUTOS	
ISSQN	5%
Subtotal	5%
3. TRASPORTES	
Frete	0.5%
Subtotal	0.5%
4. DESPESAS ADMINISTRATIVAS	
	0.5%
Subtotal	0.5%
5. LUCRO	
	4%
Subtotal	4%
6. OUTROS	
	0%
Subtotal	0%
TOTAL	100%

Declaramos que tomamos conhecimento de todas as informações e condições para o cumprimento das obrigações objeto desta licitação e que atendemos todas as condições do Edital.

Data: .16./ 12./ .2003

José Eduardo Pires do Rio Ribeiro
Representante Legal

61.797.924/0001-55

HEWLETT PACKARD BRASIL LTDA

Al. Rio Negro, 750
Alphaville - CEP.: 06454-000
BARUERI - SP

Pregão nº RQS 8/2003 2005-LAC-
CPMI - CORREIOS
Fls. Nº 0320
Doc. 3740

2. Características Técnicas

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0321
3740
Doc:

Especificação Técnica
Licenças de Software para Gerenciamento

	Características Mínimas
1. Descrição	Software HPOpenView Network Node Manager Enterprise v. 6.20 ou superior
2. Quantidade de Licenças	5 (cinco)
3. Garantia	- 12 (doze) meses a contar do Termo de Aceite Final -A garantia deve compreender a correção de falhas no produto, independentemente de correções tornadas públicas, desde que tenham sido detectadas e formalmente comunicadas à contratada. - Caso seja detectado bugs ou falhas no software, a empresa contratada deverá fornecer atualizações necessárias à correção do problema. Os produtos devem ser isentos de back doors. - A versão deve ser a última disponível no mercado na data de entrega do produto.
4. Compatibilidade	O produto deve ser compatível com o sistema operacional SUN SOLARIS e HP-UX.
5. Documentação Técnica	O produto deve ser entregue com documentação técnica do fabricante. Deverá ser fornecida documentação: – das parametrizações (customizações) realizadas nas ferramentas no processo de instalação e configuração; e – de instalação, configuração e operação.
6. Outros	O produto deve: – Ser fornecido em CD/ROM; – Ser fornecido, instalado, configurado e integrado às ferramentas HP OpenView NNM e VP/O já existentes no ambiente de gerência da ECT, mantendo a padronização existente; – A instalação compreende, dentre outros, a preparação dos servidores SUN e/ou HP, instalação e parametrização dos respectivos Sistemas Operacionais (Solaris e/ou HP UX). Os servidores e sistemas operacionais serão fornecidos pela ECT. – A instalação compreende, dentre outros, a implementação de alarmes definidos segundo padronização da ECT, integração com as consoles do HP-VP/O e descoberta (discovery) dos elementos a serem gerenciados.
7. Prazos	Entrega: até 10 (dez) dias, após a assinatura do contrato; Instalação e Configuração Final: até 40 (quarenta) dias após a Entrega; Termo de Aceite Final: até 5 (cinco) dias após a Instalação e Configuração Final; Pagamento: até 15 (quinze) dias após o Termo de Aceite Final.

FRQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 0322
Doc: 3740

Especificação Técnica
Licenças de Software para Gerenciamento

8. Atendimento e Suporte	- Deve ser fornecido a referência completa do canal de atendimento e suporte técnico do produto ofertado, com a nomeação e o telefone do(s) responsável(eis) técnicos que possa(m) responder questionamentos sobre todas as características do produto em pauta. - O atendimento e suporte ao produto deve compreender o acesso a help-desk para atendimento e abertura de chamados em língua portuguesa (durante horário comercial), incluindo o atendimento telefônico e o atendimento via e-mail. - Na descrição dos requisitos técnicos constantes de proposta referente ao produto devem ser apresentadas as demais modalidades de suporte técnico disponibilizadas, com detalhamento dos seus meios de acesso, quando existentes. -O atendimento a chamadas deve ocorrer, se necessário, nos dias úteis da semana no horário comercial, no esquema 8 x 5, até 4 (quatro) horas da abertura dos chamados por uma central de atendimento 0800 do fabricante. - O prazo de Atendimento e Suporte é de 12 (doze) meses a contar do Termo de Aceite Final.
9. Garantia Contratual	5% (cinco porcento) do valor global do contrato. Vigência: até o prazo final do Atendimento e Suporte.
10. Atualização	-A contratada deverá prover toda e qualquer atualização pertinente ao produto pelo período mínimo de um ano. -Em caso de upgrades, quando a aplicação da nova versão resultar em perda de dados, incapacidade de abertura ou gravação de arquivos ou qualquer outra incompatibilidade relativamente às versões anteriores, tais restrições deverão estar claramente relatadas na descrição dos requisitos de natureza técnica das propostas -Para fins desta especificação técnica, entende-se como atualização o provimento de toda e qualquer evolução do produto, incluindo: - patches, fixes, correções, updates e service packs; - novas releases, builds e funcionalidades; - o provimento de upgrades para novas versões de mercado ou lançamentos (tal como ocorre, por exemplo, na migração de *Produto* 6 para *Produto* 7 e similares); e, - o provimento de upgrades englobando, inclusive, versões não sucessivas, caso a disponibilização de tais versões ocorra durante o período da garantia (como exemplo, a migração de *Produto* 5 para *Produto* 7, 8 ou posterior). -A contratada deverá fornecer tais atualizações independentemente de solicitação expressa da contratante.

(X) Atende ( ) Não atende

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0323
3740
Doc:

3. Certificação Técnica

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0324
3740
Doc:

declaração

Hewlett Packard Brasil Ltda.
Alameda Rio Negro, 750 - Alphaville
06454-000 - Barueri - SP
CNPJ: 61.797.924/0001-55
Fone: (11) 4197 8000
Fax: (11) 4197 8432

www.hp.com.br

690469-BR

DECLARAÇÃO DE CERTIFICAÇÃO TECNICA

À

EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS - ECT

SBN, Quadra 01 – Bloco "A" – 4º andar – Ala Norte – Ed. Sede/ECT – CEP 70002-900 – Brasília/DF

Fax.: 61. 426.2759

REF.: PREGÃO Nº 118/2003 – CPL/AC

Hewlett-Packard Brasil Ltda., CNPJ nº 61.797.924/0001-55, por intermédio de seu representante legal o Sr. Jose Eduardo Pires do Rio Ribeiro, portador da Carteira de Identidade nº 15.319.247 (SSP/SP) e do CPF nº 071.885.858-14, DECLARA, para os devido fins que, possuimos Certificação Técnica para prestação de suporte, manutenção e garantia.

Barueri, 15 de dezembro de 2003.

Jose Eduardo Pires do Rio Ribeiro
Gerente Contas Governo
Hewlett Packard Brasil Ltda
CNPJ Nº 61.797.924/0001-55

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0325
3740
Doc:

4. Termo de Garantia Técnico

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0326
3740
Doc:

declaração

Hewlett Packard Brasil Ltda.
Alameda Rio Negro, 750 - Alphaville
06454-000 - Barueri - SP
CNPJ: 61.797.924/0001-55
Fone: (11) 4197 8000
Fax: (11) 4197 8432

www.hp.com.br

690469-BR

ANEXO 6

TERMO DE GARANTIA TECNICA

Inicio de Vigência:

As empresas abaixo descritas, firmam entre si o presente Instrumento, doravante denominado simplesmente de TERMO DE GARANTIA TECNICA.

DESIGNAÇÃO DAS PARTES DORAVANTE NO TERMO	ECT	FORNECEDORA
Razão Social	EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS	HEWLETT-PACKARD BRASIL LTDA
Endereço	SBN, Qd. 01 – Bloco "A" – 4º andar – Ala Norte – Ed.Sede/ECT	Al. Rio Negro, 750 – Alphaville – Barueri/SP
CEP	70002-900	06454-000
Cidade	Brasília	Barueri
Estado	DF	SP
CNPJ		61.797.924/0001-55
I.E.		206.203.572.117

1. **OBJETO**: Garantia Técnica do software HPOpen View Network Node Manager Enterprise v.6.20 ou superior, englobando o atendimento e suporte.
2. **PRAZO DE GARANTIA:** a partir da data de emissão do Termo de Aceite Final, encerrando-se 12 (doze) meses após a emissão deste Termo de aceite final.
3. RESPONSABILIDADE DA FORNECEDORA:

3.1 – Corrigir falhas no produto, independentemente de correções tornadas públicas, desde que tenham sido detectadas e formalmente comunicadas à FORNECEDORA.
3.2 – Fornecer autalizações necessárias à correção de problemas como bugs ou falhas no software. Os produtos devem ser isentos de back doors.
3.3 – entregar a última versão disponível no mercado na data de entrega do produto.

12

RQS nº 03/2005 - CN
CPMI - CORREIO
Fls. Nº 0327
Doc: 3740

declaração

Hewlett Packard Brasil Ltda.
Alameda Rio Negro, 750 - Alphaville
06454-000 - Barueri - SP
CNPJ: 61.797.924/0001-55
Fone: (11) 4197 8000
Fax: (11) 4197 8432

www.hp.com.br

3.4 – Comprometemo-nos a fornecer à ECT todas as atualizações de versões do software adquirido durante a vigência deste TERMO.

3.5 Forneceremos a referência completa do canal de atendimento e suporte técnico do produto ofertado, com a nomeação e o telefone dos responsáveis técnicos que possam responder questionamentos sobre todas as características do produto em pauta.

3.6 Prestar atendimento de suporte técnico a ECT, pelo período de 1(um) ano, visando sanar eventuais problemas, observando-se os seguintes prazos:
a) atendimento: no prazo de 04(quatro) horas corridas; e
b) solução do problema: 12(doze) horas corridas.

3.6.1. Define-se como tempo de atendimento o período compreendido entre o horário de comunicação do chamado feito pela ECT e o horário de chegada ao local de atendimento.

3.6.2. Define-se como tempo de solução do problema, o período compreendido entre o horário de comunicação do chamado feito pela ECT e o horário de término da solução, deixando o software em condições normais de operação.

3.7. o atendimento e suporte ao produto devem compreender o acesso a help-desk para atendimento e abertura de chamados em língua portuguesa(durante horário comercial), incluindo o atendimento telefônico e o atendimento via e-mail.

3.8 – Na descrição dos requisitos técnicos constantes da proposta referente ao produto serão apresentadas as demais modalidades de suporte técnico disponibilizadas, com detalhamento dos seus meios de acesso, quando existentes.

3.9. o atendimento a chamados deve ocorrer, se necessário, nos dias úteis da semana no horário comercial, no esquema 8 x 5, até (quatro) horas da abertura dos chamados por uma central de atendimento nº 0800.130.999 da HP.

3.10. o prazo de atendimento e suporte é de 12(doze) mesesa contar da data de emissão do termo de aceite final – TAF, pela ECT.

3.11. a HP proverá toda e qualquer atualização pertinente ao produto pelo período mínimo de um ano.

3.12. em caso de upgrades, quando a aplicação da nova versão resultar em perda de dados, incapacidade de abertura ou gravação de arquivos ou qualquer outra incompatibilidade relativamente às versões anteriores, tais restrições estarão claramente relatadas na descrição dos requisitos de natureza técnica das palavras.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0328
3740
Doc:

declaração

Hewlett Packard Brasil Ltda.
Alameda Rio Negro, 750 - Alphaville
06454-000 - Barueri - SP
CNPJ: 61.797.924/0001-55
Fone: (11) 4197 8000
Fax: (11) 4197 8432

www.hp.com.br

3.13. – Para fins da especificação técnica constante neste contrato, entende-se como atualização o provimento de toda e qualquer evolução do produto, incluindo:
- patches, fixes, correções, updates e serviços packs
- novas releases, builds e funcionalidades;
- o provimento de upgrades para novas versões de mercado ou lançamentos (tal como ocorre, por exemplo, na migração de produto 6 para Produto 7 e similares); e
- o provimento de upgrades englobando, inclusive, versões não sucessivas, caso a disponibilização de tais versões ocorra durante o período da garantia(como exemplo, a migração de Produto 5 para Produto 7, 8 ou posterior).

3.14. A HP fornecerá tais atualizações independentemente de solicitação expressa da ECT.

4. – DAS PENALIDADES:

4.1. 0 não atendimento do suporte técnico e solução de problemas à ECT, dentro dos prazos estabelecidos no subitem 3.4. deste Termo: 1% (um por cento) sobre o valor unitário da ferramenta, cujo atendimento foi reclamado, por hora de atraso.

4.2. – o não atendimento de qualquer item descrito neste Termo de Garantia Técnica : 1% (um por cento) sobre o valor unitário da ferramenta.

Barueri, 15 de dezembro de 2003.

CONTRATADA:

Representante LegaL.: Jose Eduardo Ribeiro

Representante Legal.: Raul Papaleo

Testemunha:

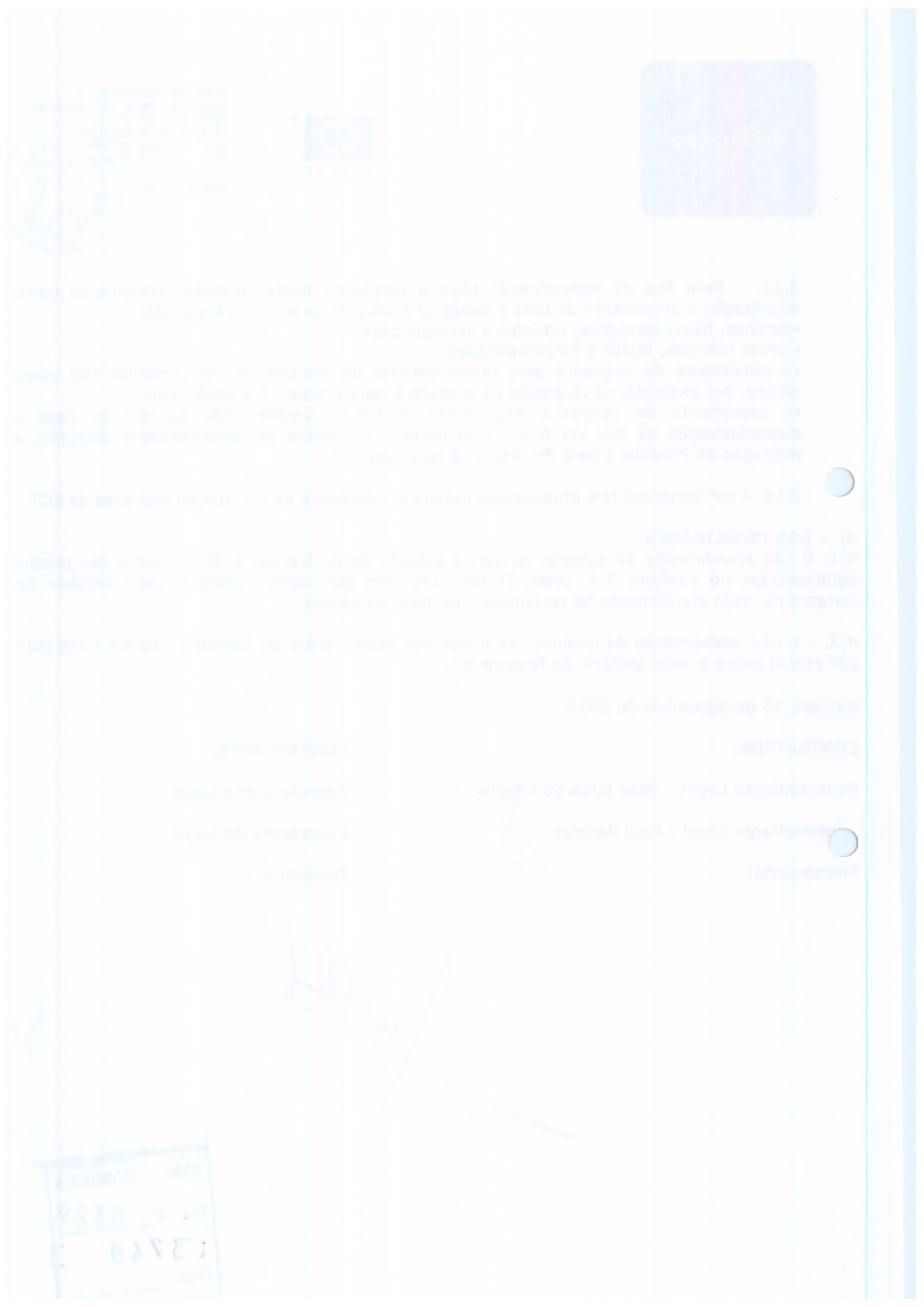
CONTRATANTE:

Representante Legal

Representante Legal

Testemunha:

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0329
3740
Doc:



Apêndices

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls.: Nº 0330
Doc: 3740

HP OpenView Network Node Manager

A Guide to Scalability and Distribution

HP-UX, Solaris, and Windows operating systems



Manufacturing Part Number: J5323-90001
January, 2003

© Copyright 2003 Hewlett-Packard Company.

RQS nº 03/2005 - CN
CPMI - CORREIOS
0331
Fls. Nº
740
Doc:

Legal Notices

Warranty.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices.

©Copyright 1983-2003 Hewlett-Packard Company.

No part of this document may be copied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

Contains software from AirMedia, Inc.

© Copyright 1996 AirMedia, Inc.

Trademark Notices

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

Windows® and MS Windows® are U.S. registered trademarks of Microsoft Corporation.

Windows® 2000 is a U.S. registered trademark of Microsoft Corporation.

Windows NT® is a U.S. registered trademark of Microsoft Corporation.

Netscape and Netscape Navigator are U.S. trademarks of Netscape Communications Corporation

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

Oracle7TM is a trademark of Oracle Corporation, Redwood City, California.

OSF/Motif® and Open Software Foundation® are trademarks of the Open Software Foundation, Inc. in the U.S. and other countries.

Pentium® is a U.S. registered trademark of Intel Corporation.

UNIX® is a registered trademark of The Open Group.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0332
3740
Doc:

Support

1. Overview of Scalability and Distribution in NNM

Scalability and Distribution in NNM 15
Benefits of Scalability 15
What Makes NNM a Scalable Solution for Network Management? 16
Network, System, and Operator Efficiency via Filtering 19
Distributed Internet Discovery and Monitoring 20
Capacity Planning 21
About Management Stations and Collection Stations 22
Management Consoles 24
On-Demand Submaps 26
Distributed Threshold Monitoring and Event Forwarding 27
General Events 27
Threshold Events 28
Trend Data Collection in a Distributed NNM Solution 28
Large-Map Viewing Support 29
The Panner 30
The Quick Navigator 30

2. The Scalable Architecture of Network Node Manager

The Distribution Model for Network Node Manager 33
Network Connections between Distributed Components 36
Filters 37
Discovery Filtering 40
Topology Filtering 41
Map Filtering 42
Defining New Filters 43
Filter Utilities 45
Distributed Internet Discovery and Monitoring 46
About Collection Domains 46
Distributed Services Architecture 48
High Availability Management Information 50
Overlapping Collection Domains 52
Configuration Concepts 56
Distributed Threshold Monitoring and Event Forwarding 59

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0333
3740
Doc:

Event Correlation for "Connector Down" 60
Data Collection for Distributed Threshold Monitoring 62
On-Demand Submaps 64
Transient Submaps and the Submap List Dialog 67
Persistence Filtering 68
Comparing Map Filters and Persistence Filters 69
Management Consoles 70
Management Consoles and On-Demand Submaps 72
Customized Views of the Network 72
Management Consoles and X-Terminals 73
Interface Managed-state Automation 74
Microsoft Terminal Server Access 75
Accessing a Single NNM Station From Multiple Terminal Server Clients 75
Accessing Multiple NNM Stations From a Single Terminal Server Client 77
Accessing Multiple NNM Stations From Multiple Terminal Server Clients 78

3. Strategies for Deploying Network Node Manager

Planning the Right Approach 83
General Considerations about Scalability and Distribution 84
General Strategies for Deployment 87
Deployment Strategies for NNM 89
Use of Scalability Features in NNM Deployment 89
Fully Centralized Management 92
Implementation Tactics 93
Implications of Using the Fully Centralized Management Model 94
Centralized-Hierarchical Management 95
Implementation Tactics 96
Implications of Using Centralized-Hierarchical Management 97
Hierarchical Management 98
Implementation Tactics 100
Implications of Using the Hierarchical Management Model 101
Cooperative Independent Management 103
Implementation Tactics 104
Implications of Using the Cooperative Independent Model 105

4. Procedures for Scaling NNM

Configuring Management Consoles 109
Configuring a Windows System Console Server 111
Installing a Management Console on Windows for an NNM Server on Windows . 111
UNIX System Server Configuration 112
Installing Management Consoles on Windows for UNIX System Management Servers 115
UNIX System Console Configuration 117
Increasing Security for Management Consoles 119
Undoing a Management Console 120
Configuring On-Demand Submaps 121
Configuring Demand Level 121
Specifying a Persistence Filter 124
Integrating Applications With On-Demand Submaps 125
Configuring a Map Filter 127
Configuring Data Collection for a Station 128
Configuring a Discovery Filter 128
Managing and Unmanaging Locally Monitored Objects 132
Configuring Collection Stations 133
Configuring Security for a Collection Station 133
Configuring a Topology Filter for a Collection Station 134
Changing the Topology Filter for a Collection Station 135
Configuring IPX on a Collection Station under Windows 136
Configuring Management Stations 137
Determining if a Node is a Collection Station 137
Determining All Objects Monitored by a Collection Station 138
Configuring for a Specific Collection Station 138
Unmanaging a Collection Station 140
Removing a Collection Station from a Management Station 141
Configuring a Remote Communication Timeout and Retry Count 141
Performing a Full Topology Synchronization 144
Identifying Collection Station Communication Problems 145
Troubleshooting Collection Station Communication 147
Configuring Domain Overlaps and Failover 150
Determining the Primary Collection Station for an Object 150
Changing the Primary Collection Station for an Object 151
Changing the Overlap Mode 152

RQS nº 03/2005 - CN 1
CPMI - CORREIOS
Fls. Nº 0334
Doc: 3740

Collection Station Failover 153
Configuring Event Forwarding and Correlation 154
Forwarding an Event 154
Using Distributed Data Collection 159

5. Dynamic Views and Distributed Management

Dynamic Views and Distributed Management 163
NNM Neighbor View 164
NNM Path View 165

A. The Filter Definition Language

The Filter Definition File 169
Filters and Filter-Expressions 170
Sets 171
Attribute Value Assertions 172
Valid Operators for AVAs 173
Boolean AVAs 174
Integer AVAs 175
Enumerated (Enum) AVAs 175
String AVAs 175
Excluding a Node 180
Relationships Between Nodes and Interfaces 180
Valid Operators for Logical Combinations of AVAs or Filters 180
Filterable Objects and Attributes 181
Filter File Grammar 187
Filter File Example 189
Setting Up Collection Domains 190
Excluding Nodes 192
Failover Filters 193
Important Node Filters 193
Topology Filters 194
Map Filters 195
Using the Network Presenter 195
Default Filter File 197

B. Using NNM Under a Mixed Codeset Environment

Glossary **209**

Index **213**

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0335
Doc: 3740

Support

Please visit the HP OpenView web site at:

`http://openview.hp.com/`

There you will find contact information and details about the products, services, and support that HP OpenView offers.

The support area of the HP OpenView web site includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0336
3740
Doc:

1 Overview of Scalability and Distribution in NNM

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0337
Doc: 3740

Scalability and Distribution in NNM

You can configure NNM to perform well for a wide range of network sizes and degrees of complexity. This attribute is commonly referred to as the **scalability** of NNM. Scalability gives NNM the potential to handle almost any size network, in both local and wide-area environments.

One approach to making a product like NNM scalable, and an important feature of NNM, is to distribute the network management workload to multiple, usually remote, systems. NNM makes **distribution** possible, so you can monitor and manage much larger networks while minimizing the management resources required.

In summary, the scalability and distribution of NNM optimizes the use of two key resources:

- First, NNM includes features that help you use the *system resources* at the management station very efficiently.
- Second, other features of NNM, especially distribution, reduce the amount of management traffic over your *network*, most importantly, over congested or expensive links.

Benefits of Scalability

Having a scalable network management platform, implemented in part through distribution, provides you with many benefits in your application of NNM as a network management solution.

First, scalability gives your network management solution the ability to evolve with your organization. Networks are dynamic entities that reflect the changing structures and needs of the organizations they serve. As your network changes and grows, the scalable features of NNM make it easier to adapt your network management to handle new networking landscapes.

Second, a distributed network management solution can dramatically reduce the traffic overhead that network management can impose on congested or expensive network links. Most large (enterprise) networks include serial or wide-area (WAN) links. Such links are both relatively slow and expensive. Without a distributed network management solution, it is simply impractical to monitor tens of thousands of nodes from a single workstation; the networking load emanating from the

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0338
Doc: 3740

management station becomes a bottle neck. Distribution minimizes the amount of network management traffic on these links, freeing bandwidth for business purposes.

Third, a distributed solution makes it possible to share network management responsibility and resource requirements among multiple sites. By spreading the resources and responsibilities out, you reduce the risk of losing all network management in the event of an unexpected shutdown of your management station. Distribution also makes it easier to perform maintenance shutdowns without losing your overall network management.

Fourth, a scalable network management solution, sensibly deployed and properly configured, results in faster response times and better performance. You spend less time waiting for data and more time acting on it. Furthermore, it improves network reliability by allowing local management actions even when contact is lost with a remote central management site.

Finally, deploying a scalable network management platform means everyone in your organization can share a single customizable tool. This naturally leads to a common vocabulary, common experiences, sharable expertise, and the ability to more easily articulate and implement standard processes and procedures in your organization.

All together, NNM's scalability and distribution gives you the power to manage the large and geographically dispersed enterprise networks that are critical to key business or organizational processes. You can use common applications at every level to create a more integrated, consistent solution to the complex problems in these environments.

What Makes NNM a Scalable Solution for Network Management?

The idea of "scalability" is abstract, but HP OpenView Network Node Manager has several broad categories of features that make scalability a concrete reality.

Distributed Internet Discovery and Monitoring

Distributed Internet Discovery and Monitoring lets remote collection stations monitor their part of the network and inform the central management station about it. This reduces network traffic, and also reduces the load on the central station.

Management Consoles

Management consoles off-load display processing from the management station to a display station. With management consoles, you can have more operators monitoring and managing your network without loss of performance; these operators can handle larger environments.

Web Browser Interface

Accessing network management functions from your web browser lets you monitor your network from any location with a web browser installed, even if it is not a management console. See *Managing Your Network with HP OpenView Network Node Manager* for more information.

Large-Map Viewing Support

NNM gives you two essential features for examining large maps:

- The panner, which makes it easy to navigate submaps with hundreds of symbols.
- The quick navigator, which gives you instant access to your most critical or frequently visited submaps.

On-Demand Submaps

The on-demand submap feature provides a very significant boost in the performance of NNM, allowing it to manage many more objects (up to ten times) than with persistent submaps. Enabling the on-demand submap feature lets your management station use less memory to perform the same tasks.

Filtering

Filters let you reduce the amount of extraneous data being handled by the system, or presented to the operator. This provides improved performance, and reduces visual clutter for the operator.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0339
3740
Doc:

Event Forwarding

You can configure your remote stations so that events from managed nodes, or from non-NNM applications on the collection station, get forwarded to interested management stations. This can be set up to occur whether or not the event triggers local actions, or has already been correlated.

Important events generated internally to NNM, such as topology or status change events, are automatically forwarded from a collection station to the interested management stations, without additional configuration steps.

Distributed Threshold Monitoring

Distributed threshold monitoring reduces management traffic on the network by allowing remote stations, instead of the management station, to collect SNMP trend data and trigger threshold events based on that data.

Interface Managed-state Automation

NNM lets you automatically manage or unmanage interfaces based on filters. Interface managed-state automation makes it easier to manage large environments, where frequently many discovered interfaces do not require active status polling.

High Availability and Fault Tolerance

NNM stations can be run on HP Service Guard clusters to provide continuous availability. Also, if a collection station fails, you can configure its status polling duties to transfer over to a management station. You can also perform backup of your network management data without losing incoming information during that time.

Your practical limits in using all the above depend on the size of your network environment, your management strategy, and the resources available on the management and collection stations. For the most current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide*, available at `http://openview.hp.com/`.

NOTE The upper limits of operators and managed devices depends very heavily on the level of monitoring and data collection you require. In general, increasing the polling intervals on noncritical nodes increases the number of nodes that can be handled.

Network, System, and Operator Efficiency via Filtering

For NNM to manage very large environments, all resources (network, system, and human) must be used as efficiently as possible. To maximize the efficient use of these resources, NNM employs a strategy of data reduction via filters.

A **filter** is essentially just a way to remove unneeded data from consideration for further processing. The result of less data in the system is higher performance for NNM, and improved usability for the operators.

For example, you may have an operator whose only concern is the routers and hubs in your environment. For that operator, any other objects on his map are merely clutter. With NNM, you can apply a filter to the map, so that only routers and hubs appear.

See "Filters" on page 37 for more details about filtering in NNM.

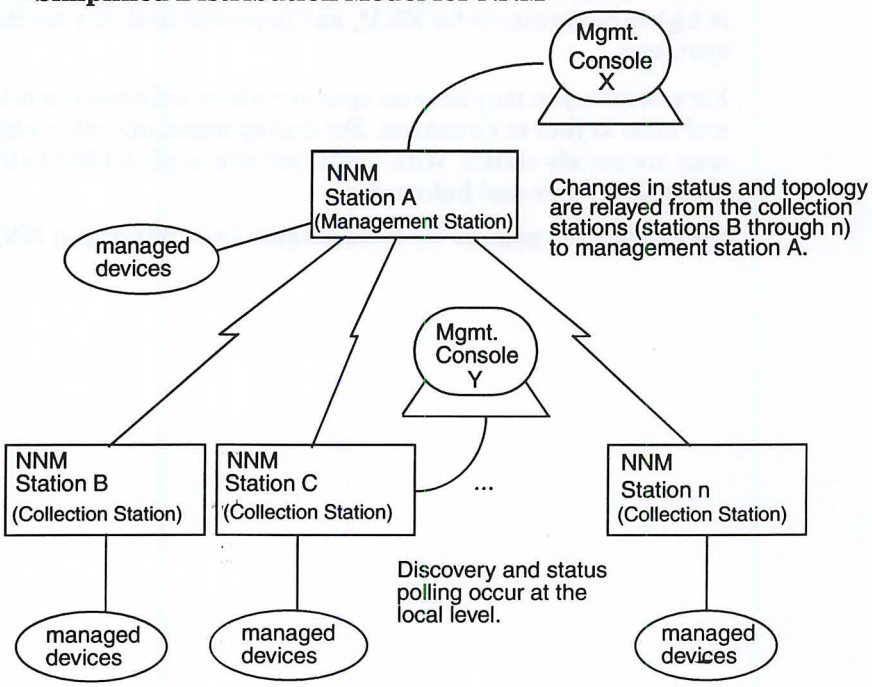
RQS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 0340
3740
Doc:

Distributed Internet Discovery and Monitoring

A network management system can consume significant resources while performing discovery, topology monitoring, and status polling. One feature of HP OpenView Network Node Manager is the ability to move much of this load from the management station to one or more remote machines.

This capability is called **Distributed Internet Discovery and Monitoring**, and is illustrated in Figure 1-1. The device count for this model assumes one interface per device, on average. Note that the management console at Station C indicates that it also serves as a management station for the objects it monitors; this is the usual configuration of NNM.

Figure 1-1 Simplified Distribution Model for NNM



To use distributed internet discovery and monitoring, you designate one or more remote machines as **collection station**s. Each collection station takes over the task of monitoring some portion of the network, while informing all interested management stations of any changes in the status or topology of the network it monitors.

Capacity Planning

Because distributed management partitions the work of discovery and status polling, it also dramatically reduces traffic on the network, most importantly on expensive or congested links.

When considering performance and configuration issues, you must distinguish between nodes and objects. There is a one to many relationship between the number of nodes and the number of objects in the object database. Even though a network model is typically described in terms of the number of nodes the application manages, it is the number and type of managed objects that is the most important parameter when predicting how the application will scale and perform.

Determining the exact number of managed objects is especially critical when predicting, for example, the size of a database, the load on `netmon`'s polling cycle, or the load imposed on a management station when synchronizing with a collection station. You'll want to determine the appropriate node to object multiplier for your environment.

Not all network environments conform to the typical environment described above. In some environments, the ratio of objects to nodes is higher because enterprise routers tend to have more than two physical interfaces. For example a network center responsible for monitoring only backbone routers would have a higher ratio. In some cases nodes may have additional virtual interfaces. Secondary addresses, for example, increase the number of objects associated with that particular managed node.

There is no concrete limit to the number of objects or devices you can manage, or to the management stations you can deploy. Your practical limits depend on the size of your network environment, your management strategy, and the resources available on the management and collection stations. For the most current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide*, available at `http://openview.hp.com/`.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0341
Doc: 3740

About Management Stations and Collection Stations

In the previous section (including Figure 1-1), two terms were introduced:

- Management station
- Collection station

It is important to recognize that these labels state the *roles* of the machines involved, and do not refer to different software on them. In this vein, you should note that a single NNM station can perform either role, or both at once. Regardless of the role it is playing (as a collection or management station, or both), every NNM station has the full capabilities of NNM[1]. HP Service Guard clusters for UNIX systems may be used for any type of management station to ensure constant availability.

The role of a management station is to make the network management functionality available to users, either directly or via one or more management consoles.[2]

The role of a collection station is to be a collection point in the overall network management system. A collection station typically performs topology and IP status monitoring, threshold data collection, local event correlation, and event forwarding or handling on behalf of one or more management stations.

When changes occur in topology or status, or when a configured threshold is crossed, the necessary information is forwarded from the collection station to any interested management stations, so that the end-user at a management console is informed. The set of objects for which topology and status information is forwarded can be controlled via filtering.[3]

---

1. Only NNM Enterprise nodes (unlimited license) can receive information from collection stations.
2. See "Management Consoles" on page 24.
3. See "Use of Scalability Features in NNM Deployment" on page 89 for introductory information, and "Filters" on page 37 for more details about filtering.

Management and collection stations alike have all components of the HP OpenView NNM software running on them. The only difference is that a collection station has been designated and configured to serve one role, and a management station has been designated and configured to serve another.

Stated another way, every NNM station (regardless of operating system or license limit) is inherently a management station, but it must be configured to use the management resources of a remote collection station. Likewise, every NNM station is *also* inherently a collection station, but it must be configured to provide its data to a remote management station.

In Network Node Manager, a computer acting as a collection station is generally also a management station in its own right, with local users performing network monitoring and management, either independently or in cooperation with the users at a remote management station.

This is illustrated in Figure 1-1. In that illustration, the operator at Management Console Y can see only the nodes directly managed by NNM Station C. On the other hand, the operator at Management Console X can (depending on how the collection stations are configured) see all the objects in the entire scope of management for NNM Station A.

NNM Station View

The NNM Station view is useful in a distributed management environment. It shows you a graphical representation of the collection stations and management stations in your topology. You can use this view to troubleshoot communications between collection stations and management stations. See "Identifying Collection Station Communication Problems" on page 145 for detailed information.

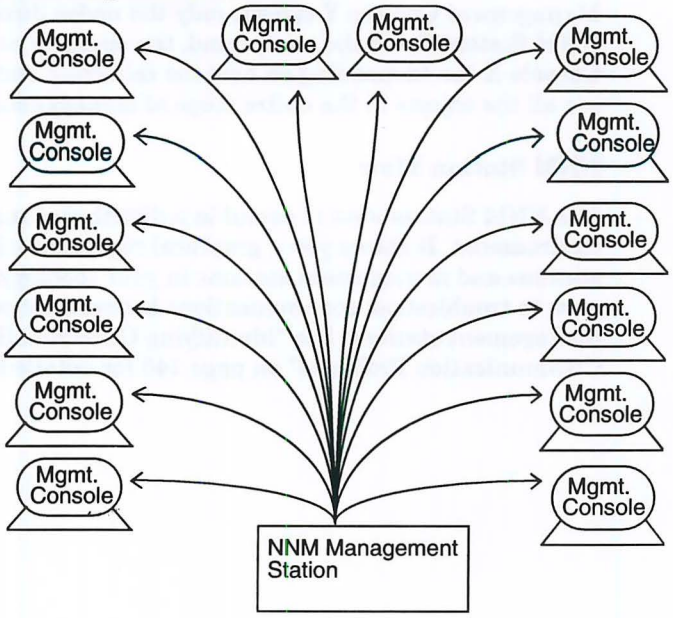
RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 03427
3740
Doc:

Management Consoles

One of the main problems associated with managing large networks is providing access to enough operators to handle all the objects in the map.

With HP OpenView Network Node Manager, you can have many operators simultaneously monitoring your network, as shown in Figure 1-2, operating from the same topology database and sharing common discovery and monitoring processes at the management station. Operators can share one map, or have individual maps. The limit on how many again depends on the size of your environment and the resources available to the management solution. For the most current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide*, available at `http://openview.hp.com/`.

Figure 1-2 Multiple Management Consoles



Consoles run on UNIX[4] or Windows[5] operating systems work with management stations on a UNIX system. These management consoles communicate with the UNIX system management station via NFS and socket connections on a LAN link. Management stations on the Windows operating system only support consoles run on Windows, not consoles run on UNIX. This is because a management station on a Windows operating system uses Windows file sharing, not NFS.

Web browsers using Network Presenter may reside on any system, including the same system as a management console. However, the web server must reside on a full management station, not a console.

4. In this manual, the term UNIX, when used without other qualifications, refers to the supported UNIX operating systems, as described in the Release Notes.
5. in this manual, the term Windows, when used without other qualifications, refers to the supported Windows operating systems, as described in the Release Notes.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0343
3740
Doc:

On-Demand Submaps

One of the potential problems with having maps that contain thousands of nodes involves the use of available memory.

The `ipmap` application[6] typically creates a hierarchy of several levels of submaps (root, Internet, segment, node). An interesting and important point is that many of these submaps are rarely, if ever, visited by an operator.

Imagine if NNM kept every submap in the map in memory at all times. In a large map, with literally thousands of submaps, this approach would create a substantial requirement for memory.

However, NNM makes it possible to specify that only *some* of the submaps be kept persistently in memory; any *other* submap is created if and only if a user requests it. This means that for a management station with a given amount of memory, you can manage maps with many more submaps containing many more objects.

The main benefit of the on-demand submap feature is a dramatic improvement in performance, especially during synchronization. Meanwhile, the features and functionality of NNM are essentially identical whether or not on-demand submaps are enabled. Whenever you double-click on an explodable object in `ipmap`, the submap opens promptly (though submaps with many objects may take several seconds to open). Furthermore, all features of NNM, including "find" and IP status propagation, work as usual.

Some applications that were created before this feature was part of NNM may not be compatible with the on-demand submap feature. They may expect certain objects to be available in memory at all times. In this case, you can use **persistence filtering** to make those objects persistent.[7] Persistence filtering provides per-object exceptions to the on-demand feature, so that certain objects and their submaps are always present in memory even if on-demand submaps are enabled.

6. See *Managing Your Network with HP OpenView Network Node Manager* for information about this and other key NNM processes.
7. See "Persistence Filtering" on page 68 for details.

Distributed Threshold Monitoring and Event Forwarding

In an NNM distributed environment, it is necessary that operators at the management console be aware of critical events wherever they occur. This is commonly called "management by exception." For this reason, NNM has the ability to forward events, typically from collection stations to management stations.

Using the graphical `Event Configuration` window, you can configure any event, on a case-by-case basis, to be forwarded to any or all of the following:

- All managers currently using the NNM station as a collection station.
- Particular hosts, identified by hostname or IP address.
- Hosts listed (by hostname or IP address) in a specific file.

All configurable events, including threshold events, can be configured for forwarding. Internal NNM events are automatically forwarded to management stations as needed.

When defining new events, we recommend that you use multiple varbinds with individual pieces of data rather than using a full string. This allows the receiving machine to specify the formatting. Refer to the reference page in NNM online help (or the UNIX system manpage) for *trapd.conf* more information.

General Events

You can forward any or all events from collection stations to management stations. This is most useful when a collection station receives little or no local attention, or when you have applications that issue events which you want to have forwarded to the management station.

For example, suppose you have a collection station that monitors an agent that generates an event called `FuseIsLit`. At the collection station, you can configure that event to be forwarded to the management station, and thereby alert the operator that the device is not functioning properly.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0344
Doc: 3740

Threshold Events

Threshold events give you a way to be notified of traffic patterns that are outside normal expectations. For example, you could set a threshold to monitor disk utilization on a server. If the amount of free disk falls below the threshold you set, NNM can notify an operator, or take other predetermined actions (such as mailing a message). Threshold events help operators detect and isolate problems as they arise, before users experience difficulty.

In the context of a distributed network management solution, the ability to forward threshold events means that the management station does not itself have to perform data-collection on all the objects that need thresholds monitored. That effort, and the associated network traffic, is delegated to the various collection stations that the manager uses.

Trend Data Collection in a Distributed NNM Solution

Some users may be interested in having trend data collected at remote locations and forwarded back to a central point, such as an NNM management station, for trend analysis.

Distributed data collection doesn't reduce the load on a management station if the data is sent back to the management station in real time. Therefore, in NNM the remote station stores any trend data in its own database. Data can then be transferred to a relational database if that is available.[8]

NNM does not provide a way to automatically synchronize data back to the management station. It does, however, offer some basic tools that you can use to create custom solutions. For example, you can transfer NNM's data files from the collection stations to the management station (via FTP or a similar utility) during off-peak periods. Then you can use NNM's data-merging tool (see the *ovcoltosql* reference page in NNM online help (or the UNIX system manpage)) to merge the data into an SQL database. Then you can use database tools to create reports on the data.

8. See *Reporting and Data Analysis with HP OpenView Network Node Manager* for information on supported database.

Large-Map Viewing Support

When a submap contains hundreds of nodes, the symbols and connections get smaller, and it becomes difficult to make sense of the graphical picture. Also, changes in status are not as noticeable.

HP OpenView Network Node Manager has two features that make it easy to use maps that contain hundreds, even thousands, of nodes:

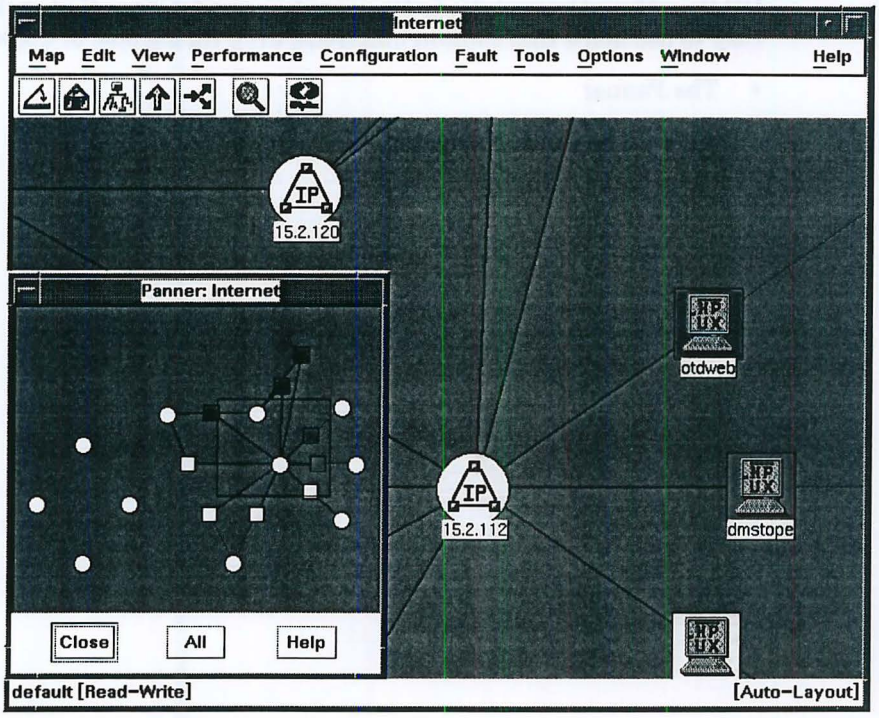
- The Panner
- The Quick Navigator

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0345
3740
Doc:

The Panner

The panner, shown in Figure 1-3, provides a way to zoom in on regions of a submap, and drag the zoomed region around. See *Managing Your Network with HP OpenView Network Node Manager*, or NNM's online help, for details.

Figure 1-3 The Panner



The Quick Navigator

The Quick Navigator is a special window that you can customize easily for quick access to your most frequently visited submaps. Your tool bar has a Quick Navigator button, which is described in the online help.

Each operator can customize their own Quick Navigator window by following the simple directions in the online help.

2 The Scalable Architecture of Network Node Manager

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0346
Doc: 3740 . 0

This chapter contains more detailed information about the distribution and scalability features of HP OpenView Network Node Manager (NNM). It includes diagrams and descriptions of the major elements of the distributed, scalable NNM architecture, and shows how data moves through the system.

NOTE

The information in this chapter is not introductory; readers are assumed to have read the previous chapter. Readers are also assumed to be conversant with NNM's key features for network monitoring, data collection, event handling, and so on. This includes a functional understanding of some key services (background processes on UNIX systems) in non-distributed NNM, including `ovw`, `ipmap`, `snmpCollect`, `ovtopmd`, and `netmon`. See *Managing Your Network with HP OpenView Network Node Manager* for details about the key services in Network Node Manager.

Later chapters contain guidelines on how to deploy NNM effectively in your organization, and specific configuration procedures to use with the scaling and distribution features of NNM.

The Distribution Model for Network Node Manager

Figure 2-1 illustrates the key components of the distribution scheme implemented by NNM. This diagram is fairly complex, and much of the remainder of this chapter is devoted to explaining many of the concepts it illustrates.

The diagram shows several components that can, and often do, run on different systems. These include full NNM management stations, NNM 250 management stations, NNM stations in the role of collection stations, and management consoles. These components can be run in any combination of supported operating systems (except for management consoles: Windows operating system servers can only serve Windows operating system clients).

NOTE The Windows operating system workstation provides status and topology information on IP and IPX devices. The IPX information exported by the Windows operating system collection station is passed to the UNIX system management station, thus providing a graphical representation of the IPX network topology and status of the individual devices.

In Figure 2-1, stations with no local management console are labeled as collection stations; stations that do have a local management console are labeled as management stations.

NOTE The labelling of management and collection stations in Figure 2-1 is for illustrative purposes only; most (if not all) collection stations also serve as management stations. See "About Management Stations and Collection Stations" on page 22.

Again, whether a particular system is a management station or collection station may be a matter of whose point of view one has at the moment. From the point of view of an operator at Management Console

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0347
3740
Doc:

1, it appears that NNM Station C is a collection station (just like NNM Station D). But from the point of view of an operator at Management Console 4, NNM Station C is the management station he is using.

Each management station can support approximately 15 management consoles via a LAN connection. The management consoles run the per-operator services, freeing up resources on the management station. A later section of this chapter covers this in more detail.[1] As shown in Figure 2-1 at NNM station A, it is still possible to run the per-operator services on the management station, routing the display to an X terminal, or, for NNM on a Windows operating system, a Windows operating system console connected to a Windows operating system collection station.[2]

The number of devices that a full NNM management station can manage in a distributed configuration varies with several different factors:

- The management station's resources (CPU, memory, and disk storage)
- Network performance
- Status and discovery polling intervals
- The level of data collection and threshold monitoring you have configured
- The number of collection stations being managed
- The number of nodes being managed by each collection station

For more information on selecting and sizing the correct computer system for your NNM management station, see the latest version of the *NNM Performance and Configuration Guide*.

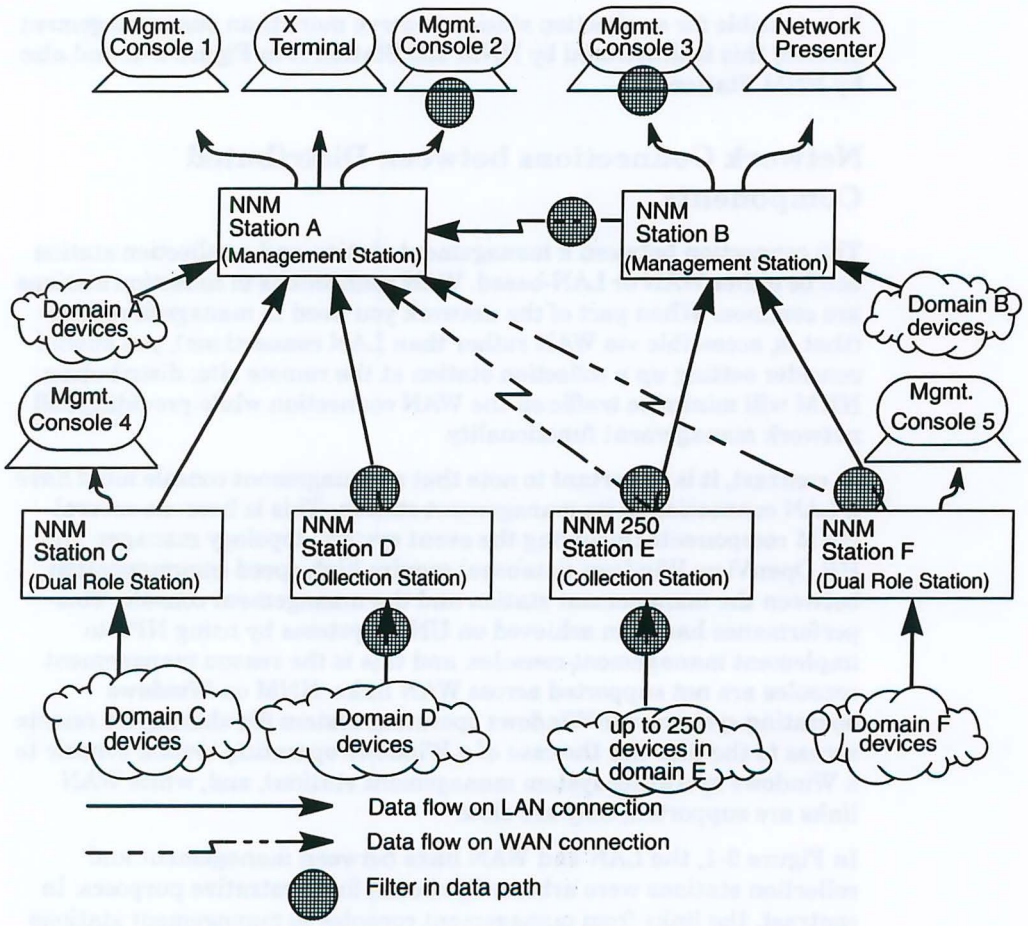
To attain your desired IP monitoring response times, you need to maximize the management station resources and set polling intervals to the maximums you can tolerate.

The only differences between a full NNM management station and an NNM 250 management station are that the NNM 250 management stations can manage only up to 250 nodes per license and cannot manage collection stations.

---

1. See "Management Consoles" on page 70
2. See also "Management Consoles and X-Terminals" on page 73

Figure 2-1 The Distribution Model for Network Node Manager



With NNM, it is also possible to obtain management information from one or more NNM stations acting as collection stations. In Figure 2-1, most of the NNM stations (Stations B, C, D, E, and F) are operating in the role of collection stations.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0348
3740
Doc:

Stations C and F illustrate how an NNM station can have the role of a management station (possibly making use of collection stations), a collection station (serving one or more management stations), or both roles at once.[3]

It is possible for a collection station to serve more than one management station; this is illustrated by NNM 250 Station E in Figure 2-1, and also by NNM Station F.

Network Connections between Distributed Components

The connection between a management station and a collection station can be either WAN or LAN-based. WAN connections to collection stations are common. When part of the network you need to manage is remote (that is, accessible via WAN rather than LAN connections), you should consider setting up a collection station at the remote site; distributing NNM will minimize traffic on the WAN connection while providing full network management functionality.

In contrast, it is important to note that a management console must have a LAN connection to its management station. This is because several NNM components (including the event system, topology manager, and HP OpenView Windows database) require high speed communication between the management station and the management console. This performance has been achieved on UNIX systems by using NFS to implement management consoles, and this is the reason management consoles are not supported across WAN links. NNM on Windows operating systems use Windows operating system file sharing for remote access to the files (for the case of a Windows operating system console to a Windows operating system management station), and, while WAN links are supported, they are slow.

In Figure 2-1, the LAN and WAN links between management and collection stations were arbitrarily chosen for illustrative purposes. In contrast, the links from management consoles to management stations are necessarily LAN connections.

3. See "About Management Stations and Collection Stations" on page 22.

Filters

The function of most filters is to select network management data that is of sufficient value to be kept, and to eliminate other data.[4] Data that is useful at one point (say, a site management station) can be filtered out before it gets sent to another (say, regional management station) where it is unneeded.

NNM uses two basic types of filters:

- A **data-stream filter** acts as a sieve through which objects flow. This type of filter contains criteria that permit some objects to proceed, and blocks other objects. Downstream from a data-stream filter, the data stream includes only those objects that the filter passed; other objects are blocked, and thus eliminated from the data at the point of the filter.

  Note that once an object has passed a data-stream filter, later changes to the filter have no effect on it. It remains in the data stream.

- A **set-defining filter** is applied to a pool of candidate objects, and determines which objects belong in the final set based on the criteria contained in the filter. Before a new object can be added to the set, it is tested by the set-defining filter to determine if it is a valid member or not.

  If a set-defining filter is changed, all candidate objects are reevaluated to determine which ones belong in the new set and which do not. Then the set is reconstituted out of valid members.

The difference may seem abstract at first. As an analogy, you can compare a data-stream filter to a wire-mesh sieve, of the kind used to sort stones. Once a large stone has passed through the sieve, it is in the sorted pile beneath regardless of whether you later switch to a finer mesh in the sieve.

Imagine, on the other hand, that your sieve behaved like a set-defining filter. In that case, changing to a finer mesh in the sieve would cause all the source material to be refiltered, yielding a sorted pile of uniformly smaller stones.

4. See "Persistence Filtering" on page 68 for an important exception.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0349
3740
Doc:

In either case, remember that a filter specifies or describes the objects you want it to pass, *not* the objects you want it to reject. When the filter is applied, it passes the selected objects through, eliminating the rest from the data stream. As a user, you can apply filters only to object data; however, applications can filter events also.[5]

Filtering is based on the information contained in a subset of the fields of the object database (ovwdb).[6] These fields are candidates to be all or part of the criteria by which objects are assessed in a filter.

Filters can eliminate unnecessary data at different points in the system:

- Discovery filtering at any NNM station.
- Exported topology filtering at the collection station.
- Map filtering at the management station.
- Failover filtering on the management station.

Table 2-1, Comparing Types of Filters, compares the types of filters. See "Filter File Example" on page 189 for more information.

Table 2-1 Comparing Types of Filters

Filter Type	Apply on Incoming Data	Reevaluate If Filter Changes	Purpose	Applied So Data Is	Reference
Discovery	X		Limit scope of objects added to database.	Excluded	page 40
Topology	X	X	Limit information forwarded from collection station to management station.	Excluded	page 41

5. Interested application developers should see the *HP OpenView Integration Series: SNMP Developer's Guide*.
6. See "Filterable Objects and Attributes" on page 181 for specifics.

Table 2-1 Comparing Types of Filters (Continued)

Filter Type	Apply on Incoming Data	Reevaluate If Filter Changes	Purpose	Applied So Data Is	Reference
Map	X	X	Show only items of interest to operator on map.	Excluded	page 42
Persistence	X	X	Disable on-demand submaps for third party applications.	Included	page 68
Failover	X	X	Limit nodes polled by management station when collection station fails.	Included	page 52
Important Nodes	X	X	List unreachable important nodes as primary alarms in the Alarm Browser rather than children of a connector down event.	Included	*Managing Your Network with HP OpenView Network Node Manager*
DHCP Range	X		Identify DHCP (shared or floating) IP addresses	Included	*Managing Your Network with HP OpenView Network Node Manager*

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0350
3740
Doc:

Discovery Filtering

Discovery filters specify which devices an NNM station is actively discovering and monitoring. The purpose of discovery filtering is to reduce the discovery and monitoring effort of the station. Different stations have independent (though possibly identical) discovery filters.

Discovery filtering limits the scope of objects that `netmon` adds to the collection station topology database. To unmanage objects and limit the set of nodes that are polled at all, refer to *Managing Your Network with HP OpenView Network Node Manager*. The filter may be set to pass, for example:[6]

- Gateways.
- Bridges, routers, and hubs.
- All devices.
- Nodes based on their `sysObjectID`.
- Objects inside or outside of a particular range of IP addresses.

By default, Segments and Networks pass the discovery filter.

Discovery filtering is achieved by configuring the `netmon` service[7]; the filter is then applied to all newly discovered objects. Objects that are rejected by the discovery filter never appear in any topology or object database.

Discovery filters are data-stream filters; changes to a discovery filter affect new data *only*. All objects that previously passed the filter remain in the data stream, regardless of whether they would currently pass or not, and polling is still done on all previously discovered objects whether or not they would now pass the filter. You can, however, use the `ovtopofix` command to change the set of previously discovered objects.[8]

---

7. See "Configuring a Discovery Filter" on page 128, for details, *netmon* and *xnmpolling* reference pages in NNM online help (or the manpages on UNIX systems), the NNM online help, and "Distributed Services Architecture" on page 48.
8. See the *ovtopofix* reference page in NNM online help (or the UNIX system manpage) for details.

Implement any discovery filtering on an NNM station before you begin using it as a collection station; this will improve overall performance, by reducing the amount of synchronization effort.

Topology Filtering

Topology filters specify which topology data gets forwarded to a management station. The result is less management traffic on the network and lower data storage requirements at the management station. By default, the topology filter does not pass Networks and Segments.

A topology filter at a collection station defines the subset of topology data that management stations can see. The idea is to have the topology filter at the collection station pass information about only those objects in which the manager is interested. Data about objects outside the manager's interest doesn't clog up the link to the management station.

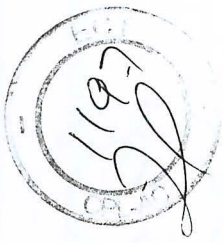
Objects rejected by a topology filter remain in the collection station's topology database. They are not, however, provided to a higher-level management station. Each collection station has only one topology filter in place. Note that this means the topology filter of a collection station must meet the needs of all management stations.Through topology filtering, you can choose to provide the following kinds of topology data to interested managers (many other choices exist):[9]

- All topology data, by using no filter at all.
- Nodes with (or specifically without) a certain `sysObjectID`.
- Objects inside or outside of a particular range of IP addresses.
- Nodes from a particular vendor.
- Objects with particular physical address.
- All token ring segments.

Topology filtering is achieved by configuring the `ovtopmd` service.[10] You should test topology filters at the collection station before the station goes into service.[11]

9. See "Filterable Objects and Attributes" on page 181 for specifics.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0359
3740
Doc:



Topology filters are, technically, data-stream filters. However, in effect, any change to a topology filter affects new and old data *alike*. When a topology filter is changed, the topology database of the management station is resynchronized with the filtered collection station topology database. Some objects may be deleted from the management station topology (if they do not pass the new topology filter), and some objects may be added (if they were previously rejected, but now pass the topology filter). As a result, the database of the management station ends up reflecting the topology being passed by the new topology filter, so the effect is that of a set-defining filter.

NOTE Topology filters do not affect the events that are passed from collection stations to management stations. This means that any events that you have configured to be forwarded are in fact forwarded from the collection station to the management stations, regardless of whether the objects to which the events refer pass the topology filter or not. Listing particular event sources in the event configuration at the management station can reduce the likelihood of operator confusion.

Map Filtering

The purpose of map filtering is to give the operator visibility of only those objects in which he or she has interest. By default, Networks and Segments do not pass the map filter.

Map filtering occurs on a per-map basis, not a per-display basis. All operators who use a particular map have the same filtered view. Additional maps can be created and separately filtered for specific purposes.

10. See "Distributed Internet Discovery and Monitoring" on page 46, Chapter 4, Procedures for Scaling NNM, and the *ovtopmd* reference page in NNM online help (or the UNIX system manpage), for further details.
11. See the reference page in NNM online help (or the UNIX system manpage) for *ovtopodump*, especially the `-f` option, for instructions on testing topology filters.

Objects that are rejected by a map filter remain in the management station's topology database, and are still subject to status polling. Events from these objects pass through and are visible in the event subsystem, but this can be changed to show only events from objects on the operator's current map.[12]

Like the previously discussed types of filtering, map filtering can be configured so that (regardless of how much other topology data exists in the database) the map seen by the operator displays only the objects of interest to that operator. In general, this means objects that match some combination of attributes and attribute values; among the many choices, this can include:[13]

- All objects, by using no filter at all.
- Connectors, networks, and segments only.
- Nodes with specific `sysObjectIDs`.
- Bridges, hubs, and their segments.
- Objects inside or outside of a particular range of IP addresses.
- Only nodes that support SNMP.

Map filtering is generally configured in the NNM interface.[14]

Map filters are set-defining filters. When you change a map filter, all the objects currently in the map are reevaluated to see if they pass the new filter; new objects must also pass the filter before being added to the map.

Defining New Filters

All filters, discovery, topology, map, and persistence, are configured by creating a text file in which you use a special filter definition language to define filters that pass and reject objects in the ways you want.[15]

---

12. See the *xnmevents* reference page for details on the "filter by map" feature.
13. See "Filterable Objects and Attributes" on page 181 for specifics.
14. See the online help and Chapter 4, Procedures for Scaling NNM, for further details.
15. See Appendix A, The Filter Definition Language, for details on the syntax, semantics, and mechanics of filter definition.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0352
Doc: 3740

NOTE While you can create multiple filter definition files, you can use only one at any given time. Hence, only the filters defined in the currently in-use filter definition file are available.

You can give each filter you define a sensible name. For example, a map filter that would pass only routers might be named `Routers`.

Effective use of filtering lets you monitor a broader domain with a given management station. For example, suppose you have a site with 5000 workstations and PCs connected by 300 hubs and routers.

If you are only interested in the connecting devices, you might be able to use a single collection station with filters configured to discover and monitor only the 300 hubs and routers. Without such filtering, monitoring all 5300 nodes might require three or more collection stations to maintain equivalent performance.

NOTE As a rule, the sooner you can filter out a particular object, the better overall performance of the network management solution will be. For example, by using discovery filtering to discover and monitor exactly and only those objects of interest, you can dramatically reduce the amount of data that all other parts of the system have to handle. The next-best type of filter, to reduce the data load on the distributed management system, is a topology filter. While a local collection station may need broader discovery for its own management domain, the management stations that use the collection station frequently do not require a full copy of the topology at the collection station; topology filtering is the way to prevent unnecessary data from being exported to the management station.

Filter Utilities

NNM provides the utilities shown in Table 2-2, Filter Utilities, to help you build filters that do what you want and expect.

Table 2-2 Filter Utilities

Utility Name	Description
On Windows operating systems: *install_dir*\bin\ovfiltercheck On UNIX systems: $OV_BIN/ovfiltercheck	Provides syntax validation for a filter file. Can also be used to check individual Set, Filter, and Filter-Expression statements for correct syntax.
On Windows operating systems: *install_dir*\bin\ovfiltertest On UNIX systems: $OV_BIN/ovfiltertest	Tests all or part of a specific object database (ovwdb) against a filter. Objects that pass the filter are reported to the output. Use the -c option to specify a collection station to determine which objects the management station polls on failover.
On Windows operating systems: *install_dir*\bin\ovtopodump On UNIX systems: $OV_BIN/ovtopodump	Use the -f option to compare a filter against the current topology database.

See the reference pages in NNM's online help (or the UNIX system manpages) for these commands to obtain details on their syntax and use.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0353
3740
Doc:

Distributed Internet Discovery and Monitoring

Distributed Internet Discovery and Monitoring is one of NNM's keys to providing a scalable network management solution. The purpose of this section is to give you a picture of exactly which parts of NNM are distributed, and how data flows through the distributed solution. With this knowledge, you will be able to better understand what is occurring as you deploy NNM.

About Collection Domains

Within the NNM model of distribution outlined in "The Distribution Model for Network Node Manager" on page 33, it is useful to distinguish these two sets of objects:

Management domain

> This is the set of all objects that are of interest to the user. In Figure 2-1, the management domain of the operator at Management Console 1 contains all the objects in the whole network (except objects that are removed by intervening filters). On the other hand, the management domain of the operator at Management Console 6 consists of only the objects directly monitored by Station F; no other objects are visible from that station.
>
> Keep in mind that the management domain is an attribute of the management station, not the operator. Different operators might deal with different subsets of the management domain, based on map definitions and map filters.

Collection domain

> This is the set of objects that are directly discovered and monitored by an NNM station. This typically includes any objects on which data collection (for trends or thresholds) is occurring.

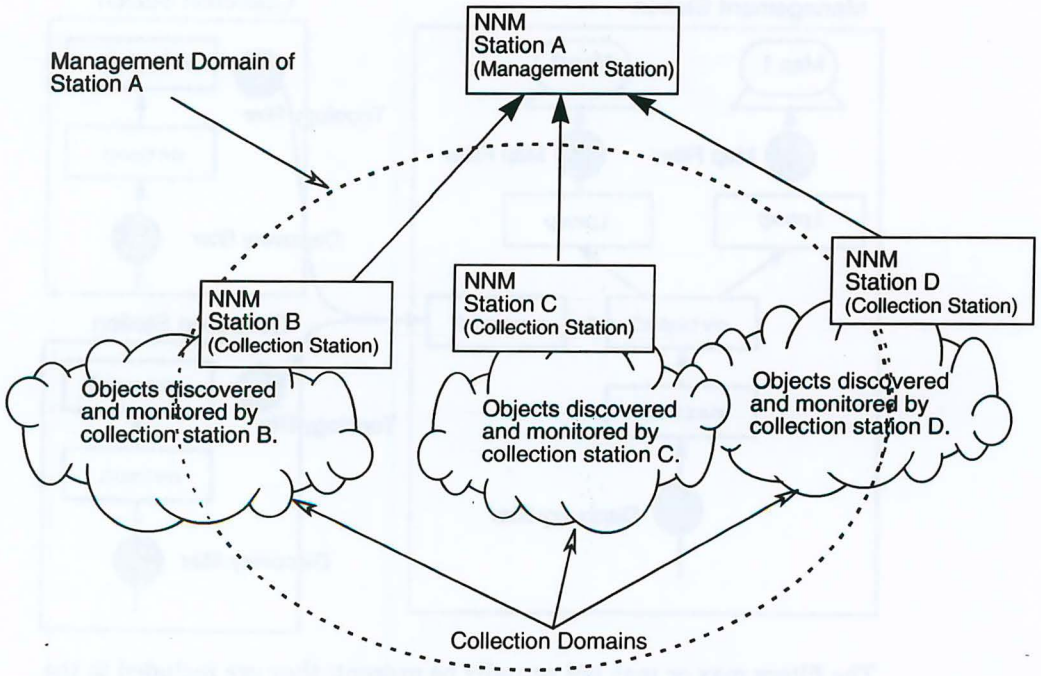
At a high level, these definitions can be depicted as in Figure 2-2.

In the diagram, the management domain of station A does not include all the objects in the collection domains of all the collection stations. Remember, the collection stations are probably management stations too. For each of these, the management domain is coincident with the collection domain.

However, the administrator of the overall network, working from Management Station A, is quite possibly very selective about which objects within the various collection domains of the collection stations are of interest to operators at the management station.

You can use filtering to select exactly those objects, and thus constrain your management domain to those objects that make the most sense for you.

Figure 2-2 Management and Collection Domains



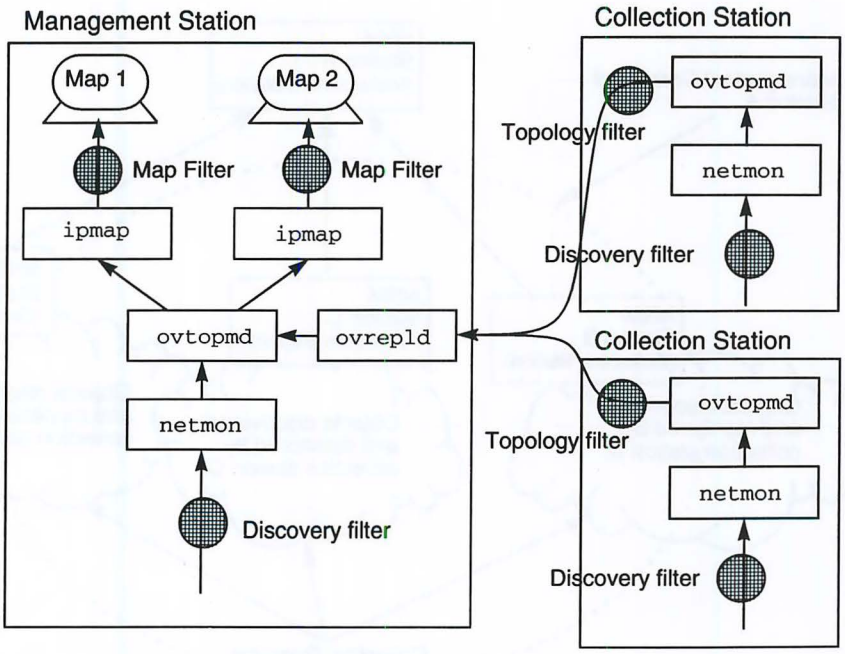
RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0354
3740
Doc:

Distributed Services Architecture

Network Node Manager relies on the complex interplay of several different services (background processes on UNIX systems) to provide the level of functionality and performance you need. In making NNM a scalable solution, several of these services appear in locations remote from the management station.

Figure 2-3 is a diagram of the key services involved in a distributed deployment of NNM. Of these, the `ovrepld` service is central to the distribution of network topology; the others have other, stand-alone functionality. The `ovrepld` service is the "replicator" of the topology, responsible for integrating topology data from multiple collection stations into the management station's topology database.

Figure 2-3 Service Components in Distributed Internet Monitoring



The filters may or may not actually be present; they are included in the illustration at all the points where they would potentially exist. Note also that when a collection station is also fulfilling a local management

role, it runs local ipmap and ovw services too. And finally, understand that in the interest of simplicity, Figure 2-3 omits the role of the event system, which is illustrated in Figure 2-4.

How Distributed Internet Discovery and Monitoring Works

Figure 2-3, shows two collection stations working on behalf of the management station. Each collection station has its own collection domain, which is the responsibility of the local netmon service. You can set discovery filters to minimize unnecessary discovery and monitoring.

Having a station take the role of a collection station, or make use of collection stations, requires several other configuration steps. "Configuration Concepts" on page 56 introduces these configurations steps, and "Configuring Collection Stations" on page 133 gives complete details.

After the stations have been configured correctly, start the collection station as usual. The netmon service begins IP and level-2 discovery, and (along with the ovtopmd service) populates the local topology database.[16] It takes time for this process to finish, but to minimize management traffic on the network, you should allow NNM to finish (or nearly finish) discovery before you begin to use it as a collection station. The Performance:Network Polling Statistics tool can help you determine when the collection station has reached a steady state.[17]

After waiting for the collection station to build its topology database and reach a steady state, the management station administrator uses the xnmtopoconf command to begin using the discovery and monitoring services of the collection station.[18]

At this point, the management station obtains access to the topology data at the collection station. It requests the collection station to send the objects in the collection station's topology database across the network. If the collection station has a topology filter configured, only those objects that pass the filter are provided to the management station.

16. See *Managing Your Network with HP OpenView Network Node Manager* for details about these and other services (background processes on UNIX systems) in Network Node Manager.
17. See the online help about this tool for more information about the procedure.
18. See the reference page in NNM online help (or the UNIX system manpage) for *xnmtopoconf*.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0354
3740
Doc:

Topology data that is not derived from a local `netmon` service is not sent to the management station. This precludes the possibility of cycles (where station "A" discovers and reports "B," which discovers and reports "C," which again discovers and reports "A," ...). It also precludes indirect multiple-level hierarchical management.[19]

The `ovrepld` service on the management station replicates the topology data from the collection station in the local topology database. "Replication" does not imply a 100% mirroring of the collection station topology database at the management station. Remember that topology filtering at the collection station means that some of the objects present in the collection station's topology database may *not* be present at the management station. The topology data that *does* pass the topology filter is kept synchronized between the collection station and the management station.

NOTE The `ovrepld` service provides synchronization of the topology data *only*. It does not affect any other databases (such as `ovwdb`, `snmpCollect`, or `ovw`).

Once the topology merging is done, the `ovtopmd` service treats the new objects just like objects obtained from the local `netmon` service.

After the synchronization phase is complete, only *changes* in status and topology get sent to the management station. The `ovrepld` service updates the topology database of the management station to reflect the changes.

High Availability Management Information

One way to ensure your network management information is always available is to run your management stations on HP Service Guard clusters. If the primary processor goes down, processing automatically and transparently rolls over to another processor in the cluster. Configure Service Guard NNM stations using the `ov.conf` configuration file parameter `HOSTNAME=`. See the *ov.conf* reference page in NNM online help (or the UNIX system manpage) for more information.

19. See "Hierarchical Management" on page 98, especially Figure 3-4 and Figure 3-5, for more information on multilevel hierarchical management.

As part of the Service Guard interface, NNM offers `ovwrs` (self-restarting `ovw`). This interface runs `ovw` while monitoring the status of the console server process on the management station. If the connection to the server is lost, the it informs the user and re-establishes its connection to the server. See the reference page in NNM online help (or the UNIX system manpage) for *ovwrs* for more information.

Collection Station Failover

NNM also provides capability to continue data collection when a collection station goes down. The management station's `ovrepld` service performs periodic status checks to verify the status and state of the currently managed collections stations. When a status check fails, the status of the collection station is downgraded one level. The default interval between checks is five minutes (but this can be reconfigured via the `xnmtopoconf` command). Thus, it will take 20 minutes before a "Collection Station Critical" event is generated; an event confirmation popup dialog is presented to the operator. The nodes affected by the failure are left with the status they had at the time the collection station stopped responding.

Collection Station failover enables a management station to take over status polling responsibilities for a collection station which is temporarily unreachable. When the collection station returns to normal, the management station returns to its previous state, delegating discovery and monitoring of those objects to the collection station. This feature is not intended to provide support for collection stations which will be down for a long time or which have been permanently removed from service.

In order to prevent `netmon` from being overloaded, failover only takes over status polling, not the full responsibilities of the collection station. Discovery and SNMP configuration polling are not picked up.

When the collection station returns to normal operation, the management station removes the failed over topology list from its polling queue and resynchronizes with the collection station. The status from the collection station is considered to be current, which means it takes priority and overwrites the status for the objects where were stored in the management station database.

IP and IPX (Windows operating systems) collection stations can failover to a management station. IPX interfaces from a Windows operating system collection station are not polled by a UNIX system management station.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0356
3740
Doc:

You control failover operations through the management station's `Options:Network Polling Configuration:IP` menu selection, "`Status Polling`" tab; or through the `xnmtopoconf` flags "`failover`," "`nofailover`," and "`failoverFilter`." Refer to the reference page in NNM online help (or the UNIX system manpage) for more information.

Failover Filtering

The default operation is for the management station to pick up status polling responsibility for all nodes loaded in the management station's topology from that collection station. However, you can control the load on the management station by providing a failover filter that lists specifically which nodes should be polled. The failover filter behaves like a discovery filter which loads networks and segments, and then filters on nodes and interfaces before the data is given to `netmon`. The interfaces and the node to which they are attached are considered a unit. If one interface on the node passes the filter, then the entire node and all of its interfaces that the collection station polls pass the filter as well. You determine which objects are picked up on failover on a collection station by collection station basis.

Failover Considerations

The management station must have access to the interfaces which are to be picked up in a failover situation. A route needs to exist to the interface to be polled.

The possibility of overloading the management station is a consideration when configuring failover. The devices for which continuous status polling is especially important, such as routers and gateways, are good candidates for inclusion in a failover filter. The management station needs information about connection devices in order to detect secondary failures.

Overlapping Collection Domains

Reexamine Figure 2-2, and notice that sometimes the objects in the collection domain of one collection station are *also* within the collection domain of a different collection station.

For example, in Figure 2-2 the collection domain of Station C overlaps that of Station D, and both serve as collection stations for Station A. Such instances are not uncommon in practice. It is easy to imagine a

router that Stations C and D both care about and monitor. At Station A, that one router will appear in the topology data arriving from both collection stations.

When a management station receives multiple versions of the same object from different collection stations, it uses the rules described in the next section to automatically choose one version as the "primary" version; it then treats all other versions as "secondary."

The station that provides the primary version of an object's data is called the **primary collection station** for the object; any other station that provides information about that object is a **secondary collection station** for the object.

Note that a collection station can be a primary for one object, and a secondary for another object. In other words, the choice of primary vs. secondary is on a per object basis, not a per station basis. Furthermore, a collection station does not know or care whether it is the primary or secondary station for a given object.

Only the primary version of data is displayed in the operator's map. Unless you specifically request information from a secondary version, all topology queries return information from the primary version.

Overlapping collection domains cause redundancy and can therefore waste memory, processing and network resources. In order to reduce the overlap, set the DeleteSecondary mode via `xnmtopoconf` on the management station.

The Selection of Primary and Secondary Collection Stations

NNM uses several rules to decide which of several versions of an object is primary (and by implication, which collection station is the primary collection station). The rules are evaluated in order, and the first rule that distinguishes a primary collection station is applied and the process terminates; remaining rules are ignored.

The rules NNM uses to establish the primary collection station for an object are as follows:

1. If only one station is reporting the object, that station is the primary collection station for the object.
2. If the object is an interface (`isInterface == TRUE`), skip to rule 7.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0357
3740
Doc:

3. If only one station reporting the object is *a.)* managed (meaning currently in active use as a collection station), and *b.)* has noncritical status or has failed over, that station is the primary collection station for the object.
4. If the user has expressed a preferred primary collection station for the object[20], that station is the primary collection station for the object.
5. If only one station reporting the object is managing the object (meaning actively managing it, either by default or via `Edit:Manage/Unmanage Objects`, that station is the primary collection station for the object.
6. If one station reporting the object is a gateway, that station is the primary collection station for the object. (A gateway is a node with multiple interfaces performing IP routing functions.)
7. If the object (A) is completely contained in another object (B), the collection station for the container object (B) is the primary collection station for the object (A). For example, a non-gateway node should have the same primary collection station as the network that contains it.
8. If one of only two stations reporting the object is non-local, the non-local station is the primary collection station for the object.
9. The first station to report the object is the primary collection station for it.

You can express a preferred primary collection station for an object.[21] However, you should be aware that if conditions force NNM to reevaluate the primary collection station, your preference may be temporarily overridden, according to the preceding rules.

---

20. See the *xnmtopoconf* reference page in NNM online help (or the UNIX system manpage), especially the `-preferred` and `-clearPreferred` options.
21. See the *xnmtopoconf* reference page in NNM online help (or the UNIX system manpage).

For example, suppose the preferred primary collection station you selected for an object goes down and you have configured `nofailover`. If a secondary collection station can pick up reporting for that object, that station becomes the primary collection station for the object until the preferred primary station is again available.

If the down primary collection station has failed over to the management station, the management station does not make its local version of the object the primary. Where failed over objects were in overlapping domains with the management station, `netmon` handles the duplicate objects by only polling the device once and updating all of the objects with the status.

A management station will not pick up status polling on secondary objects during failover. There is already a primary collection station still providing information for those objects.

Overlaps with the Collection Domain of the Management Station

In some cases, particularly when an existing large collection domain is partitioned by collection stations, the collection domain of the management station overlaps the collection domain of a collection station. The question then arises, what should be done with the secondary (local) version of information about objects in the overlap?

You have three choices:

1. "`Allow Overlap`", which means that the `netmon` running on the management station should continue polling the node even though a collection station is also polling the node. This would also accept the associated resource consumption caused by duplicate monitoring (potentially over an expensive link) and duplicate information in the topology database.
2. "`Unmanage Secondary`", which unmanages the local version of objects (networks, segments, and nodes) in the overlap region, but keeps them in the database. (The local unmanaged version of the object will not be shown on any maps.) This eliminates the duplicate polling, but still incurs the data storage overhead. If the collection station should fail, the management station can be made the primary collection station to quickly restore management to the affected objects. This will not happen automatically. Refer to "Changing the Primary Collection Station for an Object" on page 151 or to the *xnmtopoconf* reference page in NNM online help (or the UNIX system manpage) for information on configuring failover.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0358
3740
Doc:

3. "`Delete Secondary`" deletes the local version of overlapping objects from the topology database. This eliminates the overhead of both duplicate monitoring and duplicate objects in the database. You then rely on the collection station to provide all information about the objects in the overlap.

   When this is the mode, a local version of any overlapping networks is retained in an unmanaged state. The `netmon` on the management station will not discover nodes that belong to an unmanaged network. If a collection station fails, you will have to delete the collection station, then manage the networks and wait for `netmon` to discover the nodes that have been deleted unless you have failover configured.

The third option is the default behavior of an NNM management station. However, only non-connector nodes are deleted; NNM does not delete networks, segments or routers that overlap with the collection station's collection domain. This maintains visibility to the boundary of the collection domain of the collection station even in the event of collection station failure. The local versions of connector objects are put in the "unmanaged" state. If the normal primary collection station for these objects becomes unavailable, the local versions can become the primary version.

You can choose which behavior you prefer by using `xnmtopoconf`.[22]

Configuration Concepts

For a station to either be, or make use of, a collection station requires additional configuration steps.

This section provides only a brief summary of configuration to acquaint you with the general concepts, and gain a better understanding of what is required when deploying distributed IP discovery and monitoring. Detailed steps for configuring management and collection stations are provided in "Configuring Collection Stations" on page 133.

NOTE

NNM does not provide remote configuration utilities. Therefore, the configuration steps used to set up a collection station have to be made from the collection station itself. You can, of course, use `telnet` to log in

22. See the *xnmtopoconf* reference page in NNM online help (or the UNIX system manpage).

and remotely configure the collection station. Similarly, you could redirect an X display from the collection station back to the management console to do the configuration, but the speed of the display will degrade noticeably when using a wide-area network connection. You may have security issues as well in taking either approach.

Overview of Collection Station Configuration

To set up an NNM station to be used as a collection station, you have to do the following:[23]

- Configure the local collection domain, including any discovery filters desired.
- Configure the exported collection domain, by setting up topology filters.
- Configure SNMP security (get and set community names) in a way that will match the SNMP security configuration on the management station.

Once the above configuration steps are done, you need to restart the platform, via `ovstart`.

About the Remote Managers List As noted earlier, a management station designates and begins to use the services of a collection station by using the `xnmtopoconf` command to begin managing the collection station.

This causes the collection station to add that management station to a list of remote managers that it maintains. The remote managers list keeps up with the changes as management stations come and go.

At various places in the NNM interface, such as the `Event Configuration` window (when you are configuring event forwarding), this list is called the "`%REMOTE_MANAGERS_LIST%`".[24] Forwarding events

23. See "Configuring Collection Stations" on page 133 for more details.
24. See "Configuring Event Forwarding and Correlation" on page 154 for more details.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0359
Doc: 13740

to this list makes system administration much easier, since you are not required to make individual updates whenever DIDM configuration changes.

For example, in Figure 2-1, suppose Station A has been using Station E as a collection station; the list of remote managers that Station E maintains includes Station A.

If Station B now starts using Station E as a collection station, it gets added to Station E's list of remote managers. That list now includes both Station A and Station B.

Overview of Management Station Configuration

To make use of collection stations, a management station needs to be configured as follows:[25]

- The `ovrepld` service must be running (it normally starts with `ovstart`).
- Any nodes on the network that are running NNM are potential collection stations; `xnmtopoconf -print` can help you identify the ones that have been discovered by the local `netmon` service. You have to select which ones you want to use, and manually add in any that have not been discovered locally. Versions of NNM that predate NNM 4.1 can not be collection stations.
- You need to configure SNMP security (get and set community names) using `xnmsnmpconf` in a way that will match the SNMP security configuration on the collection stations.

After this configuration is done, you can use the `xnmtopoconf` command to begin "managing" the collection station. In this context, "manage" means to use the IP discovery and monitoring services of the collection station.

25. See "Configuring for a Specific Collection Station" on page 138 for more details on this procedure.

Distributed Threshold Monitoring and Event Forwarding

The event subsystem for NNM allows forwarding of events (including topology changes, correlated events, and threshold events) from collection stations to management stations.

The services (background processes on UNIX systems) that NNM uses in basic event forwarding are:

- The trap service (`ovtrapd`).
- The postmaster service (`pmd`).

Figure 2-4 illustrates these services, and their relationship to other key NNM files and services.

The `ovtrapd` service is responsible for receiving SNMP traps and inform-requests on port 162 via UDP, the protocol of the SNMP standard. It buffers them, and passes them to the postmaster (pmd) service.

The `ovtrapd` service automatically provides an inform-reply to inbound SNMPv2C inform-requests.

The postmaster service routes the traps it receives from `ovtrapd` to the appropriate subsystem. Moreover, the postmaster service is the central dispatcher that all management applications (both NNM and third-party) use to communicate with each other. It uses the TCP protocol to route events between them so messages are not dropped, even over noisy or congested links.

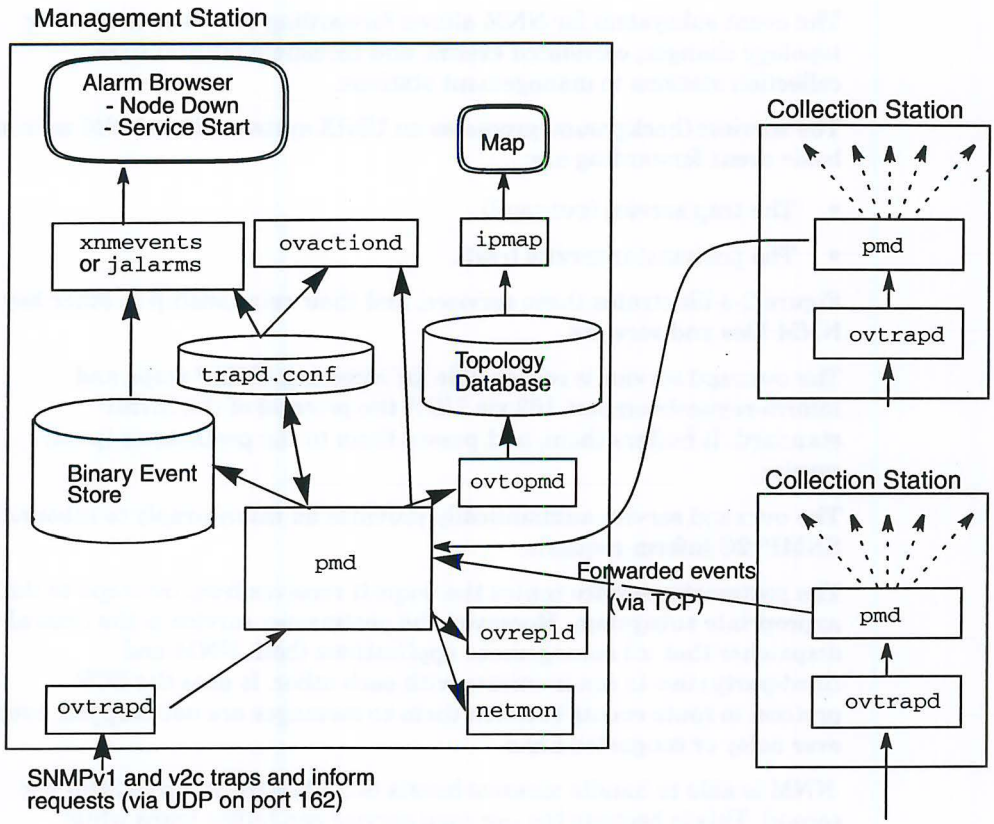
NNM is able to handle massive bursts of SNMP traps, up to 2000 per second. This is because the `ovtrapd` service can buffer traps while forwarding them to the postmaster for routing. This buffering reduces the likelihood that traps in a burst will be dropped.

The `Event Configuration` window supports event forwarding. It also supports an event-identifier naming convention, where SNMP version 1 traps, SNMP version 2C traps, and SNMP version 2C inform requests

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0360
3740
Doc:

use the same naming conventions for event IDs. See the online help and the *trapd.conf* reference page in NNM online help (or the UNIX system manpage) for details.

Figure 2-4 The Basic Event System in NNM



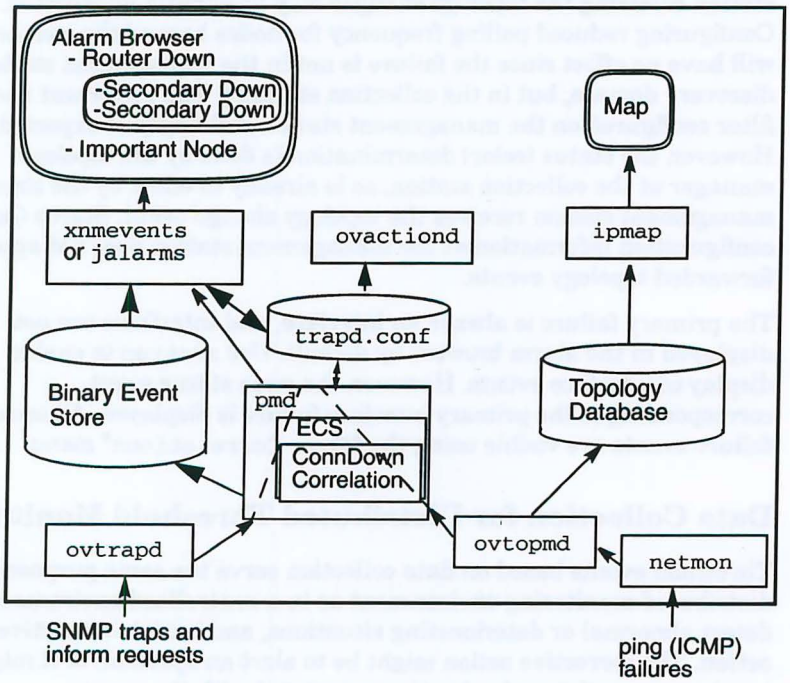
Event Correlation for "Connector Down"

One of NNM's key features is its ability to correlate incoming event information. See *Managing Your Network with HP OpenView Network Node Manager* for a complete description. The most useful correlation

rules for a distributed environment clarify information coming in when a connector (router, gateway, etc.) goes down and all the nodes beyond the connector become unreachable.

Since these events originate from `netmon` polling rather than from SNMP traps coming in through `ovtrapd`, the internal handling and forwarding is somewhat different from basic events. This is shown in Figure 2-5.

Figure 2-5 The Correlated Event System for "Connector Down"



When `netmon` recognizes a ping failure, which in the case of interest happens to be a connector failure, it notifies `ovtopmd` to update the topology database. `ovtopmd` notifies `pmd` that it has done so, and `pmd` runs the event through the Event Correlation System while `ipmap` updates the map. The correlated event then appears with a "children" indicator in the Alarm Browser.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0361
Doc: 3740

In a distributed environment, pmd forwards the topology change for the nodes to the management station. At the management station, the pmd informs ovrepld to update the topology database. When ovtopmd makes that change, it informs pmd of the topology change. pmd then handles that topology change notice just like a local topology change notice, and routes it through the ECS correlation for "Connector Down." Note that the "Connector Down" event itself was not forwarded. The management station automatically derives that event from the topology change notification.

Operation of the "Connector Down" correlation on the management station receiving the topology changes may be slightly unexpected. Configuring reduced polling frequency for nodes beyond the connector will have no effect since the failure is not in the management station's discovery domain, but in the collection station's. The important node filter configured on the management station will apply as expected. However, the status (color) determination is done by the topology manager at the collection station, so is already in effect by the time the management station receives the topology change event. Status (color) configuration information at the management station does not apply to forwarded topology events.

The primary failure is always an interface, and interfaces are not displayed in the alarm browser by default. Use xnmtrap to enable display of interface events. However, the node status event corresponding to the primary interface failure is displayed. All secondary failure events are visible using the "Show Correlations" menu.

Data Collection for Distributed Threshold Monitoring

Threshold events based on data collection serve the same purpose in a distributed monitoring environment as in a centralized environment: to detect abnormal or deteriorating situations, and initiate corrective action. The corrective action might be to alert an operator, or it might be to trigger a predetermined action associated with the event.

A collection station can independently collect data (from the objects that it monitors) for threshold monitoring. When a threshold event is triggered, it can be automatically forwarded to a management station.

At the management station, it doesn't matter whether a threshold event was triggered by local data collection (done at the management station), or forwarded from a collection station. Forwarded threshold events are

automatically consolidated with local threshold events. Whether forwarded or locally triggered, the threshold event looks the same to the management station, and receives the same treatment.

NOTE

Topology filters do not affect the events that are passed from collection stations to management stations. This means that any events that you have configured to be forwarded are in fact forwarded from the collection station to the management stations, regardless of whether the objects to which the events refer pass the topology filter or not. Listing particular event sources in the event configuration at the management station can reduce the likelihood of operator confusion. Also, this note does not apply to events internal to NNM.

See "Configuring Event Forwarding and Correlation" on page 154 for details about configuring event forwarding, including threshold event forwarding.

Remote Thresholds with Remote Actions

For some threshold events on collections stations, you may want to consider creating actions at the collection station. Where this is a reasonable tactic, it has the advantage that the action will be invoked even if contact is lost with the central site.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0362
Fls. Nº
3740
Doc:

On-Demand Submaps

As described in "On-Demand Submaps" on page 26, the reason for enabling the on-demand submap feature is to improve NNM's performance and reduce it's use of memory and disk space. Rather than keep all the submaps in memory (which, for a large map, can require large amounts of memory), you can specify that many of the submaps only be created at the moment you need them.

A **persistent submap** is created and maintained for the life of the map. In contrast, a **transient submap** is created (and removed) only as necessary; that is, "on-demand." Transient submaps are created and maintained by the `ipmap` service, and removed by the `ovw` service.

Figure 2-6, A Typical Hierarchy of Persistent Submaps, and Figure 2-7, A Typical Hierarchy of Transient Submaps, show the difference between persistent submaps and transient submaps.

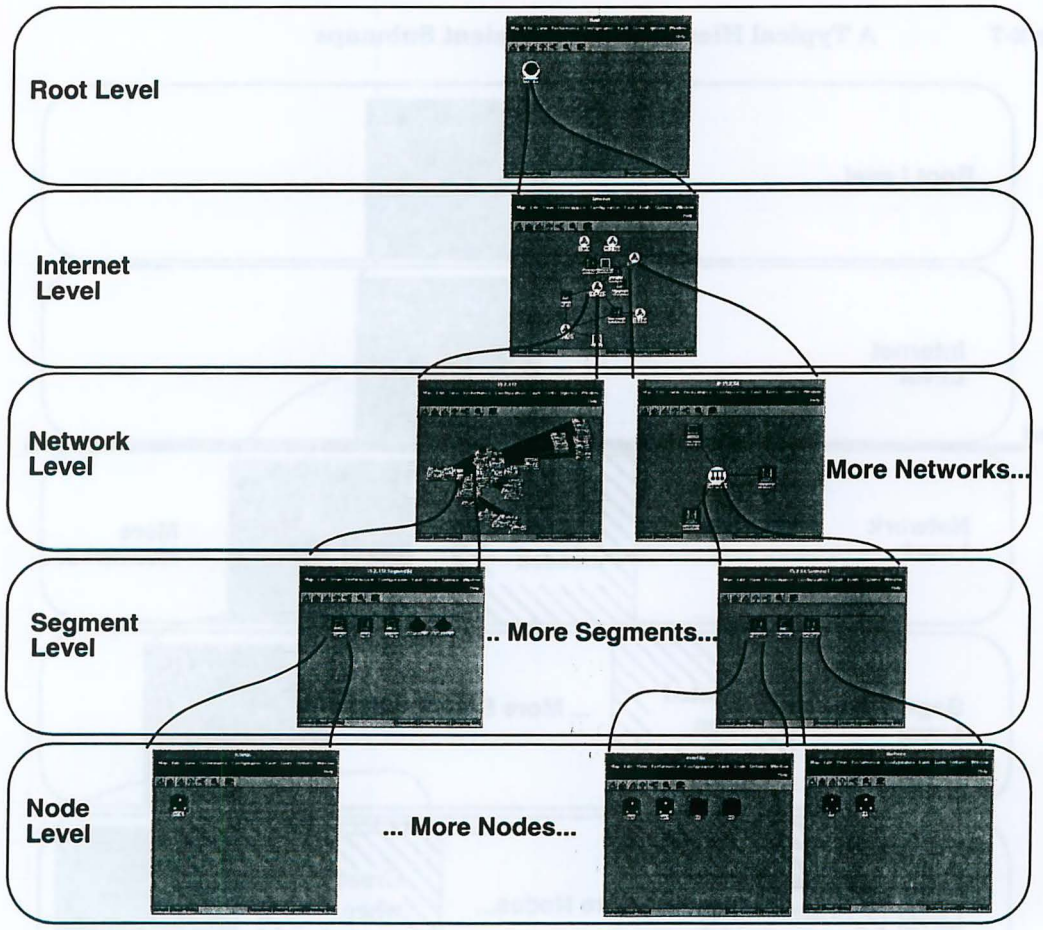
All the submaps in Figure 2-6 are persistent; this is the default when you first install NNM on UNIX systems. On Windows operating system management stations, the default is `Internet Level`. In contrast, in Figure 2-7 only the "Root" and "Internet" submap levels are persistent. Submaps from the "Network" level down are transient submaps. These are created only as they are needed. The `ipmap` service does not allocate memory for them, nor does it maintain topology changes in them. This saves both memory and execution time. Note that status from transient submaps is propagated up in the usual way.

The visible submaps (when on the same levels as the crossed-out ones) are also transient submaps, but the operator has navigated into that part of the submap hierarchy, and so these submaps are currently resident in memory.

You use the `IP Map Configuration` dialog box to set submaps to be persistent down to whatever level of the submap hierarchy you select. On Windows operating systems, the initial configuration for demand level is `Internet Level`.

For example, in Figure 2-7, the level of persistence is set to `Internet Level`, so submaps at and above that level are persistent.

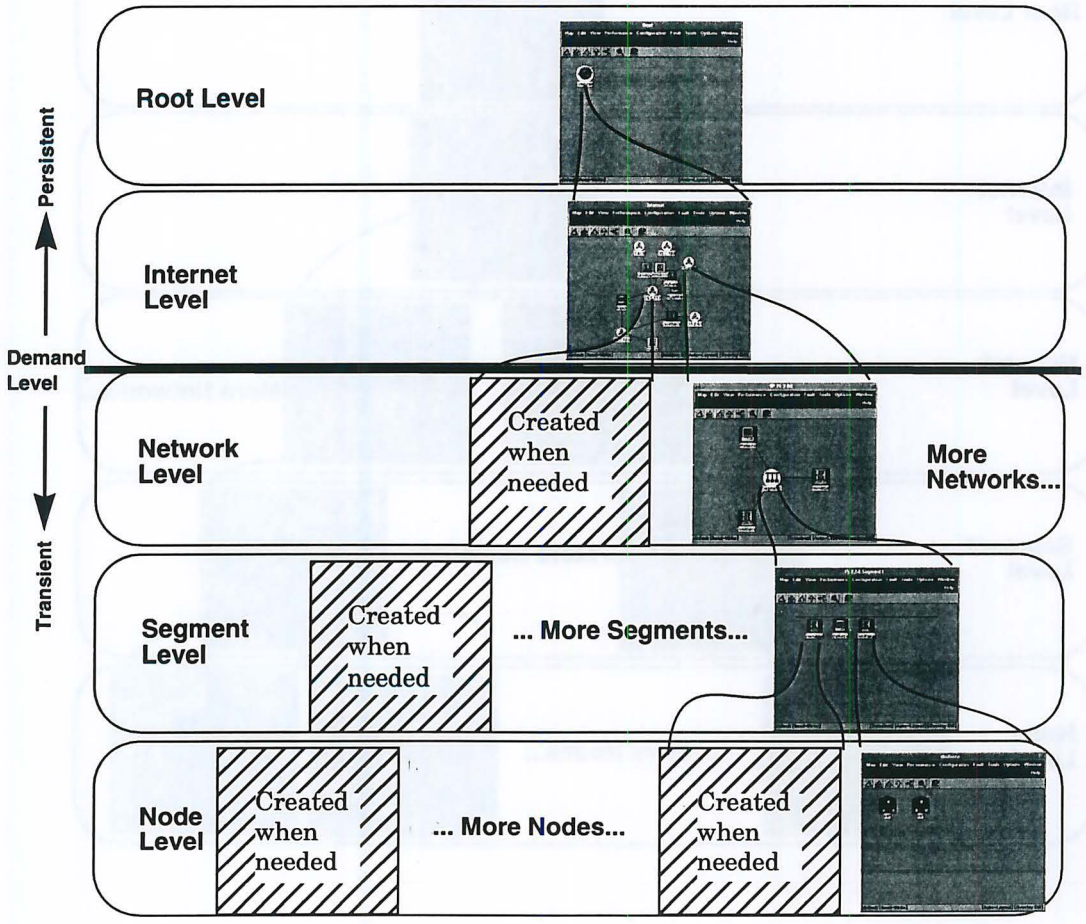
Figure 2-6 A Typical Hierarchy of Persistent Submaps



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0363
3740
Doc:

You can choose to make submaps persistent down to the `Internet Level` (as shown Figure 2-7), `Network Level`, `Segment Level`, or `All Levels` of the submap hierarchy. Submaps below the level you select will be transient. Of course, selecting `All Levels` means no submaps are transient.[26]

Figure 2-7 A Typical Hierarchy of Transient Submaps



26. Also see "Persistence Filtering" on page 68.

Most users of this feature will start with submaps set to be persistent at the `Internet Level` (as in Figure 2-7), and set it to lower levels only to improve submap-opening performance. This is typically necessary only when the higher-level submaps are densely populated.[27]

If you want to reset the on-demand submap feature to its default, use the `IP Map Configuration` dialog box in NNM to set submap persistence to `Unset`. On Windows operating systems, `Unset` sets the persistence level to `Internet Level`. On UNIX systems, `Unset` sets the persistence level to `All Levels`.

With on-demand submaps enabled at any level, most NNM features and operations work as they always have. Locate operations and IP status propagation, in particular, are not limited to what is currently in memory. Both functions work across all submaps, regardless of whether they are persistent or transient.

In cases where a located item is not yet in memory, the necessary submap is created, on-demand, if and when the user opens that submap from the locate dialog box.

Transient Submaps and the Submap List Dialog

The only feature that changes its behavior when the on-demand feature is enabled, is the `Submaps in Map` dialog box. Only submaps that are currently in memory (that is, either persistent, or transient but currently in memory) can appear in the `Submaps in Map` dialog box.[28]

In other words, when the on-demand submap feature is enabled, submaps that are not presently in memory are not present in the `Submaps in Map` list. This behavior may alter the usefulness of the `Submaps in Map` dialog box, depending on the expectations of the operator.

To reduce the possibility of operator confusion when the on-demand submap feature is enabled, you may wish to remove the following menu item (which opens the `Submaps in Map` dialog box):

```
Map:Submap->Open
```

27. See also the "Caution" block on "Configuring Management Consoles" on page 109.
28. See the online help for more information about this dialog box.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0364
Doc: 3740



See *Managing Your Network with HP OpenView Network Node Manager* for information about how to remove a menu item.

Persistence Filtering

Unlike the filters described earlier, the purpose of persistence filtering is not to reduce the amount of unnecessary management data in the data stream. Instead, the purpose of persistence filtering is to let some older applications that are not inherently compatible with the on-demand submap feature operate normally when the on-demand submap feature is enabled.

NOTE This is probably not an issue on Windows operating systems, since there are few "older" applications. However, some third-party developers may port their older UNIX system applications without changes.

Suppose an application has been created with the implicit assumption that the object or objects it is interested in are always available in memory. Such an application may fail or exhibit unstable behavior if the object it needs resides in a transient submap, and is thus not in memory at all times.

For example, a vendor you use may have developed an application that adds statistics component symbols under the router symbols created by the `ipmap` service. Such an application may assume that routers are part of the map (that is, present in memory) as soon as they are discovered. The on-demand feature, when enabled, invalidates that assumption.

A persistence filter can provide backwards compatibility for this type of application. The necessary persistence filter for the example application passes all routers. Then any submap that contains a router is made persistent, so that the expectation of the application is met.

A persistence filter tells the `ipmap` service that any submap containing an object that passes the filter should be made into a persistent submap. The object will then be in memory, as the application expects.

Persistence filters are set-defining type filters. A persistence filter is automatically applied to existing map and object data to determine which submaps must be persistent. When you change a persistence filter, all the objects currently in the topology database are reevaluated to see if

they pass the new filter. Submaps containing objects that pass the new filter are made persistent. Submaps that do not contain such objects are made transient if they are below the current persistence level. [29]

Comparing Map Filters and Persistence Filters

A persistence filter is different from a map filter. A map filter specifies a subset of the topology data that is allowed on the map. The persistence filter states which objects should be made persistent in memory; those objects are made persistent by making the submaps they reside on persistent.

You can think of this as a two step process. First, the map filter passes a set of objects that are allowed to be present on the map. Then the persistence filter tests these objects to see which, if any, must be persistent in memory.

No matter what the persistence filter specifies, the user still has access to all of the objects that passed through the map filter.

When an object is found to meet the criteria in the persistence filter, all submaps containing that object are made persistent. That is, a submap is made persistent if it contains even one persistent object; it might also contain objects that do not meet the persistence specification criteria. In addition, the child submap of the persistent object is also made persistent.

Because persistence and map filters are both set-defining filters, if you change either for a given map (via the `IP Map Configuration` dialog box; see the online help for details), the `ipmap` service recalculates which submaps should be persistent. This might take a long time for larger databases.[30]

---

29. See "On-Demand Submaps" on page 64 for more details on persistence filtering. See "Specifying a Persistence Filter" on page 124 for configuration information.
30. See also "Map Filtering" on page 42.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0365
3740
Doc:

Management Consoles

Distribution of management consoles is done via NFS (or Windows operating system file sharing) mounting of the map database and the appropriate configuration files, and by then using the distributed RPC capability of the object database service, ovwdb, the topology database, and the event system.

Figure 2-8 is a diagram of the resulting services, and where they are located. As shown, each management console actually runs the user-specific ovw-related services. The management station keeps the common databases, and runs the services (background processes on UNIX systems) common to all users.

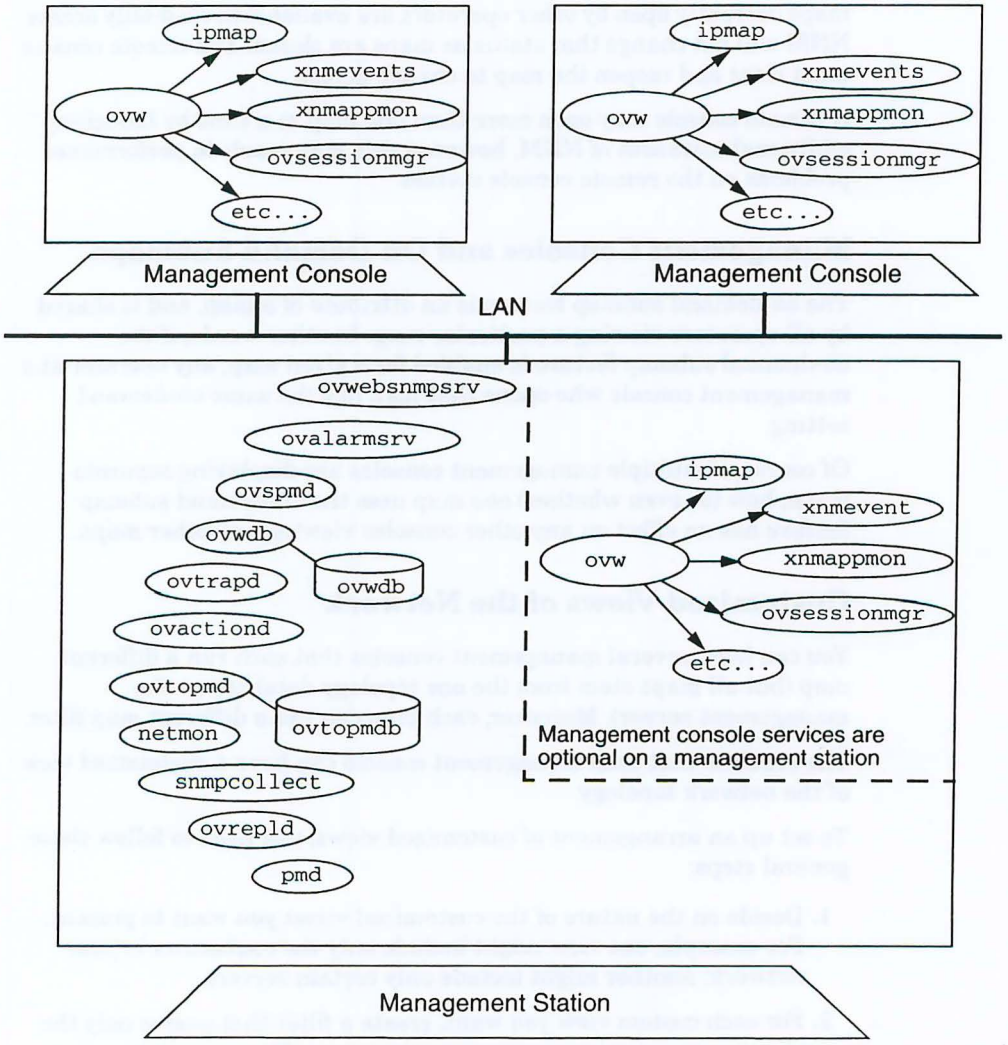
This relieves the management station of a significant demand for its resources (memory and CPU), since otherwise each operator would have independent copies of these services executing on the management station.

Relocating the ovw-related services allows the management station to apply more of its resources to network management and monitoring activities, and less to supporting the operators.

The object database remains centrally located on the management station, and is accessed by the management consoles over the network sockets. In addition to the various ovw-related services that communicate with the NNM services via socket connections, the map database and configuration files use NFS (or Windows operating system) file sharing.

NOTE Management consoles are *not* the same as NFS diskless clients. NFS diskless is an operating system concept. As described above, the distribution mechanism for management consoles uses NFS and sockets.

Figure 2-8 Management Consoles



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0366
3740
Doc:

Operators can each have their own maps. If, on the other hand, they share a map, only the first operator to open the map can edit it; others have read-only access. When using remote console into a management server that is being accessed by other remote or local console operators, maps currently open by other operators are available in read-only access. NNM will not change that status as maps are closed. The remote console must close and reopen the map to change access.

A remote console may open more than one map at a time by launching additional instances of NNM, however, this may result in performance problems on the remote console station.

Management Consoles and On-Demand Submaps

The on-demand submap feature is an attribute of a map, and is shared by all operators viewing a particular map. In other words, if the on-demand submap feature is enabled for a given map, any operator at a management console who opens that map has the same on-demand setting.

Of course, if multiple management consoles are displaying separate maps, how (or even whether) one map uses the on-demand submap feature has no effect on any other consoles viewing any other maps.

Customized Views of the Network

You can have several management consoles that each run a different map (but all maps stem from the one topology database on the management server). Moreover, each map can use a different map filter.

The result is that each management console can have a customized view of the network topology.

To set up an arrangement of customized views, you need to follow these general steps:

1. Decide on the nature of the customized views you want to present. For example, one view might include only the connectors in your network; another might include only certain servers.
2. For each custom view you want, create a filter that passes only the objects you want visible in that custom view.[31]
3. At each management console, create a new map (`Map:New`), and apply the appropriate map filter for the operator at that console.

Management Consoles and X-Terminals

In principle, it is possible to run several X-terminal sessions from a management console, or directly from the management station. You might speculate that this would allow NNM to support more operators.

However, due to internal constraints, this approach *does not* allow the management server to support more operators. You should limit the number of operators per management station to avoid degrading the performance of the interface.

Attaching X-terminals to a management console might nevertheless have cost savings, if the management console host has sufficient CPU, memory, and disk space to support the X-sessions, and low cost X-terminals are available and suitable for the operators. The key services described earlier are still off-loaded from the management station to the management console.

31. See "Filters" on page 37 and Appendix A, The Filter Definition Language, for more information on creating filters.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
036752
Fls. Nº
3740
Doc:

Interface Managed-state Automation

As you probably know, NNM lets you "unmanage" interfaces. NNM does not do status polling on unmanged interfaces, so setting interfaces to the Unmanaged state significantly lightens the load on the management station.

NNM lets you automatically manage or unmanage interfaces based on filters. Interface managed-state automation makes it easier to manage large environments, where frequently many discovered interfaces do not require active status polling.

Interface managed-state automation relys on a command (`ovautoifmgr`) that periodically sweeps through the topology and sets the managed state of interface objects according to rules in the managed-state configuration file (`ovautoifmgr.conf`).

Based on the rules in the configuration file, interfaces that do not need to be managed are put into the Unmanaged state. Interfaces which do need to be managed (and are not already) are put into the Managed state with their status set to `UNKNOWN`. Then `netmon` begins to monitor the interface's operational status and generate events.

The the `ovautoifmgr` command is not a continuously-running process. Instead, it is designed to be run periodically by a scheduling mechanism. It requires that `ovtopmd` be running.

For further information and instructions on using interface managed-state automation, refer to the `ovautoifmgr(1m)` and `ovautoifmgr.conf(4)` reference (man) pages.

Microsoft Terminal Server Access

You can connect to Network Node Manager (on a Microsoft Terminal Server) from a remote workstation through a Terminal Server Client. You can do any of the following:

- Install or upgrade NNM on the remote server.
- Perform administrative NNM functions such as backup/restore of NNM database.
- Open NNM and display the network map onto the local workstation.
- Start multiple Terminal Server Client sessions to the same remote NNM management station, open NNM in each session and display the network maps onto the local workstation.
- Start multiple Terminal Server Client sessions to different remote NNM management stations, open NNM on each NNM management station and display the network maps onto the local workstation.

The following examples provide a few of the possible implementation strategies available to network managers when running the NNM application on servers with the Microsoft Terminal Server features enabled.

Accessing a Single NNM Station From Multiple Terminal Server Clients

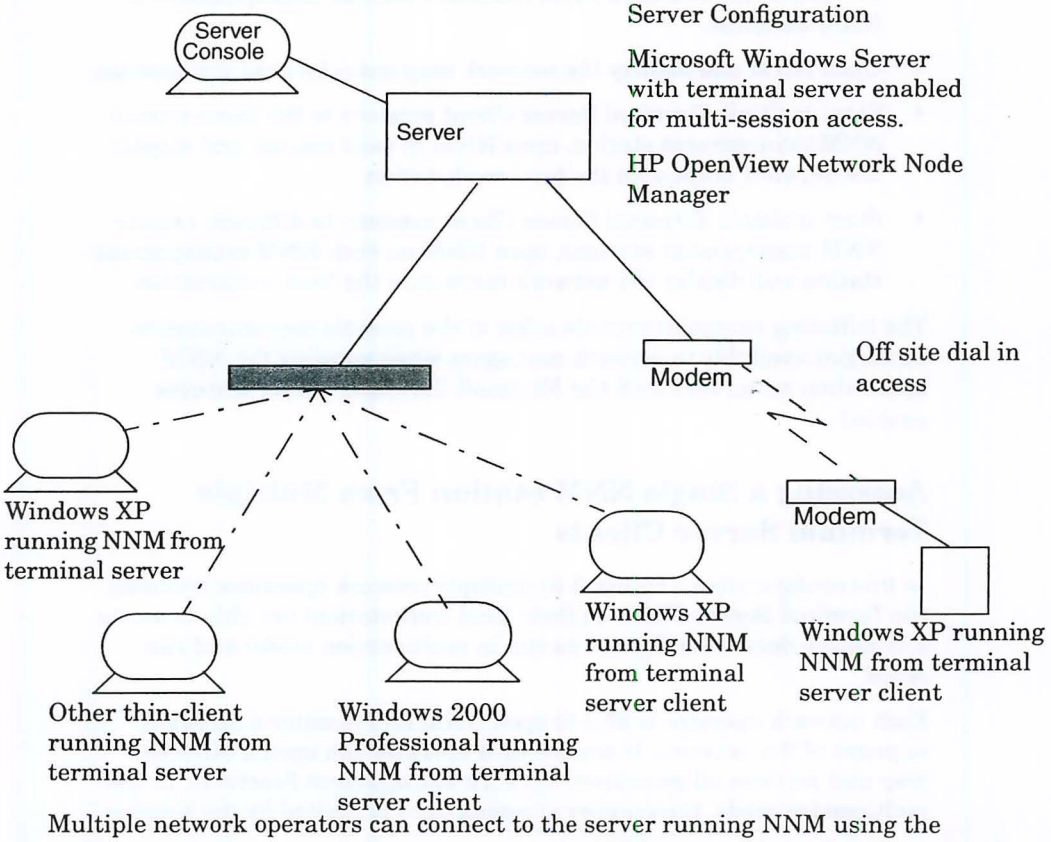
In this configuration, (Figure 2-9) multiple network operators (running the Terminal Server Client on their local workstation) are able to access a Windows Server (configured to run in multisession mode) and run NNM.

Each network operator is able to open NNM and monitor a different segment of the network. If needed each operator can open a different map and perform all associated network management functions. In the multisession mode, the number of connections is limited by the number

IRQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0368
3740
Doc.

of client licenses available. Accounts with administrator privileges can be used to start and stop NNM processes, run NNM database backups, and install NNM patches.

Figure 2-9 Multiple Terminal Server Clients Accessing a Single NNM Station



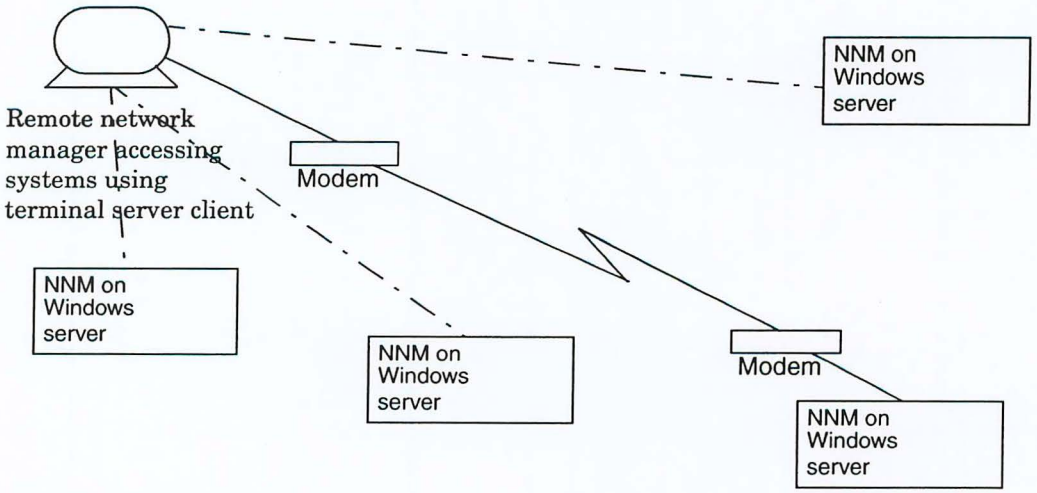
Multiple network operators can connect to the server running NNM using the terminal server client. The operators can open NNM maps and monitor the network segment from their local workstation.

Accessing Multiple NNM Stations From a Single Terminal Server Client

In this configuration, (Figure 2-10) a single network manager is able to access multiple Windows servers configured to run under Remote Administrator mode. The NNM application is installed on each Windows server. The remote network manager, using the Terminal Server Client, is able to connect to each remote system, monitor the network, and perform all network management functions. With this configuration a network manager has the ability to access and display multiple NNM sessions on their local workstation.

The remote administration mode limits the number of connections to the server (maximum of two) and only grants connections to accounts that have administrator privileges.

Figure 2-10 Accessing Multiple NNM Stations



Server Configuration

Microsoft Windows Server with terminal server enabled and installed as Remote Administrator mode.

HP OpenView Network Node Manager running on each server to manage the local network

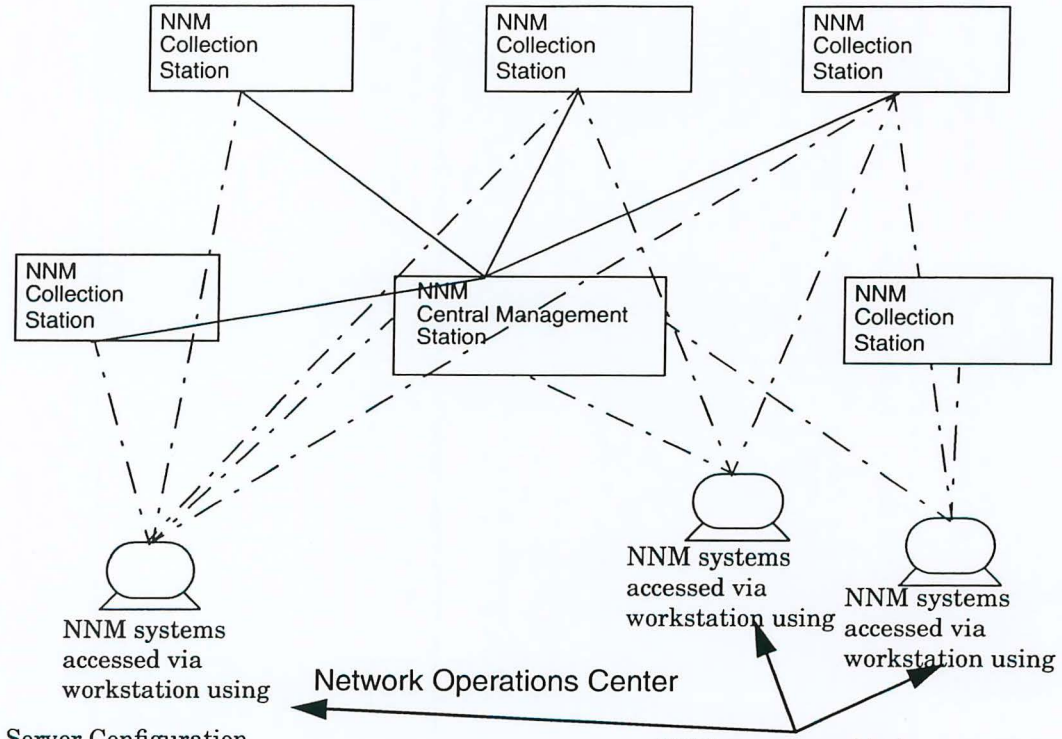
RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0369
3740
Doc:

Accessing Multiple NNM Stations From Multiple Terminal Server Clients

In this configuration, (Figure 2-11) a central Network Operations Center (NOC) is responsible for monitoring the entire network. The network management architecture is constructed of multiple Windows servers running NNM configured as collection stations, each collection station forwards information to a central NNM management station. The NOC operators are responsible for monitoring the health of the network.

The Terminal Server Client enables operators to access multiple NNM stations and to monitor different segments of the entire network from a single workstation. Operators can open multiple NNM sessions on each NNM station to view more than one map. Operators with administrator privileges can remotely start and stop NNM processes, run NNM database backups, and install NNM patches.

Figure 2-11 **Multiple NNM Stations Accessed by Multiple Terminal Server Clients**



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0376
3740
Doc:

3 Strategies for Deploying Network Node Manager

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0371
3740
Doc:

This chapter contains guidelines and ideas for deploying an HP OpenView Network Node Manager (NNM) solution that meets your goals and fits well with your organization.

The purpose of this chapter is to help you understand some of the reasonable models you can use as you plan your network management solution, and some criteria you can use to select a model.

It includes general approaches and general tips to help you succeed. With this knowledge, you will be able to better plan and implement your distributed, scalable network management solution.

NOTE

The information in this chapter is not introductory; readers are assumed to have read the previous chapters. Readers are also assumed to be conversant with NNM's key features for network monitoring, data collection, event handling, and so on. This includes a functional understanding of some key elements in non-distributed NNM, including `ovw`, `ipmap`, `ovtopmd`, and `netmon`. See *Managing Your Network with HP OpenView Network Node Manager* for details about these key services (background processes on UNIX systems) in Network Node Manager.

The remaining chapters and appendices contain specific configuration procedures to use with the scaling and distribution features of NNM.

Planning the Right Approach

Now that you understand Network Node Manager's scalable and distributable features, your questions naturally turn to issues like:

- "What should I *do* with all this?"
- "Can I just ignore NNM's scalability features for now? Should I?"
- "How would I employ distribution and scalability on a massive scale?"
- "What makes sense in my organization?"

You have a wide range of choices in your deployment of NNM. The simplest choice, and one that will make sense to some, is to use none of the scalability features at all. Others, who manage large, dispersed networks, will elect to scale up their use of NNM to deal with that large environment. Still others will find that a mix of some scalability features meets their requirements.

You can combine several different models as you plan your strategy. Each fits well with a particular set of goals. Your choice of approach will be driven, in large measure, by the nature of your organization and the problems you are solving with your network management solution.

Remember as you plan that you are never "locked-in" to one strategy; as your organization changes, you can adapt your use of NNM to keep up with those changes.

Organizations differ in many ways. Organizational variables to consider as you begin planning your deployment of NNM include:

Size The needs of a small organization, with perhaps a few hundred nodes, are very different from the needs of a corporate campus where you may have thousands or tens of thousands of networked objects. The networks in larger organizations are inevitably larger and more complex than in small organizations. Consequently, the larger the organization, the stronger are the reasons to use more of the scalability features of NNM.

Structure Some organizations, like the military, have clear hierarchies of authority and reporting. Others, like universities, may consist of looser affiliations between

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 037257
3740
Doc:



cooperating but largely autonomous groups. These structural differences will have a significant effect on how network management is conducted.

Geography Some organizations, like a hospital, are geographically compact but require reliable network management. Within the confines of the hospital, NNM may have few requirements for scaling. But suppose that hospital is part of a medical services company; the central site, located thousands of miles away, may want to perform network management functions in *all* their many hospitals. Then issues of distribution and scalability are very important.

Trends The network that supports an organization is in a constant state of change. Yet it is important to understand general trends in how a network is evolving: is it stable? is it becoming more geographically dispersed? bigger? more expensive to manage? You will want your network management plans to account, as best you can, for the trends in your network.

General Considerations about Scalability and Distribution

The following general points are useful when planning your deployment of NNM. Margin notes summarize key concepts from the adjoining text.

Limits to netmon affect the maximum number of nodes you can monitor.

Due to the nature of ICMP pings, the `netmon` service (background process on UNIX systems) has limits to the amount of polling it can perform in a given period of time. You can maximize the number of nodes the `netmon` service can handle (while maintaining a consistent five-minute status polling cycle) by increasing the polling interval, especially for less important nodes. See "Configuring SNMP" in *Managing Your Network with HP OpenView Network Node Manager* for details on how to set special polling intervals. For more current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide.*

You may also want to take advantage of interface managed-state automation, as described in "Interface Managed-state Automation" on page 74.

If the environment you want to manage has more nodes than you can monitor efficiently with a single netmon service, you will want to have another netmon service, in the form of another collection station, to off-load some of the polling work from the management station.

WAN performance also limits remote monitoring.

A WAN link introduces propagation delays that compound the above issue. That means that if your environment is split, with part of it accessible via LAN and the rest via WAN, the actual limit of managed nodes for a netmon service will be less than the limit stated above. How much less depends on the proportion of nodes on the LAN link vs. on the WAN link. In general, you will want to avoid monitoring nodes over a WAN link, unless you have only a few nodes at the remote site, or the node there are unimportant, and can receive infrequent polling.

In some circumstances, however, remote monitoring is necessary. As a rule-of-thumb, if a netmon service is monitoring remote sites, reduce the number of nodes it handles by one-tenth for each remote site. Thus, if a collection station is monitoring, say, 3 remote sites, you would expect it to handle up to 1400 nodes, rather than 2000.[1] The calculation for this estimate is as follows: 2000 - ((0.1 x 2000) x 3) = 1400.

In addition, remote monitoring via a WAN has very high operating costs in network traffic compared to the operating cost of monitoring via a remote collection station. Each status and configuration poll and response would have to cross the link, rather than simply any topology changes.

Take advantage of NNM wherever you can.

Given the low performance of WAN links, you can always achieve higher NNM performance by using a collection station for remote (WAN) nodes.

Since scalability is part of every NNM station (including NNM 250), it makes excellent sense to take advantage of NNM wherever it exists in your network. For example, you might have a "hidden" NNM station at a remote site, running NNM as the basis for another application like HP OpenView Operations. Consider using it as a collection station.

If your remote site has no NNM installation, you may want to install a collection station if you have perhaps fifty or more nodes to be monitored; NNM 250 might be a good choice for a small remote site. As an alternative, you could have a collection station located at one remote site, and monitoring multiple other remote sites.

1. Again, this estimate assumes that reliable 5-minute polling of all nodes is required.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 037358
3740
Doc:

The final layout of your solution will depend at least in part on an analysis of the costs involved with each alternative you consider.

Ensure that you can always contact your collection stations.

Relying on a remote station for network management carries certain risks, but that risk can be driven down or eliminated.

As an example, suppose some collection station is your sole source of information for a part of your network, and the main gateway between the management station and that collection station goes down. By default, it takes up to twenty minutes before a "Collection Station Critical" event is generated, and an event confirmation popup dialog is presented to the operator. The nodes affected by the failure are *not* marked "Unknown".[2]

You can diminish the likelihood and effect of such a situation in three ways.

- First, arrange to have overlapping management domains or failover coverage, particularly for key connection nodes between the management station and collection stations.
- Second, make contingency arrangements that allow alternative communication paths to the collection station. You can establish redundant routes to the collection station via multiple gateways, or by adding a direct link from the manager to the collection station if that is possible. Consider lower-cost approaches that may have lower (but still acceptable) performance in an emergency.

  Third, use HP Service Guard for your management and/or collection stations.

Use as many collection stations as you can efficiently manage.

The more collection stations you have, the smaller the impact of temporarily losing any one of them, and the easier it is to roll management of that region to a different collection station. Within the limits of your ability to configure and manage collection stations, use as many collection stations as possible to ensure redundancy and off-load polling. For more current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide.*

2. See the note about `ovrepld`'s periodic status checks in "How Distributed Internet Discovery and Monitoring Works" on page 49.

Consider the flexibility of NNM 250

The NNM 250 product is limited to managing 250 nodes per license, but you can purchase multiple licenses to increase that number incrementally. Check current pricing to decide if multiple NNM 250 licenses are preferable to a full NNM product in your situation. NNM 250 can act as a collection station for multiple management stations, but cannot receive data from other collection stations.

Partition your Internet submap to reduce the visual complexity

Because it is feasible to manage many thousands of nodes, your internet submap may become densely populated, and difficult to work with. You can solve this problem by creating Partitioned Internet submaps to create reasonable groups of nodes. See "Partitioned Internet submap" in the index of *Managing Your Network with HP OpenView Network Node Manager* for details.

NOTE

Be sure to consult the latest version of the *HP OpenView Network Node Manager Performance and Configuration Guide* for more information about configuring NNM in large environments.

General Strategies for Deployment

This section gives a few general pointers on how to deploy a distributed network management solution in your organization.

Plan ahead

Create a master plan for your organization that substantially outlines your goals for network management distribution and scaling. Keep in mind that your plan will continue to evolve along with your network.

Network planners, operations managers, and HP OpenView administrators need to collaborate in the planning process. They each bring a unique perspective, and getting early and continuing consensus important to the success of the project.

Describe and diagram the current state of your network management solution. Do the same for the final state you intend to achieve. Work together to identify each step that will be needed to migrate to the new arrangement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0374
Fls. Nº
3740
Doc:

Start small You don't have to implement every aspect of your final plan all at once. Begin by setting up just one piece of the final picture.

You might choose to implement on-demand submaps on a management console. Or, you might decide to set up one collection station to see how that goes. Choose something that makes sense in your final plan, implement it, and then test it thoroughly before you proceed.

Go slowly Add more small pieces of your final plan one at a time. As you go, keep testing and rechecking your implementation to ensure that you are obtaining the results you want.

Be particularly attentive to your filters. Carefully designed and implemented filtering can be central to the effectiveness of your solution, and the set of filters provided in the default filter file will be useful to many people. Those who need to design other filters should be aware that creating filters can be complicated, and requires considerable attention to detail.

Also, review your polling intervals (under the menu item `Options:SNMP Configuration`). Poll your most important nodes more often (for example, every 3 minutes) than your less important nodes (for example, every 15 or 30 minutes). This will help you maximize the benefits of scalability.

Keep records Maintaining a large network management solution is not trivial. Along with the planning documents, keep records of what steps have been taken and when. Note any issues that came up with a step, and, more importantly, the resolution of those issues. This "paper trail" can be useful in the event that you want to roll back to an earlier configuration for troubleshooting or re-engineering your distribution scheme.

Backup your system NNM pauses all services yet queues information coming in from collection stations, so you can backup your database without missing any information. Refer to *Managing Your Network with HP OpenView Network Node Manager* for more information.

Deployment Strategies for NNM

You have a number of choices about which of the scalability features of NNM you want to use, and to what degree you want to use them. This section describes several models of deployment to help you understand some alternatives to consider as you put scalable NNM into operation.

The following models are considered in this chapter:

- Fully centralized
- Centralized hierarchical
- Hierarchical
- Cooperative independent

NOTE

This chapter uses the above models to show how different organizational structures can be reflected in the deployment of network management within the organization. The deployment models in this chapter are not, by any means, the only way to convey the ideas presented here. This can not be overemphasized. Few organizations, if any, will use one of these models in a pure form. As you read this section, you are encouraged to look for ideas and approaches that can be applied in some part of your own organization. It can be helpful to imagine that the strategies in this section apply to very small parts of your overall network management solution. For example, a management station that has a hierarchical relationship to one collection station might simultaneously have a cooperative relationship with another management station.

Use of Scalability Features in NNM Deployment

All of these features are available to you in any way you choose to deploy NNM. The following table shows the most common scalable features used in each type of NNM scenario.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0375
Fls. Nº 60
3740
Doc:

Table 3-1 Scalability Features in Use Models

Scalability Feature	Centralized page 92	Centralized/ Hierarchical page 95	Hierarchical page 98	Cooperative page 103
Scalable Product Structure	X	X	X	X
Distributed Collection Stations, page 48		X	X	X
Management Consoles, page 70	X	X	X	X
Network Presenter web GUI, *Managing Your Network with HP OpenView Network Node Manager*,	X	X	X	X
On-Demand Submaps, page 64	X	X	X	X
Discovery Filtering, page 40	X	X	X	X
Topology Filtering from Collection Station to Management Station, page 41			X	X
Map Filtering for Operators, page 42	X	X	X	X
Event Forwarding, page 59		X	X	X
Threshold Event Forwarding, page 59		X	X	X
High Availability - Service Guard, page 50	X	X	X	X

Table 3-1 Scalability Features in Use Models (Continued)

Scalability Feature	Centralized page 92	Centralized/ Hierarchical page 95	Hierarchical page 98	Cooperative page 103
High Availability - Failover with Failover Filtering, page 52		X	X	X
High Availability - Overlapping Domains, page 55			X	X

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0376
Doc 3740

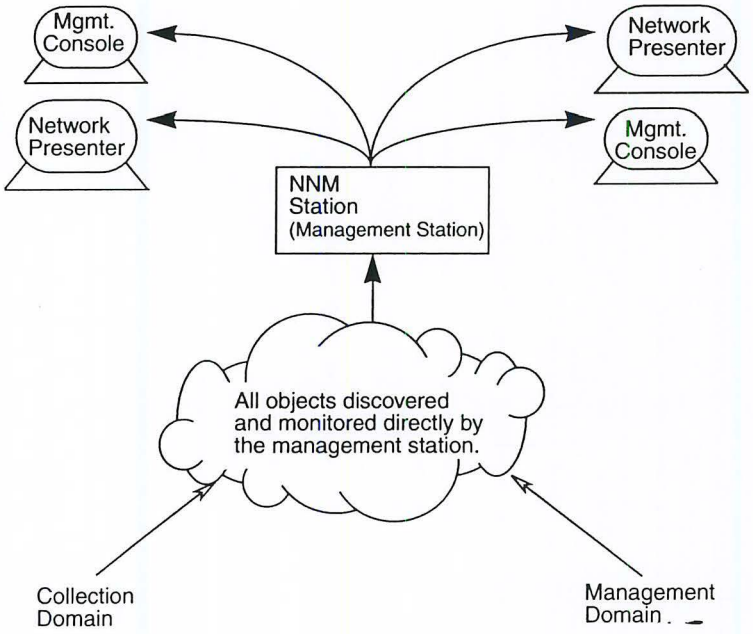
Fully Centralized Management

In a fully centralized network management scheme, one management station performs all monitoring and data collection functions for a whole management domain. There is little or no remote network management hardware or personnel. The primary focus is probably network management, with primary attention to the main connectors, like bridges, hubs, and routers.

Users of non-distributed network management products (including early versions of Network Node Manager) naturally use this model, since it is the only strongly supported model available. In fact, for many situations, a fully centralized usage of NNM is a highly functional and reasonable choice. Even in this model, scalability can be very useful.

Figure 3-1 illustrates a fully centralized network management scheme.

Figure 3-1 Fully Centralized Management Model



Notice that the collection domain and the management domain are identical. This is characteristic of this management model.

Remember that the management domain is an attribute of the management station, not the operators. You may have several operators, each of whom has a different view of the overall topology (via map filtering), and who therefore deal only with subsets of the management domain.

Implementation Tactics

Using a fully centralized model is probably the simplest (though not always the most efficient) way to use Network Node Manager. Depending on the nature of your situation, it might make sense to use one or more of the following scalability features in a fully centralized management situation:[3]

- Management consoles, for multiple operators and Network Presenter GUI for location independence.
- Map filtering, for specialized views of the topology.
- On-demand submaps, for better performance, especially on low-end management consoles.
- Discovery filtering, to eliminate unnecessary objects, enhancing performance.

  Consider an HP Service Guard cluster for the critical management station.

These features are especially useful if you have a large environment that you are managing centrally, and you have several specialized operators to monitor it. They are also useful features in a smaller management station, where you want to get the maximum performance from the available system.

3. See "Filters" on page 37, "On-Demand Submaps" on page 64, and "Management Consoles" on page 70.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0377
3740
Doc:

Implications of Using the Fully Centralized Management Model

A centralized management model is simple to understand and control. Using a centralized model puts the management responsibilities (and expertise) in one location, which works well in some organizations. However, if you do not use the scalability features of NNM, performance of the map may become problematic in a very large environment.

If you have to monitor remote nodes over a WAN, a centralized approach causes unnecessary traffic on those expensive links. Furthermore, in a very large network, the overall performance of your network management solution is probably slowest if you use a fully centralized approach, and will require that you tune polling intervals so that the `netmon` service doesn't fall behind in polling.[4]

You may also want to take advantage of interface managed-state automation, as described in "Interface Managed-state Automation" on page 74.

For the most current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide.*

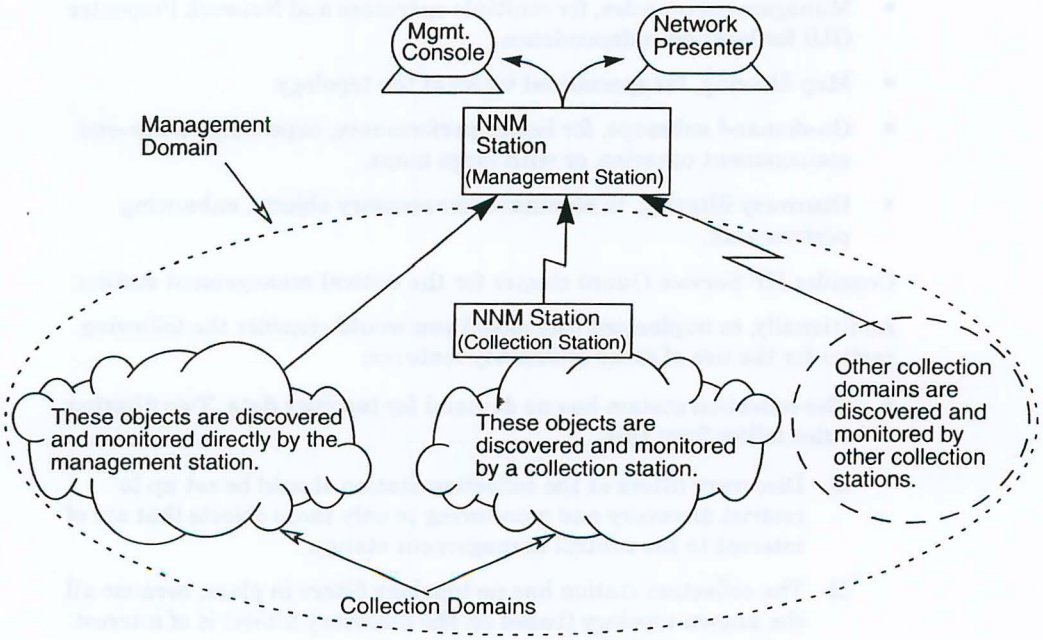
4. See the `Performance:Network Polling Statistics` menu item, and associated online help, for information on how to see if `netmon` is keeping up with polling.

Centralized-Hierarchical Management

Sometimes, one primary group has responsibility for a large network management environment. The centralized-hierarchical model involves a network that for some reason is not suitable for monitoring by a fully centralized model. The environment may be too large,[5] or you may have sizeable remote sites where network management support is minimal.

In Figure 3-2, all operators are located at the management station; this is the main characteristic of a centralized-hierarchical situation.

Figure 3-2 Centralized-Hierarchical Management Model



5. See "General Considerations about Scalability and Distribution" on page 84.

RQS nº 03/2005 - CN - CPMI - CORREIOS
0378
Fls. Nº
3740
Doc:

While the management station in the diagram has its own collection domain, it keeps a hierarchy of several remote collection stations that provide distributed network management services. Human support for network management at the remote sites is minimal and probably does not extend to operating NNM from a console.

Implementation Tactics

Implementing a centralized-hierarchical management model is, like all distributed models, more complex than a simple centralized approach.

All of the scalability features mentioned for the fully centralized model are still applicable in exactly the same way, and for the same purposes, as for the centralized-hierarchical model:[6]

- Management consoles, for multiple operators and Network Presenter GUI for location independence.
- Map filtering, for specialized views of the topology.
- On-demand submaps, for better performance, especially on low-end management consoles, or with large maps.
- Discovery filtering, to eliminate unnecessary objects, enhancing performance.

Consider HP Service Guard cluster for the critical management station.

Additionally, to implement this model you would consider the following tactics for the use of other scalability features:

- The collection station has no demand for topology data. Two filtering rules follow from this:
  - ❑ Discovery filters at the collection station should be set up to restrict discovery and monitoring to only those objects that are of interest to the central management station.
  - ❑ The collection station has no topology filters in place, because all the known topology (based on the discovery filters) is of interest to the central management station.
- Configure collection station failover so that the management station can pick up for critical collection stations.

6. See "Filters" on page 37, "On-Demand Submaps" on page 64, and "Management Consoles" on page 70.

- You will probably want to forward all threshold events that you configure for the collection station. The most likely forwarding would be to the %REMOTE_MANAGERS_LIST%, so that any interested manager would receive the events.

  One potential exception to this rule would occur if you only want a local action performed for a particular threshold event, and no higher level attention to the matter.

- If you are dealing with a large environment and using the centralized-hierarchical model, you may want the collection stations (even though essentially unmanned) to perform remote trend data collection. You would then plan to pull that data to the central management station for merging, report generation, and analysis.[7]

Implications of Using Centralized-Hierarchical Management

The centralized-hierarchical model is somewhat more complex to deploy and maintain than the fully centralized model, because each collection station requires special configuration. However, it has many advantages for environments that are either geographically dispersed, or too large to monitor from a single station.

You can manage networks with up to about 25,000 devices (assuming one interface per device, on average), and roughly fifteen operators. Performance of the map in a large environment can be improved by using map filtering and on-demand submaps.

A centralized-hierarchical model (like a fully centralized approach) puts the management responsibilities (and expertise) in one location, which works well in some organizations.

If you have to monitor remote nodes over a WAN, and still want centralized network management, a centralized-hierarchical approach can reduce traffic on expensive WAN links. The risk is slightly higher, since you are relying on the remote collection stations for data.

Finally, in a large network, the overall performance of your network management solution is probably better, because you are not performing polling over the lower performance WAN links.

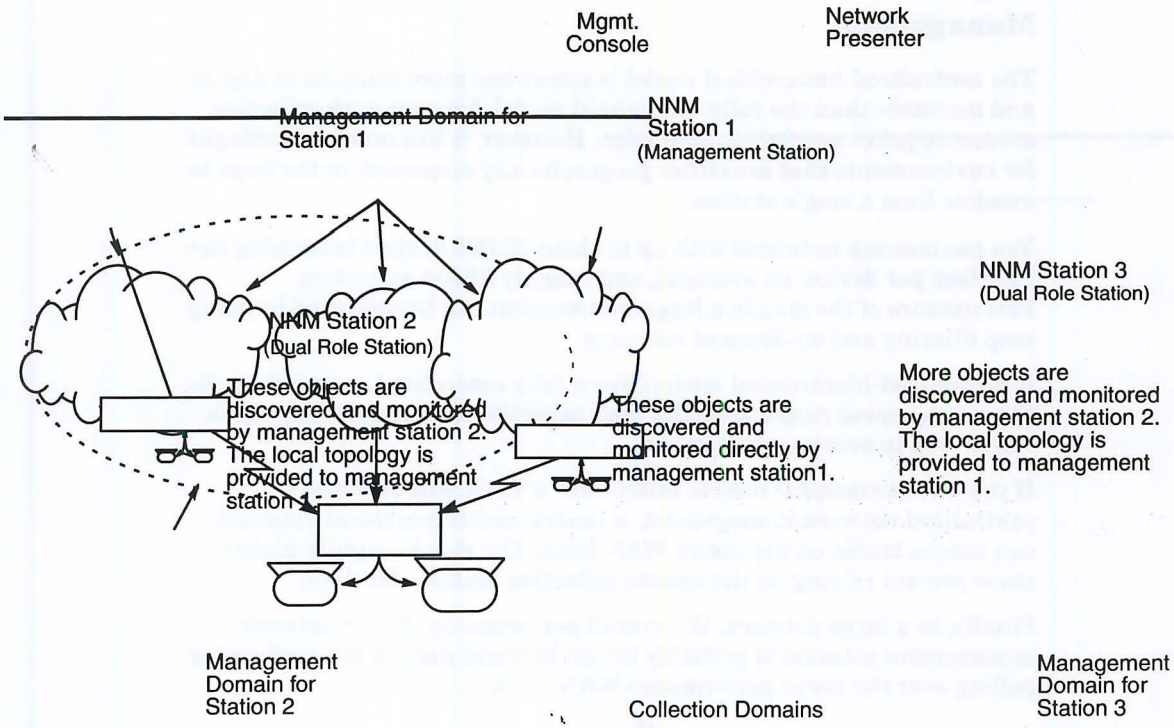
7. See the reference page in NNM online help (or the UNIX system manpage) for *ovcoltosql*.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0379
3740
Doc:

Hierarchical Management

In many large organizations, a central group has broad responsibility for the network resources of the organization, usually for the major gateways and connecting infrastructure of the network (commonly called the network "backbone"). In the outlying sites, local network managers control the local configuration, usually including local connectivity, server availability, etc. This hierarchy of responsibility is reflected in the scheme illustrated in Figure 3-3, where NNM Stations are 2 and 3 are independent management stations, while also acting as collection stations for NNM Station 1.

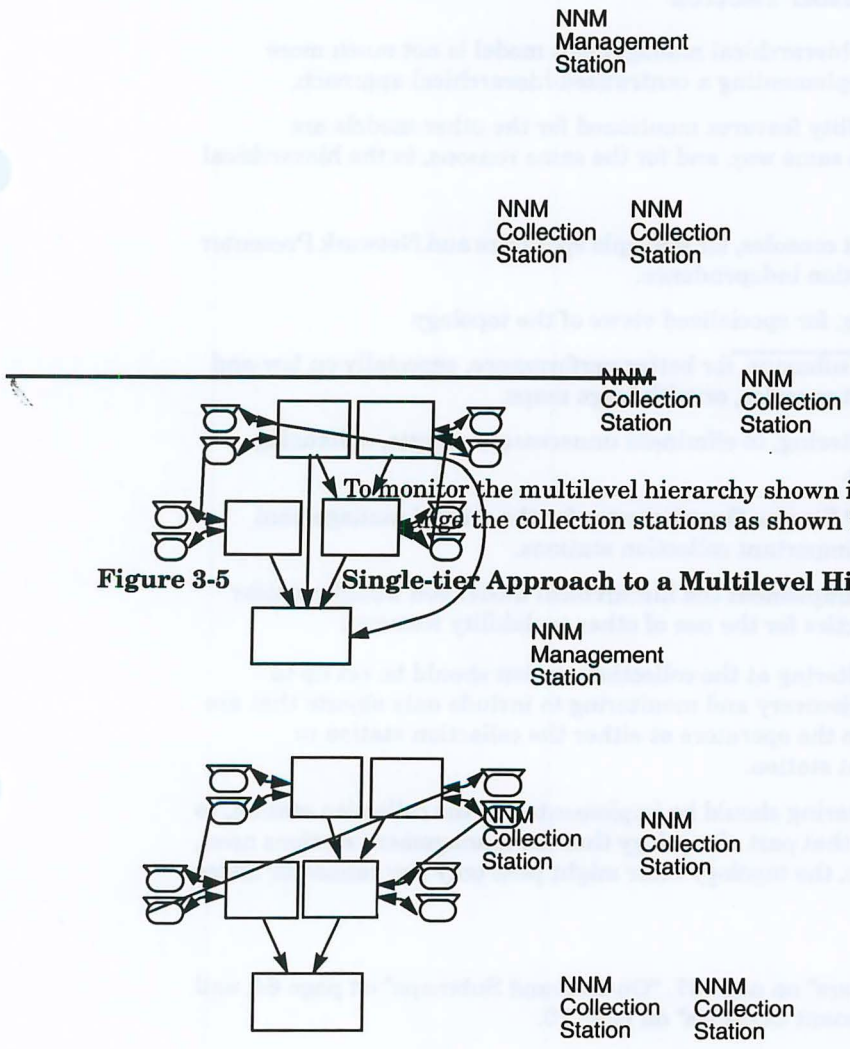
Figure 3-3 Hierarchical Management Model



While the management station in the diagram has its own collection domain, it keeps a hierarchy of several remote collection stations that provide distributed network management services. Human support for network management at the remote sites may not be available and probably does not extend to managing NNM itself.

While multiple levels are possible in a hierarchical environment, Network Node Manager passes topology and status data only one level. That is, topology data received from a collection station can not be forwarded again. Only topology and status data that is derived from a local `netmon` service can be forwarded to remote managers.

Figure 3-4 Unsupported Multilevel Hierarchical Management



To monitor the multilevel hierarchy shown in Figure 3-4, you would have to change the collection stations as shown in Figure 3-5.

Figure 3-5 Single-tier Approach to a Multilevel Hierarchy

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0380
3740
Doc:

In Figure 3-5, the top-level management station uses both the first- *and* second-tier collection stations directly, to obtain all the information it needs.

Topology filters at the second-tier must pass all the objects needed by either first-tier or top-level management stations, but the same would be true even if multiple-level management were possible.

Implementation Tactics

Implementing a hierarchical management model is not much more complex than implementing a centralized-hierarchical approach.

All of the scalability features mentioned for the other models are applicable in the same way, and for the same reasons, in the hierarchical model:[8]

- Management consoles, for multiple operators and Network Presenter GUI for location independence.
- Map filtering, for specialized views of the topology.
- On-demand submaps, for better performance, especially on low-end management consoles, or with large maps.
- Discovery filtering, to eliminate unnecessary objects, enhancing performance.

  Consider HP Service Guard cluster for the critical management station and important collection stations.

Additionally, to implement the hierarchical model you would consider the following tactics for the use of other scalability features:

- Discovery filtering at the collection station should be set up to restrict IP discovery and monitoring to include only objects that are of interest to the operators at either the collection station or management station.
- Topology filtering should be implemented at the collection station, to expose only that part of topology that the management stations need. For example, the topology filter might pass only key connector nodes.

8. See "Filters" on page 37, "On-Demand Submaps" on page 64, and "Management Consoles" on page 70.

- The interests of operators at the management stations and the collection stations may overlap on some objects. Map filtering can be cooperatively designed and implemented between the management stations and the collection stations, so that any overlap is considered and deliberate.
- Configure collection station failover so that the management station can pick up for critical collection stations.
- You might want to forward some threshold events that you configure on the collection station, most probably to the `%REMOTE_MANAGERS_LIST%`, so that all interested managers receive those events.

  Or, you might want to duplicate a MIB variable via a MIB expression. This lets you set two different thresholds on the value, one that triggers local action and one that triggers attention at the management station.

  Of course, some thresholds might be of local interest only, and not be forwarded to the managers.
- If you are dealing with a large environment and using the hierarchical model, you may want collection stations to perform remote trend data collection.

  You would then plan to pull that data to the central management station for merging, report generation, and analysis. The administrators at the remote site may also have local use for the same trend data, or a subset of it.[9]

Implications of Using the Hierarchical Management Model

The hierarchical management model takes full advantage of the benefits that scalability offers. On the other hand, it can be complex to deploy and maintain in a large environment.

9. See "Trend Data Collection in a Distributed NNM Solution" on page 28 for more information.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 381
3740
Doc:

Implementing a fully hierarchical management scheme makes it possible to manage larger environments than any other approach. Such environments are often geographically dispersed, too large to monitor effectively from a single site, and staffed, at least some of the time, with network management personnel at the remote sites.

Performance of the maps at any management station can always be improved through map filtering and using on-demand submaps. Your experiences will depend on the resources you have available, and the performance tuning you implement.[10] For the most current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide*.

A hierarchical model (unlike any centralized approach) disperses the management responsibilities and expertise across the organization. Failures at any point in the system are less likely to have wide ranging consequences.

A hierarchical approach can significantly cut traffic on costly WAN links.

Finally, in a large network, the overall performance of your network management solution is probably better this way than with any other approach, in part because situations that develop in the collection domain of the collection stations can be generally handled by the local operators.

10. See "General Considerations about Scalability and Distribution" on page 84 for ideas.

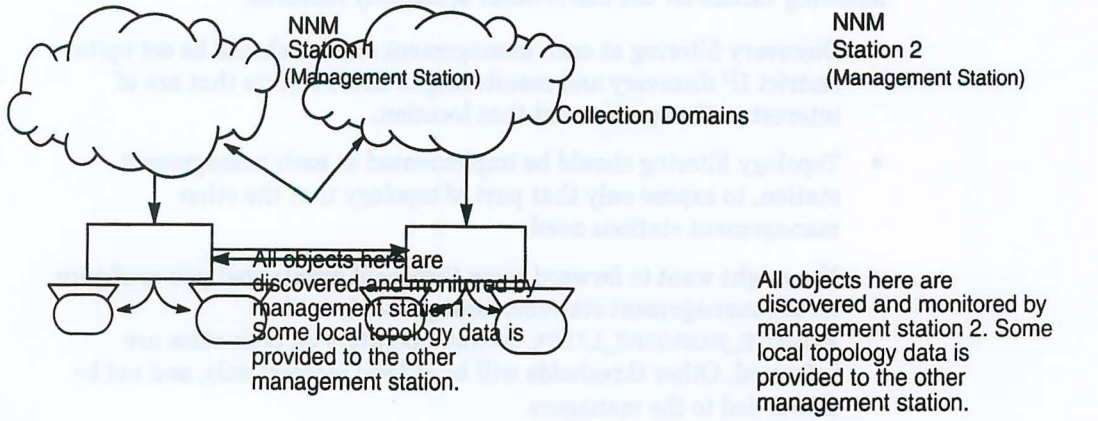
Cooperative Independent Management

In some situations, two largely independent sites need to share information at the boundaries of their management domains. Administrators at each site have primary responsibility for their part of the overall managed domain. This is shown in Figure 3-6.

In addition, these administrators are likely to have a strong interest in the major connecting nodes they share with other sites, in the primary servers at other sites, or in other key nodes or resources that reside in the domains of other sites.

This peer relationship may or may not reflect the organizational structure. You might choose this model because of the need for tight cooperation, even though one site is actually "higher" in the organizational hierarchy.

Figure 3-6 Cooperative Independent Management Model



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0382
3740
Doc:

Implementation Tactics

Implementing a cooperative management model is similar to implementing a hierarchical approach. In fact, cooperative management could be viewed as simply a variant of the hierarchical model, where each management station is, from the perspective of the other, just a subordinate collection station.

Again, all of the scalability features useful in the centralized model are still applicable in exactly the same way, and for exactly the same reasons, in the cooperative model:[11]

- Management consoles, for multiple operators and Network Presenter GUI for location independence.
- Map filtering, for specialized views of the topology.
- On-demand submaps, for better performance, especially on low-end management consoles, or with large maps.
- Discovery filtering at each management station can eliminate unnecessary objects, enhancing performance.

Consider HP Service Guard cluster for critical management or collection stations.

Additionally, to implement the cooperative model you would consider the following tactics for the use of other scalability features:

- Discovery filtering at each management station should be set up to restrict IP discovery and monitoring to those objects that are of interest to the operators at that location.
- Topology filtering should be implemented at each management station, to expose only that part of topology that the other management stations need.
- You might want to forward some threshold events that you configure on the management stations, most probably to the `%REMOTE_MANAGERS_LIST%`, so that operators on both sides are informed. Other thresholds will be of local interest only, and not be forwarded to the managers.

11. See "Filters" on page 37, "On-Demand Submaps" on page 64, and "Management Consoles" on page 70.

- When using the cooperative independent model, you may want to collect trend data on the shared resources. Depending on the actual configuration of the resources, you may want one or all management stations to perform trend data collection. If multiple stations are collecting trend data, you might want to choose one to act as the central location for merging the data, report generation, and analysis. The administrators at each management site may also have local use for the same trend data.

Implications of Using the Cooperative Independent Model

The cooperative independent management model is very similar in technical complexity to a more purely hierarchical approach, and likewise requires that the sites cooperate in nontechnical ways as well. For example, scheduled downtime of critical or shared resources at one site should not come as a surprise to the other sites.

In implementing a cooperative independent management scheme, you can assume that each site has complete responsibility for local management of non-shared resources and objects.

A management station with a cooperative relationship to another management station can, at the same time, have a hierarchical relationship with one or more other collection stations.

The cooperative model acknowledges that management responsibilities and expertise are not centralized in the organization, and that unique skills and requirements exist at different sites. While a failure at one point in the system is unlikely to have wide ranging consequences, a local problem may get little attention from a remote site.

Finally, the overall performance of your network management solution is good, in part because situations that develop in the collection domains are generally handled locally.[12] Thus, a cooperative approach provides benefits without creating significant traffic on costly WAN links.

12. See "Filters" on page 37, "On-Demand Submaps" on page 64, and "Management Consoles" on page 70.

RQS nº 03/2005 - CN - CPMI - CORREIOS
0383
Fls. Nº
3740
Doc:

4 Procedures for Scaling NNM

ROS 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0384
3740
Doc:
69

This chapter is not an introduction to NNM procedures. Readers are assumed to be conversant with NNM's key features for network monitoring, data collection, event handling, and so on. Readers who are looking for that information should turn to *Managing Your Network with HP OpenView Network Node Manager* instead. That manual also covers basic configuration of NNM station options that are not exclusive to distributed management.

This chapter covers procedures for scaling NNM. These procedures are:

- Configuring management consoles.
- Configuring on-demand submaps.
- Configuring distributed internet monitoring.
  - Data collection
  - Collection station
  - Management station
  - Domain overlap and failover
- Configuring event forwarding.
- Using distributed data collection.

The accompanying diagram serves as your roadmap through this chapter. As new areas of configuration are introduced, they are circled on the diagram.

All of the documentation for HP OpenView Windows and Network Node Manager is written with the assumption that you have activated environment variables on UNIX systems. For information about environment variables, see the reference page in NNM online help (manpage on UNIX systems) for *ov.envvars*.

NOTE This chapter refers to operating systems in the form OS Version.X (for example, HP-UX 11.X). Refer to the Release Notes, Supported Configurations topic for the operating systems that are supported with this release.

Configuring Management Consoles

Distribution of the HP OpenView Windows Graphical User Interface (GUI) is done via NFS mounting (Windows operating system file sharing for Windows operating system servers) of the map database and the appropriate configuration files, and by using the distributed RPC capability of the object database service (or background process on UNIX systems), `ovwdb`.

Display

Mgmt. Station

Domain

Collection Station

This section has five components:

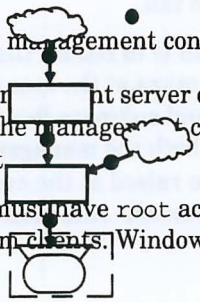
- Configuring an NNM server on a machine running the Windows operating system (Windows operating system file sharing).

Domain

Filter

- Configuring a client on a Windows system for server on a Windows system (Windows operating system file sharing).
- Configuring a server on a UNIX operating system.
- Configuring a client on a Windows system to use a server on a UNIX
- Configuring a client on a UNIX system.

NOTE The management console (client) and the server must run the same revision of NNM. Refer to the Release Notes, Supported Configurations topic for the operating systems that are supported with this release.



To set up management consoles, the following must be true:

- A management server on UNIX must be configured as an NFS server and the management console (client) must be configured as an NFS client.
- You must have `root` access on UNIX system servers and UNIX system clients. Windows systems require `Administrator` rights.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0385
Doc. 3740

- The client must have read-write access to a UNIX system server's file system via NFS.
- User and group IDs must be synchronized between the client and server.

The basic steps in installing management consoles are:

1. Install NNM on the server system, following the instructions in the *HP OpenView Network Node Manager Installation Quick Start*. (You do not need an additional license for the client.)
2. Mount the server's HP OpenView data directories on the client system.
3. Install NNM on the client system.
4. For UNIX system clients, run the `ovwsetupclient` configuration script on the client to have it use the mounted databases for maps and objects.
5. Run `ovstart` on the server system.
6. Run `ovw` on the client system.

CAUTION If a "lightweight" system (for example, a HP9000/715 with 64 Mbytes of RAM) is configured as a management console client for a server with a large database, it is possible that the resulting performance of the client system will be unacceptably slow, or that one or more of the background processes that run on the management console will run out of memory.

This is because `ipmap` and the `ovw` process sizes grow in proportion to the number of objects that are associated with persistent maps. For example, suppose that management station has 40,000 objects in its default map and the on-demand submap feature is disabled. If a lightweight management console tries to open this map, the synchronization process on the management console will cause `ovw` and `ipmap` to grow so large that either performance will be exceedingly slow, or one of the processes will run out of memory and fail.

The solution to this problem is to reduce the number of objects that are associated with persistent maps at the management console. This can be done by using the on-demand submaps feature, or map filters, or both. If the map is to be shared by both the management station and the console, the demand level should be raised at the *management* station *prior* to starting the management console. Alternatively, a copy of the map can be

created at the management station, and that copy can be configured with a higher demand level and/or filters. This new map can then be started up by the management console. For the best performance at the management console, set the demand level to Internet.

Configuring a Windows System Console Server

1. Share the *install_dir* directory from the NNM management server as *ShareName*. You may use Windows Explorer using a right mouse click. Give the users `Full Control` access.
2. Start the NNM services from the Control Panel at the NNM management server. These services must run during installation, or installation will fail.

Installing a Management Console on Windows for an NNM Server on Windows

First, install NNM on the Windows operating system machine that will be the management server, then follow these steps. You will need to know the name of the server to which the console will connect and the *ShareName* on the server.

ı NNM remote console, verify that you can connect to the *ShareName* share. You may use Windows Explorer.

NOTE

During installation, the *install_dir*`\conf\*.auth` files are edited to give the remote console access to the manager's database and services. If you experience problems connecting to a management server, you may want to verify the rights granted in these files. You may also edit these files to customize rights for remote console operators.

2. On the NNM remote console system, insert the CD-ROM and run `setup.exe`. When installing, pick the `[Remote Console Installation]`. This removes any databases or local configuration files (these files might be in place if you had previously installed the full NNM management server). Supply the machine name of the NNM management server and share name *ShareName*.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0386
3740
Doc:

3. You can now run NNM from this remote console as if you were at a full management server. The remote console has no icons for `[ovstop]` and `[ovstart]`, since to use these from a remote console, you must explicitly name what to start-up or shutdown. However, you can run these services from the command line.

Remote console operator rights to view maps are controlled the same way as operators viewing maps directly on the management server. Use NTFS file system access assignments to the *`install_dir`*`\databases\openview\mapdb` directory and subdirectories. Refer to *Managing Your Network with HP OpenView Network Node Manager* for details.

UNIX System Server Configuration

The server system is the management station on which you installed NNM and whose map and object database you want to export to the client system. You must be `root` to perform these steps. In the following steps, replace *`client_name`* with the hostname of the client from which you want to use these databases.

The following steps allow all users, including `root`, to run `ovw` sessions

1. Install NNM on the server as described in the *HP OpenView Network Node Manager Installation Quick Start* for the system.
2. If management consoles are connecting to this server from a Windows system, verify that the `pcnfsd` process is running on the server. This process lets your Windows operating system consoles know the name of the management station and that the station is running the `pcnfsd` daemons.

NOTE This step explains how to configure the `pcnfsd` process to authenticate NFS access requests from Windows clients. Although the `pcnfsd` process is commonly used for authentication, third-party providers of Windows NFS client products offer alternative methods, such as NIS authentication. If you prefer to use the `pcnfsd` process, complete this step. If you skip this step and use a third-party authentication procedure, it must be configured to allow access to user IDs in the range of 0-60002.

a. Create the file `/etc/pcnfsd.conf`. It will contain one line that reads:

   `uidrange 0-60002`

   Save and close this file.

b. Start PCNFS.

- On HP-UX:

  Edit the `/etc/rc.config.d/nfsconf` file. In it, change the PCNFS_SERVER= line to look like this:

  `PCNFS_SERVER=1`

  Save and close this file. To start the service, run the command:

  `/sbin/init.d/nfs.server start`

- On Solaris:

  Verify that the PCNFS product is installed on the management station and that `pcnfsd` is running:

  `ps -ef | grep pcnfsd`

  If it is not running, start it with `/opt/SUNW/pcnfs/scripts/pcnfs start`.

3. Ensure that NFS is running on the server.

- **On HP-UX:**

  a. Run this command:

  `ps -ef | grep nfsd`

  b. If the `nfsd` process is not running, edit the file `/etc/rc.config.d/nfsconf` and change `NFS_SERVER=0` to `NFS_SERVER=1` and run the following command:

  `/sbin/init.d/nfs.server start`

- **On Solaris 2.X systems** (NFS must already be installed):

  a. Run this command:

  `ps -ef | grep nfsd`

  b. If the `nfsd` process is not running, execute:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0387
3740
Doc:

```
/etc/init.d/nfs.server start
```

4. Configure the exportation of the HP OpenView file system to the client as follows:

   - For an HP-UX server, edit the `/etc/exports` file. You will either modify two existing lines or add new ones, depending on the contents of this file.

     -- If the line `/etc/opt/OV/share -root=` is present, add your console system's name after the equal sign. If there is already a system name after the equal sign, then add a colon (:) followed by your console system's name after the first system name.

     -- If the line `/etc/opt/OV/share -root=` is not present, add it and include your console system's name.

     -- Do the same for the line `/var/opt/OV/share -root=`.

     When you have finished editing, the file should look like this:

     ```
     /etc/opt/OV/share root=First_System:Console_System
     /var/opt/OV/share -root=First_System:Console_System
     ```

     or

     ```
     /etc/opt/OV/share -root=Console_System
     /var/opt/OV/share -root=Console_System
     ```

     Save and close the `/etc/exports` file.

   - For a Solaris server, edit the `/etc/dfs/dfstab` file by adding the following two lines to it:

     ```
     share -F nfs -o root=Console_System /etc/opt/OV/share
     share -F nfs -o root=Console_System /var/opt/OV/share
     ```

     Save and close the `/etc/dfs/dfstab` file.

5. Run the following two commands to unexport and re-export the directories from the server:

   On HP-UX:

   ```
   /usr/sbin/exportfs  -au
   /usr/sbin/exportfs  -av
   ```

   On Solaris 2.X:

   ```
   share -F nfs -o root=client_name /var/opt/OV/share
   share -F nfs -o root=client_name /etc/opt/OV/share
   ```

Use the fully qualified domain name when specifying the *client_name*.

6. Verify that NNM is running on the management station. Type

   /opt/OV/bin/ovstatus | more

   You should see a list of processes that are currently running. Check the list to verify that the ovwdb process is running. If ovwdb is not, type

   /opt/OV/bin/ovstart ovwdb

   Then, type **/opt/OV/bin/ovstatus | more** again to verify that ovwdb is now running.

Installing Management Consoles on Windows for UNIX System Management Servers

To set up a remote management console on a Windows operating system to use a UNIX management station server, first satisfy the following prerequisites:

- Make sure that the management station server is not already mapped as a network drive on your Windows operating system console. If it is, remove the network drive connection.
- Verify that you have a compatible NFS client product installed on your Windows operating system console. (See the NNM Release Notes for a list of NFS client products that have been tested with NNM.)
- You will need to know the name of the server to which the console will connect and the two directories exported in step 4 and 5 of "UNIX System Server Configuration" on page 112.

Once the prerequisites are satisfied, perform the following steps:

1. Verify or configure the following settings in the NFS client software on the system running Windows that will be a management console.
   - The name of the management station you are connecting your management console to. Indicate the station by name, not by IP address.
   - The root login name and password for connecting to the management station.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0388
Doc: 3740

5. Once installation is completed, it is recommended that you change the configuration of your PCNFS server product so that the authentication is that of the user using NNM on the Windows operating system console, instead of `root`. For example, if a user called `ovuser` is running NNM on both the management station and the Windows operating system station, the configured PCNFS authentication should be `ovuser` instead of `root`. By changing the authentication, you ensure that any files generated during an NNM session will be accessible from both the station and the Windows operating system console.

UNIX System Console Configuration

Before you begin, you will need to know the name of the server to which the console will connect. Perform the following steps on each client machine:

1. Install NNM on the console as described in the *HP OpenView Network Node Manager Installation Quick Start* for the system.
2. Ensure that the console is running as an NFS client.

- **On HP-UX:**
  a. Run this command:

     `ps -ef | grep biod`

  b. If the `biod` process is not running, edit the file `/etc/rc.config.d/nfsconf` and change `NFS_CLIENT=0` to `NFS_CLIENT=1` and run the following command:

     `/sbin/init.d/nfs.client start`

- **On Solaris 2.X**:
  a. Run this command:

     `ps -ef | grep -e "statd|lockd"`

  b. If you do not see both the `/usr/lib/nfs/statd` and the `/usr/lib/nfs/lockd` processes running, execute:

     `/etc/init.d/nfs.client start`

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0389
Doc: 3740

3. Choose a mount point for the server's HP OpenView file systems. To make sure this file system is mounted at boot time, you must modify the appropriate file shown below. You must be `root` to modify these files. Replace *server_name* with the name of the server whose databases you want to use on this client.

NOTE As an alternative to these steps, NFS access may be provided via the NFS automounter. Consult your operating system's manual for details.

- On **HP-UX:**
  a. Run these commands:

     mkdir -p /opt/OV/nfs/*server***/var/opt/OV/share**

     mkdir -p /opt/OV/nfs/*server***/etc/opt/OV/share**

  b. Add these lines to the `/etc/fstab` file:

```
server:/var/opt/OV/share /opt/OV/nfs/server/var/opt/OV/share nfs rw 0 0
server:/etc/opt/OV/share /opt/OV/nfs/server/etc/opt/OV/share nfs rw 0 0
```

  c. Run these commands:

     /etc/mount *server***:/etc/opt/OV/share**

     /etc/mount *server***:/var/opt/OV/share**

- **On Solaris 2.X**:
  a. Run these commands:

     mkdir -p /opt/OV/nfs/*server***/var/opt/OV/share**

     mkdir -p /opt/OV/nfs/*server***/etc/opt/OV/share**

  b. Add these lines to the `/etc/vfstab` file:

```
server:/var/opt/OV/share - /opt/OV/nfs/server/var/opt/OV/share/ nfs - yes rw
server:/etc/opt/OV/share - /opt/OV/nfs/server/etc/opt/OV/share/ nfs - yes rw
```

  c. Run these commands:

     /etc/mount *server***:/etc/opt/OV/share**

     /etc/mount *server***:/var/opt/OV/share**

4. Set up the client by running the following script:

   $OV_BIN/ovwsetupclient /opt/OV/nfs/*server*

NOTE If you have used the NFS automounter, the path may be different.

5. To verify that the configuration is correct, run the following command:

   ovw -server

   Look at the return value from the ovw -server command on your display. It should look similar to:

   ```
   %ovw -server
   your server name shows up here
   ```

6. Run **ovw** on the management console.

   If you are running on an HP Service Guard cluster, you may run **ovwrs** rather than **ovw**, if NNM is configured as a package. Refer to the *ovwrs* man page for more information about restartable **ovw**.

Increasing Security for Management Consoles

Authorization files on the server allow you to limit which consoles may access the information on the server. If you have modified default authorizations, add the server hostname and each client hostname to the authorization file for ovwdb and ovw. Be sure to add the line *client_name* + for each client you are giving access to the server. The files ovwdb.auth and ovw.auth are located in $OV_CONF.

```
server_name +
client_name_1 +
client_name_2 +
```

where *server_name* is the name of the system where your map database resides. The addition of these lines enables any user from *client_name_1* or *client_name_2* to use the database on *server_name*.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0390
3740
Doc:

NOTE A third authorization file also exists, `ovspmd.auth`. This file limits which consoles have permission to run `ovstop` and `ovstart`. **You should be careful about giving too many users this permission.**

Undoing a Management Console

If you want to undo the management console setup and run NNM in a normal manner, you must follow these steps in the order listed.

CAUTION Failure to follow these steps could result in damage to your databases.

- On UNIX systems:
  1. Run the following command on the console:

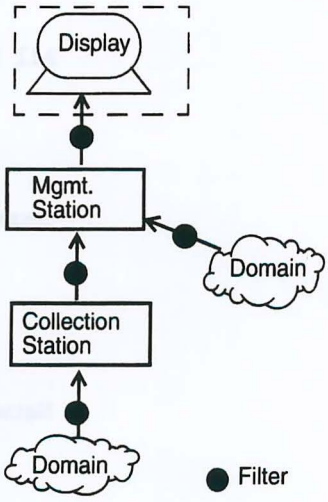
     ```
     $OV_BIN/ovwsetupclient -u
     ```

  2. Remove the lines that were added to the `/etc` files in the previous Server Configuration and Client Configuration sections.
- On Windows systems:
  1. Reinstall NNM from the installation CD.

Configuring On-Demand Submaps

This section discusses how to:

- Configure on-demand submaps.
- Specify a persistence filter.
- Integrate applications with on-demand submaps.



Configuring Demand Level

You can set the demand level of maps as you create them or after you have already created the map. You can set the submap demand level using the `-D` option on the `ipmap` command or using the `IP Map Configuration` dialog box. See the reference page in NNM online help (or manpage on UNIX systems) for *ipmap* for information setting the demand level using the command line.

To set the demand level as you are creating the map, use the following procedure:

1. Select `Map:New...` from the menu bar; the `New Map` wizard (dialog box on UNIX systems) appears.
2. Select `IP Map` from the `Configurable Applications` list. Figure 4-1 illustrates the list under the Windows operating system.
3. Click `[Configure For This Map...]`; the `IP Map Configuration` dialog box differs according to the operating system, as shown in Figure 4-2 and Figure 4-3.
4. On UNIX systems, in the `IP Map Configuration` dialog box, use the scroll bar in the top pane to scroll down to the `------ On-Demand Specification -----` section of the pane.
5. Use the option button under the question "`To what level should submaps be persistent?`" to specify the demand level. You can specify one of the following:

RQS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 0391
3740
Doc:

`Unset`

Resets the demand level to the platform default. On systems running the Windows operating system, this is `Internet Level`. On UNIX systems, it is `All Levels`.

`All Levels`

Specifies all submaps as persistent. This is the same as specifying level 1 when using the `ipmap -D` command.

`Segment Level and Higher`

Specifies that segment, network, and Internet level submaps are persistent. This is the same as specifying level 2 when using the `ipmap -D` command.

`Network Level and Higher`

Specifies that network and Internet level submaps are persistent. This is the same as specifying level 3 when using the `ipmap -D` command.

`Internet Level`

Specifies that Internet level submaps are persistent. This is the same as specifying level 4 when using the `ipmap -D` command.

6. Click `[Verify]` to verify that the values are valid.
7. Click `[OK]` to close the `IP Map Configuration` dialog box.
8. On systems running the Windows operating system, click `[Next]` to continue filling in the wizard windows. On UNIX systems, click `[OK]` from the `New Map` dialog box after you have completed the required fields.

You can use the `Map:Properties` menu from the menu bar to change the demand level after the map has already been created.

Click the `[Applications]` tab in the `Map:Properties` dialog box on systems running the Windows operating system. Using the `Map Properties` dialog box, follow the above procedure for setting the demand level of a new map. You must have read-write access to the map in order to change its demand level.

Refer to "On-Demand Submaps" on page 64 for more information about the on-demand submap feature.

Figure 4-1 **Windows Map Properties Property Sheet, Applications Tab**

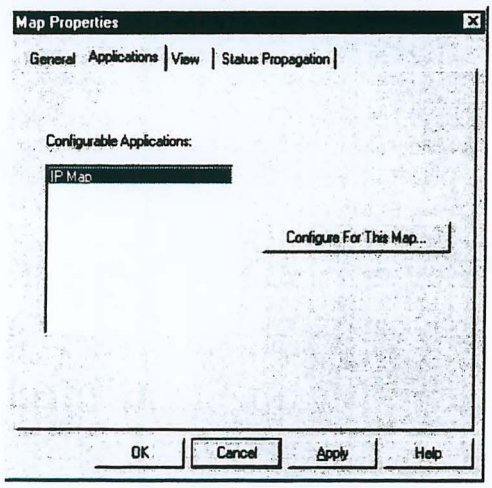
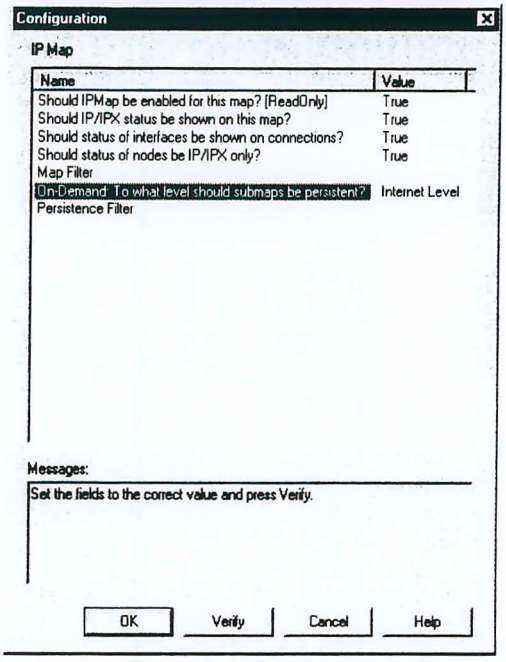


Figure 4-2 **Windows Map Configuration Dialog Box**



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0392
Doc. 13740

4. Click [Configure For This Map...]; the IP Map Configuration dialog box appears, as shown in Figure 4-2 and Figure 4-3.
5. On Windows systems, select Persistence Filter. The Persistence Filter dialog box opens.

   On UNIX systems, in the IP Map Configuration dialog box, use the scroll bar in the top pane to scroll down to the ------ On-Demand Specification----- section of the pane.
6. In the Persistence Filter text field, enter a filter name or expression.
7. Click [Verify] to verify that the values are valid.
8. Click [OK] to close the IP Map Configuration dialog box.
9. On Windows systems, click [Next] to continue filling in the wizard windows.

   On UNIX systems, click [OK] from the New Map dialog box after you have completed the required fields.

You can use Map:Properties from the menu bar to change the persistence filter after the map has already been created.

Using [Applications] tab in the Map:Properties dialog box, as shown in Figure 4-1 on page 123, (or the Map Description dialog box on UNIX systems), follow the above procedure for setting the persistence filter of a new map. You must have read-write access to the map in order to specify a persistence filter.

Refer to "Persistence Filtering" on page 68 for more information about persistence filters.

Integrating Applications With On-Demand Submaps

Before integrating a new application with NNM, you should have a good understanding of how your application works so your application can produce the same results whether you are using the on-demand submap feature of NNM or not. This may require a persistence filter to use when on-demand submaps are enabled.

For example, if your application adds a hub symbol to a segment submap and needs the status of the hubs to propagate up the submap hierarchy, then you need to specify a persistence filter.

RQS nº 03/2005 - CN - CPMI - CORREIOS 0393 Fls: Nº 3740 Doc:

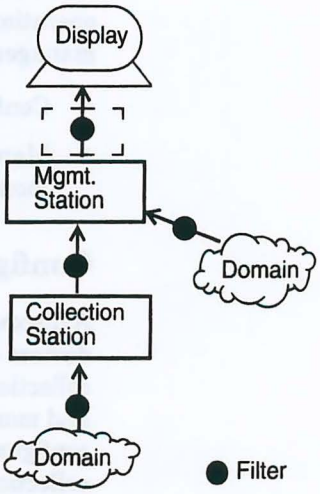
Another example of when a persistence filter is needed is if your application, at start-up, queries the map for all objects of a certain type and performs an operation for each of those objects found. Your application needs to ensure that the objects of this type are on the map by including a persistence filter that specifies this object type.

Use the following procedure to create and specify a persistence filter.

1. Determine what objects your application requires in the map.
2. Start your application running on NNM.
3. Select an object that your application has added and that you want to remain persistent in the submap.
4. Select `Edit:Object Properties` from the menu bar.
5. From the `Object Description` dialog box, view the object attributes for `Capabilities`.
6. Determine which capabilities are unique to that object type, for example, which are set to true.
7. With this information you can create a filter that will allow this object type to pass through.
8. Follow the steps for configuring the demand level and specifying a persistence filter.

Configuring a Map Filter

A map filter allows the operator to display only the objects of interest to that operator. Objects that are rejected by a map filter remain in the management station's topology database and are still subject to status polling. Use the following procedure to configure a map filter on a management station:



1. Create a filter in the file *install_dir*\conf\C\filters (`$OV_CONF/$LANG/filters` on UNIX systems). You can either use a predefined filter or create a new filter. Refer to Appendix A, "The Filter Definition Language," on page 167 for information on filters.
2. On systems running the Windows operating system, select the `Applications` tab in the `Map:Properties` dialog box.

   On UNIX systems, select `Map:Properties` from the menu bar. The `Map Description` dialog box appears.
3. Select `IP Map` from the `Configurable Applications` list and click `[Configure For This Map]`. The `IP Map Configuration` dialog box appears, as shown in Figure 4-2 on page 123 (Figure 4-3 for UNIX systems).
4. You must have read/write rights to the current map.

   On systems running the Windows operating system, select `Map Filter`, and enter the filter name.

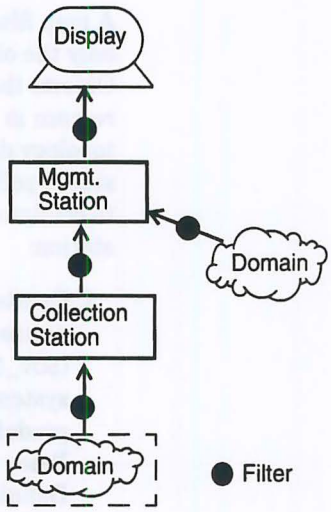
   On UNIX systems, enter the filter name that you created in the text box under `Map Filter`.
5. Click `[Verify]` to make sure the filter name or expression you specified is a valid filter.
6. Click `[OK]` to save the changes and close the dialog box.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0394
3740
Doc:

Configuring Data Collection for a Station

This section describes how to perform operations required on all collection and management stations:

- Configure a discovery filter.
- Manage and unmanage a locally monitored object.



Configuring a Discovery Filter

A discovery filter reduces the number of devices a management station or collection station is actively discovering and monitoring. A discovery filter can be configured on a management station or a collection station. Use the following procedure to configure a discovery filter:

1. Create a filter in the file *install_dir*\conf\C\filters ($OV_CONF/$LANG/filters on UNIX systems). You can either use a predefined filter or create a new filter. Refer to Appendix A, "The Filter Definition Language," on page 167 for information on filters.
2. Select Options:Network Polling Configuration:IP/IPX (Options:Network Polling Configuration:IP on UNIX systems) from the menu bar. The dialog box tabs under the Windows operating system are shown in Figure 4-4, Figure 4-5, and Figure 4-6. The Network Polling Configuration dialog box for UNIX systems appears as shown in Figure 4-7.
3. Make sure the Discover New Nodes option button is on in the IP and IPX tabs, as needed. (There is no IPX on UNIX systems.)
4. On Windows systems, click the [Use Filter] option button on the [General] tab and choose a filter from the list box.

   On UNIX systems, click the Use Discovery Filter option button to the on position. The corresponding text box will ungray.
5. Enter the filter name as defined in the filters file into this text box.

6. Click [OK] to save the changes and close the dialog box.

The discovery filter will be applied to all newly discovered objects. Polling is still done on all previously discovered objects whether or not they would have passed the filter.

To apply the filter to previously discovered objects you need to perform the following steps (from a command window on the Windows operating system):

1. Stop netmon by typing

   ovstop netmon

2. Once netmon is stopped, execute the following command:

   ovtopofix -f *filtername*

3. Then start netmon by typing:

   ovstart netmon

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0395
Doc:

Figure 4-4 Windows Network Polling Configuration, General Tab

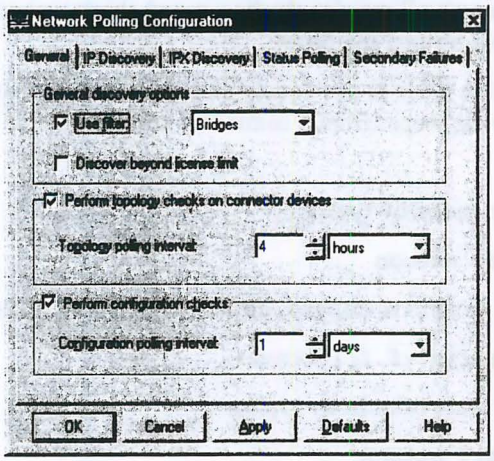


Figure 4-5 Windows Network Polling Configuration, IP Discovery Tab

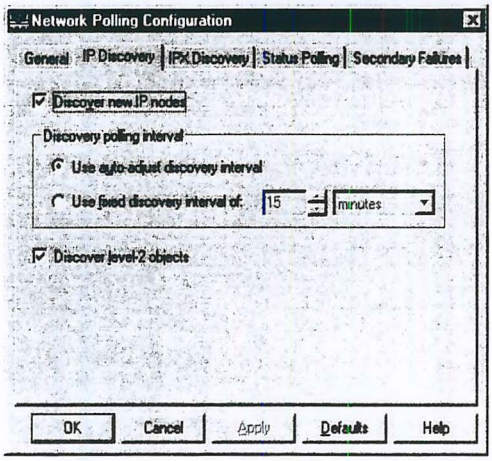


Figure 4-6 Windows Network Polling Configuration, IPX Discovery Tab

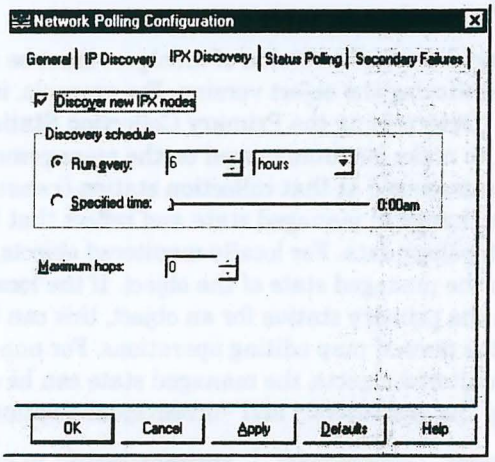
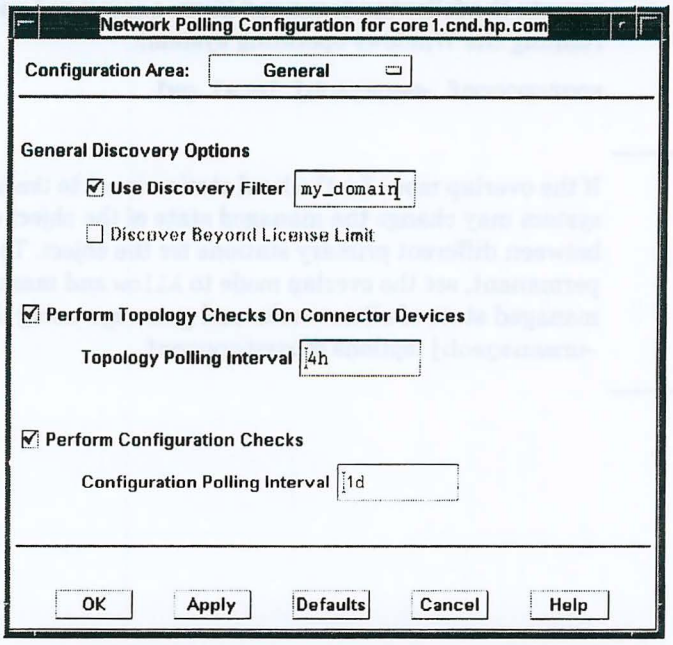


Figure 4-7 UNIX System Network Polling Configuration Dialog Box



FRQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0396
3740
Doc:

Managing and Unmanaging Locally Monitored Objects

The managed state of a version of an object must be set on the collection station monitoring the object version. For example, in the examples shown in "Determining the Primary Collection Station for an Object" on page 150, to make `gw1` unmanaged on the management station, the node must be unmanaged at that collection station (`remstn1`). `remstn1` will detect the change in managed state and reflect that in the management station's topology data. For locally monitored objects, it may be desirable to change the managed state of the object. If the local management station is the primary station for an object, this can be accomplished through the normal map editing operations. For non-primary versions of locally monitored objects, the managed state can be changed by specifying the `-manageobj` and `-unmanageobj` options of `xnmtopoconf`:

`xnmtopoconf [-manageobj | -unmanageobj]` *`station object`*

For example, to manage the locally monitored version of node `gw1` execute the following command (from a command window on systems running the Windows operating system):

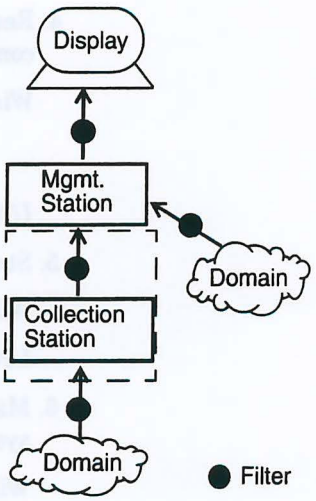
```
xnmtopoconf -manageobj local gw1
```

NOTE If the overlap mode for the local station is set to `Unmanage` or `Delete`, the system may change the managed state of the object during a transition between different primary stations for the object. To make your changes permanent, set the overlap mode to `Allow` and manually set the managed state of all networks and gateways using the `-manageobj` and `-unmanageobj` options of `xnmtopoconf`.

Configuring Collection Stations

This section describes how to:

- Configure security for a collection station.
- Configure a topology filter for a collection station.
- Change the topology filter a collection station.
- Configure a Windowsoperating system IPX collection station.



Configuring Security for a Collection Station

On the collection station, you need to configure SNMP security to allow the exporting of topology information. Use the following procedure to do this (on UNIX systems, you must be `root` to execute this procedure).

1. Make sure NNM is not running. If NNM is running,

   Windows Stop all NNM services by clicking the `NNM Services - Stop` icon.

   UNIX Exit all sessions and issue the command **`ovstop`**

2. Make sure the SNMP master agent is not running by executing the following command:

   Windows Stop `SNMP EMANATE Adapter for Windows` and `SNMP EMANATE Master Agent` using the `Control Panel Services` applet.

   UNIX **`/usr/sbin/snmpd -k`**

3. Edit the set community name line in the *`install_dir`*`\conf\SnmpAgent\snmpd.conf` (`/etc/SnmpAgent.d/snmpd.conf` on UNIX systems) file to read as follows:

RQS nº 133/2005 - CN - CPMI - CORREIOS
Fls. Nº 0397
3740
Doc:

`set-community-name: name #enter community name`

where, *name* is the community name of your choice. By default, NNM does not install a default set community name. You must set this value before attempting to manage a station.

4. Restart the SNMP master agent by executing the following commands:

   Windows Restart `SNMP Emanate Adaptor` and `SNMP Emanate Master Agent` using the `Control Panel Services` applet.

   UNIX **`/usr/sbin/snmpd`**

5. Start NNM by executing the following command:

   Windows Click the `NNM Services - Start` icon.

   UNIX **`ovstart -v`**

6. Make sure the `ovtopmd` service (background process on UNIX systems) is running by executing the following command:

   Windows Click the `NNM Status` icon.

   UNIX **`ovstatus ovtopmd`**

Configuring a Topology Filter for a Collection Station

A topology filter at a collection station defines the subset of topology data that management stations can access. For more information, see "Topology Filtering" on page 41. Use the following procedure to configure a topology filter on a collection station:

1. Create a filter for the *install_dir*`\conf\C\filters` (`$OV_CONF/$LANG/filters` on UNIX systems) file. You can either use a predefined filter or create a new filter. Refer to Appendix A, "The Filter Definition Language," on page 167 for information on filters.
2. Make sure NNM is not running. If NNM is running, exit all sessions and issue the following command:

   Windows Click the `NNM Services - Stop` icon.

   UNIX **`ovstop`**

3. Edit the `vtopmd.lrf` file to include the `-f` option followed by the desired filter name or filter expression name. For example,

```
ovtopmd:ovtopmd:
OVs_YES_START:pmd,ovwdb:0 -f Routers: OVs_WELL_BEHAVED:15:
```

where, `Routers` is a predefined filter contained in the standard filter definition file.

4. Reconfigure `ovtopmd` by executing the following command (from a command window on systems running the Windows operating system):

`ovaddobj ovtopmd.lrf`

5. Start the NNM services by executing the following command:

Windows Click the `NNM Services - Start` icon.

UNIX **`ovstart -v`**

The start-up of NNM may take a little longer the first time, to adjust for `ovtopmd` to apply the filter to the existing topology database.

Only information that passes the topology filter is passed on to the management station. Existing information on the management station that does not pass the newly-configured filter will be removed from the management station's topology database.

Changing the Topology Filter for a Collection Station

You can change the topology filter for a collection without stopping NNM using the following procedure.

1. Create a filter for the *install_dir*`\conf\C\filters` (`$OV_CONF/$LANG/filters` on UNIX systems) file. You can either use a predefined filter or create a new filter. Refer to Appendix A, "The Filter Definition Language," on page 167 for information on filters.

2. Execute the following command (from a command window on systems running Windows):

`ovtopmd -f` *`filtername`*

where filtername is the new filter that you want to apply to the database. This command sends an event that tells `ovtopmd` to apply the new filter to the topology database.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0398
3740
Doc:

To remove the topology filter, execute the following command (from a command window on systems running Windows):

```
ovtopmd -f ""
```

NOTE To make the filter application permanent, perform steps 3 and 4 from the "Configuring a Topology Filter for a Collection Station" on page 134.

Configuring IPX on a Collection Station under Windows

If you want to prevent IPX information from being passed to the NNM management station, do one of the following:

- During installation of the NNM collection station, disable IPX discovery. The following procedure prevents IPX discovery from occurring on the collection station.

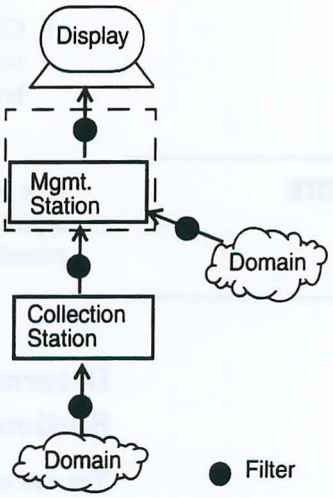
  1. Choose the `Custom Installation` option, and disable the automatic starting of network discovery.
  2. Once installation is complete, start the NNM user interface.
  3. Select the `Options:Network Polling Configuration:IP/IPX` menu item.
  4. From the `[IPX Discovery]` tab, click on the `[Discover New Nodes]` button to disable IPX discovery.
  5. Start the IP discovery services using the `NNM Services - Start` icon in the `HP OpenView` program group.

- If you want IPX discovery enabled on the NNM collection station, proceed with a normal installation. After the system is installed, configure the `IPOnlyObjects` filter as a topology filter. Refer to "Configuring a Topology Filter for a Collection Station" on page 134 for this information. This prevents any IPX networks or IPX-only objects from being propagated to the management station. However, nodes that are discovered to support both IP and IPX will still contain IPX interfaces, with only a physical address and no IP address.

Configuring Management Stations

This section describes how to:

- Determine if a node is a collection station.
- Determine all objects monitored by a specific collection station.
- Configure a management station to use a specific collection station.
- Unmanage a collection station from a management station.
- Remove a collection station from a management station.
- Configure a remote communication timeout and retry count.
- Perform a full synchronization.



Determining if a Node is a Collection Station

There are several ways to determine what nodes are collection stations.

- The easiest is to use the Station view available from the `Tools:Views->Station` menu, or at this URL: `http://`*`nodename`*`:7510/topology/stationView`, where *nodename* is an NNM management station.
- Alternatively, you can execute the following command (from a command window on systems running a Windows operating system):

  ```
  xnmtopoconf -print
  ```

  This will give you a list of current collection stations and tell you if they are managed or unmanaged. The nodes with a managed status are currently acting as collection stations.
- Finally, you can also use ovw to determine which nodes are acting as collection stations. Use the following procedure:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 0399
3740
Doc:

1. From the menu bar select `Edit:Find->Object By Attribute`. The `Find by Attribute` dialog box appears.
2. In the `Objects Attributes` list, select `isCollectionStationNode`.
3. Click `[Apply]`. The known collection stations will be in the `Located and Highlighted` list in the `Locate Attribute` dialog box.

NOTE It is possible for collection stations to exist without having a node object. For example, when a collection station is being used from a remote location and it is not part of the locally discovered topology.

Determining All Objects Monitored by a Collection Station

You can see all the objects monitored by a given collection station by specifying the `ovtopodump` command with the `-r` and `-C` options together. For example, (from a command window on systems running a Windows operating system)

```
ovtopodump -rRISC stn2
```

If there is both a node and a collection station with the same name, it may be necessary to use the object ID to distinguish the two objects with the `-r` option. Another option is to print all objects and use the `grep` command to find the objects from that collection station. For example,

```
ovtopodump -RISC | grep stn2
```

Configuring for a Specific Collection Station

You can configure a management station to connect to a collection station. Use the following procedure to do this (you must be `Administrator` on systems running a Windows operating system or `root` on UNIX systems to execute this procedure):

1. Make sure the NNM services (background processes on UNIX systems) are running:

- On Windows , use the `Control Panel Services` applet to check status. If the NNM services are not running, use the `Control Panel Services` applet to start the services.
- On UNIX, execute the following command:

  `ovstatus`

  If the NNM services are not running, execute the following command:

  `ovstart`

2. Determine what collection stations already exist as described in "Determining if a Node is a Collection Station" on page 137to get a list of current collection stations and see if they are managed or unmanaged. If the collection station you want does not appear, continue to the next step. If the collection station *does* appear, continue with step 4.
3. Add the collection station to the topology by executing the following command:

   `xnmtopoconf -add -unmanage` *`collectionstation`*

TIP When NNM is first started, all the collection stations attempt to report to the management station at the same time, slowing down the system. Unmanage them and bring them on one at a time.

This same command is used for the floating host name of a Service Guard cluster on UNIX systems. As part of your Service Guard configuration process, you updated the `ov.conf` configuration file `HOSTNAME= parameter`. Refer to the *ov.conf* reference page in NNM online help (or manpage on UNIX systems) for more information.

4. Configure the `set` community name to be used when communicating with the collection station by selecting `Options:SNMP Configuration` from the menu bar. This displays the `SNMP Configuration` dialog box.
5. In the "`Specific Nodes`" tab (`SNMP Parameters` pane of the dialog box on UNIX systems), specify in the `Set Community` text field the same set community name that you configured on the collection station.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0400
3740
Doc:

6. Click [OK] to close the SNMP Configuration dialog box.
7. To make sure the collection station is configured correctly, execute the following command (from a command window on systems running a Windows operating system):

   xnmtopoconf -test *collectionstation*

   If you see SNMP errors or timeouts reported, refer to "Troubleshooting Collection Station Communication" on page 147 for more information.
8. Manage the collection station by executing the following command:

   xnmtopoconf -manage *collectionstation*

   This causes the management station to start monitoring and synchronizing with the remote collection station. As part of this, the management station will be added to the collection station's internal list of interested managers. This internal list is referred to as %REMOTE_MANAGERS_LIST% in various places in the interface, such as the event configuration system, when forwarding is being configured.

Unmanaging a Collection Station

To unmanage a collection station from a management station, execute the following command (as Administrator on systems running a Windows operating system or root on UNIX systems) from the management station (from a command window on systems running a Windows operating system):

xnmtopoconf -unmanage *collectionstation*

This removes the management station from the list of active management stations (%REMOTE_MANAGERS_LIST%) for this collection station. The collection station however remains in the management station's database. This command may take a few minutes to complete. All objects for which the collection station is the primary collection station are either assigned a new primary collection station or have their status set to unknown.

Since new primary collection stations are being assigned, this command may take some time to complete.

Removing a Collection Station from a Management Station

Determine what collection stations already exist as described in "Determining if a Node is a Collection Station" on page 137to get a list of current collection stations and see if they are managed or unmanaged.

To remove a collection station from the management station's database, execute the following command (as `Administrator` on systems running a Windows operating system or `root` on UNIX systems) from the management station (from a command window on systems running a Windows operating system):

xnmtopoconf -delete *collectionstation*

This will remove all the symbols representing the collection station objects from the maps on the management station. When a collection station is deleted, a new primary is picked automatically. If none exists, the node is deleted from the management station.

This command may take some time to complete since all data reported from that collection station is removed. If you will be using this data in the future, you may want to unmanage the collection station instead of removing it.

Configuring a Remote Communication Timeout and Retry Count

A WAN link connecting a management station and a collection station will likely have a slow response time and a larger packet loss rate due to congestion. The following procedure will determine the appropriate set of timeouts to use for remote communication.

1. Ping the remote collection station by executing the following command (from a command window on systems running a Windows operating system):

   ping *collectionstation*

   For Solaris, use **ping -s** *collectionstation*.

   After a period of time, stop the ping and note the average round trip time and the packet loss rate.

2. Configure the timeouts and retry count for the remote collection station, based on the behavior received from the ping.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0401
3740
Doc:

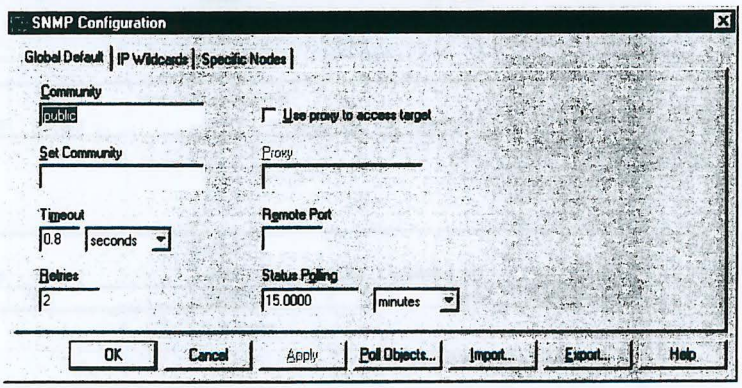
For example, for a reasonable timeout configuration, take the average ping round-trip time, double it, and add a little. For a retry count, the higher the packet loss rate, the more retransmissions you should specify to occur before a failed SNMP request. You should keep a retry count of at least 3.

3. Select `Options:SNMP Configuration` from the menu bar; the `SNMP Configuration` dialog box appears, as shown in Figure 4-8 (Figure 4-9 for UNIX systems).
4. In the `SNMP Parameters` section of the dialog box, specify the timeout configuration in the `Timeout` text box and the retry count in the `Retry Count` text box.
5. Click `[OK]` to save the changes and close the dialog box.
6. Verify communication with the remote collection station by executing the following command (from a command window on systems running a Windows operating system):

   xnmtopoconf -test *collectionstation*

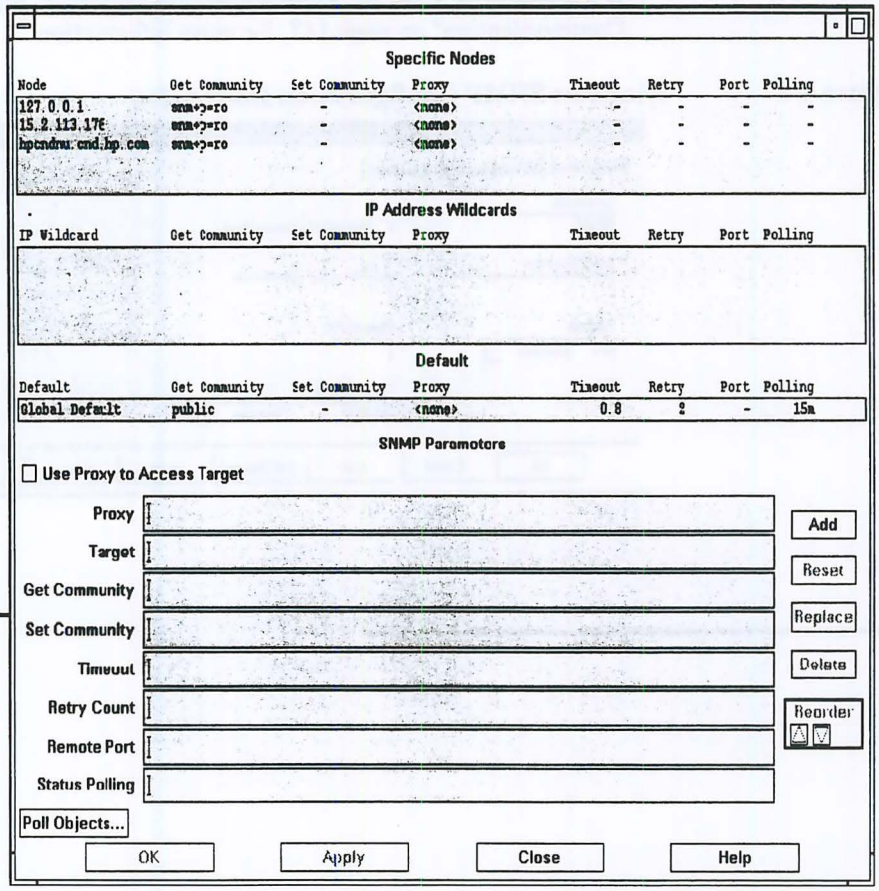
If the test fails, refer to "Troubleshooting Collection Station Communication" on page 147, for more information.

Figure 4-8 Windows SNMP Configuration Dialog Box



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0402
Doc: 3740

Figure 4-9 UNIX System SNMP Configuration Dialog Box



Performing a Full Topology Synchronization

A full topology synchronization causes a complete check of every attribute of every object reported by the remote collection station. This includes adding objects that are unknown and deleting objects that are not known at the remote collection station.

Perform a full synchronization by executing the command (from a command window on aWindows operating system):

```
nmdemandpoll -s collectionstation
```

All results and actions taken are reported to the command line. The output consists of the following:

- General processing status. There will be output noting the general flow of the synchronization process as well as general information related to the remote collection station (for example, hostname, port, version).
- Detailed output concerning the processing of all objects, regardless of whether any changes were detected.
- Warnings about objects that have conflicts or other errors in updating the objects in the database.
- Information about objects that no longer exist in the remote site's database and that are being removed from the local topology database.

TIP When resynchronizing peer-to-peer management stations, the simultaneous resynchronization can cause NNM to slow down and fail. Unmanage one until the other has resynchronized, then remanage it to synchronize it.

Identifying Collection Station Communication Problems

You can check the status of a collection station or management station using the NNM Station view.

One way to open an NNM Station view is by using the NNM `Tools:Views->Station` command. For other ways of opening an NNM Station view, see the *Interacting with Views* section of the HP OpenView web online help.

The status color of the local management station indicates whether or not it is responding to NNM status polls. The status color of a collection station indicates whether or not the local management station is receiving data from that remote collection station:

- Tan color: The collection station is unmanaged.
- Green color (management station): The management station operational status is normal.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0403
3740
Doc:

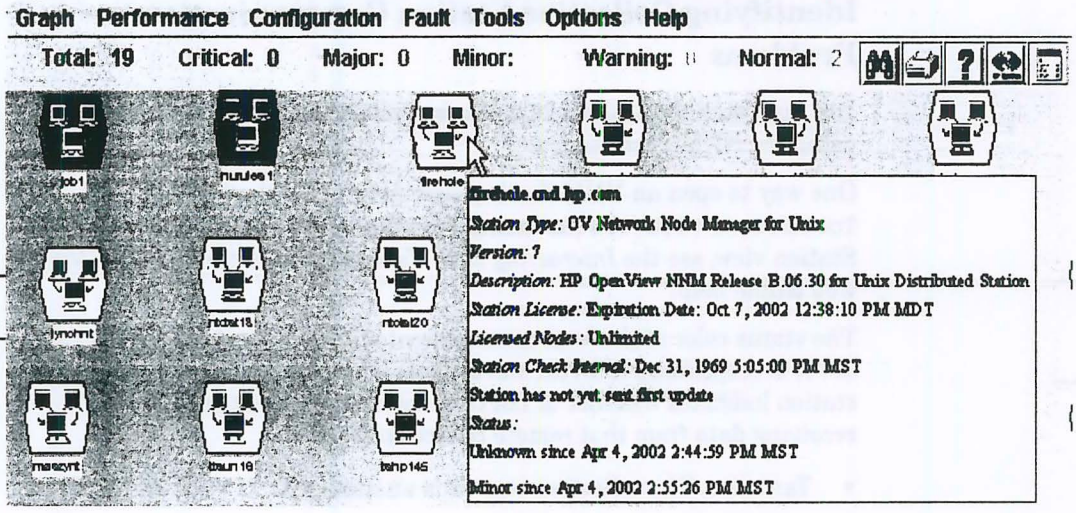
- Other color (management station): The management station operational status is abnormal.
- Green color (collection station): The collection station to management station communication status is normal.
- Other color (collection station): The collection station to management station communication status is abnormal.

In Figure 4-10 on page 146, the NNM Station view shows you that management station `job1` is managing `nurules1`. The status of both collection station `nurules1` and management station `job1` is normal.

However, the communication status of collection station `firehole` recently changed, as shown by the exclamation point, and is now showing an abnormal status color. You need to troubleshoot the communication from collection station `firehole` to management station `nurules1`. See "Troubleshooting Collection Station Communication" on page 147for troubleshooting techniques.

NOTE By resting your mouse pointer over collection station `firehole`, NNM displays some additional information.

Figure 4-10 Station View: Identifying Communication Problems



Troubleshooting Collection Station Communication

To troubleshoot the communication between a management station and a collection station use `xnmtopoconf`, as shown in the following procedure.

1. To determine the status of the managed collection stations, execute the command (from a command window on systems running a Windows operating system):

   `xnmtopoconf -print`

   This will produce a list of managed collection stations and their status as follows:

```
STATION          STATUS    INTERVAL OVERLAP MODE    FAILOVER   FAILOVER FILTER
ab.cnd.hp.com    Unmanaged 5m       AllowOverlap    off        <none>
be.cnd.hp.com    Critical  2m       AllowOverlap    ON         Routers
cat.cnd.hp.com   Unmanaged 5m       AllowOverlap    off        <none>
dog.cnd.hp.com   Normal    5m       AllowOverlap    configured <none>
emu.cnd.hp.com   Critical  5m       AllowOverlap    off        <none>
local            Normal    5m       DeleteSecondary off        <none>
yak.cnd.hp.com   Unmanaged 5m       AllowOverlap    off        <none>
```

   The `STATUS` is determined by the status checks, which are performed, by default, at 5 minute intervals. The `STATUS` can be one of the following values:

`Unmanaged`	The collection station is currently not being monitored.
`Unknown`	The collection station has not yet had a status check. The initial synchronization may be in progress.
`Normal`	The collection station has responded to the most recent status check.
`Warning`	The collection station has not responded to the most recent status check, but it did respond to the status check before that.
`Minor`	The collection station has not responded to two consecutive status checks.
`Major`	The collection station has not responded to three consecutive status checks.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0404
Doc:
3720

`Critical`	The collection station has not responded to four consecutive status checks.

2. If the results of this command produce any collection stations with a status other than unmanaged, unknown, or normal, execute the following command to help determine the problem with this Windows operating system):

   `xnmtopoconf -test` *`collectionstation`*

   For example, executing this command on `hobbes.msr.hp.com` produces output similar to the following:

```
Testing station hobbes.msr.hp.com.
ICMP round trip time = 120 ms.
  Ping test to hobbes.msr.hp.com (15.31.16.141) succeeded.
  Get sysObjectID test failed:
    Error in SNMP reply: No response arrived before timeout
Test for station hobbes.msr.hp.com failed
```

   In this example, the get `sysObjectID` test failed. (Refer to the information below for potential causes.)

   Executing `xnmtopoconf -test` on a collection station with a status other than unmanaged, unknown, or normal can produce one of the following results:

   - `Ping test to the` *`collection station`* `failed:`

     This could be because the node is down or that the SNMP timeout or retry count needs to be increased.

   - `Get sysObjectID test to the` *`collection station`* `failed:`

     This could be because

     — the SNMP agent on the collection station is down.

     — the SNMP timeout or retry count needs to be increased.

     — the get community name is incorrectly configured.

   - `Get topology info test to the` *`collection station`* `failed:`

This could be because

— one or more of the services (background processes on UNIX systems) are not running on the collection station. Run `ovstatus` on the collection station to determine which services are not running. If necessary, run `ovstart` to start the services.

— the get community name is incorrectly configured.

- `Set event forwarding test to the` *`collection station`* `failed:`

  This could be because the set community name is incorrectly configured on either the collection station or the management station.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0405
3740
Doc:

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0406
3740
Doc:

Configuring Domain Overlaps and Failover

This section describes how to:

- Determine the primary station for an object.
- Change the primary station for an object.
- Change the overlap mode.
- Configure collection station failover.

Display

Mgmt. Station

Collection Station

Domain

Domain

Filter

Determining the Primary Collection Station for an Object

To determine the primary collection station for a given object, execute the following command (from a command window on systems running a Windows operating system):

ovtopodump -C *object*

This will print the primary version of the object with the name of the collection station reporting that version. For example, executing

ovtopodump -C gw1

produces the following output:

```
OBJECT ID(S)    OBJECT      STATUS       IP ADDRESS       STATION
146/145          gw1        Normal       10.2.112.1       remstn1
146/145          gw1        Normal       10.2.112.1       remstn1
146/595          gw1        Normal       10.2.104.1       remstn1
146/1158         gw1        Unmanaged    10.2.120.1       remstn1
```

In this example, the object gw1 is a gateway being monitored by the collection station remstn1.

You can see which collections stations are monitoring an object by using the -RISC option of ovtopodump. For example, executing

ovtopodump -RISC gw1

produces the following output:

```
OBJECT ID(S)    OBJECT      STATUS      IP ADDRESS      STATION
146              gw1        Normal      10.2.104.1      remstn1
146/145          gw1        Normal      10.2.112.1      remstn1
146/595          gw1        Normal      10.2.104.1      remstn1
146/1158         gw1        Normal      10.2.120.1      remstn1
146             &gw1        Unmanaged   10.2.104.1      local
146/145         &gw1        Unmanaged   10.2.112.1      local
146/595         &gw1        Unmanaged   10.2.104.1      local
146/1158        &gw1        Unmanaged   10.2.120.1      local
146             &gw1        Unknown     10.2.104.1      stn2
146/145         &gw1        Unknown     10.2.112.1      stn2
146/595         &gw1        Unknown     10.2.104.1      stn2
146/1158        &gw1        Unknown     10.2.120.1      stn2
```

In the second example, the node `gw1` has the collection station `remstn1` as its primary station, but is also known to be monitored by `stn2` and by the local management station. (The special station name `local` is used to represent locally monitored objects.) The "`&`" symbol designates the secondary versions of the objects. (Meanings of other symbols in this location are documented in the *ovtopodump* reference page in NNM online help (or manpage on UNIX systems)).

Changing the Primary Collection Station for an Object

The system will choose a primary collection station for an object, based on the rules as described in "The Selection of Primary and Secondary Collection Stations" on page 53. This choice should be adequate for most purposes. However, you can explicitly override the choice of primary by specifying the `-primary` option to the `xnmtopoconf` command. For example, executing the following command makes the designated collection station the primary for the listed objects. This requires `root` access on UNIX systems or `Administrator` privileges on systems running a Windows operating system.

`xnmtopoconf -primary` *`collectionstation object`*

For example, if it was desired that `stn2` be the primary for `gw1`, the following command could be executed (from a command window on systems running a Windows operating system):

```
xnmtopoconf -primary stn2 gw1
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0407
3740
Doc:

This temporarily overrides the system's choice of primary. If something changes to affect the choice of primary according to the described rules, the system will change to a new primary. The choice can be made stronger by specifying the `-preferred` option of `xnmtopoconf`. For example, execute the following command (from a command window on systems running a Windows operating system):

```
xnmtopoconf -preferred -primary stn2 gw1
```

to mark the version from `stn2` as the preferred choice for the primary collection station for this object. So long as `stn2` is managed and in a noncritical state it will be the primary collection station for `gw1`. You can clear the preference by specifying the `-clearPreferred` option (from a command window on systems running a Windows operating system):

```
xnmtopoconf -clearPreferred stn2 gw1
```

Changing the Overlap Mode

The overlap mode determines how the system behaves when an overlap is detected between the local management station and a remote collection station. The overlap mode applies to the collection station from the management station's perspective. The overlap mode is applied when an object is made a secondary to another remotely monitored version of the object. (See "Overlaps with the Collection Domain of the Management Station" on page 55 for a complete description.) To change the overlap mode use the `-overlap` option of `xnmtopoconf` (from a command window on systems running a Windows operating system):

```
xnmtopoconf -overlap mode local
```

where *mode* can be one of the following:

- `Allow Secondary Local Objects`
- `Unmanage Secondary Local Objects`
- `Delete Secondary Local Objects` (default)

The mode applies to all monitored objects for the local management station that are made secondaries for other remotely monitored objects. The mode cannot be changed on an individual object basis.

Collection Station Failover

Collection station failover allows a management station to pick up status polling responsibility for a collection station that fails. To enable failover (from a command window on systems running a Windows operating system):

xnmtopoconf -failover *stationlist*

The station or stations in the *stationlist* will have status polling automatically taken over when the collection station is downgraded to critical. See the *xnmtopoconf* reference page in NNM online help (or manpage on UNIX systems) for details. If the collection station is currently critical, `-failover` causes the management station to take over status polling immediately.

To disable failover, use xnmtopo -f

Failover Filters

To specify which objects from th lle gy to include in status polling, specify a failov ilt om a command window on systems ru ng ng system):

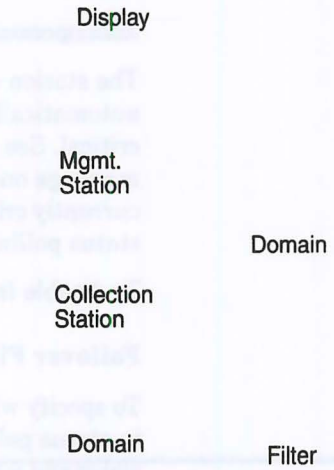
xnmtopoconf -failoverFilte fil

A new or changed filter is applie t with the collection stations in the *static* st tion is not failed over, the filter will be appl th owever if the objects from a station are alread ile management station releases the objects asso ed ation(s) and then reloads the collection station topology and applies the new filter as it loads the topology.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0408
3740
Doc: 93

Configuring Event Forwarding and Correlation

You can configure the event system to forward events to multiple management stations. You can forward an event to remote managers that are using your station as a collection station, other management hosts, or a combination of these. Forwarding events provides distribution of events for the SNMP data collector and for distributed internet discovery and monitoring.



NOTE When forwarding threshold events, be sure that you forward the corresponding rearm event. See the *Managing Your Network with HP OpenView Network Node Manager* manual for information on configuring threshold and rearm events.

Forwarding an Event

You can modify events to have them forwarded to multiple management stations. When you create a new event, you can specify to have that event forwarded. HP recommends that you use multiple varbinds with individual pieces of data rather than using a full string. This allows the receiving application to specify the formatting. This procedure explains how to modify an event.

1. Select Options:Event Configuration from the menu bar; the Event Configuration window appears. From the command line, you may run xnmtrap.

2. Select an enterprise from the `Enterprise list` (the `Enterprise Identification` pane on UNIX systems).
3. Select an event that you want to forward from the `Event Identification` pane.
4. On Windows systems, select `Edit:Events->Modify Event` from the menu bar in the `Event Configuration` window; the `Modify Events` dialog box appears. See Figure 4-11.

   On UNIX systems, select `Edit:Modify Event` from the menu bar in the `Event Configuration` window; the `Event Configurator/Modify Event` dialog box appears. Figure 4-12 shows the `Event Configurator/Modify Event` dialog box.
5. On Windows systems, click the `[Forwarding]` tab.

   On UNIX systems, click on the `Forward Event` check box to expand the dialog box to display the `Forwarded Event Destinations` pane.
6. Complete the `Forwarded Event Destinations` pane (`[Forwarding]` tab) by specifying the destinations to forward the events to.

   You can add destinations in the following ways:

   - Clicking `[Remote Mgrs]` to add all remote management stations to the `Forwarded Event Destinations` list. The remote ons are specified in a list indicated by the special string `%REMOTE_MANAGERS_LIST%`. This list is created automatically as systems are defined to be collection stations.
   - Clicking `[Add From Map]` to add the destinations that are p.

   NOTE Even though the `%REMOTE_MANAGERS_LIST%` string exists, the actual file (*`install_dir`*`\bin\databases\remoteMgrs` on stations running a Windows operating system, `$OV_DB/remoteMgrs` on UNIX systems) may not exist, or may not contain the remote management stations you expect. You can verify the contents of the `remoteMgrs` file using a text editor.

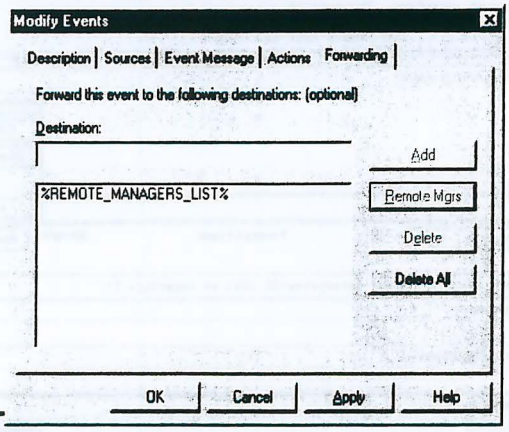
   - Typing the destination in the `Destination` text box and clicking `[Add]`. The destination you specify can be a file containing a list of destinations, a hostname, or an Internet address.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0409
3740
Doc:

7. Click `[OK]` from the `Modify Events` dialog box.
8. Click `File:Save` from the `Event Configuration` window to save the changes.

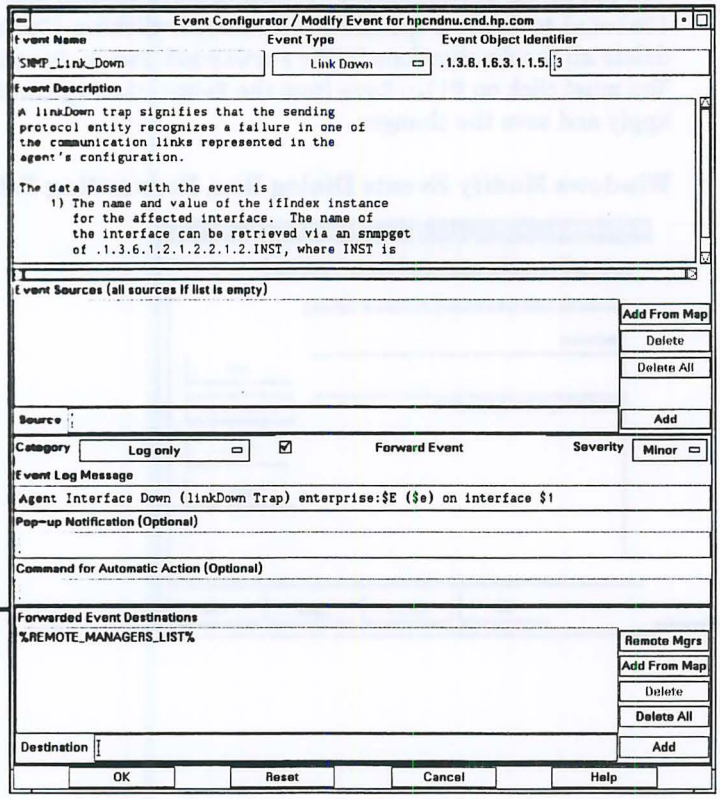
You can delete destinations by selecting a destination and clicking `[Delete]` to delete a specific destination, or clicking `[Delete All]` to delete all the destinations in the `Forwarded Event Destinations` list. You must click on `File:Save` from the `Event Configuration` window to apply and save the changes.

Figure 4-11 Windows Modify Events Dialog Box, Forwarding Tab



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0410
3740
Doc:

Figure 4-12 UNIX System Event Configuration/Modify Event Dialog Box



Using Distributed Data Collection

This section discusses how to export data from collection stations into a single Relational Database Management System (RDBMS) for report generation. For each collection station, use the following procedure:

1. Use the Network Node Manager data collector tool to collect MIB data. Refer to the *Managing Your Network with HP OpenView Network Node Manager* manual for information on data collection.
2. Determine which data collector files you want to merge into the RDBMS. These files are located in *install_dir*\databases\snmpCollect (`$OV_DB/snmpCollect` on UNIX systems).
3. Use `ftp` or `rcp` to copy the files from the collection station to a temporary data directory on the management station. You should also copy each data file's corresponding description file. The description file is named identically to the data file, except that an exclamation mark (`!`) is appended to the end of the filename. For example,

   ```
   rcp $OV_DB/snmpCollect/ifInOctets.1 clifford:/tmp/collsta5
   rcp $OV_DB/snmpCollect/ifInOctets.1! clifford:/tmp/collsta5
   ```

   copies the data and description files for instance 1 of MIB variable `ifInOctets` to the management station `clifford`.

   Alternately, if the network link between the management station and collection station is of sufficient capacity, you may make the files accessible via NFS.
4. If the file *install_dir*\conf\collectProxyMap (`$OV_CONF/collectProxyMap` on UNIX systems) exists on the collection station, copy it to the management station as well, either in the temporary data directory or another directory.
5. Make sure the temporary directory on the management station has `drwxrwxrwx` permission and that each data file has `-rw-rw-rw` permission.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0411
3740
Doc:

6. On the management station, run the `ovcoltosql` command as `root`, to export the data into the RDBMS. Specify the temporary data directory as the data source by using the `-s` option. For example, (from a command window on systems running a Windows operating system):

   `ovcoltosql -Ro -s /tmp/collsta5`

   This example exports data from the directory `/tmp/collsta5` into an Oracle database.

   If there is a `collectProxyMap` file for the collection station, use the `-p` option of `ovcoltosql` to specify the proxy map file location.

   Refer to the *ovcoltosql* reference page in NNM online help (or manpage on UNIX systems), and to the *Reporting and Data Analysis with HP OpenView Network Node Manager* manual for options that you can specify with this command.

If two or more collection stations collect on the same instance of the same MIB variable on the same node, they are said to have an overlapping collection. If data from an overlapping collection is merged into a single RDBMS, some of the data will not be entered into the RDBMS. `ovcoltosql` exports the data that is more recent than that already in the RDBMS. The collection station from which data is exported first will have data from its overlapping collection entered into the RDBMS, while most, if not all of the overlapping data from the second collection station

NOTE

You can execute `ovcoltosql` on the collection stations themselves to a common RDBMS server, but it is not recommended. This can cause potential performance problems when slow network links are traversed. Also, this approach results in the `topo_id` column of the `snmp_trend_dataset` table, which consists of topology IDs, to be assigned by different collection stations. Hence, the column will be useless for performing SQL joins across topology and trend tables.

Refer to the *Reporting and Data Analysis with HP OpenView Network Node Manager* online manual for information on RDBMS querying and administering operations.

5 Dynamic Views and Distributed Management

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0412
3740
Doc:

This chapter discusses how several NNM dynamic views function when you use them with DIDM. Readers are assumed to have read previous chapters and understand how to configure collection station to management station communication.

Dynamic Views and Distributed Management

Numerous dynamic views are available from NNM. These views present a graphical (or tabular) representation of your network infrastructure.

Management station views of the Neighbor view and Path view will display links to views from collection stations or provide additional information in the following situation:

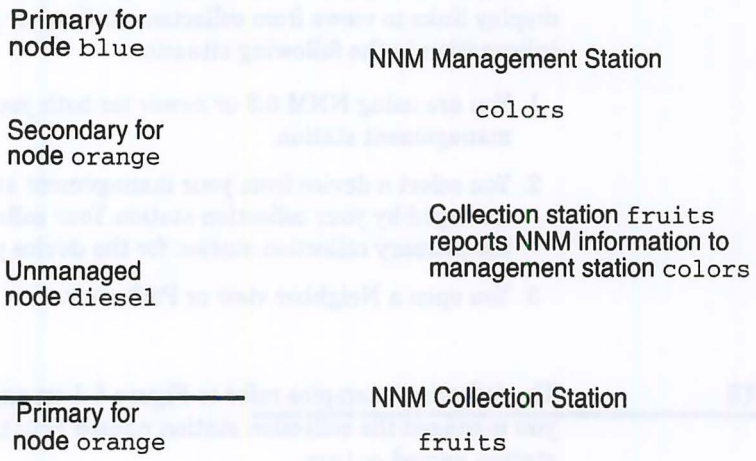
1. You are using NNM 6.3 or newer for both your collection station and management station.
2. You select a device from your management station that is being managed by your collection station.Your collection station must be the primary collection station for the device you select.
3. You open a Neighbor view or Path view.

NOTE The following examples refer to Figure 5-1 on page 164 and assume that you managed the collection station named `fruits` from management station named `colors`.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0413
3740
Doc:

Figure 5-1 shows node `colors` acting as a management station that manages node `blue` and collection station `fruits` within an NNM distributed environment. In this example, collection station `fruits` forwards NNM information to management station `colors`.

Figure 5-1 NNM Dynamic Views: Collection Station to Management Station Communication



NNM Neighbor View

The Neighbor view shows you a graphical representation of the selected device and the connector devices related to it, within a specified number of hops of the selected device.

To open a Neighbor view from NNM, use the `Tools:Views->Neighbor` me wser to htt 0/topology/neighborView.

NOTE Replace *hostname* in the examples with the actual hostname or the IP address of the system NNM is installed on.

A N es the following information in the environment shown in Figure 5-1:

- The management station `colors` is primary for `blue`. If you open a Neighbor view from `colors` with `blue` selected, it does not show nodes that are managed remotely. In this example, `orange` is not in the view, even if it is within the hop distance, because it is remotely managed by `fruits`. The Neighbor view includes a graphical representation of `blue` and other locally managed nodes of `colors`.
- Assume `colors` has a secondary copy of `orange` in its topology database, but that `fruits` is primary for `orange`. If you open a Neighbor view from `colors` with `orange` selected, it does not show nodes that are managed locally. In this example, `blue` is not in the view, even if it is within the hop distance, because it is locally managed by `colors`. The Neighbor view includes a graphical representation of `orange` and other locally managed nodes of `fruits`. This view also provides a link to a Neighbor view from `fruits`.
- If you try to open a Neighbor view of `diesel`, the Neighbor view tells you that `diesel` does not exist in the topology.

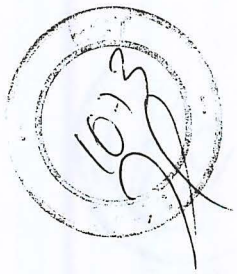
NNM Path View

The Path view presents a graphical representation of the path between two nodes and a table of interface information about the devices contained in the path.

To open a Path view from NNM with Extended Topology, use the `Tools:Views->Path` menu or point your browser to `http://`*`hostname`*`:7510/topology/pathView`.

Refer to Figure 5-1 on page 164. If you open a Path view from `colors` with `blue` as the source node and `orange` as the destination node, NNM displays the Path view, a table of interface information about the devices contained in the path, and tells you that `orange` is managed by `fruits`.

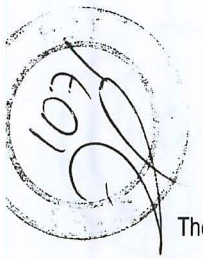
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0414
3740
Doc:



Dynamic Views and Distributed Management

A The Filter Definition Language

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0415
3740
Doc:



This appendix discusses in detail the language used to define filters in the filter definition file, giving you the information you need to modify existing filters, or define new ones.

This appendix is a reference to the contents of the filter definition file, and to the grammar of the filter definition language.

NOTE

This appendix assumes that you are familiar with two topics normally covered in the study of computer science: Boolean expressions and Backus-Naur Form (BNF) grammars. This appendix makes no attempt to teach the fundamentals of either Boolean expressions or BNF grammars. If you are unfamiliar with these topics, you may find it helpful to review these ideas in a computer science text book before you feel entirely comfortable defining new filters.

The Filter Definition File

Filters are defined in an editable file of ASCII characters; this is called the filter definition file. The format and contents of this file make up the subject of this appendix.

The filter definition file for all the filters you use with HP OpenView Network Node Manager (discovery, topology, map, and persistence) is *install_dir*\conf\C\filters on Windows operating systems and $OV_CONF/$LANG/filters on UNIX systems.

After you install NNM, the filter definition file contains a selection of useful definitions that you may be able to use as is, or with some modifications.

The filter definition file has several key components, and they appear in the file in the following order:

- Set definitions.
- Filter definitions, which each include one or more Attribute Value Assertions.
- Filter-Expression definitions, which each refer to one or more filters.

Each of these components is described in considerable detail in later sections of this appendix.

The filter definition file contains many instances of the above elements, always in order. That is, all set definitions are together at the top of the file, all filter definitions follow next, and all filter-expression definitions are at the end of the file.

As you examine the filter and filter-expression definitions in the sample filter definition file ("Default Filter File" on page 197), you will notice that some are intended for use as map filters, others are for discovery filtering. This distinction helps clarify the purpose of each filter and its components, and simplifies your troubleshooting of new or modified filters. Also, remember which types of filters are intended to *exclude* items and which are to *include*. Refer to Table 2-1 on page 38 for more information.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0416
3740
Doc:

Filters and Filter-Expressions

The whole purpose of the filter definition file is to define the filters that are used with the scalability features of NNM. You have two basic types of filters: "simple" filters (which are simple only in that they do not refer to other filters), and filter-expressions.

Filters and filter-expressions are closely related and used identically. Everywhere else, they are referred to broadly as "filters." Within the filter definition file, however, there is a distinction between them:

- A **filter** is a combination (or "expression") of one or more Attribute Value Assertions.[1]
- A **filter-expression** is a combination (or "expression") of one or more previously defined filters. In other words, a filter-expression is a "high- level filter," created by combining lower-level filters that are already defined.

In every other respect, a filter-expression is exactly like a filter. You use filters and filter-expressions in exactly the same way. That is, anywhere a filter can be used, a filter-expression can also be used. Although most of the examples in this section uses filters, filter-expressions would be equally valid in those same examples.

You use logical, also called Boolean, operators (that is, And (`&&`), Or (`||`), and Not (`!`)), and normal precedence grouping via parentheses, to combine multiple filters in a filter-expression, or to combine multiple Attribute Value Assertions (AVAs) in a filter.

Defining filters and filter-expressions has two important rules:

1. A filter definition can include *only* AVAs. A filter definition can *not* include filters or filter-expressions.
2. A filter-expression definition can include *only* filters or filter-expressions that are defined earlier in the filter file. A filter-expression definition can *not* include AVAs.

1. See "Attribute Value Assertions" on page 172 for more details.

Sets

String-valued attributes can be tested for membership in a set. A **set** is simply a list of strings. The only operation available on sets is the test for membership.

You can enumerate the members of a set in two ways:

- Within the filter file itself, according the filter file grammar.[1]
- In a separate file, where set members are listed, one per line. You cannot use wildcards or ranges. If the set member begins with a slash ("/"), it is used as the absolute pathname of such a file. Relative pathnames and environment variables are invalid. In the Windows operating system, filter files must use the forward slash and should include a drive specification.

Files and member strings can be mixed in the same set definition. Set definitions can not be nested.

1. See "Filter File Grammar" on page 187 for details

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0417
3740
Doc:

Attribute Value Assertions

An **attribute value assertion** (**AVA**) is a statement about the value of an attribute. For example, here is an AVA about the `"IP Hostname"` attribute:

```
"IP Hostname" == "server7"
```

An object can be compared against an AVA to determine whether that assertion is true or false for the object. In other words, an AVA is a condition that an object either does or does not meet. When an AVA is tested against a particular object, one of three results can occur:

- The object does not have that attribute.
- The object has the attribute, but the value of the attribute does not match the value in the filter.
- The object has the attribute, and the value of the attribute matches the value in the filter.

The above AVA will be false when the object has an IP hostname attribute, but the IP hostname of the object is *not* "server7". It will *also* be false when the IP hostname attribute is not present in an object.

The above AVA will only be true when the object has an IP hostname attribute, and the IP hostname of the object is "server7". Similarly the AVA `isRouter==TRUE` is only true for routers.

AVAs are defined in terms the of fields of an object and possible values of those fields. The fields used in creating AVAs for filters are a subset of the fields contained in the object database (`ovwdb`).[1]

NOTE Many field names in the object database have embedded white space. Any field name or field value containing white space must be enclosed in double quotes (for example `"Selection Name"`).

In the object database, attributes can have four types:

1. See "Filterable Objects and Attributes" on page 181 for the specific fields you can use in filters.

- Boolean
- Integer
- String
- Enumerated

Attribute value assertions fall into one of these four categories, depending on the attribute type.

After a short section that discusses the operators that are valid in AVAs, AVAs for each of the above types of attributes are covered in more detail.

NOTE Attribute Value Assertions can only be tested against literal constant values. The attributes of two different objects cannot be tested against each other.

Valid Operators for AVAs

These are the operators that you can use to express AVAs:

Operator	Meaning
==	Equal to
!=	Not equal to
>	Greater than
>=	Greater than or equal to
<	Less than
<=	Less than or equal to
~	Like, which used for pattern matching.[1]
!~	Not like, also used for pattern matching.
IN	Is a member of the set

1. See "String AVAs" on page 175 for more information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0418
3740
Doc: 103

TIP Filters are "short-circuit" evaluated. This means NNM only reads far enough to get an answer, then doesn't read the rest of the filter definition. For best performance, put likely TRUE clauses first when OR-in, and put likely FALSE clauses first when AND-ing.

Table A-1, Operators Allowed in AVAs for Each Field Type, shows which of these operators are valid in particular AVAs, depending on the field type of the attribute.

Table A-1 Operators Allowed in AVAs for Each Field Type

Operator	ovwStringValue	ovwEnumValue	ovwIntValue	ovwBooleanValue
==	Yes	Yes	Yes	Yes
!=	Yes	Yes	Yes	Yes
>	Yes	No	Yes	No
>=	Yes	No	Yes	No
<	Yes	No	Yes	No
<=	Yes	No	Yes	No
~	Yes	No	No	No
!~	Yes	No	No	No
IN	Yes[1]	No	No	No

1. Valid only if the value of the expression is the name of a defined set. See "Sets" on page 171 for details.

Boolean AVAs

Boolean AVAs can be expressed with just an attribute name (with an optional, leading `NOT` operator), or can be explicitly tested against the keyword values `TRUE` and `FALSE`. For example, testing for a object being a router can be expressed in either of the two following ways:

```
(isRouter)

(isRouter == TRUE)
```

The inverse expression, testing for a non-router, could be expressed in either of following ways:

```
(! isRouter)
```

```
(isRouter == FALSE)
```

Integer AVAs

Integer AVAs can be tested for equality, inequality, greater than, greater than or equal to, less than, and less than and equal to (==, !=, >, >=, <, <=). For example, to test for a multi-homed node, an expression using an integer AVA might look like this:

```
(numInterfaces > 1)
```

Enumerated (Enum) AVAs

In the object database, enum valued attributes have their enumerated values expressed explicitly. In enumerated AVAs these same enumerated values are used. For example, to test whether an object is from a particular vendor, the following AVA might be used:

```
(vendor == "HP")
```

Enum AVAs can only test for equality or inequality. Because the integer value of a given enum value can change, you must use enum strings in enum AVAs, and not their integer equivalents.

All enumerated values must be delimited (enclosed) in double quotes ("), as in the above example.

String AVAs

String AVAs can be tested using any lexical operator (==, !=, >, >=, <, <=). For example, if you were testing for a particular host, you might use the following AVA:

```
("IP Hostname" == "gomez")
```

Strings are tested using the `strcoll` function, and thus take advantage of any natural language semantics provided by that function.[1]

1. See the manpage on UNIX systems for *strcoll*(3).

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0419
3740
Doc: 104

In addition to standard lexical comparison, extended regular-expression matching (as defined in *regcomp*(3))[1] is also available via the "like" (~) operator. When you use this operator, the string is treated as a `regcomp`-style regular expression, in which certain characters have special meaning.

The AVA below matches *any* hostname with the sub-string "morticia" in it:

```
("IP Hostname" ~ "morticia")
```

while the next AVA (because it tests for "equality" rather than "like", and thus does not use regular-expression matching) matches only and exactly the hostname composed of the string "morticia":

```
("IP Hostname" == "morticia")
```

All regular expressions must be delimited (enclosed) in double quotes (" "), as in the above example.

CAUTION

When negating the "is like" operator (~), place the negation *outside* of the expression. This is necessary due to NNM discovering all level 2 interfaces, including objects like serial cards which have no IP address. When no IP address is present, the object is assigned 0.0.0.0. If you negate the operator, as in `"IP Address" !~ 1.2.3.4`, you will inadvertently *include* all non-IP level 2 interfaces. By negating the `dress" ~ 1.2.3.4)`, you get the set of all objects that *have* an IP address, and it is not like the one in the expression.

NOTE

See the "Caution" block in "Set Specifications in SNMP OIDs" on page 179 before using regular-expression matching with SNMP object identifiers or with IP addresses.

1. See the manpage on UNIX systems for *regcomp*(3).

Specialized Pattern Matching in NNM Filters

There are two special types of string-valued AVAs for which NNM provides specialized pattern matching on the associated attributes:

SNMP Object IDs (SNMP OIDs)	In a filter, an SNMP OID is identified as a leading period followed by decimal octets separated by periods. For example: `.1.3.6.34.2.209`
IP addresses	An IP address is identified as a string of exactly four (4) decimal octets separated by periods, but *without* a leading period: `23.26.11.14`

Three types of specialized pattern matching are available—wildcards, ranges, and sets. Set patterns are available only for SNMP OIDs. You can replace any decimal octet in an IP address or SNMP OID with a special pattern matching string.

NOTE Do not overlook the "Caution" block in "Set Specifications in SNMP OIDs" on page 179.

Wildcard Characters in SNMP OIDs and IP Addresses For IP address and SNMP OID pattern matching, the wildcard operator is the asterisk (*). An asterisk in an IP address indicates that any value is acceptable in the given decimal octet.

For example, to pass any address in the Class A IP network "23", you would use the following in your AVA:

```
"IP Address" ~ 2 3.*.*.*
```

The wildcard character acts slightly differently for SNMP OIDs. In this case, a wildcard indicates that any value *for zero or more* decimal octets is acceptable. For example, the following pattern:

```
.1.4.5.1.*.13.2.*
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0420
3740
Doc:

matches any OID with ".1.4.5.1" followed by any number of decimal octets of any value (including no octets at all), followed by "13.2" followed by zero or more trailing decimal octets. Therefore, the above pattern would match the following OIDs:

- .1.4.5.1.13.2
- .1.4.5.1.22.33.13.2
- .1.4.5.1.13.2.14.55.232
- .1.4.5.1.22.44.33.13.2.23.32.1

but not:

- .1.4.5.1.13 (no 2 after the 13)
- .1.4.5.2.2.13.2 (no 1 after the 5)
- .1.4.5.1.33.22.2 (missing the 13)

Range Specifications in SNMP OIDs and IP Addresses A range is expressed by a decimal integer, a hyphen (-), and another decimal integer that is greater than the first. Decimal octet values between 2 and 68 would be specified as follows:

```
2-68
```

A range indicates that any value in the range (inclusive) is acceptable in the given decimal octet. Ranges are significant for the given decimal octet only, in both SNMP OIDs and IP addresses. The values specified in a range must be in their natural order, from smallest to largest; a reversed range (like, for example, 68-2) is not permitted.

The following are more examples of valid SNMP OIDs and IP address AVAs, using sets, wildcards, and ranges in combinations:

```
("IP Address" ~ 23.2.*.*)
("IP Address" ~ 23.2.3-9.*)
("IP Address" ~ 23.2.16-22.0-1)
("SNMP sysObjectID" ~ .1.3.6.*.9.5)
("SNMP sysObjectID" ~ .1.3.6.8-9.*)
("SNMP sysObjectID" ~ .1.3.6.7-8.12-13)
```

Set Specifications in SNMP OIDs In SNMP OIDs (but not IP addresses), you can specify a set of decimal octets in any position by separating the members by a comma. For example, in the following AVA:

```
("SNMP sysObjectID" ~ .1.3.6.34.8,9,11,23)
```

would match the following SNMP OIDs:

```
("SNMP sysObjectID" ~ .1.3.6.34.8)
("SNMP sysObjectID" ~ .1.3.6.34.9)
("SNMP sysObjectID" ~ .1.3.6.34.11)
("SNMP sysObjectID" ~ .1.3.6.34.23)
```

CAUTION

To invoke special pattern matching on IP address and SNMP OID strings, either the "like" operator (~) or "not like (!~) *must* be used.

Furthermore, to use NNM's specialized pattern matching facility, the IP address or SNMP OID string *must not* be enclosed in quotation marks. The presence of enclosing quotation marks means that the string will be treated as a regular expression, and *not* given specialized pattern matching; the absence of such quotation marks means the comparison *will* use NNM's specialized pattern matching facility.

The difference is important. Consider this AVA, where the value is quoted:

```
"IP Address" ~ "23.18.3.*"
```

With the quotation marks around the value (`"23.18.3.*"`), it is treated as a regular expression. The result is that *many* IP addresses beginning with "`23.18.3`" would cause the AVA to evaluate to `TRUE`, including, for example, `23.18.34.7`, which was probably not intended. In fact, even some strange and improbable IP address strings (like, for example, `23518.3711.1011.23033`) would pass this AVA. The reason is that, for regular expressions, the period character (`.`) matches *any* character in that location of the comparison string (including, confusingly, the period character itself).

However, if we use the same AVA, but *without* the quotation marks around the value (`"IP Address" ~ 23.18.3.*`), NNM's special pattern matching facility guarantees that only IP addresses in the apparently intended range would cause the AVA to evaluate to `TRUE`.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0421
3740
Doc.

Excluding a Node

For the purposes of building and using filters, a node can be thought of as a "super-object", which comprises the node and all its interfaces.

Thus, if a node object passes a filter, the filter will also pass all interfaces of the node regardless of whether they would, considered in isolation, pass the filter.

Similarly, if an interface passes a filter, the node object it belongs to, and all other interfaces of that node, also pass the filter.

Consequently, if you want a filter to exclude a node, the filter must block the node object itself and all of its interfaces.

NOTE Keep in mind that the `ovfiltertest` comm ol is pattern. Instead of treating a node and its i s bject,", the `ovfiltertest` command treats nodes a ate objects. See the *ovfiltertest* reference page i in the UNIX system manpage) for more informati

Relationships Between Nodes a fa

You can create a filter that combines nodes ac vn in the following example.

```
nodeNinterface "" {(vendor = "SUN") && (IP Address ~ 1    }
```

Valid Operators for Logical Combinations of AVAs or Filters

AVAs, filter names, and filter-expression names are combined to create filter and filter-expression definitions (as noted before, *only* AVAs are allowed in a filter definition, and AVAs are *never* allowed in a filter-expression definition).

You use the following operators to create logical combinations (or "expressions") of these components. Likewise, you combine filters or filter-expressions in a filter-expression definition with these operators:

Operator	Meaning
&&	Logical "and", used to combine multiple AVAs and filter names into logical expressions.
||	Logical "or", used to combine multiple AVAs and filter names into logical expressions.
!	Logical negation, used to negate stand-alone field names and other logical expressions. Fields that are already part of an expression cannot be negated; rather the entire expression should be negated.

Use parentheses—"(" and ")"—to specify explicit precedence in a group of operations. For example, a filter definition might look like this:

```
Filtr1 "" { isRouter && (numInterfaces > 1) }
```

Or a filter-expression definition might look like this:

```
FiltrExpr1 "" { (Filtr1 || Filtr2) && Filtr3 }
```

Filterable Objects and Attributes

The following four tables specify, for each type of object, the attributes (fields) for which filters can be defined. This is a subset of the objects and attributes in the ovwdb database.

Table A-2 Filterable Fields in Node Object

Field	Field Type
IP Hostname	String
IP Status	Enumerated
isATM *	Boolean
isBGP4 *	Boolean
isBridge	Boolean
isCDP *	Boolean
isCollectionStationNode	Boolean
isConnector	Boolean
isDS1 *	Boolean

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0422
3740
Doc: 107

Table A-2 Filterable Fields in Node Object (Continued)

Field	Field Type
isDS3 *	Boolean
isFrameRelay *	Boolean
isHSRP *	Boolean
isHub	Boolean
isIP	Boolean
isIPRouter	Boolean
isIPV6 *	Boolean
isIPX	Boolean
isIPXRouter	Boolean
isMcClusterMember	Boolean
isMPLS *	Boolean
isNetWareServer	Boolean
isNode	Boolean
isOSPF *	Boolean
isRMON *	Boolean
isRMON2 *	Boolean
isRouter	Boolean
isSONET *	Boolean
isSNMPSupported	Boolean
isSTP *	Boolean
isVRRP *	Boolean
isWireless *	Boolean
NetWare Server Name	String

Table A-2 Filterable Fields in Node Object (Continued)

Field	Field Type
Selection Name	String
SNMPAgent	Enumerated
SNMP sysContact	String
SNMP sysDescr	String
SNMP sysLocation	String
SNMP sysName	String
SNMP sysObjectID	String
TopM Interface Count	Integer
vendor	Enumerated

IMPORTANT * Fields marked with an asterisk have no effect on discovery filters.

Table A-3 Filterable Fields in Interface Object

Field	Field Type
isInterface	Boolean
isIP	Boolean
isIPX	Boolean
IPX Address	String
IP Address	String
IP Status	Enumerated
IP Subnet Mask	String
Selection Name	String

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0423
3740
Doc:

Table A-3 Filterable Fields in Interface Object

Field	Field Type
SNMP ifDescr	String
SNMP ifName	String
SNMP ifPhysAddr	String
SNMP ifType	Enumerated
TopM Network ID	Integer
TopM Node ID	Integer
TopM Segment ID	Integer

Table A-4 Filterable Fields in Segment Object

Field	Field Type
IP Segment Name	String
IP Status	Enumerated
isBusSegment	Boolean
isFDDIRingSegment	Boolean
isSegment	Boolean
isSerialSegment	Boolean
isStarSegment	Boolean
isTokenRingSegment	Boolean
Selection Name	String
TopM Interface Count	Integer
TopM Network ID	Integer

Table A-5 Filterable Fields in Network Object

Field	Field Type
IP Address	String
IP Network Name	String
IP Status	Enumerated
IP Subnet Mask	String
IPX Address	String
IPX Network Hop Count	Integer
isIP	Boolean
isIPX	Boolean
isNetwork	Boolean
Selection Name	String
TopM Default Seg ID	Integer
TopM Interface Count	Integer
TopM Segment Count	Integer

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0424
3740
Doc.

Valid values for the enumerated fields can be found in the files listed in Table A-6, Value Definitions for Enumerated Fields,

Table A-6 Value Definitions for Enumerated Fields

For the field named:	The enumerated values are defined in:
IP Status	On Windows operating systems: *install_dir*\fields\C\ip_fields On UNIX systems: $OV_FIELDS/$LANG/ip_fields
SNMP ifType	On Windows operating systems: *install_dir*\fields\C\snmp_fields On UNIX systems: $OV_FIELDS/$LANG/snmp_fields
SNMPAgent	On Windows operating systems: *install_dir*\fields\C\snmp_fields On UNIX systems: $OV_FIELDS/$LANG/snmp_fields
vendor	On Windows operating systems: *install_dir*\fields\C\ovw_fields On UNIX systems: $OV_FIELDS/$LANG/ovw_fields

Filter File Grammar

The following is the formal Backus-Naur Form (BNF) grammar for a filter file. See "Filters" on page 37 for details about where such a file is used.

```
Filter_File          ::=   Filters
                           | Filters FilterExprs
                           | Sets Filters
                           | Sets FiltersFilterExprs

Sets                 ::=   "Sets" "{" Set_Stmts"}
                           | "Sets" "{" "}"

Set_Stmts            ::=   Set_Stmt
                           | Set_Stmts Set_Stmt

Set_Stmt             ::=   SetName Description "{" Memberlist"}"

Memberlist           ::=   Member_Stmt
                           | Memberlist "," Member_Stmt

Member_Stmt          ::=   StringOrIdentifier
                           | <absolute_file_pathname>

Filters              ::=   Filters" "{" Filter_Stmts"}"
                           | "Filters" "{" "}"

Filter_Stmts         ::=   Filter_Stmt
                           | Filter_Stmts Filter_Stmt

Filter_Stmt          ::=   FilterName Description "{" Expression"}"

Expression           ::=   Expression "&&" Expression
                           | Expression"||" Expression
                           | "!" Expression
                           | "(" Expression ")""
                           | BoolExpr
                           | SetExpr

BoolExpr             ::=   FieldName
                           | FieldName ExprOperator <string>
                           | FieldName ExprOperator <integer>
                           | FieldName PatternOperator <string>
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0425
3740
Doc:

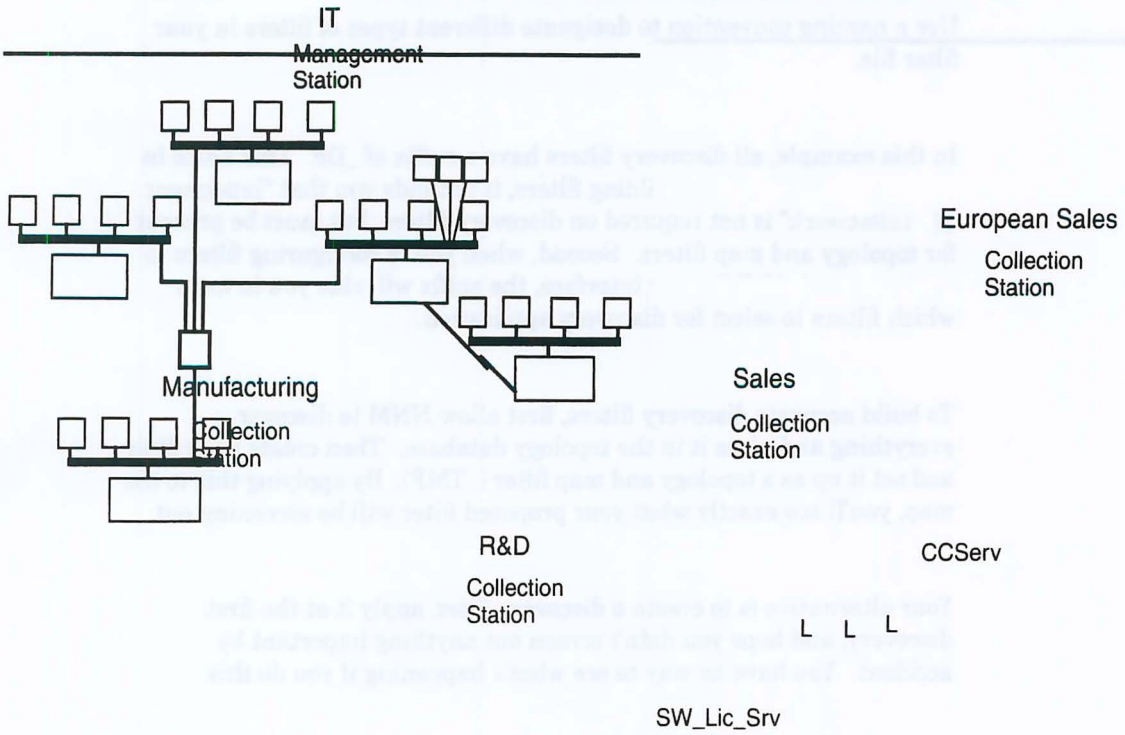
```
SetExpr              ::=    FieldName "IN" SetName

FilterExprs          ::=    "FilterExpressions" "{" FilterExpr_Stmts "}"
                            | "FilterExpressions" "{" "}"

FilterExpr_Stmts     ::=    FilterExpr_Stmt
                            | FilterExpr_Stmts FilterExpr_Stmt

FilterExpr_Stmt      ::=    FilterExprName Description "{" FiltExpr "}"

FiltExpr             ::=  FiltExpr "&&" FiltExpr
                          | FiltExpr "||" FiltExpr
                          | "!" FiltExpr
                          | "(" FiltExpr ")"
                          | FilterName

FieldName            ::=  StringOrIdentifier

ExprOperator         ::=  "==" | "!=" | "<" | "<=" | ">" | ">="

PatternOperator      ::=  "~" | "!~"

FilterExprName       ::= <unquoted_string>

FilterName           ::= <unquoted_string>

SetName              ::= <unquoted_string>

StringOrIdentifier   ::= <quoted_string> | <unquoted_string>

Description            ::=  <quoted_string>
```

Filter File Example

This example describes how these rules translate into usable filters for a sample network management solution. Hemispheres-Petroleum Company has decided to implement HP OpenView Network Node Manager's distribution capabilities to gain control over their overall network. They have a typical network organization that parallels their personnel organization -- local area networks for the Research and Development, Manufacturing, and Sales departments, with an additional network in place in Paris for European Sales. The network architecture is diagrammed in Figure A-1.

The IT department will be responsible for managing these networks, along with their own. They have decided to have a collection station for each department report to the management station in IT.

Figure A-1 Hemispheres-Petroleum Company Network Layout



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0426
3740
Doc:

The default filter file shipped with NNM has several useful building blocks already in place. (The default filter file appears on page 197.) Simple filters appear in the second section of the files, in the format `FilterName "Description" { AVA }`. For example, look at the line that says `Hubs "Any multi-port repeater" { isHub }`. The name of the filter, as it would later be used from the ovw user interface or in building filter expressions, is Hubs. `netmon` compares every node's SNMP response, looking for the `isHub` property. Any object possessing this property fits the filter `Hubs`. Similarly useful simple filters are in place for Networks, Segments, Nodes, IPRouters, Bridges, SNMPNode, HPNodes, and NonHPNodes.

Setting Up Collection Domains

Collection domains are specified through discovery filters. Setting these up demonstrates several tips that will help you manage filters for your network.

TIP Use a naming convention to designate different types of filters in your filter file.

In this example, all discovery filters have a suffix of _DF. This helps in building filters, it reminds you that "`isSegment || isNetwork`" is not required on discovery filters, but must be present for topology and map filters. Second, when you're configuring filters to interface, the suffix will clue you in as to which filters to select for discovery application.

TIP To build accurate discovery filters, first allow NNM to discover everything and place it in the topology database. Then create your filter and set it up as a topology and map filter (_TMF). By applying this to the map, you'll see exactly what your proposed filter will be screening out.

Your alternative is to create a discovery filter, apply it at the first discovery, and hope you didn't screen out anything important by accident. You have no way to see what's happening if you do this.

First set up the collection domain for the IT department's own management station. Using the pattern filter named EngrLan in the default filter file, add a filter named ITLan_DF, which includes the IP address range for IT nodes (15.2.107-117):

```
ITLan_DF "IT's IP subnet" { ("IP Address" ~ 15.2.107-117.*) }
```

Reading that back, the name of the filter is ITLan_DF and can be referred to by filter expressions and user interface fields that ask for a filter name. It passes objects whose IP Address field in their SNMP data is between (is like) 15.2.107.* and 15.2.117.*.

Now build a filter expression (combination of filters) to turn that into a topology and map filter:

```
ITLan_TMF "IT's IP subnet" {("IP Address" ~ 15.2.107-117.*)|| NetsNSegs}
```

The addition of NetsNSegs, a standard NNM filter, passes all objects with SNMP data matching isSegment or isNetwork. A discovery filter includes these by default, but topology and map filters must add them explicitly. Networks and segments are required so that node objects will have containers in which to reside. Without them, your map database becomes corrupted.

Now is the time to use the tip above. First allow NNM to discover everything and place it in the topology database. Then apply the TMF filter to the map using ovtopodump -f, showing exactly what will be screened out.

The IT network management administrator sets up similar filters for SalesLan, MfgLan, RDLan, and ESalesLan. Here is the filter file so far (without all the comment lines):

```
Filters {
Networks "Any network" { isNetwork }
Segments "Any segment" { isSegment }
NetsNSegs "All networks & segments" { isNetwork || isSegment }
Nodes "Any node" { isNode }
IPRouters "Any IP Router" { isIPRouter }
Bridges "Any bridge" { isBridge }
Hubs "Any multi-port repeater" { isHub }
SNMPNode "Any node supporting SNMP" { isNode && isSNMPSupported }
HPNodes "Hewlett-Packard nodes" { isNode && ( vendor == "Hewlett-Packard" ) }
UBNodes "Ungermann-Bass Nodes"  { isNode && vendor == "Ungermann-Bass" }
NonHPNodes "Non-HP nodes" { isNode && ( vendor != "Hewlett-Packard" ) }
ITLan_DF "IT's IP subnet" { ("IP Address" ~ 15.2.107-117."*) }
SalesLan_DF "Sales's IP subnet" { ("IP Address" ~ 15.2.125-140.*) }
MfgLan_DF "Manufacturing's IP subnet" { ("IP Address" ~ 15.2.145-160.*) }
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0427
3740
Doc:

```
RDLan_DF "R&D's IP subnet" { ("IP Address" ~ 15.2.175-250.*) }
ESalesLan_DF "European Sales's IP subnet" { ("IP Address" ~ 192.5.32-50.*) }
}

FilterExpressions {
ITLan_TMF "IT's IP subnet map filter" { ITLan_DF || NetsNSegs }
SalesLan_TMF "Sales's IP subnet map filter" { SalesLan_DF || NetsNSegs }
MfgLan_TMF "Manufacturing's IP subnet map filter" { MfgLan_DF || NetsNSegs }
RDLan_TMF "R&D's IP subnet map filter" { RDLan_DF || NetsNSegs }
ESalesLan_TMF "European Sale's IP subnet map filter" { ESalesLan_DF || NetsNSegs
}
}
```

With these filters, each collection station can specify its own domain of interest with no overlap.

TIP Build your overall filter file once and propagate it from your management station to all the collection stations. Use RCS for version control on the file and `rcp` to copy it to the collection stations. This way you know exactly what each collection station operator is looking at. You retain control over the file contents. And you can see a collection station's view of the network from the management station by applying the collection station's topology filter as a map filter on the management station.

Excluding Nodes

Take another look at the Sales LAN. It includes three laptop computers for sales people who are often on the road. The network operator really doesn't need to track whether those nodes are up or down, so write a DHCP filter that can exclude them:

```
SalesLaptops "Laptop units often offline in Sales
department" {"IP Address" ~ 15.2.135-140.*}
```

Now in a filter expression you can refer to `{SalesLan && !(SalesLaptops)}`. This is rather long, but it allows you to identify those laptops separately sometimes. Certainly, you could use this in a topology filter on the Sales collection station that would disable the status of these nodes being sent to the management station continuously.

1046

You could also have specified `&& !("IP Address" ~ 15.2.135-140.*)` on the overall `SalesLan` filter if you knew you would never want the laptops included.

CAUTION

When negating the "is like" operator (~), place the negation *outside* of the expression. This is necessary due to NNM discovering all level 2 interfaces, including objects like serial cards which have no IP address. When no IP address is present, the object is assigned 0.0.0.0. If you negate the operator, as in `"IP Address" !~ 1.2.3.4`, you will inadvertently *include* all non-IP level 2 interfaces. By negating the expression, as in `!("IP Address" ~ 1.2.3.4)`, you get the set of all objects that *have* an IP address, and it is not like the one in the expression.

Failover Filters

What would happen if the Sales collection station failed? Assuming you have the management station configured for failover, all the nodes that the Sales collection station has in its topology database are polled by the management station. A failover filter would specify only the most critical nodes for which the management station would actually pick up status polling.

Sales is currently a fairly small department, so no filter is needed yet. When the Sales department grows, IT will probably want to limit which ones qualify for management failover.

Important Node Filters

Suppose the hub between the management station and the Sales collection station (actually, all the collection stations in this example) goes down. The management station will log an event that the hub is down, with secondary information that each of the nodes behind the hub is also unreachable. Getting that hub back online is a top priority, and most of the other stations are indeed secondary -- except that credit card authorization server. Access to that server is critical to business and the network operator needs to know about that immediately. By setting up an important node filter, you can assure that this node always qualifies as a primary event in the alarm browser.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0428
3740
Doc:

```
SalesImptNodes "Critical nodes to have primary alarms if
Sales becomes unreachable" { "IP Hostname" == "ccserv" }
```

Similarly, the network management administrator creates important node filters for the other departments and adds them to the file.

Topology Filters

Looking at performance on the management station, IT realizes that they still see every node in the network -- it's as if they had never bothered with collection stations at all. Every bit of information is getting passed right on up to the management station.

Reviewing the Manufacturing LAN, they realize that it contains over 100 actual nodes, mostly PCs automating fabrication processes. At this point, PCs are not critical to your success, but the production servers from which they run their inventory and instruction data are vital. The collection station operator can monitor the availability of the PCs. All you need to monitor at the management station are the servers.

Use the set construct in the filter file to build your topology filter that only forwards information about the servers to the management station.

```
Sets{
MfgServersSet = { "parts", "prefab", "finalfinish",
"inventory" }
}
```

The previous filter expression for Manufacturing was `MfgLan_TMF "Manufacturing's IP subnet map filter" { MfgLan_DF || NetsNSegs }`. You still only want the Manufacturing domain, and you do want all the networks and segments. Use the set of servers to limit what gets forwarded:

```
MfgLan_TMF "Manufacturing's IP subnet map filter"
      { (MfgLan_DF && MfgServersSet) || NetsNSegs }
```

The collection station in Manufacturing uses `MfgLan_DF` to discover all nodes in its domain. The topology database on the collection station contains all these nodes. When the collection station starts to forward information to the management station, it applies `MfgLan_TMF` to the data stream. Only the servers in the `MfgServersSet` and the networks and segments pass the filter and get sent to the management station. The management station's topology database contains only this information and not the rest of the nodes on the Manufacturing LAN.

1044

The network administrator in IT creates similar topology filters to reduce clutter coming in to the management station from the other collection stations.

Map Filters

The management station serves various operators in the IT department. Connie has received extensive training in troubleshooting connector devices, and specializes in them throughout the network. Sergai only cares about the servers for the various departments. Look at each of their map filters.

The filter expression from which Connie works looks like this:

```
Connectors "All connector devices"
      { Bridges || IPRouters || Hubs }
```

But there is a problem. IT's topology filter from Manufac , for example, only passes servers, networks, and segments. T have to modify the topology filter to give you the connector inform first:

```
MfgLan_TMF "Manufacturing's IP subnet map filte
      { (MfgLan_DF && MfgServersSet)
        || Connectors || NetsNSegs }
```

Now Connie needs a map filter which includes NetsNSeg er map database to work:

```
Connectors_MF "All connector devices"
      { Bridges || IPRouters || Hubs || NetsNSe
```

With this map, Connie will see all the connecting devices all the LANs.

Using the Network Presenter

With so many PCs on the site, IT hires Paul to keep them all up and running. But Paul's map on the management station has a problem. It says there are no PCs for him to manage. You have specifically filtered out the PCs before they reach the management station.

You could add all the PCs back in for all the topology filters. Paul would have one view with all the PCs and could do combined trend analysis. However, the management station topology database would get bogged down and everyone would have to filter them back out with their map filters.

RQS nº 03/2005 - SN
CPMI - CORREIOS
Fls. Nº 0429
3740
Doc:

You might think to purchase a separate management station for Paul and set up the collection station topology filters to only send PC information. However, topology filters are defined only once per collection station; a collection station cannot pass different data to different management stations.

As an alternative, Paul can use the Network Presenter through his web browser to act as a console on each of the collection stations. He would have more windows to watch, but network traffic would be minimized. Paul would be able to see the maps, but he would not be able to do any NNM administration through the Network Presenter since it is read-only.

This is an example of the trade-offs your organization will consider during your network management planning phase.

Default Filter File

The following is the default filter file, based on the above grammar:

```
//
// @(#)$OV_CONF/$LANG/filters
// @(#)HP OpenView NNM Pre-Release X.06.20 (Pre-Preview)  Jan 17 2001
// @(#)Copyright (c) 1990-2001 Hewlett-Packard Company
// $Revision: /main/PULSAR/PULSAR_REP/NEPTUNE/4 $  $Date: 2001/01/11 23:58 UTC $
//
// This is the default filter file.  These filters are examples
// which may be useful in your environment.  Feel free to modify this
// file and/or add your own.
// See OVfilterIntro(5) for more information on this file.
//

// Sets are a simple way to list string values to test
// against in a filter.  The "IN" operator tests a field value
// for membership in a set defined here.
//

Sets {

        // These are simple examples of sets.
        //
        // servers "Set of Servers" { "sv1", "sv2", "sv3" }
        // gateways "Backbone gateways " { "gw1", "gw2", "gw3" }
        //
        // sets can include a filename which contains the entries.
        // On Windows, the set file must be on the partition where NNM
        // is installed.

        // routers "Set of Routers" { /openview/conf/routers.set }
}

//
// Filters and FilterExpressions are used as Topology, Discovery,
// Map or Persistence filters.  Applications which use filters
// (like ipmap(1), ovtopmd(1m), ovtopodump(1), and ovtopofix(1m))
// can take the name of a Filter or a FilterExpression.
//

Filters {

        // The following filters are potentially useful as either Discovery
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0430
3740
Doc:

```
// or Topology filters, or components for building Map filters.
//
// NOTES CONCERNING DISCOVERY FILTERS:
// Networks and Segments are not directly testing with Discovery
// filters (and so there is no need to include
// "isNetwork || isSegment" in these filters).
// However, it does not hurt to include networks or segments in
// a discovery filter, so long as you realize that they will not
// be acted on.
//
// Since nodes are only discovered in managed networks, the network
// must already exist and be managed before the filtering test
// will be applied.  New networks connected to discovered nodes will
// be discovered unmanaged.   For discovery filters,
// a node and all its interfaces can be thought of
// as a single object. If any interface or the node itself passes the
// filter, the node and all of its interfaces will pass the filter.
//
// ovtopofix -f follows the discovery filter semantics and only
// applies to locally monitored objects.  However, if a network or
// segment is empty after the processing of the nodes with the -f
// option, that segment or network will also be removed.
//
// ovtopodump(1) also follows the discovery filter semantic, and
// the filter only applies to nodes/interfaces.
//
// NOTES CONCERNING MAP AND TOPOLOGY FILTERS:
// For these filters, all objects are subject to filtering.
// One must specify the networks and segments to be passed.
// Furthermore, objects are displayed/included only if all their
// parent objects (submaps) pass the map/topology filter.  For example,
// if no networks would pass the filter ("isNetwork" is not included),
// then all segments and non-gateways nodes would be filtered out.
// Like Discovery filters, if any interface or
// node passes a Map filter, the node and all of its interfaces
// also pass the filter.
//
// See the FilterExpressions section for map and topology
// filter examples.
//

Networks "Any network" { isNetwork }
Segments "Any segment" { isSegment }
Nodes "Any node" { isNode }
```

```
// The following filters are primarily for example purposes, though
// they might be useful as discovery filters.  They do not generally
// make sense as map or topology filters because they do not specify
// the inclusion of networks and segments.  They also make sense as
// parts of a filter expression.

Routers "Any Router" { isRouter }
IPRouters "Any IP Router" { isIPRouter }
Bridges "Any bridge" { isBridge }
Hubs "Any multi-port repeater" { isHub }
SNMPNode "Any node supporting SNMP" { isNode && isSNMPSupported }

// The next filter is useful for defining map and topology filters
// (see the FilterExpresssions section).  It is not
// particularly useful as a discovery filter
// since all networks and segments automatically pass Discovery
// filters.  Nor is it useful as a standalone
// map filter, since it doesn't pass any nodes.

NetsNSegs "All networks & segments" { isNetwork || isSegment }

// This filter specifies that only objects that support IP should
// be included.  This filter should be used as a topology filter on
// any collection station discovering non-IP information (Level 2
// or IPX only nodes or networks) that is forwarding to a
// NNM 4.X management station.  This will not completely remove
// all non-IP information (e.g. IPX interfaces on a node that also
// supports IP will come through), but will limit the impact on the
// management station, and make migration to NNM 5.X easier.

IPOnlyObjects "Only objects that support IP"
        { isIP || isSegment }

// The following filters are examples that you can customize to
// match your environment.

// LocalLAN "Nodes with interfaces on the 15.2.112-119 subnet"
//      { "IP Address" ~ 15.2.112-119.* }
// NeighborLANs "Node with interfaces on the neighboring LANs on site"
//      { "IP Address" ~ 192.1.2-10.* }
// HPNodes "Hewlett-Packard nodes"
//      { isNode && ( vendor == "Hewlett-Packard" ) }
// NonHPNodes "Non-HP nodes"
//      { isNode && ( vendor != "Hewlett-Packard" ) }

// These are example filters using the sets defined above.
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0431
3740
Doc:

```
// GatewaysSet "Any designated Gateway node"
//      { "IP Hostname" in gateways }
// ServersSet "Any designated Server node"
//      { "IP Hostname" in servers }

// The next filter is useful for defining map and topology filters
// (see the FilterExpresssions section).  It is not
// particularly useful as a discovery filter
// since all networks and segments automatically pass Discovery
// filters.  Nor is it useful as a standalone
// map filter, since it doesn't pass any nodes.
//
// The network name below assumes an entry in /etc/networks.
// If no such entry exists, the actual network name will be
// something like "15.2.112".
// MyNet "The network in which I'm interested"
//      { isNetwork && "IP Network Name" == "yellow-lan" }

// This filter would be an example of a way to pass all objects
// contained in the subnet 15.2.112.0 with a subnet mask
// of 255.255.248.0 (so the subnet range is 15.2.112.0 to
// 15.2.119.255).  Note that the inclusion of "isSegment" is
// not a concern, because all segments outside of this network
// would be filtered out because the networks containing them
// were filtered out.  We must have some specification of segments
// if we want the segment contents to be included.

// EngrLan "The 15.2.112 subnet used by engineering"
//      { ("IP Address" ~ 15.2.112-119.* ) || isSegment }

// This filter accomplishes the same thing, but is more restrictive
// in the specification of segments to only include segments in that
// engineering network.  This assumes there is an entry in /etc/networks
// such that the subnet gets the name "engr-LAN", and hence the segments
// in that network all have a name of form "engr-LAN.<something>"
// Generally, the above will accomplish what you want, but this
// may be necessary in some situations if you want specific segments.
// In particular, it works well if you want to use this to EXCLUDE
// the objects in this network.  See the example in the Filter
// expressions below.

// EngrLan2 "The 15.2.112 subnet used by engineering"
//      { ( "IP Address" ~ 15.2.112-119.* ) ||
//        ( "IP Segment Name" ~ "engr-LAN.*" ) }
```

```
        // The following are some sample DHCPFilters.
        // They can be specified by using the Network Polling Configuration
        // dialog application, xnmpolling, on the Status Polling page.

        // DHCPSubnet "Addresses in subnet 15.70.177 are DHCP allocated"
        //      { "IP Address" ~ 15.70.177.* }

        // DHCPNode  "A particular address is DHCP allocated"
        //      { "IP Address" ~ 15.70.177.9 }

        // DHCPRange "IP Addresses from 15.70.177.5 through 15.70.177.10"
        //      { "IP Address" ~ 15.70.177.5-10 }

        //
        // Access to various nodes based on SNMP MIBs that have
        // been discovered as supporting a particular MIB
        //

        CDPnodes "Nodes supporting Cisco Discovery Protocol" { isCDP }
        ATMnodes "Nodes supporting ATM" { ("SNMP ifType" == "ATM")  ||
            ("SNMP ifType" == "atmLogical") ||
            ("SNMP ifType" == "atmDxi") ||
            ("SNMP ifType" == "atmFuni") || ("SNMP ifType" == "atmIma") }
        DS1nodes "Nodes supporting DS1" { "SNMP ifType" == "T-1 Carrier (ds1)" }
        DS3nodes "Nodes supporting DS3" { "SNMP ifType" == "T-3 Carrier (ds3)" }
        SONETnodes "Nodes supporting SONET" { "SNMP ifType" == "SONET" }
        FrameRelayNodes "Nodes supporting Frame-Relay" {
            ("SNMP ifType" == "Frame Relay") ||
            ("SNMP ifType" == "Frame Relay Service") ||
            ("SNMP ifType" == "frameRelayInterconnect") }
        RMON1nodes "Nodes supporting RMON-1" { isRMON }
        RMON2nodes "Nodes supporting RMON-2" { isRMON2 }
        // Short-hand for any RMON device
        RMONnodes "Nodes supporting RMON-1 or RMON-2" { isRMON || isRMON2 }
}

// FilterExpressions are simply combinations of filters defined in the
// same filter file (above).  FilterExpressions make it simple to
// combine filters without reproducing the expressions of each
// filter again

FilterExpressions {

        // One can turn the filters defined above into viable map or
        // topology filters by simply adding "|| NetsNSegs".  (Doing so
        // does not invalidate the filters as discovery
        // filters.  It just adds a superfluous test.)
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0432
3740
Doc:

```
NetInfrastructure "Any network connecting device and what they connect"
        { Routers || Bridges || Hubs || NetsNSegs }
NetBackbone "Networks and gateways/routers"
        { Routers || Networks }

// The following combines the two set filters
// defined above into one FilterExpression.
// It works unmodified as a discovery filter.
// To work as a map filter, network and segment filtering
// must be added (see below).

// VitalNodes "All Gateways and Servers"
//      { GatewaysSet || ServersSet }
// One can turn the filters defined above into viable map or
// topology filters by simply adding "|| NetsNSegs".  (Doing so
// does not invalidate the filters as discovery
// filters.  It just adds a superfluous test.)

// VitalNodesMap "All nets & segs, but only gateway and server nodes"
//      { GatewaysSet || ServersSet || NetsNSegs}
// LocalLANView "All nets & segs, but only local nodes"
//      { LocalLAN || NetsNSegs }

// Using the filters defined above that include only a specific
// network, we can also exclude the specific network like this
// Note the use of the more specific form to exclude only the segments
// in the engineering lan.  This could have been specified directly
// as a negation in the filter part, but this form works well if you
// have several networks to manipulate in this manner.
// EverythingButEngr "Everything but the engineering LAN"
//      { !EngrLan2 }

// Of course the above filter expressions, when used as
// map filters, pass all networks and segments.  You
// may wish to see only a particular network.  The following map
// filters accomplish this.  Note that though segments
// and nodes from other networks will pass the filters, IP Map
// will ignore them because their parent networks will not pass.
// NOTE:  These filters will not work as Discovery
// filters because all network and segments automatically pass
// Discovery and Topology filters.

// MyNetMap "Only the network of interest and all its constituent parts"
//      { MyNet || Segments || Nodes}
// MyVitalNodesMap "Gateways, servers and segments in net of interest"
//      { MyNet || Segments ||  GatewaysSet || ServersSet }
```

1036


```
        // This is a map persistence filter which ensures that
        // all Ungermann-Bass are kept in memory and up to date.
        // Note that this will also keep any containing submaps in memory.

        // PersFilter "Objects to keep in map memory"
        //      { HPNodes }
}
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0433
3740
Doc:

1035

B Using NNM Under a Mixed Codeset Environment

Appendix B

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 434
3740
Doc:
179

This chapter covers requirements for using NNM's alarm browser, `xnmevents`, in a mixed-codeset environment. These steps are not required if you are using the web interface to alarms, `jalarms`.

Event forwarding in NNM's distribution and scalability model expects that the management station and the collection station share a codeset. That is, if a management station is operating under the ISO8859-1 codeset, then the collection station must share its data using the ISO8859-1 codeset.

This restriction is minimal for English and European language users since ISO8859-1 contains both English (ASCII) characters and most of the European accented characters. Furthermore, NNM is not localized to any of the European languages.

However, this restriction becomes a problem for the Japanese language users that may need to use both Japanese EUC and Shift-JIS codesets. For instance, if a management station is running under Japanese EUC, but one of its collection station is running under Japanese Shift-JIS, the management station's GUI will fail to display the Shift-JIS data obtained from a Shift-JIS collection station. This is because a management station assumes that the data from the collection stations are using the same codeset as itself, and parses and displays all data (including the Shift-JIS data) as Japanese EUC data. This results in a data corruption of all Shift-JIS characters.

Therefore, in this mixed codeset environment, the collection stations must be configured to forward event data to the management station using ASCII only, and furthermore, "user events" must not contain non-ASCII characters. Since ASCII is a subset of all other codesets, data from the collection station will not be corrupted by the management stations' GUI.

SNMP traps do not support non-ASCII characters, but NNM does not prevent you from forwarding events that contain non-ASCII characters. Do not generate user-sendable events containing non-ASCII characters, if these events are forwarded from a collection station to a management station. For example, do not send events, such as the "`OV_Popup_Message`" or "`OV_Message`," with non-ASCII characters, using the `snmptrap` command from a collection station to a management station.

When configuring a collection station to operate under a mixed-codeset environment (Japanese system users should see Table B-1, Mixed Codeset Environment for Japanese Systems,), the following steps should be taken:

1. Create a new file called `$OV_CONF/ovlang.conf` (for example, `C:install_dir\conf\ovlang.conf`) that contains the following two entries, each on a separate line:

   ```
   ovtopmd
   netmon
   ```

   If you need to forward threshold events, add `snmpCollect` to `ovlang.conf`.

2. Restart the `ovw` processes by executing the following commands:

   ```
   ovstop
   ovstart
   ```

NOTE There is no need to remove or clear the `ovtrapd.log` file of a management station, but if it contains data from this collection station prior to this step, that data may be corrupted.

The first two steps will force the collection station to generate data forwarded to the management station with English/ASCII characters only. However, data that is not forwarded to a management station will continue to operate using the codeset specified by you or by the environment.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0435
Doc.

Table B-1 Mixed Codeset Environment for Japanese Systems

Collection Station's System/Codeset	Management Station's System / Codeset			
	Windows / SJIS	HP-UX/SJIS	HP-UX/EUC	Solaris/EUC
Windows/SJIS	(1)	(1)	(2)	(2)
HP-UX/SJIS	(1)	(1)	(2)	(2)
HP-UX/EUC	(2)	(2)	(1)	(1)
Solaris/EUC	(2)	(2)	(1)	(1)

(1) -- this is not a mixed codeset environment; no configuration necessary.

(2) -- this a mixed codeset environment; configure the collection station to forward ASCII data to the management station.

Glossary

A

agent In the network management model, the agent is the component that "instruments" or provides management information about a particular network device, such as a file server, to a network management system. *See also: proxy agent.*

C

client A computer system, on a network, that accesses a service from another computer (server). A client may run any arbitrary operating system.

client/server A concept that functionally divides the execution of a unit of work between activities initiated by an end user or program (client) and resource responses (server) to the activity request.

collection domain The set of nodes and other objects for which trend data collection and threshold checking is occurring on a collection station. Frequently the discovery domain and the collection domain include the same set of nodes and objects. Discussions in this document assume that is the case, and use this term to refer to both. *See also: management domain, discovery domain.*

collection station A management station that acts as a collection point for information being gathered on managed elements. *See also: management station.*

correlated events Multiple events analyzed by NNM and presented under a single event in the browser.

D

discovery domain The set of nodes and other objects actively being discovered and monitored by an NNM station.

discovery filter Specifies which devices an NNM station is actively discovering and monitoring. *See also: filtering.*

F

failover Configuring a management station to pick up status polling duties for a collection station that goes into critical status.

failover filter List of specific nodes the management station should poll, leaving the status of the rest as they were when the collection station went critical.

filtering Refers to the process of limiting the object the user is interested in having discovered, monitored, displayed, etc., by determining certain attributes that are of interest to the user. Filtering generally is used to limit processing to a subset of information already available, to reduce the cognitive load on the user, align presentation with the users needs, and generally reduce system load by filtering the amount of data handled as soon as possible. *See also: discovery filter, failover filter, map filter, persistence filter, and topology filter.*

I

IP address The Internet Protocol address is a network level address assigned to each system is a TCP/IP network. It is 4 bytes long. An example IP address is 192.215.15.46.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0436
3740
Doc:

M

management application Software that obtains and presents information from agents, or proxy agents. The information is usually presented in a graphical user interface.

management console An instance of the user interface from which you can control applications that do network and system management. The console may be on the system that contains the management software or it may be on another system in the management domain.

management domain The set of all nodes and other objects in the network that are of interest to the user.

management station The computer system used in the management of other objects in the network, system, and software environment. Management stations run network or system management services, daemons, processes, and/or management user interfaces. Management clients, management servers, management consoles, and stand-alone management systems are all examples of management stations. *See also: collection station.*

map A set of related objects, symbols, and submaps that provides a graphical and hierarchical presentation of your network and its systems. Because a map is defined by the collections of submaps it comprises, you never view a map directly, but rather one or more of its submaps. Maps are derived from the HP OpenView Windows object database, and multiple maps can be created from the same object database. *See also: submap.*

map filter Defines what objects in the HP OpenView Windows object database will be permitted on the map. Objects that are rejected by a map filter remain in the management station's topology database, and are still subject to status polling. Map filtering occurs on a per-map basis, not a per-display basis. *See also: filtering.*

N

node A termination point for two or more communication links - or more simply, a device on a network. The node can serve as the control location for forwarding data among the elements of a network, as well as perform other networking, and in some cases local processing functions.

O

object A computer system, interface card, printer, or any other device or object that appears in the network.

P

persistence filter Specifies one or more objects which are required to be in memory at all times, and therefore are not permitted to be on a transient submap. *See also: filtering, persistent submap, persistent object.*

persistent object An object which has passed a persistence filter, and is therefore in memory whenever the map on which it resides is open. Any submap that contains a persistent object is automatically a persistent submap. *See also: persistent submap, persistence filter.*

persistent submap A submap that is always in memory, either because it is above the configured persistence level, because it

contains a persistent object, or because it is the child of a persistent object. *See also: transient submap.*

primary collection station When applied to a particular object, this refers to the collection station which has been chosen as having primary responsibility for monitoring the object. In particular, it is used to determine the status and other attributes of the object. A given object may be reported and monitored by multiple collection stations, but only one station will be the primary station. *See also: secondary collection station.*

proxy agent A proxy agent performs information preparation and exchange on behalf of a device it is representing. For example, an agent is a proxy if it is located on the file server but is representing a client. *See also: agent.*

R

root submap A standard, top-level submap for every map.

router A router uses a packet's destination address to determine which network or network segment is its destination.

S

server A computer system that provides services to other computer systems on the network. A server could be a file server and provide data storage, application, routing, and print services.

secondary collection station When applied to a particular object, refers to a collection station that is known to be monitoring the object, but which has not been chosen as the primary collection station.

site A group of nodes connected completely by a Local Area Network (LAN), i.e. all at the same geographic location.

SNMP Simple Network Management Protocol. A protocol running above TCP/IP used to exchange network management information. SNMPv2C has extended functionality over the original protocol.

station *See: workstation, collection station, or management station.*

submap A particular view of the network environment, consisting of related symbols that are displayed in a single window. Multiple submaps can be displayed simultaneously. Submaps are typically (though not necessarily) organized in a hierarchy, with the root submap at the top of the hierarchy. *See also: map.*

T

TCP/IP Transmission Control Protocol/Internet Protocol. A set of protocols for Layers 3 and 4 of the seven-layered Open Systems Interconnect network model

topology filter A topology filter at a collection station defines the subset of local topology data that management stations can see. *See also: filtering.*

transient submap A submap that is not necessarily in memory at all times, but which is available "on-demand" when the operator opens it. Any submap that can be recreated at any time based wholly on topological information is potentially a

RQS 003/2005 - CN - CPMI - CORREIOS
Fls. Nº 0437
Doc 3740

transient submap, depending on how and whether the on- demand submap feature is enabled. *See also: persistent submap.*

W

workstation A computer or terminal that is connected to the network.

Index

Symbols

%REMOTE_MANAGERS_LIST%, 57, 97, 140, 155

A

applications
  backward compatibility, 68
  integrating, 26, 68, 125
attribute value assertion
  See AVAs
automated managed-state, 18, 74
AVAs, 172
  boolean, 174
  enumerated, 175
  enumerated field values, 186
  evaluating, 172, 174
  filterable fields, 181
  integer, 175
  operators, 173
  regular expressions, 176
  special pattern matching, 177
  string, 175
  whitespace in field name, 172

B

backup, 18, 88
backward compatibility
  applications, 68
benefits of scalability, 15

C

capacity, 21
  centralized-hierarchical model, 97
  collection stations, 86
  devices, 34, 84
  management console, 34
  remote monitoring, 85
centralized model, 92
  discovery filters, 93
  management consoles, 93
  map filters, 93
  on-demand submaps, 93
  web GUI, 93
centralized-hierarchical model, 95
  capacity, 97
  discovery filters, 96
  failover, 96
  management consoles, 96
  map filters, 96
  on-demand submaps, 96
  web GUI, 96
codeset,mixed, 206
collection domain, 46
  overlapping, 52
collection station, 33
  changing primary station for an object, 151
  checking status, 145, 146
  configuration overview, 57
  configuring, 133
  configuring remote communication, 141
  connections, 36
  determining if a node is, 137
  determining primary, 150
  failover, 51
  how many to have, 86
  identifying with Station view, 23
  in DIDM, 21
  introduction, 22
  listing monitored objects, 138
  managing, 138
  new primary, 55
  preferred, 54
  primary vs. secondary, 53
  removing from management station, 141
  security configuration, 133
  serving multiple management stations, 36
  synchronization, 144
  topology filter, 41
  troubleshooting, 147
  unmanaging, 140
configuration
  remote, 56
configuration files
  filter, 169
  nfsconf, 113
  ov.conf, 50, 139
  ovwdb.auth, 119
  pcnfsd.conf, 113
  snmpd.conf, 133
  trapd.conf, 27, 60
configurationfiles
  ovtopmd.lrf, 135
configuring
  collection station, 133
  collection station security, 133
  demand level, 121
  discovery filter, 128

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0438
3740
Doc:



Index

event forwarding, 154
failover, 150, 153
failover filter, 153
filters, 127
management console, 109
management stations, 137
on-demand submaps, 121
overlapping domains, 150
persistence filter, 124
topology filter, 134
UNIX console client, 117
UNIX console server, 112
Windows NT console for UNIX server, 115
Windows NT console server, 111
connections between components, 36
connector down, 60
forwarding, 62
important node filter, 193
console
See management console
cooperative independent model, 103
discovery filters, 104
management consoles, 104
map filters, 104
on-demand submaps, 104
threshold events, 104
topology filters, 104
web GUI, 104
correlated events, 60
forwarding, 60
custom views, 72

D

data collection
threshold, 28
trend data, 28, 159
databases, 159
SQL, 28
data-stream filters, 37
demand level
changing, 122
configuring, 121
devices
limit per station, 34
DHCP, 39, 192, 197
discovery filtering, 40
applying to previously discovered objects, 129
centralized-hierarchical model, 96
configuration, 128
cooperative independent model, 104
example, 190
fully centralized model, 93
hierarchical model, 100
distributed internet discovery and monitoring
architecture, 48
configuring, 133, 137, 150
internals, 46
introduction, 20
distribution, 19, 20, 33
architecture, 49
benefits, 15
DIDM configuration overview, 56
distributed internet discovery and monitoring, 16, 20
models, 89
network connections, 36
overview, 15
processes, 48
risks of, 86
the GUI, 109
threshold monitoring, 18

E

ECS, 60
EMANATE, 134
events, 27, 57, 59
configuring forwarding, 154
correlated, 60
forwarding, 18, 42, 62, 63
map filtering, 43

F

failover, 18, 51, 86
centralized-hierarchical model, 96
configuring, 153
disabling, 153
filter,configuration, 52, 153
hierarchical model, 101
failover filter
configuration, 153
failover filter configuration, 52
fault tolerance, 18
fields,filterable, 181
filter expression, 170
filtering, 48, 72
and scalability, 17
configuration, 127, 128

discovery, 40, 128
example, 189
filter definition file, 43, 44, 197
important nodes, 193
introduction to, 19
map, 42, 48, 127
overview, 37
performance, 17, 19
persistence, 26, 68
topology, 41, 50, 134
utilities, 45
filters, 169
attribute value assertion See AVAs
boolean expressions, 174
default file, 197
enumerated expressions, 175
enumerated field values, 186
example, 189
excluding a node, 180, 192
failover,configuring, 153
filterable fields, 181
formal grammar, 187
integer expressions, 175
language definition, 169
pattern matching, 177
regular expressions, 176
relationship between nodes and interfaces, 180
sets, 171
string expressions, 175
testing, 45
types of, 37, 38
find, 67
forwarding, 18
events, 59, 154
threshold events, 62

H

hierarchical model, 98
discovery filters, 100
failover, 101
management consoles, 100
map filters, 100
multiple levels, 99
on-demand submaps, 100
performance, 102
threshold events, 101
topology filters, 100
web GUI, 100
high availability, 18

I

inform request, 59
integrating applications
on-demand submaps, 125
interface
automatic managed-state, 18, 74
Internet level, 122
IP discovery and monitoring, 16
ipmap, 48, 61, 64, 68

L

LAN, 36
languages,international, 206
large maps, viewing, 17, 29, 87
list
of remote managers, 57
localization, 206

M

managed interfaces
automated, 18, 74
management console, 17, 20, 24, 33, 70, 73
capacity, 110
centralized-hierarchical model, 96
choosing mount point, 118
configuration overview, 110
cooperative independent model, 104
fully centralized model, 93
hierarchical model, 100
introduction, 24
modifying ovwdb.auth file, 119
platform, 110
prerequisites for, 109
read-only vs. read-write maps, 72
security, 119
supported configurations, 109
undoing, 120
UNIX client, 117
UNIX server, 112
Windows NT console for UNIX, 115
Windows NT server, 111
management domain, 46
management station, 22, 33
changing overlap mode, 152
changing primary collection station, 151
configuring, 137
remote communication, 141

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0439
3740
Doc:

configuring collection stations to manage, 138
connections, 36
identifying with Station view, 23
overlapping domains, 55
removing collection station, 141
synchronization, 144
troubleshooting, 147
unmanaging a collection station, 140
managing
locally monitored objects, 132
map filtering, 42
centralized-hierarchical model, 96
configuration, 127
cooperative independent model, 104
events, 43
example, 191, 195
fully centralized model, 93
hierarchical model, 100
recalculating for a map, 43, 68
maps, 72
Microsoft Terminal Server, 75
mixed codeset, 206
model, 33
centralized-heirarchical, 95
cooperative independent, 103
fully centralized, 92
hierarchical, 98
multi-level hierarchical, 99
monitoring domain, 46

N

Neighbor view, 163, 164
netmon, 40, 48, 49, 50, 51, 56, 58, 61, 99
limits, 84
network level, 122
Network Presenter, 25
See also web GUI, 17
NFS, 70, 109
diskless, and management consoles, 70
nmdemandpoll, 144
NNM 250
limitations, 34
multiple licenses to increase node limit, 87
nodes, excluding via filtering, 180

O

on-demand submaps, 26, 64
and find, 67
and submap list dialog, 67
centralized-hierarchical model, 96
changing demand level, 122
changing persistence filter, 125
configuring, 121
cooperative independent model, 104
disabling, 67, 122
fully centralized model, 93
hierarchical model, 100
inital configuration, 64
integrating applications, 125
ipmap and ovw, 64
performance, 17
persistence filters in, 26, 68
recalculating persistence of submaps, 69
sharing, 72
terms, 64
operators, 42
ovaddobj, 135
ovcoltosql, 28, 160
overlap mode, 152
overlapping collection domains, 52, 53, 55, 86
configuring, 152
ovfilter utilities, 45
ovrepld, 48, 50, 58, 62
ovstart, 49
ovtopmd, 48, 49, 50, 61, 135
ovtopmd.lrf, 135
ovtopodump, 138, 150
ovtopofix, 40, 129
ovtrapd, 59, 61
ovwdb, 70
ovwdb.auth file, 119
ovwrs, 51
ovwsetupclient command, 120

P

packet loss rate, 141
panner, 17, 29
partitioned internet submap, 87
Path view, 163, 165
performance, 16, 21, 97
hierarchical model, 102
memory, 26
persistence filtering, 26, 68, 69
changing, 125
configuring, 124
persistent submaps, 64
pmd, 59, 61
primary collection station, 53, 150
changing, 151

preferred, 54, 152
with failover, 55
processes, distribution for IP discovery and monitoring, 48

Q

quick navigator, 17, 30

R

remote communication
configuring, 141
remote configuration, 56
remote managers list, 57, 97, 155
replication of topology, 50
resident submaps, 64
retry count, 141

S

scalability, 15
benefits, 15
general considerations, 84
strategies for deployment, 87, 89
secondary collection station, 53
security
collection station configuration, 133
management console, 119
segment level, 122
Service Guard, 18, 50, 86, 93, 96, 100, 104, 119, 139
set-defining filters, 37
sets, 171
snmpd.conf, 133
SNMPv2C
inform request, 59
SQL databases, 28
Station view, 145, 146
collection station
checking status, 146
submap list dialog, effect of on-demand, 67
submaps
partitioned, 87
synchronization, 144

T

Terminal Server, 75
threshold events
cooperative independent model, 104
forwarding, 62, 154
hierarchical model, 101
monitoring, 27
remote, and remote actions, 63
threshold monitoring, 18, 28
timeout value, 141
topology filtering, 41, 50
changing, 135
configuration, 134
cooperative independent model, 104
events, 42, 63
example, 191, 194
hierarchical model, 100
removing, 136
topology replicator, 50
transient submaps, 64
trapd.conf, 59
traps, 59
troubleshooting
communication between management station and collection station, 147

U

UDP, 59
undoing
management console, 120
on-demand submaps, 122
UNIX, 117
unmanage
automated, 18, 74
unmanaging
collection station, 140
objects, 132
use models, 89
centralized-hierarchical, 95
cooperative independent, 103
fully centralized, 92
hierarchical, 98

V

view
Neighbor, 163, 164
Path, 163, 165
Station, 145, 146
views
custom, 42, 72

W

WAN, 15, 36
and remote monitoring, 85, 94, 97
configuring, 141
web GUI, 17, 25

ECT 1024
ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0440
3740
Doc:



Index

centralized-hierarchical model, 96
cooperative independent model, 104
fully centralized model, 93
hierarchical model, 100
web server, 25
wide area network
See WAN

X

xnmsnmpconf, 58
xnmtopoconf, 49, 52, 53, 54, 56, 57, 58, 132, 137, 140, 141, 147, 152
xnmtrap, 60
X-terminals, 33, 34
and management consoles, 73



hp

invent

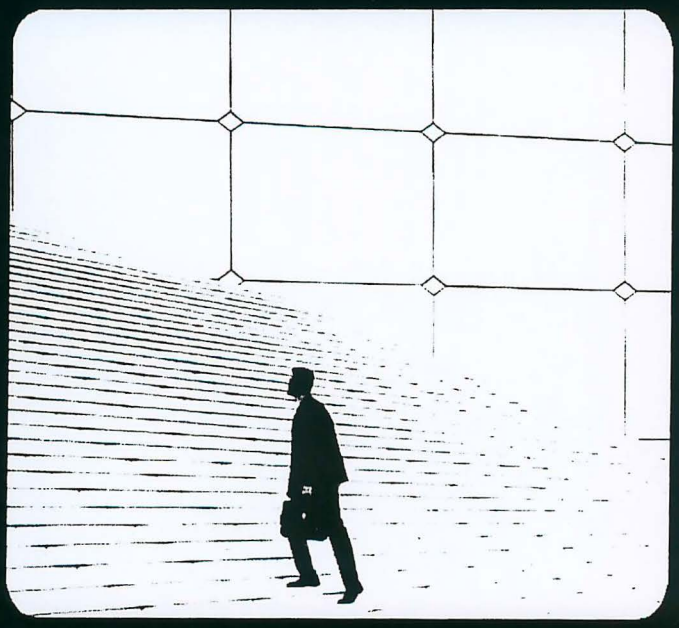
1020

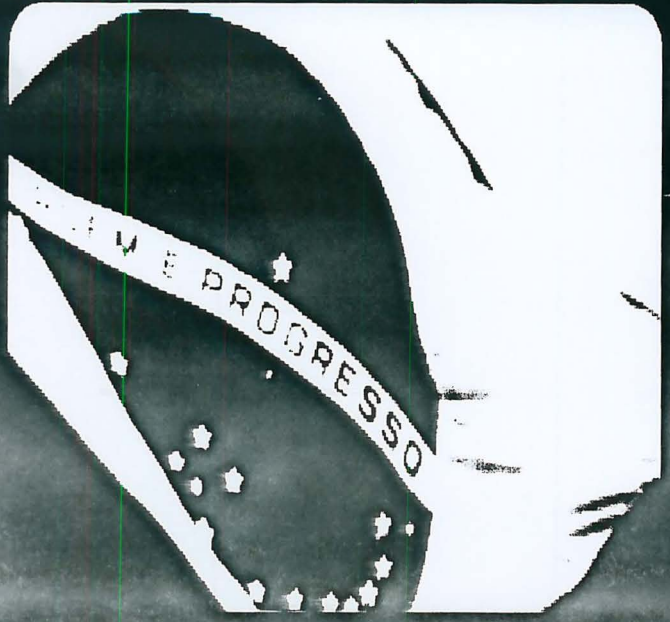
Pregão nº 118/2003 – CPUAC

Caderno 2

Apêndice

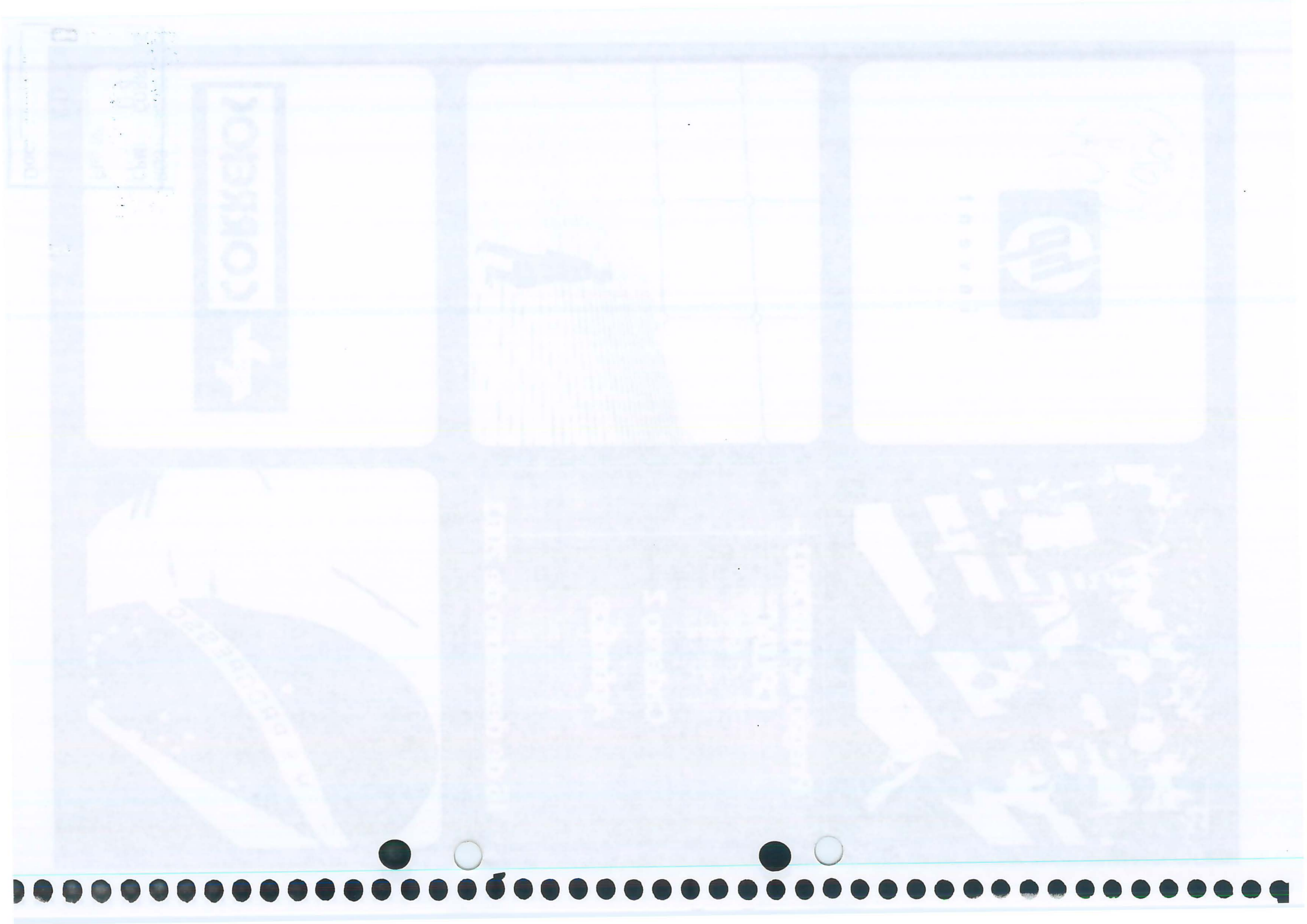
16 de dezembro de 2003





CORREIOS

RQS nº 03/2005 - CN -
CPMI - CORREIOS
044
Fls. Nº
3740
Doc:


KOMMEK

1019

HP OpenView Network Node Manager

Managing Your Network with HP OpenView Network Node Manager

Version: 6.4



Manufacturing Part Number : J5323-90000

January, 2003

© Copyright 2003 Hewlett-Packard Company.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0442
3740
Doc:

Legal Notices

Warranty.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices.

No part of this document may be copied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

©Copyright 1983-2003 Hewlett-Packard Company, all rights reserved.

Contains software from AirMedia, Inc.

© Copyright 1996 AirMedia, Inc.

Trademark Notices.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

Windows NT® is a U.S. registered trademark of Microsoft Corporation.

Windows® 2000 is a U.S. registered trademark of Microsoft Corporation.

Windows® and MS Windows® are U.S. registered trademarks of Microsoft Corporation.

Netscape™ and Netscape Navigator™ are U.S. trademarks of Netscape Communications Corporation.

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

Oracle7™ is a trademark of Oracle Corporation, Redwood City, California.

OSF/Motif® and Open Software Foundation® are trademarks of Open Software Foundation in the U.S. and other countries.

Pentium® is a U.S. registered trademark of Intel Corporation.

UNIX® is a registered trademark of The Open Group.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0443
3740
Doc:

1. Network Management with NNM

The Network Management Challenge 39
How Network Node Manager Can Help 39
Moving to Proactive Network Management 40
Poll for Network Information 40
Watch for Events 41
Network Management Functions 42
Fault/Problem Management 43
Performance Management 45
Configuration and Change Management 46
Additional HP OpenView Product Information 47

2. How Does NNM Work?

Collecting Critical Information 51
SNMP's Network Management Model 51
Desktop Management Interface (DMI) 54
Automatic Discovery and Layout 56
How IP Discovery and Layout Work 56
How IPX Discovery and Layout Work 57
Interactions Between IPX Discovery and IP Discovery 58
Level 2 Discovery 59
Event Reduction Capabilities 61
NNM's Databases 62
Operational Databases 62
Data Warehouse 63

3. Resources Available While Learning NNM

Resources Included with NNM 67
NNM Online Help System 67
Tip of the Day 69
Manuals: Printed and Online 69
Release Notes 71
Reference Pages (Manpages) 71
The contrib Directory 74
The support Directory 74
White Papers 75

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0444
3740
Doc:

Resources and Services Available Through HP 76
HP Web Sites 76
HP Consulting Service 76
HP Education 77
HP Product Support 77
OpenView Forum 77
Summary of HP OpenView Web Sites 78

4. Planning Your NNM Configuration

Budgeting Time for Planning and Configuration 81
Time for Planning 81
Time for Configuration 81
Taking Over NNM from Someone Else 82
Understanding the Network Information Needs of Your Organization 83
Who Needs What Information? 83
Work Sheet for Planning 85
Knowing Your Network 87
Deciding to Manage or Not to Manage Devices 87
Starting with a Well-Configured Network 90
Consistent IP Addressing Scheme 90
Consistent Name Resolution Scheme 91
SNMP Agents and Their MIBs Configured 93
DMI Service Providers and Their MIFs Configured 94

5. Initial Network Discovery: Options and Troubleshooting

Install Network Node Manager (if you have not already done so) 100
Installing IPX Transport Software (Windows only) 100
Establishing Universal Pathnames (UNIX only) 100
Discover the Network... Let NNM Do It 103
Overview 103
Start the NNM Services (background processes) 105
Make Sure NNM's Services Are Successfully Running 106
Open NNM 106
Configure an Inventory Report 107
Let NNM Run Over Night to Populate the Maps 107
Verify the Accuracy of the Initial Discovery 109

Printing the Inventory Report 110
Viewing the Properties of Your Network Configuration 111
Finding Specific Devices on the Map 113
Interactively Expand/Limit Your Management Domain 117
Adding Networks to Your Management Domain 117
Managing an Unmanaged Network Device 118
Unmanaging a Managed Network Device 118
Automatically Expand Your Management Domain 119
Create a Seed File Specifying Multiple IP Networks to Manage 120
Use loadhosts 122
Expand the IPX Hop Count (Windows only) 123
Automatically Limit Your Management Domain 124
Create a netmon.noDiscover File to Exclude Devices 125
Use loadhosts 127
Create a Discovery Filter Identifying Which Devices to Include 128
Modify the oid_to_type File to Unmanage Devices by Type 129
Limit the IPX Hop Count (Windows only) 130
Troubleshooting Discovery 131
IP Discovery and Layout 131
General IP Suggestions 144
IPX Discovery and Layout (Windows only) 153
Stop Everything and Start Discovery Over Again 161

6. Preserve Your Sanity: Backup and Polling Configuration

Backup/Restore to Protect Your Investment of Time 165
How Does the Backup Work? 166
Backing Up and Archiving All Critical Files 167
Restoring All of NNM (procedures/options) 171
Restoring Part of NNM (procedures/options) 173
Troubleshooting Information 174
Custom Scripts 176
Controlling the Amount of Traffic Generated by NNM 178
Status Polling 181
Configuration-Check Polling 183
Connector Topology Polling 184
New Node Discovery Polling (IP, Level-2, and IPX) 184

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0445
3740
Doc:

Controlling Level-2 Device Discovery and Layout 185
Secondary Failure Polling 192
Fine-Tuning the Polling Services 193
Watching NNM's Polling Queue 194
Running NNM Without Network Polling 195

7. Map Making Fundamentals

Maps versus Submaps 199
Maps 199
Submaps 200
Understanding Objects versus Symbols 203
Objects 204
Symbols 207

8. Map Customization

Putting It All Together 212
Which Maps for Which Users 212
Copying the Default Map 215
Your Map Strategy 215
Controlling the Display of Devices Attached to Switches or Bridges 217
Turning On Star Configuration for Attached Devices 218
Turning Off Star Configuration for Attached Devices 219
Giving Your Network Symbols Meaningful Names 221
Turning Connection Labels on or off 223
Configuring Trunking and Meshing 225
Establishing Submap Persistence Settings 229
By Logical-level of Your Network's Structure 230
By Presence of Specific Devices 230
Controlling Which Devices Appear on the Map 232
Creating a Map Filter 232
Using the Hide Feature 233
Changing/Adding Object Attribute Fields 235
Changing the Value in an Attribute Field 236
Changing Symbol Type to Switch Attribute Sets 237
Adding Attribute Fields in the Object Database 238
Making the Maps Look Like Your World 240

Controlling the Placement of the Symbols on Your Map 241
Adding Your Own Submaps 244
Customizing the Internet Level of Your Network Map 247
Customizing Network-, Segment-, or Node-Level Submaps 256
Background Graphics 260
Creating Your Own Map Symbols 263
What Is a Symbol 263
Specifying the Placement and Size of the Submap Windows 266
Window Geometry 266
Submap Overlay 266
Miscellaneous Configuration Changes 268
Windows Operating System 268
UNIX Operating Systems 269
Controlling Symbol Status 270
Object Status Colors 270
Compound Status 274
Creating New NNM Features to Meet Your Team's Needs 278
Adding to NNM's Menu Structure 278
Creating Executable Symbols with Custom Behaviors 279

9. Controlling Map Access

Establishing and Communicating a Process for Requesting Changes to the Map . . 286
Not Allowing Team Members to Make Changes 286
Allowing Team Members to Make Changes 286
Setting User Preferences Within NNM 287
Using Command Line Startup Options 289
Options 289
Examples 290
Using Operating-System Level File Permissions for the Map 292
Windows: Setting Permissions 293
UNIX: Setting Permissions 294
Using the Context Feature to Control Menu Choices 296
Using NNM's Predefined Contexts 296
Creating Your Own Contexts 297
Using ARF Files to Control Menu Choices 299
ARF File Modifications Example 305

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0446
3740
Doc:

Allowing Others to View NNM from Many Computers 317
Remote Consoles 317
NNM's Web Interface 318
Microsoft Terminal Services 318
Closing All Current Sessions 319

10. Keeping Up with Events on Your Network: Beyond the Maps

How NNM's Event System Works 323
SNMPv1 Traps / SNMPv2c Traps and Informs 325
DMI Events (Indications) 327
Alarm Browser Overview 329
Displaying Alarms 330
Alarm Categories/Alarm Browser Windows 331
Acknowledging Alarms 334
Filtering Alarms 335
Deleting Alarms 337
NNM's Map and the Alarm Browser 338
Specifying Additional Actions on Alarms 339
Launching Specific Views or URLs from Alarms 340
Configuring the Alarm Browser 342
Controlling the Size of the Event Database 343
Controlling the Size of the Alarm Browser's State File 344
Controlling How Many Alarms to Delete Automatically 345
Copy or Restore the Alarm Browser's State File 347
Controlling How the Alarm Browser Looks 347
Assigning Alarm Categories 348

11. Event Reduction Capabilities: Getting to the Root Cause

NNM's Event Reduction Capabilities 352
Correlation Concepts 354
De-Duplication of Alarms 358
ECS Correlations 360
NNM's Built-In Correlations 360
Command Line Control 380
Correlation File Structure 381
Troubleshooting 381

Obtaining Additional Event Correlations 382
Correlation Composer Correlators 386
NNM's Built-In Correlators 386
Correlator Fact Store File 397
Troubleshooting 397
Creating Additional Correlators 398
What is an SNMP Variable-Binding and How Do I Identify One? 404
Look within the MIB File 404
Check the Alarm Message Text in the Alarm Browser 405
Special SNMP Variable-Bindings within NNM Interface and Node Status Alarms 405

12. Customizing Events: Doing It Your Way

SNMP MIB Browser 412
Loading MIBs in the MIB Database 413
Prerequisites 414
Procedure Tips 415
DMI Browser 417
Creating DMI Queries 417
Loading DMI-to-SNMP Event Mappings 419
If a MIB Translation of the MIF File Is Available 420
If No MIB Translation of the MIF File Is Available 420
Event Configuration Overview 422
Prerequisites 422
Event Configuration Window 423
Controlling Alarm Message Posting and Text 431
Defining Automatic Actions for Events 433
Variables and Special Characters Allowed 436
Defining Additional Actions 441
Using the MIB Application Builder 443
Prerequisites 444
Procedure Tips 445
Data Collection & Thresholds 447
Prerequisites 447
Procedure Tips 449
Defining Thresholds for Monitored MIB Objects 453
Collecting and Storing Textual Data 460

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0447
3740
Doc:

Creating and Using MIB Expressions 460
Unique Properties of the SNMP MIB Object sysObjectID 465

13. Using Event Data

Graphing SNMP Data 471
. 471
Graphing Historical and Real-Time Data in the Same Graph 473
Grapher Operations 474
Printing a Graph 475
Data Warehouse 476
Data in the Data Warehouse 478
Reporting 478

14. NNM on the Web

Overview 484
Setting Up the HP OpenView Web 485
Role Configuration Files for the HP OpenView Web 486
The HP OpenView Launcher 492
Launcher User Interface 492
Configuring the Launcher 494
HP OpenView Network Presenter 501
Starting the Network Presenter 501
The Network Presenter Window 502
Network Presenter versus NNM on a Management Station 503
Configuring the Network Presenter 505
Using Symbol Registration Files and Bitmaps 506
Listing Multiple Maps in the Launcher 508
SNMP Data Presenter 509
Configuring the SNMP Data Presenter 511
Alarm Browser 512
Using and Configuring the Alarm Browser 513
Event Reduction 515
Reporting Interface 516
Additional Views 518
Neighbor View 518
Path View 519

Node View 520
CDP View 521
Station View 522
Internet View 522
Port-Address Mapping 522

15. Maintaining NNM

Daily Tasks 527
Check Running Services 527
Check Disk Space 527
Trim Files 528
Weekly Tasks 531
Back Up NNM 531
Check Polling Performance 531
Check Web Launcher Log Files 532
Monthly Maintenance Tasks 533
Check Patch Releases 533
Check License Requirements 533
Yearly Maintenance Tasks 534
Evaluate Latest Release 534
Other Maintenance Tasks 535
Enabling/Disabling Automatic Startup 535
Customizing the Startup Configuration 535

A. NNM Services and Files

Services and Files 541
Background Services 541
Foreground Services 543
Web CGI Programs 545
Behavior of the Services and Files 547

B. Network Troubleshooting Tools

Tools in NNM on a Management Station 555
Map Snapshots 555
Performance Tools 556
Configuration 562

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0448
3740
Doc:

Fault Resolution Tools 566
Miscellaneous Tools 569
Tools in NNM's Web Applications 575
HP OpenView Launcher 575

C. Troubleshooting NNM Itself

General Troubleshooting Considerations 579
When You Need More Information 579
Preventive Practices 579
Characterizing the Problem 582
Distinguish Local versus Remote Problems 582
Remote Nodes' Level of Manageability 582
Context: What Changed? 583
Duration: How Long or How Often? 583
Context: What Action Was Performed? 583
Troubleshooting Background Services 584
The httpd Background Service 586
The netmon Background Service 587
The ovactiond Background Service 590
The ovalarmsrv Background Service 590
The ovcapsd Background Service 591
The ovspmd Background Service 592
The ovrepld Background Service 594
The ovtopmd Background Service 594
The ovtrapd Background Service 599
The ovuispmd Background Service 600
The ovwdb Background Service 602
The pmd Background Service 604
The ovrequestd Background Service 607
Troubleshooting Data Collector Problems 608
Set-community Name and Trap-dest Loss Upon Re-Installation 612
Troubleshooting Web Components 613
Language Selection Problems 614
HP OpenView Launcher 615
Network Presenter 618
Alarm Browser 619

SNMP Data Presenter 620
Troubleshooting NNM Operations 623
Runtime Components 623
Network Management Operations 626
Browsing an Internet MIB 628
Building and Executing MIB Applications 628
Configuring Events 631
Event Reduction Capabilities 632
Loading Internet MIBs 633
X Windows Components (UNIX operating systems only) 635
Online Help 636
Troubleshooting Windows Applications 637
Problems Launching Applications 637
Windows Operating System Tools 637
Recommended Logging and Tracing Practices 639
Logging and Tracing 639
Web Launcher Error Log 653
Improving Traffic Management and Performance 654
Traffic Management 654
Performance 656

D. Changing All the Symbols for a Particular Device

Procedure 662
Example 663
Create a Symbol Registration File 664
Copy and Modify the Symbol Graphics 664
Map a sysObjectID to the New Symbol 666
Define the Capabilities for Computer_workstation_700 667
Inform NNM about the New Fields 668
Provide Additional Information in the oid_to_type File 669
Update the Database 670
Verify Symbol Changes 671
Back Up Your Efforts 673

E. Changing an Object's Vendor and SNMP Agent

How NNM Discovers Vendor and SNMP Agent Values 676

1006
RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0449
3740
Doc:

When the Vendor and SNMP Agent Would Not Be Set 677
Procedure 678
Example. 679

Index 685

Support

Please visit the HP OpenView web site at:

`http://openview.hp.com/`

There you will find contact information and details about the products, services, and support that HP OpenView offers.

The support area of the HP OpenView web site includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

RQS nº 03/2005 - CN
CPMI - CORREIOS
17
Fls. Nº 0450
3740
Doc:

What Do I Need to Know?

This chapter presents an overview of network management concepts, platforms, and technologies, and discusses how they work together. This information is intended to provide a reminder of the kind of information you need to know in order to be successful with Network Node Manager.

This chapter does not attempt to provide full details about these topics. If you need more information, check the references provided at the end of the chapter.

The following topics are covered in this chapter:

- Networking concepts, including an overview of the OSI model and network management protocols (page 20).
- Network hardware, the management protocols it uses, and how it fits into the OSI model (page 25).
- How management information is exchanged between devices, including a discussion of MIBs and MIFs (page 27).
- General operating system knowledge that you should have, including a discussion of cross-platform issues (page 31).
- References to other sources of information (page 33).

The use of the term Windows or Windows operating system in this manual refers to NNM supported Microsoft® Windows® operating systems. For a list of supported Windows operating systems, see the *Release Notes for HP OpenView Network Node Manager*.

The use of the term UNIX or UNIX operating system in this manual refers to NNM supported UNIX® operating systems. For a list of supported UNIX operating systems, see the *Release Notes for HP OpenView Network Node Manager*.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0491
3740
Doc:

Understanding Networking Concepts

To use HP OpenView Network Node Manager (NNM) successfully, you need to have a good understanding of networking concepts, hardware, protocols, and architecture.

In addition to general networking knowledge, you also need to be familiar with your specific network — the operating system platforms on your network, how the network is currently configured, what protocols are being used, and what kind of devices are on your network.

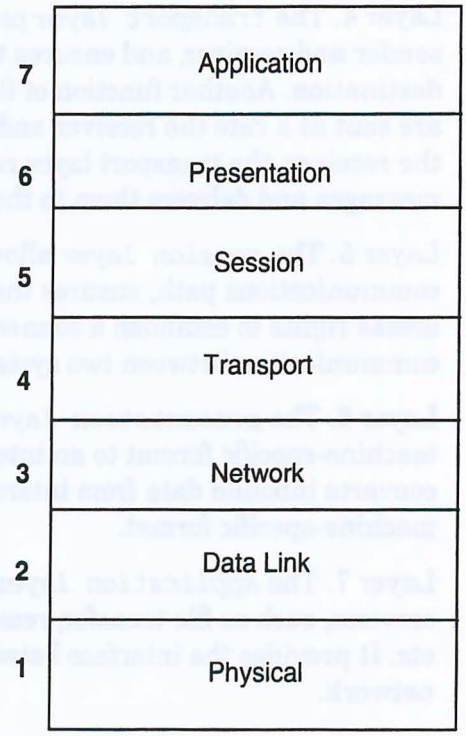
The OSI Reference Model

The need to provide communications among the devices supplied by different vendors gave rise to the Open Systems Interconnect (OSI) reference model. Because the unique network architectures and proprietary protocols developed by numerous vendors are frequently incompatible, the OSI model was developed by the International Standards Organization to resolve the compatibility issues and allow hardware from different vendors to communicate. The layer concept on which the OSI model is based establishes a set of rules for data transmission on a variety of levels.

The OSI model is important to review, because the various protocols operate at different layers, as do various hardware devices.

Figure 1 shows the layers of the OSI model.

Figure 1 Layers in the OSI Model



In a layered scheme, messages originate from the top layer (Layer 7) of a transmitting computer, move down to the lowest layer (Layer 1) and travel across the network media to the receiving computer. The message arrives at the lowest layer (Layer 1) of the receiving computer and moves up through its various layers to Layer 7.

Each of the layers is described below.

- Layer 1. The *physical layer* establishes the actual physical connection between the computer equipment and the network, and provides the transmission of bits from one system to another.
- Layer 2. The *data link layer* provides the transmission of packets, and performs error detection and correction functions to ensure that a packet contains the same information received as sent.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0452
3740
Doc:

- Layer 3. The *network layer* determines the path that will be taken through the network. The network layer also controls the rate at which the network accepts packets, to avoid and recover from congestion.
- Layer 4. The *transport layer* provides for the flow of data between sender and receiver, and ensures that the data arrives at the correct destination. Another function of this layer is to ensure that packets are sent at a rate the receiver and the application can cope with. At the receiver, the transport layer reassembles the packets into messages and delivers them to the next highest layer.
- Layer 5. The *session layer* allows the setup and termination of a communications path, ensures that the sender is authentic and has access rights to establish a connection, and synchronizes the communication between two systems.
- Layer 6. The *presentation layer* converts outbound data from a machine-specific format to an international standard format. It converts inbound data from international format to a machine-specific format.
- Layer 7. The *application layer* provides the software for network services, such as file transfer, remote login, remote execution, e-mail, etc. It provides the interface between user programs and the network.

Network Management Protocols

You should be familiar with the terminology and concepts of network management protocols, specifically the following.

SNMPv1 (Simple Network Management Protocol version 1)

SNMP is the most common management protocol in use in data networks. It provides a means of obtaining information from, and sending information to, network devices. SNMP is based on the manager-agent model, and uses Management Information Bases (MIBs) to exchange information between them (see "Exchanging Management Information" on page 27). Using the SNMP protocol, a manager can query and modify the status and configuration information on each managed device by making requests to the agent running on the managed device. All commands use the UDP/IP protocol, which means that communication between the manager and the agent is connectionless. SNMP operates at Layer 7, the application layer.

SNMPv2C (version 2) SNMPv2C includes the basic functions of SNMPv1, and adds new message types, standardized multiprotocol support, enhanced security, new MIB objects, and a way to co-exist with SNMPv1. SNMPv2C is useful for the retrieval of large amounts of management information using fewer network resources.

UDP (User Datagram Protocol) UDP is a protocol that allows an application program on one machine to exchange datagrams with an application program on another machine, without acknowledgments or guaranteed delivery. UDP operates at Layer 4, the transport layer.

TCP/IP (Transmission Control Protocol/Internet Protocol) TCP and IP are the two most widely-used Internet protocols, with TCP providing transmission of data on IP networks, and IP containing addressing and control information for packets to be routed. TCP operates at Layer 4 of the OSI model, while IP operates at Layer 3.

TCP/IP plays a significant role as a common denominator in interconnecting devices and networks, and is widely used to connect computers with dissimilar technologies. Most management solutions require TCP/IP as an information source and information carrier.

ICMP (Internet Control Message Protocol) ICMP is the part of IP that handles error and control messages. It operates at Layer 3, the network layer. ICMP supports an `echo` function, which sends a packet on a round-trip between two hosts. `ping`, which sends a signal to see if an interface is up and running, is based on this feature. ICMP can also send an address mask request that returns the address of the subnet mask on the remote system. This feature is important for non-SNMP devices.

IPX (Internet Packet Exchange) IPX is a network protocol that allows personal computers to communicate on local area networks and wide area networks. Operating at Layer 3 of the OSI model, IPX establishes a connection between the sender and the receiver. When a message is sent and the receiver does not issue a response, the message is simply retransmitted. IPX uses a broadcast technique to track all the computers and services on the network.

ARP/RARP (Address Resolution Protocol) ARP is used at Layer 2, the link layer, to map an IP address to a MAC (or link level, or hardware) address. RARP (Reverse Address Resolution Protocol) is used to map a MAC address to an IP address.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls.: Nº 23
0453
3740

DHCP (Dynamic Host Configuration Protocol)DHCP allows IP addresses to be allocated on a temporary basis (a lease). When the lease for an IP address expires, the address can be reused by a different node. This is useful in environments supporting mobile users who connect to the network with a laptop from many different places. This helps alleviate the problem of limited IP addresses and simplifies TCP/IP client configurations.

Protocols and the OSI Model

Figure 2 illustrates which protocols operate at the various layers of the OSI model. This illustration shows the major protocols used in network management; there are other protocols that are not shown in this illustration.

Figure 2 **Protocols Operating at the OSI Layers**

	Layers in the OSI Model	Protocols Operating at the OSI Layers
7	Application	SNMP Berkeley Services ARPA Services
6	Presentation	
5	Session	
4	Transport	TCP UDP
3	Network	IP/IPX ICMP
2	Data Link	ARP/RARP IEEE 802.x DHCP MAC address
1	Physical	10BASE2 10BASE5

Network Hardware Devices

The basic kinds of network communication devices include repeaters, hubs, bridges, routers, and switches. Figure 3 shows the layers at which these devices operate. These hardware devices operate at different layers of the OSI model, use different protocols, and perform different functions, thus requiring different levels of monitoring for network management. NNM will assist you with this task.

Figure 3 Hardware Devices Operating at the OSI Layers

Layers in the OSI Model		Protocols Operating at the OSI Layers	Hardware Devices at the OSI Layers
7	Application	SNMP Berkeley Services ARPA Services	Gateways
6	Presentation		
5	Session		
4	Transport	TCP UDP	
3	Network	IP/IPX ICMP	Routers Switches
2	Data Link	ARP/RARP IEEE 802.x DHCP MAC addresses	Switches Bridges
1	Physical	10BASE2 10BASE5	Simple Repeaters Hubs

- Simple Repeaters

  Simple repeaters operate at Layer 1, the physical layer, and are generally used to connect two network segments into one large segment, or to expand an existing segment. There is no filtering of messages transmitted between the two segments. A simple repeater

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: Nº 0454
3740
Doc:

enhances data signals and thus can be used to extend maximum cabling distances. There is no network intelligence built into a simple repeater; it is used strictly for signal propagation.

- Hubs

  Hubs operate at Layer 1, the physical layer. A hub is simply a multiport repeater, and can be used to increase overall network size and number of nodes on a single segment. A hub allows you to isolate faults within the subnet and add stations to a segment without disrupting the entire network.

- Bridges

  Bridges operate at Layer 2, the data link layer. A bridge is used to allow networks with different physical signaling, but with compatible data link addressing schemes, to communicate. Bridges help reduce traffic on a backbone LAN by filtering any information coming from one segment to another that does not need to be forwarded through the backbone. A common use for a bridge is to allow users on an Ethernet LAN and a Token Ring LAN to communicate with each other.

- Switches

  Switches operate at Layer 2, the data link layer. The function of a switch is to dispatch data to its destination, which it determines from the packet's lower-layer media access control (MAC) address. A switch, like a bridge, limits traffic, and does not understand network protocols. A fairly new device is the multi-layer switch, or routing switch, which operates at Layer 3, and combines the intelligence of a router with the efficiency of a switch, thus routing data at higher speeds.

- Routers

  Routers operate at Layer 3, the network layer. A router is used to connect two networks with different technologies, and provides an intelligent means of transferring packets from one network to the other. A router also forwards traffic among multiple hubs and bridges.

- Gateways

Gateways operate at Layer 7, the application layer, and can encompass all seven of the OSI model layers. A gateway is a computing system that can be programmed to do any number of intricate protocol conversions and negotiations, such as between IP and IPX.

Exchanging Management Information

There are two standard logical information exchange bases used to communicate about the configuration and status values of managed objects — MIBs for SNMP-based objects and MIFs for DMI-based objects.

MIBsThe data exchanged between managers and agents on an SNMP-based system uses the **Management Information Base** (MIB). A MIB is a standard set of definitions for exchanging information about hardware and software components. Each MIB contains a group of objects, which specify a structure and format for defining manageable elements.

Types of MIBs There are several MIBs with which you should be familiar.

- MIB-I

  MIB-I is the original standard for explaining and defining the exact information base needed for monitoring and controlling devices on TCP/IP networks. The objects included in MIB-I are essential for configuration control and fault monitoring. All other MIBs are built upon and include the definitions of MIB-I.

- MIB-II

  MIB-II extends the information defined in MIB-I by expanding the set of objects defined in the MIB. The types of objects added to MIB-II include those for dealing with various transmission media types, and those for using SNMP to control and monitor the network management itself.

- RMON MIB

  The Remote Monitoring (RMON) MIB defines information that can be collected by remote monitoring devices. The main functions of the RMON MIB are to provide offline operation of remote devices, pre-emptive monitoring, problem detection and reporting, data analysis, and support for multiple managers.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0455
3740
Doc:

- Bridge MIB

  There are two modes of bridging — transparent mode and source route. The Bridge MIB defines objects needed to manage a bridge operating in transparent mode, as well as some objects applicable to all types of bridges. NNM includes a Source Route Bridge MIB that, although not used by NNM for discovery, can be used for your own needs.

- Repeater MIB

  The Repeater MIB defines objects used to manage repeater devices, including multiple repeaters and non-standard repeaters.

- MAU MIB

  The MAU MIB defines objects used to manage Medium Attachment Units (MAUs). These MAUs may be connected to IEEE 802.3 repeaters or to 802.3 (Ethernet-like) interfaces.

- Private MIBs

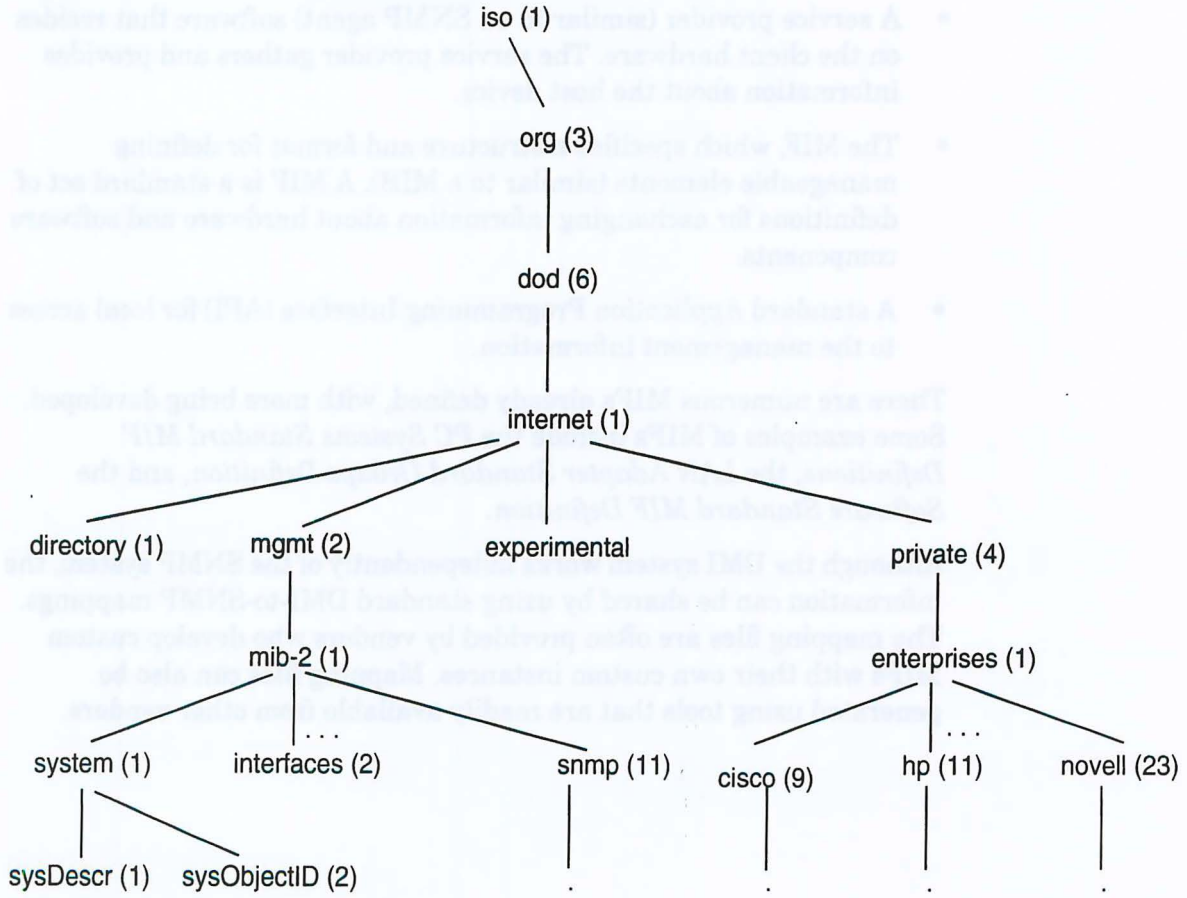
  Private MIBs are extensions to a MIB, usually developed by a vendor or a workgroup, to manage specific devices. The most common objects in these MIBs relate to information about the physical configuration and software configuration of a device.

How MIBs Are OrganizedMIB objects are conceptually organized in a hierarchical tree structure. Each branch in the tree has a unique name and numeric identifier. Intermediate branches of the tree serve as a way to group related MIB objects together. The "leaves" of the tree represent the actual MIB objects. Figure 4 illustrates the tree structure, with special attention to the Internet MIB tree.

A MIB object is uniquely identified (named) by its place in the tree. A full object identifier consists of the identifier of each branch along the path through the tree hierarchy, from the top of the tree. For example:

```
.iso.org.dod.internet.mgmt.mib-2.system.sysObjectID
(.1.3.6.1.2.1.1.2)
```

Figure 4 MIB Organization



MIB Objects and InstancesA specific type or class of management information is called a **MIB object** (for example, a system description or an interface status). The existence of a particular returned value for a MIB object in the agent database is called an **instance**. Some MIB objects have only a single instance for a given agent system (for example, system description). Other MIB objects have multiple instances for a given agent system (for example, interface status for each interface on the system).

MIFs A **MIF** is a **Management Information Framework** for objects conforming to the Desktop Management Interface specification.

IRQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0456
3740
Doc:

The **Desktop Management Interface** (**DMI**) facilitates the management of PCs in a networked environment by providing a common interface and information access method. DMI provides a management framework that consists of three elements:

- A service provider (similar to an SNMP agent) software that resides on the client hardware. The service provider gathers and provides information about the host device.
- The MIF, which specifies a structure and format for defining manageable elements (similar to a MIB). A MIF is a standard set of definitions for exchanging information about hardware and software components.
- A standard Application Programming Interface (API) for local access to the management information.

There are numerous MIFs already defined, with more being developed. Some examples of MIFs include the *PC Systems Standard MIF Definitions*, the *LAN Adapter Standard Groups Definition*, and the *Software Standard MIF Definition*.

Although the DMI system works independently of the SNMP system, the information can be shared by using standard DMI-to-SNMP mappings. The mapping files are often provided by vendors who develop custom MIFs with their own custom instances. Mapping files can also be generated using tools that are readily available from other vendors.

General Operating System Knowledge

In addition to understanding networking concepts, it is critical that you have a good working knowledge of the operating system, or systems, that are present on your network. This book does not attempt to explain any concepts of the UNIX®[1] or the Windows®[2] operating systems. It frequently refers to commands and functions of these operating systems, without further explanation. Refer to the documentation that came with your operating system for more information.

Cross-Platform Issues

Since it is likely that your network environment contains a combination of systems, you need to be aware of the differences between their operating systems. Some of the differences are listed below.

- Reference pages in NNM's online help on a Windows operating system are called manpages on a UNIX operating system.
- Directories and paths are different on each system. Consult the *ov.envvars* reference page in NNM's online help (or the UNIX manpage) for a mapping of paths across systems.
- Watch your use of the forward slash (/) and the backslash (\) when entering pathnames. When switching from a UNIX operating system to a Windows operating system, it is easy to misuse one for the other.
- Do not use spaces in directory names or file names.
- Watch the use of upper and lower case of file names. Even though the Windows operating system preserves file name case, not all applications on the Windows operating system distinguish between upper and lower case. In addition, case is significant on UNIX operating systems.
- On Solaris systems, `pc nfs` must be installed, and the `pcnfsd` process running, before a Solaris management station will interoperate with a Windows operating system.

---

1. The term *UNIX* in this manual refers to HP-UX and Solaris operating systems only.
2. See the *Release Notes* for supported versions of *Windows* operating systems.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0457
3740
Doc:

- If you are using remote consoles running a Windows operating system with a management server running a UNIX operating system, be sure your NFS client product on the Windows operating system supports file locking. Not all do.

For More Information

If you need more information about networking or operating system concepts, the following documentation may be helpful.

Internet Request for Comments (RFC) Documents

Copies of RFCs are shipped on Network Node Manager's installation CD. RFC file names other than those mentioned in Table 1 may be included in the *Windows* and *UNIX* directories mentioned below.

Windows: installed on your hard drive through a custom installation in the `install_dir\doc\RFC` directory.

UNIX: in the `$OV_DOC/RFCs` directory.

Table 1 **Where to Find RFC Documents about MIBs**

To find out about...	See...	Filename
How MIB objects are defined	*RFC1155: Structure and Identification of Management Information for TCP/IP-based Internets*	`rfc1155.txt`
The protocol used to manage the MIB objects	*RFC1157: A Simple Network Management Protocol (SNMP)*	`rfc1157.txt`
The format for creating MIB object files	*RFC1212: Concise MIB Definitions*	`rfc1212.txt`
The objects contained in the Internet-standard MIB	*RFC1213: Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*	`rfc1213.txt`
Defining objects for managing MAC bridges	*RFC1493: Definition of Managed Objects for Bridges*	`rfc1493.txt`
Defining objects for managing IEEE 802.3 Medium Attachment Units (MAUs)	*RFC1515: Definition of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)*	`rfc1515.txt`
Definitions of Community-based SNMPv2C	*RFC 1901:Introduction to Community- based SNMPv2*	`rfc1901.txt`

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0458
3740
Doc:

Table 1 Where to Find RFC Documents about MIBs (Continued)

To find out about...	See...	Filename
MIB definition language for managed objects	*RFC1902:Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)*	`rfc1902.txt`
MIB definition language for conformance and capability definitions	*RFC 1904: Conformance Statements for version 2 of the Simple Network Management Protocol (SNMPv2)*	`rfc1904.txt`
Definitions of SNMPv2C protocol	*RFC 1905: Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*	`rfc1905.txt`
Definitions of SNMPv2 transport mappings for IP, IPX, and DDP	*RFC 1906: Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)*	`rfc1906.txt`
Definitions of SNMPv2 MIBs for IP, IPX, and DDP	*RFC 1907: Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)*	`rfc1907.txt`
MIB definition language for refined data types	*RFC 1903: Textual Conventions for version 2 of the Simple Network Management Protocol (SNMPv2)*	`rfc1903.txt`
Co-existence guidelines for SNMPv1 and SNMPv2	*RFC 1908: Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework*	`rfc1908.txt`
Defining objects for managing IEEE 802.3 baseband repeaters	*RFC2108:Definition of Managed Objects for IEEE802.3 Repeater Devices*	`rfc2108.txt`

Table 2 Where to Find RFC Documents about DMI and MIFs

To find out about...	See...	Filename
Desktop Management Interface 2.0 Standard	*DMTF: Desktop Management Interface Specification, version 2.0*	`dmi-v20.doc`

Table 2 Where to Find RFC Documents about DMI and MIFs (Continued)

To find out about...	See...	Filename
Access to DMI instrumentation and events using SNMP	*DMTF: DMI to SMP Mapping Standard, Version 1.0*	`dmi-snmp.doc`
General information about the DMTF and DMI	Desktop Management Task Force web site	`www.dmtf.org`
Defining objects for managing MAC bridges	*RFC1493: Definition of Managed Objects for Bridges*	`rfc1493.txt`

Web Sites

There are numerous sites on the World Wide Web that contain lists of reference materials and links to other useful networking sites. Hewlett-Packard does not endorse these sites, but has found them to contain informative references. Note that the URLs for these sites are subject to change without notice, but were valid as of the date of printing of this document.

Table 3 Web Sites Related to Network Management

Web Site URL	Description
`www.ovforum.org`	The web site of HP OpenView Forum, an association of users and developers of HP OpenView network and system management solutions
`www.iol.unh.edu/training/index.html`	Tutorial documents on network technologies and network management
`www.ietf.org`	The web site of the Internet Engineering Task Force
`netman.cit.buffalo.edu`	Archives for `comp.dcom.net-management`
`www2.tmforum.org`	The web site of the TeleManagement Forum

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0459
3740
Doc:

Table 3 Web Sites Related to Network Management (Continued)

Web Site URL	Description
www.dmtf.org	The web site for the Distributed Management Task Force, Inc.
www.opengroup.org	The web site for The OpenGroup (X/Open and OSF®)
www.ieee.org	The web site for the Institute of Electrical and Electronic Engineers
www.simple-times.org	The *Simple Times* newsletter

1 Network Management with NNM

IRQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 0460
3740
Doc:

This chapter describes the basic challenges of network management, and how Network Node Manager and other HP OpenView products address those challenges.

Topics covered include:

- How NNM can help you move toward proactive network management (page 40).
- An overview of each function of network management, and how NNM and other HP OpenView products address several of those functions (page 42).

The Network Management Challenge

As a network administrator, you are under increasing pressure to perform the necessary tasks to meet the business demands of your organization. Some of the challenges you often face include:

- Dealing with user dissatisfaction in the face of increasing user expectations. Users want to be able to have the tools they want, when they want them to maintain their productivity.
- Deploying network services so that end users maintain productivity from their desktop systems.
- Keeping the systems operating 24 hours a day, 7 days a week.
- Producing faster, more predictable response times.
- Integrating and managing diverse and complex technologies — networks, servers, databases, applications, legacy systems, web-based systems—all from different vendors.
- Managing multiple sites and global distribution.
- Moving to proactive management techniques to keep it all running smoothly.

Clearly, the demands on a network administrator are great. Network management is now a high-pressure situation where more services are requested on tight schedules with fewer resources.

How Network Node Manager Can Help

Network Node Manager is the foundation from which most of the HP OpenView products operate. When installed, the other HP OpenView products appear as added functionality within NNM. NNM not only functions as a solution on its own, but can collect data for, and forward data to, other HP OpenView products. It is the starting point for implementing a network management solution.

IRQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: Nº 0481
3740

Moving to Proactive Network Management

By using proactive, rather than reactive, network management, you can reap the true benefits of NNM. Several things must be present in order for proactive network management to be a reality.

- First, you must find out the current state of your network—what devices are present, how they are configured, how they are behaving, their performance levels, what is currently going wrong. NNM does this for you by polling for network information and screening problems through event correlation.
- Second, you must identify trends and determine how to optimize the network by changing configurations, replacing network devices, etc. NNM assists you by collecting historical information. You can easily access the historical data that NNM gathers and use it in your favorite statistical analysis programs.
- Third, you must learn how to predict what might go wrong, determine how to prevent it from happening, and learn to avoid future problems. NNM allows you to monitor thresholds of your choosing for critical network devices.

Poll for Network Information

The first step to proactive network management is to gather all the information that you can about the current state of your network.

NNM continually polls for:

- Status of objects (for example, up, down, or marginal).
- Network topology changes, including the discovery of new nodes.
- Configuration changes.

You can configure thresholds for NNM to monitor on critical network devices and configure NNM to notify you or your team members when anything goes wrong. For example, you can set thresholds on CPU loads, disk space used, interface and link errors, and collected MIB data. You can configure NNM to dial a pager when any of these situations become critical.

Watch for Events

NNM actively notifies you when an important event occurs. The event is reflected by a change in the color of the device's symbol on the map, and is reported through NNM's Alarm Browser.

Each category of alarms has a corresponding button that changes color to show the highest severity alarm in the category. Thus, you are immediately notified of potential or current problems.

You can browse through alarms to help you diagnose problems. You can view alarms by specific node or other sort criteria to help you solve problems quickly. The event reduction features in NNM monitor incoming alarms, identify patterns of common network problems, and for an identified problem, post one meaningful alarm with all related alarms nested beneath.

You can define the format of alarm messages so that they are most useful to your team. Your team can use the Alarm Browser to notify everyone else about which issues are being covered.

You can use event customization to automate some of the common fault management tasks for your team by using NNM to configure automatic actions upon the receipt of specific alarms. You can also filter out less important events, or simply send them to a log file.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0462
3740
Doc:

Network Management Functions

Network management can be defined in general terms as the ability to have a single point of control to accomplish the activities required to manage a network. Network Node Manager provides an integrated tool for the network manager to control and manage multiple networked systems and applications from a single graphical representation of the network.

When properly implemented, a network management station can result in:

- Reduced downtime of network systems and devices.
- Quick detection and correction of network problems without disrupting the network.
- The ability to monitor data to anticipate problems (predictive).
- The ability to log information for historical analysis.
- The ability to perform an action when some pre-defined event or situation has occurred.

To understand how Network Node Manager and other HP OpenView products address these problems, it is helpful to break network management down into functional categories, listed below. Following this list is an explanation of how NNM and other HP OpenView products help you manage these areas.

- Fault and Problem Management

  This function detects, isolates, and controls problems, or faults, on the network. This is carried out by network status monitoring, alarms, alerts, reporting, and predictive tools.

- Performance Management

  This function measures the performance of network hardware, software, and media, such as throughput rate, percentage utilization, error rates, and response time, through the collection and analysis of data about the network.

- Configuration and Change Management

This function is responsible for finding and setting up the network devices that control the behavior of the network. This function also includes central control of configurations.

- Accounting Management

  This function obtains statistical information on network use. You can collect and process data related to resource consumption on the network, track each individual and group's utilization of resources, and control access to the network for individuals and groups.

- Security Management

  This function protects the network and its interconnections, systems, and network management information from unauthorized access, unauthorized use, and other harm.

Fault/Problem Management

NNM's Capabilities

Often times the most difficult management task is identifying the source of a problem when it occurs. NNM helps you identify problems and errors, recognize trends, and proactively avoid problems. NMM lets you:

- Automatically discover the IP and IPX nodes in your network.
- Automatically monitor your network's status through the map interface and the event browser interface.
- Manage any vendor device that supports the Simple Network Management Protocol (SNMP). NNM manages both standard and enterprise-specific Management Information Base (MIB) objects.
- Manage non-SNMP nodes that use IP or IPX protocols.
- Manage any vendor device that supports the Desktop Management Interface (DMI). NNM monitors both standard and enterprise-specific Management Information Format (MIF) objects.
- Include new enterprise-specific Internet MIBs in NNM's MIB. Once you have loaded the new MIB module on the management station, you can access any of the MIB objects defined in that MIB module.
- Build new MIB applications (without programming) for Internet-standard and enterprise-specific MIBs. Once you have built a MIB application, you can monitor objects through the menu bar.

CPMI CORREIOS
Fls: Nº 0463
3740
Doc:

- Define event thresholds for MIB objects; for example, an event can be generated when the disk usage on a particular device exceeds a limit.
- Define actions to be taken upon receipt of an SNMP trap.
- Manage event storms and improve the information content of events by suppressing unwanted, redundant events and adding new, more informative events, using NNM's event reduction strategies: de-duplication, ECS correlations and Correlation Composer correlators.
- Integrate your own fault detection applications into the menu bar to yield an integrated management solution.
- Diagnose network faults and performance problems from one location, and diagnose problems by looking at trends over time. This includes customizing and automating the monitoring of your network and the response of management stations to events.
- Launch Systems Management Server (SMS) Administrator, or view the SMS properties of a node. From SMS Administrator, you can select a node and open the submap containing that node.
- Launch Windowsoperating system applets such as the Event Viewer, Performance Monitor, and Registry Editor from within NNM on remote systems with the Windowsoperating system.

Other HP OpenView Products' Capabilities

HP OpenView NNM Extended Topology Extended Topology augments NNM by discovering and displaying additional device connectivity information that you can use to diagnose network problems. It includes:

- Management of heterogeneous switched layer 2 environments and routed layer 3 environments.
- An enhanced web user interface with dynamic views.
- Views from protocols and technology running on top of your network, such as OSPF and VLAN.
- Launching targeted views from events for rapid problem resolution.

HP OpenView Operations IHP OpenView Operations is an event and problem management solution that allows you to identify, locate, correlate, and resolve system and network faults. It includes:

- A central management console for monitoring events.
- Intelligent agents that can be preconfigured to solve problems immediately without interacting with the management console.
- Management of workstations running UNIX operating systems, the Windows operating systems, Novell Netware, and legacy systems.
- Integration with other OpenView products.

Performance Management

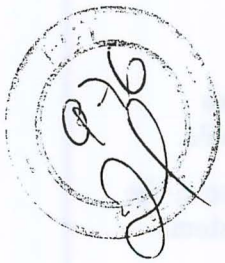
NNM's Capabilities

Figuring out how to fine-tune your network's performance can be a real challenge. To assist in this task, NNM gathers and reports information on network performance, availability, inventory, and exceptions. NNM can forward information to other HP OpenView products that provide statistical analysis on the data.

The following is a brief summary of NNM information gathering features:

- Automatically monitor your network's status.
- Collect historical MIB information about MIB objects and MIF events, store the data for trend analysis, and graph collected data. This helps you determine performance trends.
- Automatically set thresholds based upon standard deviations of historically collected data.
- Automatically collect data and generate General Availability and General Inventory reports.
- Manage and modify reports using the NNM Report Configuration Interface.
- Manage information being collected and stored in the data warehouse.
- Integrate your own performance monitoring applications with the menu bar to yield an integrated management solution.
- Diagnose network faults and performance problems from one location, and diagnose problems by looking at trends over time. This includes customizing and automating the monitoring of your network and the response of management stations to events.

EXAME Nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0464
3740
Doc:



Configuration and Change Management

NNM's Capabilities

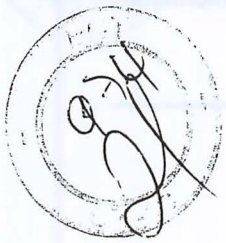
Keeping track of the devices on your network, their configurations, and their interrelationships can be time consuming. NNM helps you keep a record of this information, by allowing you to:

- Store critical configuration information from devices such as routers and switches.
- Track inventory of the devices on the network.
- Generate snapshots of your network before any departmental moves to speed reconstruction after the move.

Additional HP OpenView Product Information

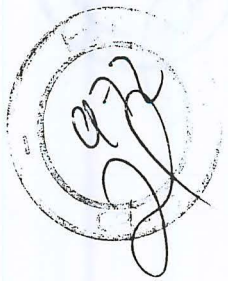
You can find additional information about other HP OpenView products and solutions at `http://openview.hp.com`.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0465
3740
Doc:



2 How Does NNM Work?

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0466
3740
Doc:



When you set up NNM to run on a management station, your team can access NNM from the management station, from remote consoles, or from the worldwide web. All three forms of access tie into the same databases running on the management station. Therefore, all members of your team continuously see the most current information. NNM works for you in the following ways, as explained in this chapter:

- Maps out your network for you. The map symbols change color to indicate if something is wrong (page 56).
- Collects critical information about your network and maintains a current log of alarms that you need to know about (page 51).
- Correlates collected information to help you quickly determine the probable cause of problems (page 61).
- Maintains a relational database from which data can be exported for historical analysis using your choice of statistical programs (page 62).
- Provides easy access to report generation, see the NNM online help for more information. See also the *Reporting and Data Analysis* online manual. You can create reports using a set of predefined templates that are populated from the data warehouse.

The remainder of this book then leads you through the process of understanding, configuring, customizing, and troubleshooting NNM.

Collecting Critical Information

NNM uses several protocols to maintain communication channels with each managed device on your network. These include:

- SNMPv1; SNMPv2
- TCP/IP
- IPX/DMI
- UDP
- ICMP
- ARP/RARP

Since SNMP is the primary protocol used for NNM's communications, an understanding of the SNMP management model will help you better understand how NNM works.

NNM also uses other, lower-level families of protocols (sometimes referred to as services), such as the ARPA family, the Berkeley family, and the NFS family. These protocols are used for functions such as file transfer, e-mail, or remote login.

SNMP's Network Management Model

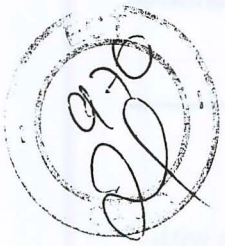
The network management model consists of a network management station, managed nodes with agents, and a network management protocol. NNM uses SNMP as its standard protocol, and uses this protocol to communicate over other protocols, such as TCP/IP, IPX, and UDP.

The Role of Manager and Agents

A manageable network consists of one or more network management stations (manager), a collection of SNMP agents, and network objects.

- A **manager** is an application that executes network management operations to monitor and control agent systems. The implementation of these network management operations is called the manager.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0467
3740
Doc:



- An **SNMP agent**, which resides on a managed node, is an application that acts on behalf of an **object** to perform network management operations requested by the manager.
- An **object** is anything that will be managed, such as a host, gateway, terminal server, hub, bridge, application, or database.

A manager and an agent may exist on the same system. The manager and agent communicate using the Simple Network Management Protocol (**SNMP**). Network Node Manager supports both SNMP version 1 (SNMPv1) and Community-based SNMP version 2 (SNMPv2C). SNMP permits the following activities:

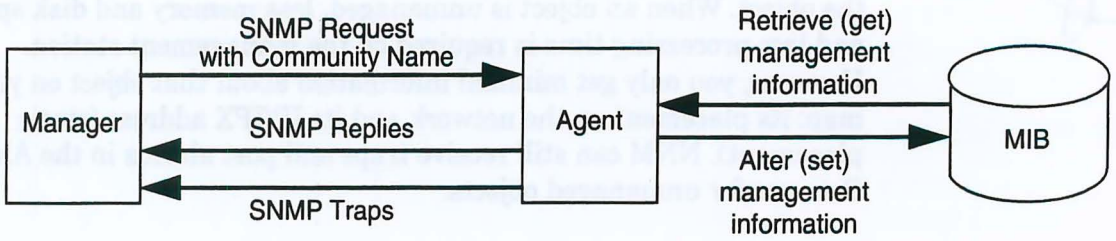
- A manager can retrieve management information from an agent. (The actual mechanism to retrieve management information depends upon the SNMP versions supported by the agent, and can include `get`, `getNext`, and `getBulk`.)
- A manager can alter, or `set`, management information on the agent's system.
- An agent can send information to the manager without an explicit request from the manager. This operation is called a **trap** in SNMPv1, or a **notification** in SNMPv2C.

Traps and notifications alert the manager to changes that occur on the agent system, such as a reboot. The agent must usually be preconfigured to know where to send traps or notifications (see page 325).

SNMP requests for information from an agent are accompanied by a **community name**. A community name is much like a password; it must be correctly received from the manager before information can be accessed from the agent. You must inform NNM about the community names that are in use on your network (see page 145). The manager accesses the agent's MIB object instances using SNMP's `get`, `getNext`, `getBulk`, and `set` operations.

Figure 2-1 shows a simplified diagram of the manager-agent interactions just described.

Figure 2-1 Manager-Agent Communication through SNMP



Basic S

There a ions associated with SNMP. They are:

- get value from a specific variable.
- getl verse information from a table of specific vari
- get
- get to a get or a set request.
- set value into a specific variable.
- tra n. A message initiated by the agent without requiring the management station to send a request.

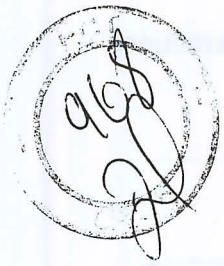
Managed versus Unmanaged Objects

A **managed object** is one that is actively being polled by NNM to determine its status and configuration. An **unmanaged object** is one that exists in the databases and within maps, but is not being polled by NNM.

NNM gives you the choice of managing or not managing objects, depending on your information needs and network resources.

When an object is managed, NNM can obtain any information that you specify about that object (as long as that object's protocol is supported). The more objects you manage, the more memory and disk space is required on the management station. In addition to the information that you specify, the management station will need processing power for the

DOS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 53
0468
3740
Doc:



routine status and configuration polling and the event monitoring of each managed object. If an object is critical to the network function, then you should manage it.

If the object is not critical to the functioning of your network, you might choose to *unmanage* it; which means that NNM will not actively monitor the object. When an object is unmanaged, less memory and disk space and less processing time is required on the management station. However, you only get minimal information about that object on your map: its placement on the network and its IP/IPX address (static placement). NNM can still receive traps and post alarms in the Alarm Browser for unmanaged objects.

Desktop Management Interface (DMI)

The Desktop Management Interface (DMI) is a parallel management strategy to SNMP. DMI standards were developed by the Desktop Management Task Force (DMTF). Although DMI is entirely independent from the SNMP protocol, there are many similarities:

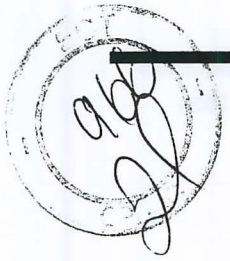
- The DMI **client** is similar to the SNMP management station.
- The DMI **service provider** is similar to the SNMP agent and must be running on each remote DMI device.
- The DMI **MIF** (Management Information Format) file is similar to the SNMP MIB file and defines the management information that can be provided by the service provider (event) or requested by the client (get/set).
- The **DMI event** is similar to the SNMP trap.

If your management station is running NNM on the Windows operating system, during discovery polling, NNM **subscribes** to receive DMI events from all managed systems running DMI version 2.0. All DMI events are received by NNM's `ovcapsd` service (background process) and converted to SNMP traps as specified in the Desktop Management Task Force's DMI to SNMP Mapping Standard. The SNMP-equivalent message is posted to NNM's Alarm Browser.

NOTE If your management station is running NNM for a UNIX operating system, you must communicate with the DMI service provider indirectly through an SNMP agent installed on the remote DMI-enabled device itself along with a DMI-to-SNMP mapping agent. The SNMP agent then

handles all communications. Therefore, NNM doesn't need to subscribe to the DMI service provider in order to receive DMI events from this node.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0469
3740
Doc:



Automatic Discovery and Layout

When you start the NNM background processes, all IP and Level 2 devices (devices that support bridge, repeater, and MAU MIBs) on your network are automatically discovered and mapped out. If you are running NNM on a management station running the Windows operating system, IPX devices are also discovered and mapped out. This map is a visual representation of the communications channels established between NNM and the devices in your network. Be aware that this map is not a physical representation; rather, it is a logical representation. The accuracy of these communications channels between NNM and your network devices determine whether or not NNM can provide the information you need in order to manage your network.

The initial polling process may take several hours, or even over night, to discover all the devices on your network. However, it is worth the wait! You start benefiting from NNM immediately. You will use NNM's default map, and Alarm Browser to pin-point any gaps in your well-configured network scheme.

How IP Discovery and Layout Work

The `netmon` service (background process) uses a combination of SNMP requests and ICMP `pings` transmitted over UDP and IPX to find out about the nodes on your network.

To discover the nodes on the network, `netmon` needs access to the following information:

- The subnet mask from the agent on the management station.
- The address of the default router in the management station's routing table.
- SNMP information from, at a minimum, the default router, and from other routers and nodes on the network.

For `netmon` to work, it requires the following:

- The management station must be correctly configured for networking.
- The management station must be running an SNMP agent.

- Nodes must be up and responding to ping requests to be discovered.
- All gateways/routers and the management station must have correctly configured subnet masks for all interfaces.

During IP discovery, netmon works best in these situations:

- The more routers in the network the better; and those routers should be running configured SNMP agents.
- The more nodes running configured SNMP agents the better.
- The more SNMP information netmon gets the better; for example, valid ARP caches and, from serial connections to routers, routing tables.

Information about the discovered nodes is stored in NNM's databases and is used to automatically generate the network map.

Over time, NNM will discover new nodes on the network. However, if a new node never talks with a gateway or other nodes on the network that support SNMP, NNM may not find it. In this instance you can use menu items within NNM to send a low-level ICMP ping that forces NNM to discover the node; or you can add the node manually.

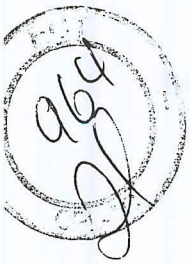
How IPX Discovery and Layout Work

If you are running NNM on a management station running the Windows operating system, in addition to discovering IP nodes on your network, netmon performs IPX discovery of your network. However, the methods used are very different from those used for IP discovery. The IP discovery process relies primarily on SNMP queries to gain hints of new IP nodes. For IPX discovery, netmon relies on using broadcast versions of various IPX protocols to discover the nodes, then uses SNMP once the node is discovered to fill in additional information about the node. In particular, netmon will be able to determine that an IPX node supports IP only if that node supports SNMP over IPX.

While the discovery model is different, the layout results in the submap are very similar. IPX network symbols are created in the Internet submap, connected by IPX gateways. IPX network symbols can be exploded to display segment and node submaps. However, IPX nodes always are connected to a single segment in the IPX network.

To discover IPX nodes on the network, netmon requires the following:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0470
3740
Doc:



- The management station must be correctly configured for IPX networking.
- At least one IPX server or router must be connected to the same network as the management station.
- Nodes must be up and responding to IPX diagnostic requests to be discovered.

During IPX discovery, `netmon` works best in the following conditions:

- The management station is not also an IPX/NetWare gateway.
- Servers, routers, and nodes in the environment respond to IPX diagnostic, Routing Information Protocol (RIP), and Service Advertising Protocol (SAP) requests.
- IPX nodes in the environment support SNMP over IPX.

As with IP discovery, the information about the discovered nodes is stored in the NNM's databases and is used to automatically generate the network map.

Because `netmon` uses broadcasts, most IPX nodes should be recognized after the first few IPX polling cycles. After the default IPX discovery interval of six hours, most IPX nodes will be discovered, with the majority coming soon after the initial discovery cycle at system installation or startup. However, this discovery rate will vary depending on the number and type of nodes in the network. So before you start to troubleshoot `netmon`, allow the process sufficient time to discover your network. This may require allowing IPX discovery to run over night.

Interactions Between IPX Discovery and IP Discovery

If an IPX node supports SNMP over IPX, `netmon` will attempt to use the MIB-II `ipAddrTable` to also include IP addresses and interfaces on the IPX node, as well as using the other MIB-II variables to provide additional information. When a node is discovered to support both IP and IPX, the following rules apply:

- Preference is generally given to the IP values as the name and labels for the node.
- After a node is determined to support IP, IP will be the preferred SNMP transport protocol.

- If a node is first discovered as an IP node, and a later IPX node is discovered to have the same set of IP addresses via SNMP, the IP node may be deleted in favor of the IPX node. For this reason, we recommend that you delay extensive map customization until IPX discovery is complete.

Level 2 Discovery

NNM takes advantage of information provided in three standard MIBs to discover bridges (switches) and hubs. These MIBs are the bridge MIB (RFC 1493), the repeater MIB (RFC 2108), and the 802.3 MAU MIB (RFC 1515). If a network device supports any of these MIBs, `netmon` will use the information reported to develop a model of the topology which better represents how and to what the device is interconnected.

In the case of switches and bridges, additional information is gathered from the bridge MIB. In the case of hubs, addition information is gathered either from the repeater MIB or the 802.3MAU MIB.

The status of non-IP or non-IPX interfaces on switches, bridges, and hubs is determined via SNMP based on the administrative and operating status of the port.

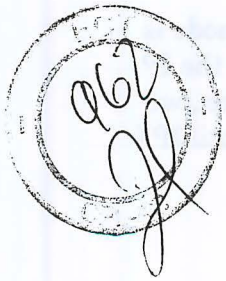
If the MAC address of a node, which does not support IP or IPX, is reported by any of these MIBs, the node is added to the topology relative to the device which hears it. A label for this device is determined by the MAC address reported by the network interface card. Because no MAC layer control message protocol is available, the status of the devices is determined indirectly via information provided by the surrounding network elements.

Trunking and Meshing

Configuring two or more ports between two network devices into a single group is referred to as port trunking. This is done to increase the available bandwidth between the two devices. For example, you can increase the available bandwidth between two devices, such as two ethernet switches, by configuring a group of two or more connections between the two devices.

Meshing involves connecting devices on the network via multiple paths. Meshing is used when devices are used in a critical function and redundant network connectivity is required.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0471
3740
Doc:



You can configure NNM to label port trunking and meshing connections with information you add to the `netmon.equivPorts` file. See "Configuring Trunking and Meshing" on page 225 for more information.

Event Reduction Capabilities

NNM includes several event reduction capabilities that identify relationships between different events to quickly determine the root cause of problems, such as event storms. This improves the information content of alarms by suppressing unwanted, redundant alarms and adding new, more meaningful alarms.

You see fewer, but more informative alarms that show the relationships and dependencies between network events. It then becomes easier to identify trends, to isolate important events, and to react more quickly to problems. You view these events through the NNM Alarm Browser.

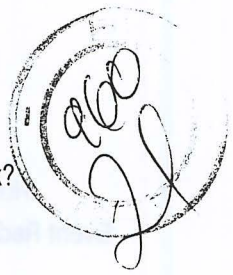
Event reduction involves processing events based upon relationships between individual events. Event reduction:

- Analyzes events based upon previous, current, or subsequent events.
- Can create new events.

  By analyzing the relationships between events in the stream, single events can replace groups of events. These events may have increased information content, and can be of a different protocol, compared to the original events.
- Dramatically reduces the number of alarms displayed by the NNM Alarm Browser.
- Correlates alarms between different event protocols.

NNM contains pre-defined event reduction configurations that you can modify, if desired. You can also create your own new ones to address specific needs within your environment. Refer to "Event Reduction Capabilities: Getting to the Root Cause" on page 351 for more information about these features.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0472
3740
Doc:



NNM's Databases

NNM provides several operational databases, each designed to store specific kinds of data and used for a variety of purposes. In addition, NNM includes a data warehouse: a relational database used to store historical information about your network.

For more information about the NNM databases and the data warehouse, consult the online manual *Reporting and Data Analysis with HP OpenView Network Node Manager*.

Operational Databases

NNM's operational databases—object, map, topology, trend, and event—can be thought of as a single logical database. These databases store the operational data used by NNM, putting critical information at your fingertips.

The Object Database

The object database contains semantic information about symbols on the map. The information is generic; that is, it is not customized to any specific application. The object database contains field definitions such as `sysObjectID`, vendor, and SNMP Agent. You can see the field values in the object database for a particular object through the `Properties` dialog box for that object.

Map Database

The map database contains presentation information specific to each map. Examples of presentation information that is stored in the map database include the exact symbol placement on the map, the symbol associated with each object, and symbol labels. NNM updates the map database based on requests from the user, or from various NNM services.

Topology Database

The topology database manages information critical to the management of IP nodes. It includes state information, such as time stamps indicating when the object last changed and when it should be polled next. This

information helps NNM detect changes and communicate them to various NNM services. The topology database is stored in a proprietary HP OpenView format.

Event Database

The event database is the repository for SNMP traps and OVW events that are received by NNM. It also stores events that are output from the Event Correlation Service (ECS). In addition, the event database stores information for the event browser tools about the state of the events displayed in the web browser applications. The information in the event database is displayed in the Alarm Browser.

Trend Database

The trend database (sometimes called the `snmpCollect` database) stores MIB data and threshold information that is gathered through the `snmpCollect` service (process). Information from the trend database is used in the Reporting and the Data Collection features, and can be viewed with the Grapher feature of NNM on a management station.

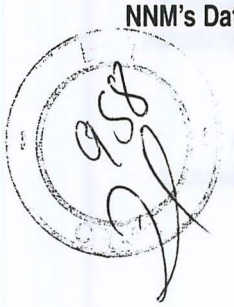
Data Warehouse

The NNM data warehouse stores data exported from the NNM databases into a relational database. You export this data to the data warehouse using the `Tools:Data Warehouse` menu choices (`Export Topology`, `Export Events`, and `Export Trend Data`).

You can use the information in the data warehouse to define your own reports. You can also use the NNM web Reporting interface to configure and view reports. When you create a report using the web Reporting interface, NNM automatically starts exporting the appropriate data to the data warehouse.

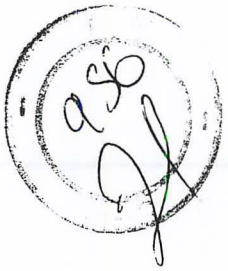
An embedded relational database is provided with NNM, and Oracle® and SQLServer are also supported.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0473
3740
Doc:



3 Resources Available While Learning NNM

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0474
3740
Doc:



There are many resources included with NNM that will help you use the product more effectively. In addition, there are also multiple additional services available through HP.

Resources included with NNM:

- Online help system (page 67)
- Tip of the Day (page 69)
- NNM's manuals, both printed and online (page 69)
- Release notes (page 71)
- Online reference pages/manpages (page 71)
- `contrib` programs (page 74)
- `support` directory (page 74)
- White papers (page 75)

Resources and services available through HP:

- HP web sites (page 76)
- HP Consulting Service (page 76)
- HP Education (page 77).
- HP Product Support (page 77)
- OpenView Forum (page 77)

Resources Included with NNM

NNM Online Help System

NNM includes an online help system that contains all the specific procedural information you will need while you are working with NNM. The help system has extensive search capabilities and a comprehensive index so you can easily find information. You can print or copy pages or sections of help information that are appropriate for the most common tasks for your organization.

TIP The help system includes hyperlinks that make it more convenient and informative. By clicking on designated link words, you gain instant access to more topics and information related to your currently selected topic.

The online help system enables you to display information on the features of NNM, explains how to perform tasks with NNM, and includes conceptual information about how NNM works. Help entries are available from three general locations:

- `Help` menu
- `[Help]` button on dialog boxes
- Help from some symbol pop-up menus

Using the Help Menu

The contents of the `Help` menu varies from one submap to another, depending on additional installed applications. The `Help` menu also differs between NNM on a workstation running the UNIX operating system, NNM on a workstation running the Windows operating system, and the NNM web interface.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0475
3740
Doc:

Printing Information from Online Help

NNM for the Windows operating system uses a standard Microsoft® Windows help system. Each help window has a `Print` button or menu item that you can use to print the current topic. You can also select multiple topics in the help table of contents, then print those topics.

On UNIX operating systems, you can select a topic in the `Contents` window of help, then select the `Print` menu item. In the `Print` dialog box, select `Print Topic` to print only that topic. If you want to print all the subtopics under that topic, select `Print Topic and All Subtopics`.

You can then combine these help printouts into a binder for future reference. This is especially useful for frequently-accessed information, so that you do not have to access the help system every time you need to look up common task or function. You can also use these printouts to supplement operating manuals.

Searching for Information

The most direct way to find a particular help topic is index search. You can search via the `Index` tab in the help system on a Windows system or by the `Index` button on a UNIX operating system. The help system is indexed by the keywords that are used in topics. When using index search, enter the word that best describes what you are looking for and that is most likely to narrow down your search. For example, if you want to find help on automatic map layout, enter the word "automatic" or "auto-generate" rather than "layout". Those words are more likely to find the entry that you want.

In a Windows operating system only: another way to find information is by using the `Find` function in the online help. The `Find` function searches every word in every topic for the word or phrase of your choice, and returns a list of the titles of topics where those words or phrases appear.

Customizing Information for Your Organization

You can create custom information for your team or for a specific site within your organization. Simply copy and paste the contents of a help window to a word processor. Then add your own site-specific information or specific procedural information for your tasks to the help text. This can save you time when writing your own training or procedural manuals.

Using Online Help Independently from the Software (Windows only)

The NNM help system on the Windows operating system is designed so that you can copy the help volume onto a diskette, take it with you, and run it independently of the software—whether on your home computer or traveling with you on your laptop.

Copy the following files to a floppy disk. These files are found in the *install_dir*\help\%LANG% directory:

- *help_file_name*.hlp
- *help_file_name*.cnt

Double-click on the *help_file_name*.hlp file to start the help system.

Using Dialog Box Help

The [Help] button in a dialog box explains the purpose of the dialog box.

Using Symbol Pop-up Menu Help

The right mouse button pop-up menu on a selected symbol may contain a help item for that symbol. You can customize this menu through the application registration file (ARF) to add a help topic if it does not already contain one.

Tip of the Day

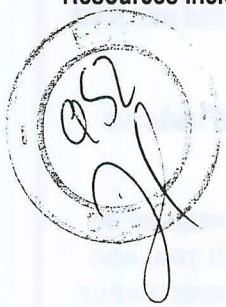
When you start NNM on the Windows operating system, the Tip of the Day appears. Add new tips by editing the *install_dir*\help\%LANG%\tipOfTheDay.txt file. Turn off Tip of the Day by removing the check from the Show tips at startup check box located in the Help:Tip of the Day menu.

Manuals: Printed and Online

NNM includes a library of detailed reference materials for your use. Some are provided in printed form, some are provided online as PDF files. Get additional information from the online help or the release notes. The following manuals are provided with NNM.

- *Installation Guide for HP OpenView Network Node Manager*

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0476
3740
Doc:



This manual contains instructions about installing and configuring NNM.

- *Welcome to Network Node Manager*

  An overview of NNM, its features, and its capabilities.

- *Managing Your Network with HP OpenView Network Node Manager*

  This manual (that you are currently reading) contains detailed information to help network administrators configure, maintain, and troubleshoot NNM for their team.

- *Correlation Composer's Guide*

  This manual provides information about the HP OpenView Correlation Composer. You can use the Correlation Composer to create new event correlation logic. Be sure to read the information in Chapter 11, "Event Reduction Capabilities: Getting to the Root Cause," on page 351 before you start.

- *Guide to Scalability and Distribution for HP OpenView Network Node Manager*

  This advanced manual outlines the steps you need to take to deploy NNM across multiple management stations within your organization. It contains specific configuration procedures for using the scaling and distribution features of NNM. These features are important when the size of your organization's network exceeds the resources of one NNM management station. They allow you to divide the work load among multiple management stations, yet share the network management information as needed.

- *Reporting and Data Analysis with HP OpenView Network Node Manager*

  This manual is available only online and contains information about configuring and using NNM's reporting and data warehouse features. This book also contains information about how to export the historical data collected by NNM for your use with other statistical analysis programs of your choice.

- *Creating and Using Registration Files*

  This advanced manual is available only online and contains information about how to create and modify NNM's registration files, customizing the appearance and behavior of NNM.

- *Integrating HP OpenView Reporter*

  NNM and HP OpenView Reporter can be integrated, so that Reporter can query the NNM data warehouse to generate reports that help you to solve real network problems. This manual shows you how to configure the integration, as well as how to run and view reports. It also describes the preconfigured reports that are provided.

To access the online manuals shipped with NNM, use the `Help` menu. When you choose `Online Manuals`, a list of manuals appears. Choose the manual you want to view, and follow the instructions in the viewer.

Numerous additional HP OpenView online manuals are available at the following web site: `http://www.docs.hp.com`

Release Notes

For information about NNM that becomes available after this book is published, refer to the `ReleaseNotes` directory or the `README.html` file on the CD-ROM.

Release notes are available on your hard drive after installing NNM. You can access the release notes from NNM's menu `Help:NNM:Release Notes` (or on the Windows operating system under `Start:Programs:HP OpenView:HP OpenView Online Documentation:NNM Release Notes`).

You can also launch the release notes in your web browser:

Windows:

install_dir\www\htdocs\%LANG%\ReleaseNotes\README.html

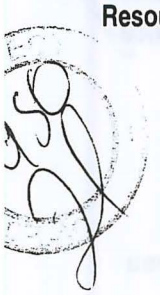
UNIX: `/opt/OV/www/htdocs/$LANG/ReleaseNotes/README.html`

NOTE In this manual, `C` and `$LANG` in directory listings are variables for the language currently in use. `C` contains the English version.

Reference Pages (Manpages)

Reference pages (Windows operating system) or manpages (UNIX operating system) document NNM configuration possibilities in much greater detail than you will find any place else. These pages include information about every possible parameter and available command line

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0477
3740
Doc:



option, as well as useful background information that may be helpful when troubleshooting issues. These pages are named according to the function or feature that they are documenting.

Throughout this book, you will be referred to specific reference pages (manpages) for more information about the topic being discussed. You may want to browse through this resource collection yourself. You will find many more reference pages than are mentioned in this book.

Accessing Reference Pages

On Windows operating systems, reference pages are provided through the help system. You can access them from these locations:

- `Start:Programs->HP OpenView->HP OpenView Online Documentation->NNM Reference Pages`.
- Any submap within NNM, through the `Help` menu.

TIP

If you are not sure which reference page to access for a specific issue, use the `Find` feature of the help system. `Find` searches every word in every reference page and provides a list of all places where the word appears. For example, if you want to learn about the `netmon` service's parameter choices and relationship to other services, type `netmon` in the `Find` dialog box.

Accessing Manpages

On HP-UX systems, the following procedure is just one suggestion for displaying or printing manpages. This procedure requires that you have manpages installed locally on your system. (If your network provides manpages remotely instead (for example, from a central server), then check with your system administrator about how to access them.)

1. Determine where on your system the manpage files are kept. Type

   `echo $MANPATH`

   You should see a list with one or more directories. Multiple directories will be separated by colons (for example, `/usr/local/man:/usr/man`). It is recommended that you check the contents of each directory to make sure it actually has manpage files in it.

If you do not see a list of directories or you get no response to the `echo $MANPATH` command, refer to the section "Establishing Universal Pathnames" in Chapter 5.

2. Determine what syntax and options the `man` command is using. At a command-line prompt, type:

   `strings /usr/bin/man | grep col`

   You should receive a message similar to the following:

   ```
   tbl -TX %s |neqn|nroff -h -man|col -x > %s
   tbl -TX %s |neqn|nroff -man|col -x|%s
   ```

3. Use the command syntax shown in Step 2 in one of two ways:

   - Specify the qualified path of the directory containing manpage files as the `%s` value in the command.

     Example: you know that the *bggen*(1) manpage is stored in the `/usr/man/man1` directory on your system, but you are not currently in that directory. To display this manpage online, type the following command:

     `tbl -TX /usr/man/man1/bggen.1 |neqn|nroff -man|col|more`

     Example: to send the *bggen*(1) command's manpage to a file for printing instead, type the following:

     `tbl -TX /usr/man/man1/bggen.1 |neqn|nroff -man|col > /filename`

   - `cd` to the directory on your system that contains manpage files. Then specify just the command name and number as the `%s` value.

     Example: you are in the `/usr/man/man1` directory. Display the *bggen*(1) command's manpage online by typing:

     `tbl -TX bggen.1 |neqn|nroff -man|col| more`

     Example: to send this manpage to a file for printing instead, type the following:

     `tbl -TX bggen.1 |neqn|nroff -man|col > /filename`

On Solaris systems, consult your system documentation for information on accessing manpages online or printing them.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0478
3740
Doc:

The contrib Directory

The NNM `contrib` directory is a collection of programs and extensions to existing NNM programs that HP programmers have developed and want to share with NNM users.

The `contrib` directory contains a README file explaining the files in the directory. Many of the individual programs have README files as well, which contain information specific to the program.

When you install NNM on a UNIX operating system, the `contrib` directory is installed by default.

To install the `contrib` directory on a Windows operating system, you must use the "Custom Installation" feature.

The files are installed in:

Windows: *`install_dir`*`\contrib\NNM`

UNIX: `$OV_CONTRIB/NNM`

These programs are not supported by Hewlett-Packard and, as such, you use them at your own risk.

The support Directory

The NNM `support` directory is a collection of programs and Perl scripts that HP support engineers have developed and want to share with NNM users.

The `support` directory contains a README file explaining the files in the directory.

When you install NNM on a UNIX operating system, the `support` directory is installed by default.

To install the `support` directory on the Windows operating system, you must copy and paste the `support` directory from the NNM Installation CD to the management station's hard drive. Place the `support` directory in the following location:

The files are installed in:

Windows: *`install_dir`*`\support\*.*`

UNIX: `opt/OV/support/*`

These programs are not supported by Hewlett-Packard and, as such, you use them at your own risk.

White Papers

White papers are documents that explain various technical aspects of NNM and network management in general. Often these topics are not documented elsewhere.

When you install NNM on a UNIX operating system, the current white papers are installed by default.

To install the white papers on a Windows operating system, you must use the "Custom Installation" feature.

The white papers are installed in:

Windows: `install_dir\Doc\WhitePapers`

UNIX: `$OV_DOC/WhitePapers`

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0479
3740
Doc:

Resources and Services Available Through HP

You can find more information from the following sources:

- HP web sites
- HP Consulting Services
- HP Education
- HP Product Support
- OpenView Forum

HP Web Sites

General Information

Using a web browser, you can learn more about HP OpenView by visiting the main HP OpenView web page at: `http://openview.hp.com`.

This web site contains information on current products, as well as literature that you can print or download for viewing. There are links to HP technical support and sales offices.

Product Manuals

There is also a web site for accessing current HP OpenView product technical manuals that you can download and print. These manuals are available in PDF format. Its URL is:

`http://openview.hp.com`

Click on the `Support` icon, then select `Manuals`.

Another web site presents HP OpenView product manuals in searchable web-based format: `http://www.docs.hp.com`.

HP Consulting Service

The HP Consulting Service provides a wide range of consulting services, including initial installation and configuration, and network planning and organization. They can also help you plan and implement advanced strategies to help you take the best advantage of NNM's capabilities to

meet the specific needs of your organization. For more information about their services, visit the main HP Conculting web site, `http://www.hp.com/go/consulting`.

HP Education

HP Education presents numerous classes on Network Node Manager and HP OpenView, geared toward different levels of training. For more information about course descriptions and class schedules, visit the main HP OpenView web site, `http://openview.hp.com`.

HP Product Support

HP has more than 40 Response Centers worldwide offering telephone support in native languages and time zones. To register for telephone support, contact your local HP sales representative, or browse the HP OpenView web site at `http://openview.hp.com`.

In addition, HP offers software and materials support contracts so that you can automatically receive the newest versions of applications as they are available.

OpenView Forum

OpenView Forum is an association of users and developers of HP OpenView network and system management solutions. An independent corporation, the OpenView Forum represents a vast body of practical knowledge and experience provided through conferences, a web server, an email reflector, and personal contacts.

The OpenView Forum online discussion center provides members with a place where they can gain information and knowledge, and provide feedback to software developers about HP OpenView products.

OpenView Forum sponsors a conference each year, which is attended by vendors and more than 1000 Forum members. You can find out more about OpenView Forum at their web site: `http://www.ovforum.org`.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0480
3740
Doc:

Summary of HP OpenView Web Sites

Table 3-1 presents a summary of the HP OpenView Web sites.

Table 3-1 Summary of HP OpenView Web Sites

HP Web Site	Contents
openview.hp.com	The primary web site for HP OpenView. Contains links to: HP OpenView training information Product literature Product manuals
www.hp.com/go/consulting	HP Consulting Services
www.docs.hp.com	Product manuals in searchable web-based format.
openview.hp.com-click on support panel	Access to HP support.
www.ovforum.org	OpenView Forum's web site where you can exchange information with other OpenView users.

4 Planning Your NNM Configuration

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0481
3740
Doc:

In order to get NNM the most benefit from NNM, you will probably want to configure NNM for your particular environment. NNM is a powerful program that can be configured in many ways. You need to budget time for planning how you wish to configure NNM and time for actually doing the configuration.

In order to make the whole process run as smoothly as possible, this chapter explains the issues to consider as you begin:

- "Budgeting Time for Planning and Configuration" on page 81
- "Taking Over NNM from Someone Else" on page 82
- "Understanding the Network Information Needs of Your Organization" on page 83
- "Knowing Your Network" on page 87
- "Starting with a Well-Configured Network" on page 90

Budgeting Time for Planning and Configuration

NNM is an extremely flexible program that can be configured to meet a large number of business needs. Read through this entire chapter before you begin configuring NNM. Clearly identify the specific ways in which you will use NNM to assist you in managing your management domain, to minimize the time you spend configuring NNM.

Time for Planning

If your management domain is small, this planning process could be quick. If your management domain is large and complex, it may take multiple meetings to gather the information that you need.

Time for Configuration

A quick sketch of the configuration process outlined in this book is:

- Install NNM--initial discovery, customization, and troubleshooting.
- Establish backup procedures for NNM's critical files.
- Configure NNM's active polling configuration.
- Configure the maps.
- Configure the event monitoring system.
- Decide what historical information is most useful, and establish data collection toward that objective.
- Establish the maintenance procedures and schedule.

Network management is complex and specific to each organization's needs. NNM can best assist you to meet your network management goals if it is optimally configured. Allow sufficient of time for the configuration process.

You need to have a clear idea about what devices you want to monitor, what kind of information you need from these devices, and how often you need the information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0482
3740
Doc:

Taking Over NNM from Someone Else

If you are responsible for taking over after someone else installed and configured NNM, browse through the chapters in this book in the order in which they are presented. As you read along, rather than configuring NNM, simply access all the configuration points as they are described to determine how NNM is currently configured. Once you understand the current configuration, you can go back through the process and implement your own ideas.

Understanding the Network Information Needs of Your Organization

To use NNM to its full potential, start with a clear idea of the business needs that NNM must address. You need to understand the groups within your organization and their information needs. You also need to start with a good understanding of your network itself.

Who Needs What Information?

First identify the groups within your organization who need access to information about the network. For example, upper management, facilities, technical support, and the printers group.

Then, identify what information each group needs, why they need it, and how they will use the information. For example, do they need real-time monitoring of specific devices around the clock or only during specific shifts for network troubleshooting? Do they need to know monthly trends of the volume of network traffic generated by each department for planning purposes?

Use the work sheet provided (page 85) as a starting point and detail the information needs of each group. Then decide which groups could share a map. Have a clear idea about what information everyone needs and how they want to receive that information before you start.

Ideal Uses for Maps

- At-a-glance notification that something has gone wrong.

  NNM's color-coded status notification alerts your team members immediately when a network or device is in trouble.

- Connectivity at-a-glance.

  A visual untangling of your network, the definitive authority of how everything is connected. The map is kept up-to-date automatically.

- Simultaneous monitoring of multiple sites.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0483
Doc: 3740

NNM can span multiple sites. In addition to NNM's map and alarm list, NNM's pull-down menus provide troubleshooting tools that allow your team to gather information and troubleshoot problems at the remote site.

- Quick response time.

  NNM's maps can be configured with floor plans of your site to speed your team's efforts in investigating hardware failures. If your team has a high turn-over rate, well designed maps can reduce training time.

- Establishing sphere of influence or management regions.

  You can have different maps for different areas of responsibility on your network. A map can manage a specific physical portion of your network or partition information about your network. Maps can have specific constraints and characteristics, run different applications, cover different geographic areas, and/or set compound status differently. You can customize maps so that they become a projection of your team member's responsibilities, showing what your team member wants to see about your network without requiring him/her to sifting through unneeded data.

Ideal Uses for the Alarm Browser

- Instant awareness of failures.

  NNM's Alarm Browser guarantees the speediest possible response, since your team members know instantly when trouble arises.

- Watching trends.

  Configure NNM to post threshold alarms from your mission-critical devices. Your team members detect developing trouble and start resolving it before users encounter network failures.

- Identify the device that is most likely causing the problem.

  NNM's event correlation system identifies the source device of certain issues and consolidates all alarms that were generated as a result of the root cause issue under the main alarm message.

- Automate responses.

You can configure NNM to automatically page or email a specific person whenever an alarm is received about a specific device. You can also configure a pop-up window to appear over the NNM map if a certain event occurs or launch any customized action that you wish.

- Facilitate team communication to eliminate duplicate efforts.

  Your support team can use NNM's Alarm Browser as a prioritized to-do list. Each team member can select issues to work on and change the alarm's status to *Acknowledged.* Everyone on the team will see immediately that the alarm is being addressed.

- Distribute responsibility.

  You can set up custom categories for incoming alarms and configure specific devices to post their alarms to your custom categories. For example, configure the alarms generated by devices in each department to post their alarms to a category identifying the department. Your team members can access the alarm list that applies to them, without needing to sort through alarms for all departments.

Work Sheet for Planning

Group/user: _____

Role/purpose: _____

Organization/Location: _____

Hours/shift: _____

Email address: _____

Phone number: _____

What do they need to know?

How often do they need this information?

Why do they need to know?

Which devices do they need to monitor?

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0484
3740
Doc:

What type of system will they use to access NNM?

Which MIB value or MIB expression would provide access to this information?

What would be the most beneficial form in which to receive the information?

___ Map displayed on a monitor (map configuration)

___ Alarm list (event configuration)

___ Email (automatic action programmed through Event configuration)

___ Pager message (automatic action programmed through Event configuration)

___ Web site access

___ Reports

Knowing Your Network

You probably maintain lists of the devices that are currently installed on your network. Use your current lists when first installing NNM in order to verify that everything has been successfully discovered. Your lists will also be useful while deciding how often NNM should monitor each device for you.

Deciding to Manage or Not to Manage Devices

Because NNM is actively polling your network devices over standard network protocols (ICMP, SNMP, and IPX), a certain amount of network traffic is generated for each managed device. You need to determine the appropriate polling frequency in your business environment. Identify the mission-critical devices on your network, typically your routers, switches, hubs, and key servers. You will want to configure NNM to monitor these devices most frequently. NNM allows you to configure groups of devices by using wildcards or a number of other identifiers. Therefore, if you have a clear idea of where you are heading, the configuration process will be much easier and quicker.

For planning purposes, consider grouping your network devices into three network management categories:

- Mission-critical devices.

  You will monitor these devices aggressively, perhaps configuring NNM to poll them two or three times per minute to verify that continuous service is available. You may want to use NNM's event configuration to maximize the use of information available through these devices' SNMP agents and MIB files. Also consider collecting performance data for later trend analysis. Balance your desire for data and polling against the overhead you are imposing on devices.

- Important, but not critical.

  You will configure NNM to monitor these devices less frequently: perhaps your printers, certain application servers, firewalls, http proxies, etc. Depending on the situation at your site:

  — Every few minutes?

  — Every few hours?

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0485
3740
Doc:

— Every few days?

- Devices that do not require active monitoring.

  Not important enough to warrant generating network traffic (for example individual PCs). Therefore, you can disable NNM's polling of these devices by setting them to *unmanaged* or you can configure polling to run very infrequently.

  Although you configure certain devices or groups of devices to be *unmanaged* by NNM, the device's SNMP agent can be configured to forward traps to the management station if anything goes wrong. These traps will appear as alarms in NNM's Alarm Browser once you configure them to do so by using NNM's event configuration feature.

  NNM can be configured either to include the unimportant devices on your maps or to exclude them from the map.

Work Sheet for Devices

Identify which devices on your network fit into the following groups. Your list will come in handy when you are troubleshooting NNM's initial discovery, when you are customizing NNM's polling configuration, and when you are creating customized maps for your team.

- Mission-critical devices.

  Must be frequently monitored on a proactive basis to ensure continuous service.

- Important (but not critical) devices.

  These devices can be monitored less frequently than mission-critical devices. For example: you may want NNM to monitor some devices every 30 minutes, or every 12 hours, or every 7 days. Decide upon meaningful monitoring frequencies for different groups of your network devices

- Devices that do not require network management.

  These devices do not require active monitoring (their SNMP agents can be configured to forward traps to the management station if anything goes wrong).

TIP Network devices that did not show up on anyone's worksheet from the previous section in this chapter probably do not need to be actively managed by NNM.

RQS nº 03/2005 - CN - CPMI CORREIOS
Fls. Nº 0486
3740
Doc:

Starting with a Well-Configured Network

As explained in Chapter 2, "How Does NNM Work?," on page 49, NNM communicates with the devices on your network through standard network protocols. For NNM to gather accurate information, your network needs to be in a well-configured state so that each device can be successfully accessed.

The following aspects of a well-configured network do not need to be in perfect shape on your network before you install NNM. However, the closer you are to having a well-configured network, the quicker and easier it will be to configure NNM. Relevant issues include:

- Consistent IP addressing scheme
- Consistent subnet masks configured
- DHCP address ranges identified
- Consistent name resolution scheme (such as DNS or NIS)
- SNMP agents configured on each device:
  - — Know the agent's GET- and SET-community names
  - — Update the trap-forwarding (trap destination) list to include the NNM management station
  - — Know which MIB is being used and obtain a copy of it to load into the NNM management station's MIB database later on

Consistent IP Addressing Scheme

A list of your *network-level* IP addresses would be handy to have during the initial discovery process so that you can quickly verify that NNM has successfully discovered everything you need. This list could also be used to create a seed file to speed the discovery process.

Remember that all devices that you wish to manage must have a valid IP address. For hubs and other network devices that normally do not have IP addresses and enabled SNMP agents, it is often possible to manually establish them. Determine if the device can support SNMP, then physically visit each device or access it through a terminal and take the necessary steps to assign an IP address and enable the SNMP agent. Contact the device's vendor if you need more information.

Subnet Masks Consistently Configured

If the subnet masks on the management station or configured on your network devices are incorrect, discovery may be different from what you expected. If the subnet mask is too restrictive, you won't discover your whole management domain. If the subnet mask is not restrictive enough, you discover more than you bargained for.

Non-contiguous subnet masks (for example, 255.255.0.255) are not supported by NNM. Also, in hierarchical subnets, two subnets having the same IP subnet address but different subnet masks are not supported. See the white paper about subnet masks ("White Papers" on page 75) for more information.

TIP

NNM does not detect proxy ARP (an alternative to defining extensive routing tables). If NNM is running in an environment using proxy ARP, alarms about misconfigured subnet masks are generated. In this case, these alarms can be ignored.

DHCP Address Ranges Identified

HP strongly suggests that you assign a range of IP addresses to be randomly assigned to mobile computers when they access your network. NNM can handle this range of addresses in a way that does not cause problems as users hook up to and disconnect from the network.

Consistent Name Resolution Scheme

NNM depends upon your network name resolution scheme being in good working order (DNS, NIS, NIS+, NetBios, local hosts files). NNM cannot conduct successful discovery if it is receiving inaccurate information. NNM will exhibit performance problems and erratic behavior when your name resolution scheme is not working. If you have name resolution in place prior to NNM's initial discovery process, hostnames are used for map symbol labels, rather than IP addresses. Hostnames generally make the NNM maps and alarm messages more meaningful to your team.

If you are using DNS, it is recommended that the management station be a caching or secondary name server. Ensure that the management station secondary name server is not serving any other clients.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0487
3740
Doc:

NOTE Point your web browser to `http://www.docs.hp.com` and search for a document titled *Installing and Administering Internet Services* (part number B2355-90147). This document contains information about configuring a caching-only name server.

Quick Check of Your Name Resolution Scheme

To test the health of the name resolution implementation before installing NNM, try the following procedure.

1. Find the `gethost.exe` tool (provided on the NNM installation CD) and copy it to the hard drive of the machine where you will install NNM.

   Windows: *CD-ROM drive*`:\support\gethost.exe`

   UNIX: Mount the CD drive,
   `/cdrom/OVDEPOT/OVNNMgr/OVNNM-RUN/opt/OV/support/gethost`

2. Choose an IP address that is not in use on your network.

3. Navigate to the directory where you copied `gethost`. At the command prompt type either:

```
gethost -a -i bogusIPaddress
gethost -i realHostName
```

4. If you receive an immediate answer, your name resolution scheme is in good shape. If your system hangs while trying to formulate an answer, clean up your network name resolution before installing NNM.

NOTE To test the health of the name resolution implementation after installing NNM, see "Opening NNM takes a long time" on page 133.

SNMP Agents and Their MIBs Configured

The SNMP agent on each network device responds to GET and SET requests from NNM and continuously monitors the device upon which it resides. The agent generates and sends SNMP traps to NNM whenever an error condition arises that is defined in the agent's MIB file.

Configure each SNMP agent's community names and trap destination list specifically for your particular network. Obtain a copy of the agent's MIB file so that you can configure NNM to take full advantage of all the management capabilities provided by the agent.

If an SNMP agent is not currently installed on a network device that you need to monitor, contact the vendor of the device.

GET- and SET-Community Naming Scheme

Community names are a lightweight security technique employed by SNMP agent software. If the network management software wants to communicate with the SNMP agent software, both must use the same community name during GET and SET requests and talk over the same port. By default, community names are often set to PUBLIC and the port is set to 161. NNM assumes that these defaults are in use unless you inform it otherwise. Many network administrators change the GET-community name so that hackers cannot obtain sensitive information about their devices. It is even more common for network administrators to change the SET-community name, since knowing this community name enables others to make system configuration changes to the device itself, either inadvertently or maliciously.

In order to work, NNM depends upon successful communication with the SNMP agents installed on your network devices. If the community names have been changed from PUBLIC or the port changed from 161, you need to inform NNM of the new ones. (NNM cannot obtain these automatically because that would defeat the security feature.) NNM tests community names in the file `netmon.cmstr`. See "GET- and SET-Community Name and SNMP Port Issues" on page 145.

Trap Destination List Updated to Include the NNM Management Station

The SNMP agent software continuously monitors its device for error conditions defined in the installed MIB. When an error condition is detected, a trap message is automatically forwarded to all devices listed in the agent's trap-forwarding list. When configuring the SNMP agent on

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0488
3740
Doc:

each network device, configure the agent's trap forwarding list (or trap destination list) to include the NNM management station's host name or IP address. NNM will then receive traps from the device and keep you informed. Refer to the agent's documentation for information about how to do this. See "Ensuring that NNM Receives Traps from Your Network Devices" on page 325.

TIP *HP-UX systems only:* For hosts with HP OpenView SNMP agents, NNM automatically updates the trap forwarding list when the device is discovered, provided that the correct SNMP SET-community name is configured within NNM. See "GET- and SET-Community Name and SNMP Port Issues" on page 145.

Obtain a Copy of the SNMP Agent's MIB File

Often vendors provide custom MIB files that define specific objects for monitoring the particular device. Be sure to request a copy of the custom MIB so that you can install it into NNM's MIB database later on.

NOTE List of all of the MIBs in use on your network devices. These same MIBs will need to be installed on the NNM management station. See "Loading MIBs in the MIB Database" on page 413. After you install the MIB you can configure NNM to handle each trap as you wish. See "Event Configuration Overview" on page 422.

To obtain the most recent version of a MIB file, check NNM's installation CD, contact the vendor who wrote the MIB file, or search the website `ftp://ftp.isi.edu/mib/` for quick access to the MIB file. Make sure the MIB file that you load onto the management station's MIB database is the same version being used by the SNMP agent on your network device.

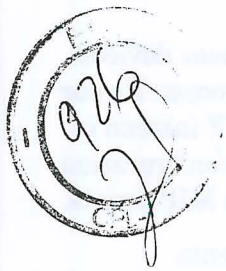
DMI Service Providers and Their MIFs Configured

If your management station uses a Windows operating system, NNM **automatically subscribes** to receive DMI events from all managed systems running DMI version 2.0.

Keep track of any vendor-specific MIF files being used on these devices. Your list will come in handy later in NNM's configuration process. If your DMI service provider software is using a vendor-specific MIF instead of or in addition to the DMTF's standard MIF, during NNM's configuration process you must configure NNM to understand the custom MIF events.

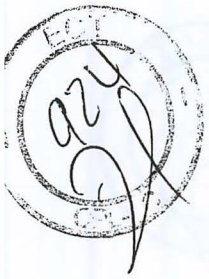
For information about configuring DMI MIFs, see "DMI Events (Indications)" on page 327, "DMI Browser" on page 417, and "Loading DMI-to-SNMP Event Mappings" on page 419.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0489
3740
Doc:



5 Initial Network Discovery: Options and Troubleshooting

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0490
3740
Doc:



The first step toward configuring Network Node Manager (NNM) is to install the software and allow initial discovery to run.

NNM automatically discovers each device on your network and its connective relationship to other devices. NNM's object and topology databases store the discovered information and NNM uses this information to draw the default map and set up the event tracking system. After initial discovery has run to completion, you use the map to identify and fix problems on your network.

Often, network administrators with routed environments simply start NNM and allow it to run initial discovery with the default settings. By default, your management domain consists of the network indicated by your *management station's IP address and subnet mask*. NNM discovers everything to the edges of that network and **manages** (monitors) the devices discovered up to the number in your license agreement limit.

If you need to manage multiple networks, you can *add* them to the management domain by:

- Manually selecting symbols on the map and setting them to *managed* (see "Interactively Expand/Limit Your Management Domain" on page 117).
- Automatically setting devices on multiple networks to *managed* by creating and using a seed file, using the `loadhosts` program, and/or increasing the IPX-Hop Count (see "Automatically Expand Your Management Domain" on page 119).

In very large enterprises and bridged environments, the initial discovery process may detect such a large number of devices that managing them all would exceed your organization's and your management station's resources. In this case, you may want to *limit* the number of devices included in the initial discovery process. You can limit initial discovery so that it only includes your organization's mission-critical devices by:

- Manually selecting unimportant symbols on the map and setting them to *unmanaged* (see "Interactively Expand/Limit Your Management Domain" on page 117).
- Creating and using a `netmon.noDiscover` file that specifies which devices to *exclude* from the discovery process, using the `loadhost` program to discover only the devices on your list, creating and using a *discovery filter* that controls which devices or types of devices to

include in the discovery process, using the `oid_to_type` file to unmanage groups of devices, and/or decreasing the IPX Hop Count (see "Automatically Limit Your Management Domain" on page 124).

If your network is quite large, but you don't want to eliminate devices from the management domain, you can visually break the map into smaller units or create multiple maps that draw information from the same databases. You can use the hide feature or map filter to show different aspects of your network on each map. See Chapter 8, "Map Customization," on page 211.

It is also possible to use multiple management stations in a hierarchical arrangement that divides up the management responsibility yet shares critical information. See *A Guide to Scalability and Distribution* for more information.

You start benefiting from NNM immediately. This initial map discovery process may reveal configuration problems on your network, such as SNMP agents that are not communicating properly, incorrect subnet masks or DNS settings, mismatched community names, and unexpected connections to network segments that you do not own. The map is a visual representation of the communications channels established between NNM and the devices in your network. The accuracy of these links determines whether or not NNM can provide valuable information to help you manage your network. Be sure to follow the directions for verifying the accuracy of your maps (see page 109) and to fix any problems before continuing with further customizations to NNM (page 131).

TIP

Your company may have purchased multiple HP OpenView products. If you are using other HP OpenView applications in addition to NNM, you may notice that the menu choices and options provided within the software vary from what is presented in this book. This is because the other HP OpenView applications integrate closely with NNM to take advantage of the features that NNM already provides. Other HP OpenView programs build upon the foundation provided by NNM.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0491
3740
Doc:



Install Network Node Manager (if you have not already done so)

See the *Quick Start Installation Guide* included with the NNM Installation CD for instructions about how to install Network Node Manager. Make sure that your management station meets the minimum requirements before you start.

NOTE In this manual, `C` and `$LANG` in directory listings are variables for the language currently in use. `C` contains the English version.

Installing IPX Transport Software (Windows only)

For management stations running a Windows operating system:

IPX discovery is an optional component of Windows operating systems. If you want to discover and monitor IPX nodes, be sure to install the NWLink IPX/SPX Compatible Transport network software stack before or during the NNM installation process. These drivers are included with the Windows operating system installation software, but are not installed by default. See the *Quick Start Installation Guide* included with NNM's installation CD for more information.

Establishing Universal Pathnames (UNIX only)

For management stations running a UNIX operating system:

This book uses directory pathnames that are independent of the underlying file structure of the operating system you are using (see your data sheet to learn specifically which operating systems and versions this release supports). For each Network Node Manager directory, a single pathname is used rather than multiple pathnames that vary by system. For example, the pathname for the NNM log file is stated as `$OV_LOG` rather than `/var/opt/OV/share/log` for HP-UX 10.X, 11.X and Solaris 2.X systems.

Take the following steps to set up each user's environment. Setting the universal pathnames and paths as shown is temporary; you will need to do this every time you start a terminal window. Or you can permanently set each user's path by modifying the path in the appropriate files shown below:

If running sh or ksh: Modify the path in the `.profile` file.

If running csh: Modify the path in the `.login` file.

If running VUE: Modify the path in the `.vueprofile` file.

1. If you want to use the universal pathnames that have been incorporated into NNM, you need to *source* the file into your current environment. Use one of the following commands, depending on which shell you are running. If you are not sure which shell you are running, execute:

   ```
   echo $SHELL
   ```

NOTE Be sure to include a space between the . and the / in the `sh` or `ksh` commands.

If running sh or ksh:

HP-UX 10.X, HP-UX 11.X,
Solaris 2.X `. /opt/OV/bin/ov.envvars.sh`

If running csh:

HP-UX 10.X, HP-UX 11.X,
Solaris 2.X `source /opt/OV/bin/ov.envvars.csh`

See the *ov.envvars* manpage for additional information about this script and information about the universal pathname equivalents.

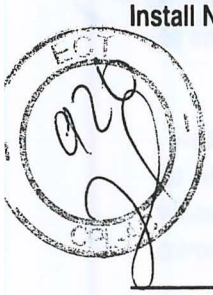
2. Set the path to include `$OV_BIN` and `$OV_MAN`. Execute the following commands:

   If running sh or ksh:

   ```
   PATH=$PATH:$OV_BIN
   MANPATH=${MANPATH:-/usr/man:/usr/share/man}:$OV_MAN
   export PATH
   export MANPATH
   ```

   If running csh:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0492
3740
Doc:



```
set path=($path $OV_BIN)
if (${?MANPATH} == 0)setenv MANPATH "/usr/man:/usr
/share/man"
setenv MANPATH "${MANPATH}:${OV_MAN}"
```

NOTE All NNM documentation referring specifically to a UNIX operating system assumes that you have activated the universal-pathname environment variables.

For example, a written procedure might include the following step:

```
cd $OV_BACKGROUNDS
```

This command takes you to the local directory containing submap backgrounds, and it works regardless of which version of the UNIX file system is involved. Note that if you need to know the actual pathname, you can always enter a command like the following:

```
echo $APP_DEFS
```

The response to this command will be the actual local pathname:

- *HP-UX*: `/usr/lib/X11/app-defaults`
- *Solaris 2. X:* `/usr/openwin/lib/app-defaults`

Discover the Network... Let NNM Do It

Let NNM do the work discovering your network for you. NNM sets up several databases, creates the default map, and establishes communication links for tracking events on your network.

Overview

First NNM's services (background processes) are started. Expect intense polling traffic at first as the network monitoring service, `netmon`, works as quickly as possible to discover each device on your network. An `ICMP ping` is issued for each device identified in any found ARP table and an `snmpwalk` command is issued to gather information about each discovered device. If a serial WAN link is discovered, NNM checks the router's routing table for clues about how to continue with discovery. The frequency of polling for new nodes automatically decreases as fewer new objects are discovered per polling cycle.

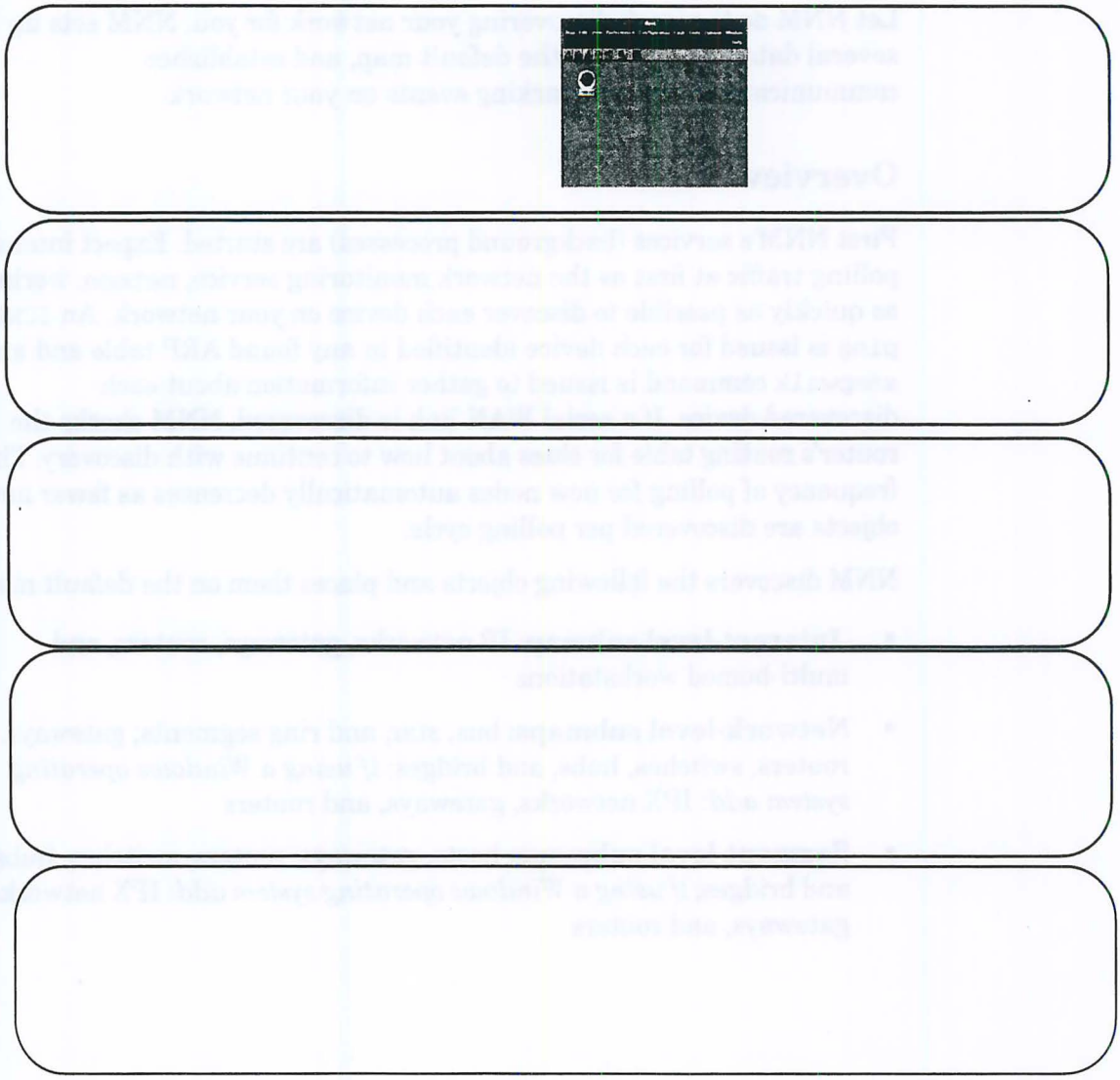
NNM discovers the following objects and places them on the default map:

- **Internet-level submap:** IP networks, gateways, routers, and multi-homed workstations
- **Network-level submaps:** bus, star, and ring segments; gateways, routers, switches, hubs, and bridges; *if using a Windows operating system add:* IPX networks, gateways, and routers
- **Segment-level submaps:** hosts, gateways, routers, switches, hubs, and bridges; *if using a Windows operating system add:* IPX networks, gateways, and routers

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0493
3740
Doc:

- **Node-level submaps:** network interface cards

Figure 5-1 A Typical Hierarchy of Persistent Submaps



NNM uses the information about each device gathered by `netmon` to determine the most accurate and descriptive symbol to use on the map. If NNM cannot match the `sysObjectID` to a specific symbol type, the node will be represented as a generic symbol on the map (a shape without a specific descriptive icon inside of the shape). For example, some IP nodes

that are not computers (connectors such as bridges and repeaters) may initially appear on the map as hosts. See "Troubleshooting Discovery" on page 131 for more information.

Figure 5-2 Generic Computer Icon versus Specific Descriptive Icon



NOTE

NNM determines which symbol to use for each device by referencing the information contained in two configuration files:

- *Windows:*

  ```
  install_dir\conf\oid_to_sym
  install_dir\conf\oid_to_type
  ```

- *UNIX:*

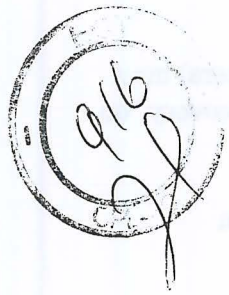
  ```
  $OV_CONF/oid_to_sym
  $OV_CONF/oid_to_type
  ```

Although the entries in these files are already extensive, you may encounter a situation where you want to make additions or changes to these files. For example, if you see a generic icon on the map and wish to assign a specific icon or if you want to create your own new icons. See the instructions at the beginning of each of these ASCII files. See also the *oid_to_type* and *oid_to_sym* reference pages in NNM's online help (or the UNIX manpages) and Appendix D, "Changing All the Symbols for a Particular Device," on page 661 and Appendix E, "Changing an Object's Vendor and SNMP Agent," on page 675 for more information.

Start the NNM Services (background processes)

NNM starts collecting the information needed to draw the default map as soon as you start the NNM services. The services continually monitor the network and track activity. You need to start them the first time you use NNM; thereafter, they run continually whether or not you have the NNM user interface open. To learn more about these services, see Appendix A, "NNM Services and Files," on page 539.

NOS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0494
3740
Doc:



To start the services (background processes):

- *Windows:*
  Select `Start:Programs:HP OpenView: Network Node Manager Admin->NNM Services - Start`.
- *UNIX:*
  As root, at the command prompt, type **ovstart**

  The `$OV_BIN` directory must be in your `PATH`. If not, you must type **$OV_BIN/ovstart** to start NNM.

  See the *ov.envvar* manpage for a complete list of the universal pathnames and their equivalents, and information about a script for setting up environmental variables that will create the pathnames on your system.

Make Sure NNM's Services Are Successfully Running

To generate a status list of the services that make NNM work:

- *Windows:*

  Select `Start:Programs:HP OpenView:Network Node Manager Admin->NNM Services - Status`
- *UNIX:* At the command line prompt, type **ovstatus -c**.

TIP Type **ovstatus -c** for concise, one-line-per-process information.

If any of the services are not successfully running, see Appendix A, "NNM Services and Files," on page 539 for information about troubleshooting services before continuing.

Open NNM

Opening NNM takes a few minutes as the maps are synchronized with the databases. To start NNM's user interface (foreground processes):

- *Windows:*
  Select `Start:Programs:HP OpenView:Network Node Manager`. NNM automatically starts all installed and registered applications.

- *UNIX:* At the command prompt, type **ovw**. NNM automatically starts all installed and registered applications.

Configure an Inventory Report

Use the web Reporting interface to configure an inventory report. An inventory report lists the network nodes that are contained in the topology database, organized by subnet. You can use this report to help verify the accuracy of the initial discovery of your network. Refer to the online help for more information on configuring an inventory report.

Let NNM Run Over Night to Populate the Maps

The initial discovery process takes time. We recommend that you let NNM run over night to gather the majority of network information available. As NNM maps your network, it constantly rearranges icons. Therefore, it is best to wait until initial discovery has finished before exploring the default map.

NNM gathers information to the limits of the network indicated by the management station's IP address and subnet mask. NNM then checks the ARP table on each discovered device and expands the map by adding devices listed in each ARP table to the map. NNM also detects serial WAN links (for which ARP caches have no entries) and then checks the resident routing table instead. Devices listed in the routing table are then discovered and the process continues. NNM follows this process each time communication is established with a device, so your maps will continue to grow over time. (See Chapter 2, "How Does NNM Work?," on page 49 for a more detailed explanation about how NNM discovers network information.)

NOTE

While NNM discovers and maps your network information, explore the *Get Acquainted with HP OpenView Network Node Manager: Training for NNM Operators* CD provided with NNM so that you will understand what you are seeing after the discovery process is complete.

After NNM completes initial discovery, verify the accuracy of the map (see page 109), making sure that any devices that you have identified as mission-critical in Chapter 4, "Planning Your NNM Configuration," on page 79 appear on the map. Then fix any problems by:

RQS nº 03/2005 - CN
CPMI - CORREIO
Fls. Nº 0495
3740
Doc:

- Interactively expanding or limiting your management domain (see page 117).
- Automatically expanding your management domain (see page 119).
- Automatically limiting your management domain (see page 124).
- Troubleshooting the initial map to ensure your network is configured properly (see page 131).
- Delete NNM's object and topology databases and restart discovery, if necessary (see page 161).

When you are satisfied with the accuracy and completeness of the initial map, go to Chapter 6, "Preserve Your Sanity: Backup and Polling Configuration," on page 163 to learn how to back up your work and to customize the polling configurations.

Verify the Accuracy of the Initial Discovery

Now that NNM has had time to map all the network connections discovered, take the time to make sure you recognize what was found. Refer to the checklists that you developed in Chapter 4, "Planning Your NNM Configuration," on page 79 to verify that all mission-critical devices are present.

Usually there are a few surprises on your map. NNM allows you to easily identify such things as connectivity problems and security risks. Take the time to fix any problems that you discover (see "Troubleshooting Discovery" on page 131).

This section includes information about NNM's tools that make verifying the information on your maps easier:

- Inventory report

  View or print the inventory report.

- Object properties information

  View a detailed description of the underlying object properties for the selected internet, network, segment, node, or interface symbol.

- Find object feature

  Locate map elements quickly using the `Edit:Find` menu item.

TIP

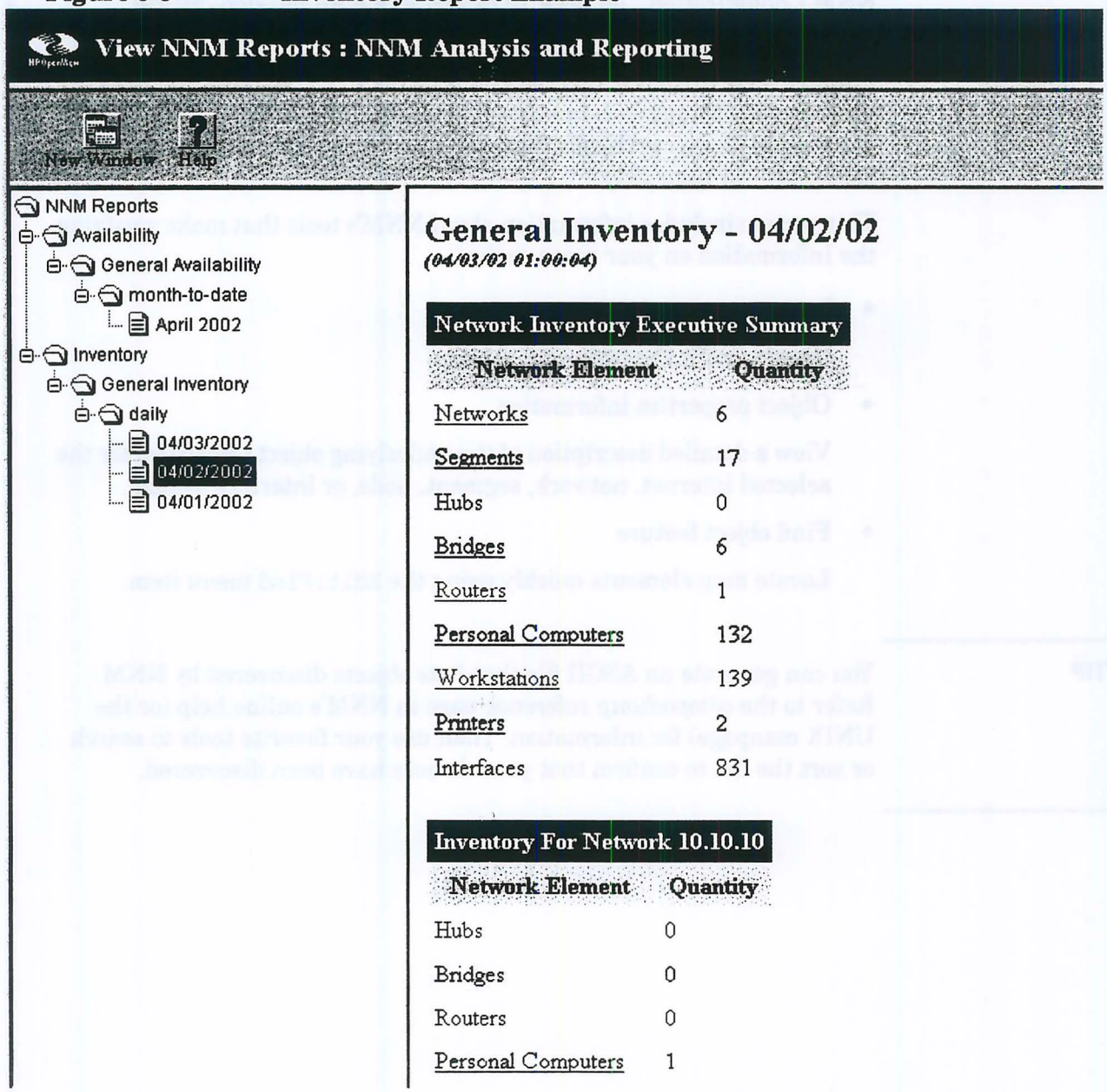
You can generate an ASCII file that lists objects discovered by NNM. Refer to the *ovtopodump* reference page in NNM's online help (or the UNIX manpage) for information. Then use your favorite tools to search or sort the list to confirm that your devices have been discovered.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0496
3740
Doc:

Printing the Inventory Report

Use the inventory report to see a detailed list of what was discovered on your network. The inventory report lists the network nodes that are contained in the topology database, organized by subnet. An example of an inventory report follows.

Figure 5-3 Inventory Report Example



From the Network Inventory Executive Summary, you can click on entries in the Network Element column to see more details.

See the NNM online help for more information on the web Reporting interface.

Viewing the Properties of Your Network Configuration

You can gain quick access to the `IP Map` service's information that describes your network and system configurations. The information in the dialog boxes for object properties can help you determine if everything is present and accounted for on the initial map.

Viewing Object Descriptions

You can view the object properties for any network element that NNM manages, such as an internet, network, segment, node, or interface. The object database maintains this information. Object properties are always as current as NNM's last polling cycle.

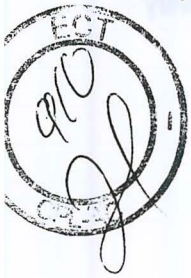
Description of an Internet Object Simply select the Internet symbol on the root submap and right-click with the mouse. Select `Object Properties` and select `IP Map`. See NNM's online help for more information and specific directions. NNM provides the following information:

- number of networks on the internet
- number of segments on the internet
- number of nodes contained within the internet
- number of interfaces contained within the internet
- number of gateways/routers on the internet
- any status or error messages may appear in the `Messages` field

Description of a Network Object Simply select any network symbol on the map and right-click with the mouse. Select `Object Properties` and select `IP Map`. See NNM's online help for more information and specific directions. NNM provides the following information:

- the network name as it appears on the map
- network address

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0497
3740
Doc:



- subnet mask associated with the network number
- status of the network
- number of segments on the network
- number of nodes contained within the network
- any status or error messages may appear in the `Messages` field

Description of a Segment Object Simply select any segment symbol on the map and right-click with the mouse. Select `Object Properties` and select `IP Map`. See NNM's online help for more information and specific directions. NNM provides the following information:

- status of the segment
- number of nodes on the segment
- any status or error messages may appear in the `Messages` field

Description of a Node Object Simply select any node symbol on the map and right-click with the mouse. Select `Object Properties` and select `IP Map`. See NNM's online help for more information and specific directions. NNM provides the following information:

- hostname that was assigned when the node was initially discovered
- status of the node
- information about and status of each interface installed on the node
- system description as returned by the SNMP agent (*)
- system location and system contact as returned by the SNMP agent (*)
- system object ID of the node (*)
- any status or error messages may appear in the `Messages` field

* The node must support SNMP to return this information.

Description of an Interface Object Simply select any interface symbol on the map and right-click with the mouse. Select `Object Properties` and select `IP Map`. See NNM's online help for more information and specific directions. NNM provides the following information:

- address of the interface

- subnet mask (IP only)
- link-level address (physical address)
- interface type
- status
- any status or error messages may appear in the `Messages` field

Finding Specific Devices on the Map

The `Edit:Find` menu item enables you to search for objects that contain a common characteristic. You can:

- Find objects in either the open map or an open snapshot based on the value of a specific attribute.
- Create a selection list of objects with particular characteristics, such as all routers.
- Open the submap of each found object.

You can find objects based upon these object and symbol characteristics (see page 205 for more information):

- Selection Name

  You can find objects based on a selection name or part of a selection name.

- Attribute

  You can search for objects based on the values of chosen attributes, such as `isRouter`.

- Comments

  You can search for all objects that have a specific comment or portion of a comment. You may establish conventions for embedded keywords and use these in the `Find By Comment` operation. In this manner, you can find objects based on a key that is not a supported attribute.

- Symbol Status

  You can find objects that are represented by a symbol with the given status. Each found symbol is listed separately.

- Symbol Type

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0498
3740
Doc:

You can find all objects that have a symbol of a given type (class and subclass).

- Label

  You can search on the label string (comments added by you).

Entering Strings in Find Operations

When you select `Edit:Find`, input in the form of a string value is sometimes required. For several operations, you have a choice between two types of searches: exact match and pattern matching.

Exact Match — Exact match finds only those objects whose attribute value exactly matches the string entered. To switch to the exact match search, click on the `Exact Match` radio button. You must enter the complete string in this mode.

Pattern Matching — When pattern matching is used, you may enter a simple substring or a regular expression. The following section, "Regular Expressions," discusses some of the special characters you can use in regular expressions.

A valid regular expression may consist completely of printable characters. However, in a regular expression, certain symbols have special meaning; see the following table. (*HP-UX only:* more regular expressions are available, see the *regexp* manpage.)

Table 5-1 Regular Expressions for Pattern Matching

Special Character	Meaning	Examples

. (period)	Matches any single printable or nonprinting character except <newline> (unless it is used inside brackets).	`node.in` matches:
		`node3interface`
		`nodeXinterface`

Table 5-1 Regular Expressions for Pattern Matching (Continued)

Special Character	Meaning	Examples
* (asterisk)	Means zero or more occurrences of the preceding character.	node* matches: nod node nodeTwo nodee
^ (Caret)	If the caret is the first symbol, then the following string must be the first part of any matching string.	^Box matches the string: Box elder but does not match the string: Big Box
$(dollar)	If dollar is the last symbol, then the preceding string must be the last part of any matching string.	long$ matches the string: belong but does not match the string: longer

Results of the Find Operation

NNM reports all found objects to you in the dialog box. The Message area reports the results of the search. It will display:

- the number of objects found
- errors
- further instructions

RQS nº 03/2005 - CN - CPMI - CORREIOS
0499
Fls. Nº
3740
Doc:

Symbols of found objects are listed by selection name in the `Located and Highlighted` area. If a found object is represented by multiple symbols, each symbol is displayed on a separate line.

Table 5-2 Results of the Find Operation

Parameter	Meaning
`Selection Name`	The selection name of the object.
`Submap Name`	The name of the submap that displays a symbol of a found object.
`Symbol Label`	The symbol label as it appears on the submap.

The following three example entries display one found object and three symbols that represent the object in three different submaps:

```
NodeBob:lanCard:IP address [connection to segment]
NodeBob [connection to segment]
NodeBob [hostname]
```

The symbols of found objects are highlighted on submaps.

Interactively Expand/Limit Your Management Domain

The NNM default map includes any devices that have already been discovered. You control which of these devices are **managed** (monitored by NNM's services) and which of these devices are **unmanaged** (placed on the map as a light-tan icon, but not monitored by NNM services). NNM does not actively monitor unmanaged devices through polling. However, you can still configure each unmanaged device's SNMP agent or DMI service provider to forward traps to the NNM management station's event tracking system (see "Ensuring that NNM Receives Traps from Your Network Devices" on page 325).

Normally, you customize the size of your management domain by interactively *managing* devices from other networks to expand it and/or *unmanaging* non-critical devices to limit network management traffic and the size of your map.

TIP If this approach seems too time consuming based upon the size of your management domain, see page 119 and page 124.

Adding Networks to Your Management Domain

To add a network to your management domain, find the IP address and hostname of at least one high-traffic device within the network that you wish to add. Gateways, routers, or multi-homed servers make the best choice. Then:

- On the Internet-level submap, select the `Edit:Add Objects` menu item.
- Select the *Connector* Symbol Class icon, then drag the *Gateway* Symbol Subclass icon onto your Internet-level submap. Choose this gateway connector regardless of the type of device you are using to start the discovery. The `Add Object Palette` appears.
- Double-click on `IP Map` to open the `Set Attributes` dialog box.

RQS nº 03/2005 - CN - CPMI CORREIOS
Fls. Nº 0500
3740
Doc:

- Type in the IP address and hostname of an SNMP enabled device within the network that you wish to add to your management domain, then click on the Verify button.

  Once NNM runs the configuration check, NNM will correct the symbol choice and (if necessary) placement for you. The device is configured to be managed by NNM.

Managing an Unmanaged Network Device

To change the status of a network device from unmanaged to managed (see NNM's online help for more information):

1. From any submap, use NNM's `Edit:Find` menu item to locate the device's symbol on the map.
2. Select the device's symbol and select `Edit:Manage Objects`.
3. Select a router that is connected to the new network symbol and use the `Fault:Network Connectivity->Poll Node` menu item.

   NNM conducts discovery on that device's assigned network or networks and the nodes within any neighboring networks. NNM updates the map, databases, and event monitoring to include these devices.

Unmanaging a Managed Network Device

If you *unmanage* a network symbol or segment symbol during active discovery, a few node symbols on that network or segment may not be reset to unmanaged. To avoid this problem while *unmanaging* the network symbol or segment symbol, do one of the following:

- Wait until NNM finishes active discovery before unmanaging an object.
- Turn *new-node discovery* polling off. From any submap, select the `Options:Network Polling Configuration`. Disable the `New Node Discovery` option. Don't forget to turn polling back on again when you are finished modifying the map.

Automatically Expand Your Management Domain

Normally, netmon generates the discovery process outward from the management station and includes only the management station's IP network in the management domain. If your NNM maps are too limited and do not show *all* the networks for which you are responsible, and adding the missing networks one by one (page 117) would be too time-consuming, you have several choices to consider for customizing the discovery process:

- Seed File(page 120)

  If your management domain contains multiple networks (especially networks that are not adjacent to each other), consider using a seed file. A **seed file** instructs netmon to generate the map starting from multiple IP addresses instead of or in addition to the management station's IP address. This saves you time by eliminating the manual process of expanding the management domain.

- loadhosts Program (page 122)

  If your management domain contains few SNMP devices, you can speed up netmon's discovery process by creating an ASCII file listing devices that need to be added to the topology database and map. The loadhosts program reads this file and adds the devices listed in this file directly to your topology database, bypassing the netmon discovery process. Upon being added to the topology database, netmon begins polling the devices as newly discovered devices and expands your management domain from these new nodes.

TIP

If you already keep a local hosts file that lists important SNMP-enabled nodes on your network, you can use that file.

- IPX Hop Count (Windows only, page 123)

  If you installed the Windows drivers for the IPX stack, during discovery gateways and servers acting as routers return a **hop count** (how many hops are allowed through gateways and routers to

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0501
3740
Doc:

get to the network) for each network of which the router is aware. You can expand the extent of discovery by setting the maximum hop count to a higher number.

TIP Remember that each additional managed network device increases the network management traffic being generated. Refer to the critical-device list that you established in Chapter 4, "Planning Your NNM Configuration," on page 79 for guidance about keeping the management polling traffic to a reasonable minimum. Unmanage devices that are not mission-critical.

Create a Seed File Specifying Multiple IP Networks to Manage

A seed file is an ASCII file containing a list of network-level IP addresses or host names (not IPX addresses). The contents of the seed file define your map's initial management region. Gateways make the best seeds because they maintain the largest ARP tables. If you add the major gateways, `netmon` will discover the rest of the nodes on the network, so you do not have to include all nodes in the seed file. All networks attached to the devices listed in your seed file will be discovered and set to *managed*. Networks implied by each node's IP address are discovered and added automatically to the map.

1. Create an ASCII file. The name and location of this ASCII seed file is up to you. In this file, list any hostnames or IP addresses that NNM should use to begin discovery. Each hostname or IP address must be on its own line, and each listed device must support SNMP. Specifically, `netmon` must be able to determine the subnet mask for each interface in a specified node. Otherwise, the seed file entry will be ignored.

   You can include notes to yourself in the seed file by using *comments* (preceded by a # sign) after the hostname or IP address on a line.

   Example seed file:

```
node1.division.company.com
router4.division.company.com  #Gateways are best
192.0.2.44
192.0.2.45
```

TIP Bridges and hubs may or may not maintain ARP tables. The ARP tables are the key to expanding NNM's discovery.

2. Make a backup copy of the netmon's local registration file:
   - *Windows:* `install_dir\lrf\netmon.lrf`
   - *UNIX:* `$OV_LRF/netmon.lrf`
3. Load the `netmon.lrf` file into your text editor. The `netmon.lrf` file consists of the following.

```
netmon:netmon:
OVs_YES_START:ovtopmd,pmd,ovwdb:-P:OVs_WELL_BEHAVED: 15:
```

4. Insert the seed file option (`-s filepath`) after the `-P`.

   For example, adding the seed file, `nodelist`, to use as input to `netmon` on a management station running the Windows operating system would change the file to look like:

   Windows (Note the required \ character after the drive letter and the \ character in the path statement.):

```
netmon:netmon:
OVs_YES_START:ovtopmd,pmd,ovwdb:-P -s
"C\:\install_dir\conf\nodelist":OVs_WELL_BEHAVED:15:
```

   UNIX:

```
netmon:netmon:
OVs_YES_START:ovtopmd,pmd,ovwdb:-P -s
/etc/opt/OV/share/conf/nodelist:OVs_WELL_BEHAVED:15:
```

5. Save the edited `netmon.lrf` file in the following location:
   - *Windows:* `install_dir\lrf\netmon.lrf`
   - *UNIX:* `$OV_LRF/netmon.lrf`
6. Stop the `netmon` service. At the command prompt, type:
   `ovstop netmon`
7. To update NNM's configuration file, `ovsuf`, at a command prompt, type:

   Windows: **`ovaddobj install_dir\lrf\netmon.lrf`**

   UNIX: **`ovaddobj $OV_LRF/netmon.lrf`**

RQS nº 03/2005 - C...
CPMI - CORREIO
Fls. Nº 0502
3740
Doc:

ovaddobj updates netmon's information in the ovsuf configuration file (which instructs the start-up process what to start).

8. Restart the netmon service. At the command prompt, type:

   ovstart netmon

NNM starts discovering from all locations identified in your seed file. Give NNM time to complete the process. Then you can manually make additions/changes to the map after the effects of the seed file are in place (see page 117).

Use loadhosts

loadhosts is a program provided with NNM that allows you to place a list of IP addresses directly into the topology database. This is useful when:

- There are few SNMP nodes on your network. Using loadhosts speeds up the discovery process.
- You already maintain a list of the important SNMP nodes on your network.

  Windows:
  \WinNT\system32\drivers\etc\hosts file or
  \WinNT\system32\drivers\etc\Lmhosts file

  UNIX: /etc/hosts file

  Using loadhosts ensures that your critical devices are immediately included in NNM's databases and on the map.
- If it is critical to keep network management traffic to an absolute minimum (see page 127).

See the *loadhosts* reference page in NNM's online help (or the UNIX manpage) for more information.

1. Create an ASCII file listing each IP address or hostname on a separate line.
2. At the command prompt, type:

loadhosts -m *subnet-mask filename*

The following example loads the \etc\hosts file on a management station running a Windows operating system, with the subnet mask set:

```
loadhosts -m 255.255.248.0 \WinNT\system32\drivers\etc\hosts
```

The netmon service receives events about the new additions to the topology database and runs the discovery and configuration poll on those newly added nodes.

Expand the IPX Hop Count (Windows only)

If you installed the Windows drivers for the IPX stack, gateways and servers acting as routers return a hop count during discovery (how many hops through gateways and routers to get to the network) for each network of which the router is aware. You can control the extent of IPX discovery allowed by NNM.

To increase the maximum hop count for discovery, open any submap and select the `Options:Network Polling Configuration IP/IPX` menu item. On the `IPX Discovery` tab, specify the hop count of your choice. This change takes effect the next time IPX discovery runs.

To discover *all* IPX networks, set the value up to 16—the maximum allowed by IPX. However, see note below.

NOTE Setting the maximum hops to 16 can cause a large number of nodes to be discovered rapidly, causing both short-term and long-term system performance problems due to polling traffic. Unless you are sure your system is appropriately configured to handle the number of IPX nodes in your environment, Hewlett-Packard recommends that you expand your management domain slowly.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0503
3740
Doc:

Automatically Limit Your Management Domain

If your network maps are too complex to be useful, you have several choices to consider for customizing the discovery process.

If all the devices that are shown on your map must remain in your management domain, you can use **container** icons (see page 248) and create custom submaps to break up the visual information into smaller chunks and customize your map in a number of ways. (See Chapter 8, "Map Customization," on page 211 for information about customizing the map itself rather than customizing the discovery process.)

If you do not need to retain all the devices that are shown on your map, NNM has options that you can use individually or in combination:

- `netmon.noDiscover` File (page 125)

  You create this file listing IP addresses or ranges of IP addresses for NNM to *exclude* from the discovery process; therefore, excluding them from NNM's databases and maps. During initial discovery when NNM discovers a device, the device's IP address is checked against the `netmon.noDiscover` file. If the IP address is matched in the `netmon.noDiscover` file, the device is dropped and not polled for any more information. The device may be discovered again during subsequent new-node-discovery polls; however, it will once again be discarded. This is the easiest method for limiting discovery and also reduces network management traffic more than using a discovery filter (explained below).

- `loadhosts` Program (page 127)

  If you need to keep network management traffic to an absolute minimum, you can turn off `netmon`'s discovery polling cycle and then use the `loadhosts` program to add your network's critical devices directly to your topology database. Only the devices that you specify in the ASCII file of IP addresses/hostnames are included in your management domain.

TIP If you already keep a local hosts file that lists important SNMP-enabled nodes on your network, you can use that file.

- Discovery Filter (page 128)

  You can write Boolean logic into the NNM filter file to specify which devices will or will not pass initial discovery and be added into NNM's object and topology databases. A discovery filter is much more work for the `netmon` service than the `netmon.noDiscover` file because *each device is polled for all MIB attributes* before it is checked against the discovery filter (this is because a discovery filter can be applied to many attributes of a device). If the device does not pass the discovery filter, all information is discarded. The device may be discovered and polled again during subsequent new node discovery polls; however, the information gathered will once again be discarded.

- `oid_to_type` File (page 129)

  You can open and modify the `oid_to_type` file so that specific *types* of devices are automatically configured as *unmanaged* during initial discovery. The devices show up on your map and are included in the NNM databases, but won't be included in the network management polling traffic generated by NNM.

- IPX Hop Count (Windows only, page 130)

  If you installed the Windows drivers for the IPX stack, during discovery gateways and servers acting as routers return a hop count (how many hops are allowed through gateways and routers to get to the network) for each network of which the router is aware. You can restrict the extent of discovery by lowering the maximum hop count.

Create a netmon.noDiscover File to Exclude Devices

The `netmon.noDiscover` file works at the very beginning of the discovery process. Entries in the `netmon.noDiscover` file are the "don't discover" list. No polling (SNMP or ICMP) is done on devices listed in the `netmon.noDiscover` file. Devices listed in your `netmon.noDiscover` file are not included in NNM's databases or displayed on NNM's maps.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0504
3740
Doc:

If you are using HSRP, you can add the virtual IP address of your HSRP-configured routers to the `$OV_CONF/netmon.noDiscover` file. This stops NNM from deleting and rediscovering the virtual IP address in a regular pattern, which can cause participating routers to be deleted from and re-added to your map. Use the following procedure:

1. Add the virtual IP address of your HSRP-configured routers to the `$OV_CONF/netmon.noDiscover` file.
2. If NNM has already discovered the virtual IP address of your HSRP-configured routers, execute `ovtopofix -r a.b.c.d` where *a.b.c.d* is the virtual IP address of your HSRP-configured routers.
3. Run `ovtopodump -lR` to make sure the virtual IP address is gone. See the `ovtopodump`, `ovtopofix`, and `netmon.noDiscover` reference page (or the UNIX manpage) for more information.

For more detailed information, see the *netmon.noDiscover* reference page in NNM's online help (or the UNIX manpage).

Use the following procedure to create entries in the `netmon.noDiscover` file.

1. Create an ASCII file. Name and place it as follows:
   - *Windows:* *install_dir*`\conf\netmon.noDiscover`
   - *UNIX:* `$OV_CONF/netmon.noDiscover`
2. List specific IP addresses or IP wildcards, one per line. Example `netmon.noDiscover` file entries are:

   ```
   10.2.112.86 # one node
   10.2.*.* # all nodes from 10.2.0.0 to 10.2.255.255
   10.2.1-255.0-49 # first 50 nodes in 10.2.1-255 range
   *.*.*.* # all nodes - nothing will be discovered
   10.2.4-5.* # all nodes in either 10.2.4.* or 10.2.5.*
   ```
3. After you have created or modified the `netmon.noDiscover` file, force `netmon` to acknowledge the change by doing one of the following:
   - To only affect future discovery, stop and restart the `netmon` service.
   - To force changes on the map as well as future discovery:

— Stop and restart the `netmon` service.

Use the `Edit:Find` feature with the same criteria that you used in your `netmon.noDiscover` file to select all the map objects to be excluded from the future discovery. Then delete them from your map. They will not be rediscovered.

-OR-

— Wipe out the databases and start again by following the directions in "Stop Everything and Start Discovery Over Again" on page 161.

TIP If you change your mind later and *remove* IP addresses from the `netmon.noDiscover` file, simply stop and restart the `netmon` service to force NNM to acknowledge the change. The nodes will be rediscovered at the next polling cycle.

Use loadhosts

`loadhosts` is a program provided with NNM that allows you to place a list of IP addresses directly into the topology database. This is useful when:

- There are few SNMP nodes on your network. Using `loadhosts` speeds up the discovery process (see page 122).
- You already maintain a list of the important SNMP nodes on your network:

  Windows:
  `\WinNT\system32\drivers\etc\hosts` file or
  `\WinNT\system32\drivers\etc\Lmhosts` file

  UNIX: `/etc/hosts` file

  Using loadhosts ensures that your critical devices are immediately included in NNM's databases and on the map.
- It is critical to keep network management traffic to an absolute minimum. Turn off the new-node discovery polling process, then use the `loadhosts` program to accomplish discovery of the critical devices you wish to monitor. As long as new-node discovery is turned off, these are the only devices that will appear on your maps.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0505
3740
Doc:

See "Controlling the Amount of Traffic Generated by NNM" on page 178 for more information about NNM's polling cycle choices.

See the *loadhosts* reference page in NNM's online help (or the UNIX manpage) for more information.

1. Create an ASCII file listing each IP address or hostname on a separate line.
2. Turn off NNM's new-node discovery polling feature.

   From any submap, select the `Options:Network Polling Configuration` menu item and disable the New-Node Discovery feature.

   See NNM's online help from this dialog box for more information.
3. If you want to start initial discovery over again, see "Stop Everything and Start Discovery Over Again" on page 161.
4. At the command prompt, type:

`loadhosts -M` *`subnet-mask filename`*

The following example loads the `\etc\hosts` file on a management station running the Windows operating system, with the subnet mask set:

```
loadhosts -m 255.255.248.0 \WinNT\system32\drivers\etc\hosts
```

The `netmon` service receives events about the new additions to the topology database and runs the discovery and configuration poll on those newly added nodes.

Create a Discovery Filter Identifying Which Devices to Include

All filters consist of sets of Boolean logic that you enter into the NNM filters file:

- *Windows:* *`install_dir`*`\conf\c\filters`
- *UNIX:* `$OV_CONF/$LANG/filters`

After creating and testing your *discovery* filter, open the `Options:Network Polling Configuration` dialog box and enter the name of your filter in the `Use filter` field. Your filter will be used during all future discovery processes.

To update the object database and enforce the filter rules upon past discoveries, you must use the `ovtopofix` command to force `netmon` to acknowledge your new filter and clean out the existing information in NNM's databases so that your discovery filter changes are reflected on your maps.

See *A Guide to Scalability and Distribution* for information about writing, testing, and implementing the discovery filter. See also the *OVfilterIntro*, *netmon*, *ovfiltercheck*, and *ovfiltertest* reference pages in NNM's online help (or the UNIX manpages) for more information.

TIP

While learning how to use the Boolean language, you may wish to explore the information about *map* filters first (rather than discovery filters). NNM interactively reflects changes to the map filter on the existing maps (rather than requiring that you run the `ovtopofix` command first). Therefore, you can try different Boolean strategies and see their effect on the map right away. See *A Guide to Scalability and Distribution* for more information.

Modify the oid_to_type File to Unmanage Devices by Type

You can instruct NNM to automatically set specific types of devices to *unmanaged* during discovery, such as all end-user PCs or all printers. If you want to use this feature *after* you have already finished initial discovery, make the changes to the `oid_to_type` file and see "Stop Everything and Start Discovery Over Again" on page 161.

The `oid_to_type` file (included with NNM) lists a large number of known `sysObjectIDs`. You can use the `U` parameter to automatically set specific types of devices to unmanaged during initial discovery. This flag only affects initial discovery status. You can change any device from unmanaged to managed at a future time.

You do not need to stop NNM when editing this file. To notify `netmon` of the changes when you are done:

- To only affect devices discovered in the future, at the command line type **`xnmpolling -event`**

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0506
3740
Doc:

- To go back and start initial discovery again so that this change affects all devices on your network, see "Stop Everything and Start Discovery Over Again" on page 161.

See the directions at the beginning of the editable ASCII `oid_to_type` file. See also the *oid_to_type* references pages in NNM's online help (or the UNIX manpages) for more information.

The following example entries would set devices containing either of two specific Windows versions to unmanaged, would set to unmanaged any IPX device that is not specifically identified elsewhere in the `oid_to_type` file, and would set to unmanaged any non-SNMP/IPX/IP device not specifically identified elsewhere in the `oid_to_type` file:

```
1.3.6.1.4.1.311.1.1.3.1::Windows NT:U # Windows NT
1.3.6.1.4.1.311.1.1.3.1.1::Windows NT:U # Windows NT
DEFAULT:::U
DEFAULT_IP:::
DEFAULT_IPX:::U
DEFAULT_SNMP:::
```

The `oid_to_type` file acknowledges specific `sysObjectIDs`, then wildcard `sysObjectIDs`, and then the `DEFAULT` settings.

Limit the IPX Hop Count (Windows only)

If you installed the Windows drivers for the IPX stack, gateways and servers acting as routers return a hop count during discovery (how many hops through gateways and routers to get to the network) for each network of which the router is aware. You can control the extent of IPX discovery allowed by NNM.

To reduce the maximum hop count for discovery, open any submap and select the `Options:Network Polling Configuration IP/IPX` menu item. On the `IPX Discovery` tab, specify the hop count of your choice.

The extra devices that were discovered based upon the old hop-count number must be manually deleted from your map. Once deleted, the discovery process will not add them again.

Troubleshooting Discovery

This section contains information about resolving common challenges encountered during NNM's discovery of your network:

- IP discovery problems and solutions (page 131)
- IPX discovery problems and solutions (page 153)

Often times, the trouble is caused because of breakdowns in your well-configured network plan (see "Starting with a Well-Configured Network" on page 90): GET and SET community names other than *public*, DNS name resolution inconsistencies, duplicate IP addresses, incorrect subnet masks, or incorrectly configured SNMP agents or DMI service providers on specific devices. NNM's map and event tracking system can make it much easier for you to identify offending devices and isolate what exactly is wrong, so you can fix the problem.

Remember to take advantage of the online discussion group, OV Forum, provided for NNM customers to communicate with each other (see "OpenView Forum" on page 77). You will find a wealth of information there.

IP Discovery and Layout

The IP troubleshooting information is broken into several groups:

- "Network Issues" on page 133
  - "Opening NNM takes a long time" on page 133
  - "NNM's initial discovery found zero nodes" on page 133
  - "All or most of the map is wrong" on page 135
  - "Whole IP networks are missing from my map" on page 135
  - "Strange networks appeared on my map" on page 136
- "Router Issues" on page 136
  - "My default router shows up on the map as a host" on page 136
  - "Some of my routers are missing" on page 136

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0507
3740
Doc:

— "One router shows up twice on my map as if it were two devices" on page 137
— "Logical interfaces (secondary IP addresses) are missing from my router's interface card submap" on page 137
— "NNM's discovery process negatively impacts my router's performance" on page 138
— "My routers are set to managed but the map doesn't expand" on page 138

- "Problems With Specific Devices" on page 138
  — "IP addresses are used to identify devices, rather than their hostnames" on page 138.
  — "The map includes devices and routing links that I have never heard of before" on page 139
  — "A few devices are depicted inaccurately on the map" on page 139
  — "An SNMP device shows up on the map as a non-SNMP node" on page 139
  — "A host shows up on the map as a router" on page 140
  — "Some of my devices are missing from the map" on page 140
  — "Devices are labeled with the IP address, when I have a name resolution system in place. What happened to the hostname" on page 141
  — "Multi-homed hosts show up as separate devices" on page 141
  — "How does NNM decide which one of multiple hostnames to use for a device" on page 142
  — "Devices have generic icons rather than manufacturer-specific icons" on page 142
  — "The name of a system running Windows is incorrect on the map" on page 143
  — "Addresses from two distinct nodes within a system running Windows are merged into a single node" on page 143
  — "DNS hostname is incorrect on map symbols for a system running Windows" on page 143
- "General IP Suggestions" on page 144

— "Check NNM's Alarm Browser: Configuration Alarms" on page 144

— "Duplicate IP Address Errors" on page 144

— "Routing Table Configuration" on page 144

— "GET- and SET-Community Name and SNMP Port Issues" on page 145

— "Subnet Mask Issues" on page 149

— "Running netmon with the Jumpstart (-J) option" on page 152

Network Issues

Opening NNM takes a long time

This is probably caused by an incorrectly configured name resolution scheme. To verify that this is the problem, do the following:

1. Find the `checkDNS.ovpl` tool.

   Windows: (located on the NNM installation CD)
   `\support\checkDNS.ovpl`

   You must copy `checkDNS.ovpl` and `gethost` into the following directory on the NNM management station:

   install_dir`\support\*`

   UNIX: `/opt/OV/support/checkDNS.ovpl`

2. Navigate to the directory containing `checkDNS.ovpl` on the NNM management station. At the command prompt type:

   `checkDNS.ovpl -v`

3. Every device listed in the NNM topology database is issued an appropriate `gethostbyaddr` or `gethostbyname` system call. Addresses or hostnames that are too slow in responding are identified in the output on the screen. Clean up the name resolution for addresses or hostnames identified as being too slow.

NNM's initial discovery found zero nodes

- First, verify that NNM's `netmon` service is running:

  — *Windows:* Select `Start:Programs:HP OpenView: Network Node Manager Admin->NNM Services - Status`

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0508
3740
Doc:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0509
Doc. 3740

— *UNIX:* At the command line prompt, type **ovstatus -c**.

If any of the services are not successfully running, see "Troubleshooting NNM Itself" on page 577 for information about troubleshooting services before continuing.

- Make sure that your network devices are running and responding to pings and SNMP requests. From the command line, issue the `ping` commands and the SNMP requests (`snmpget` and `snmpwalk`), or from any submap use the `Fault:Network Connectivity` menu choices.

  Make sure that SNMP agents are installed and running on each agent system, particularly on gateways. The problem may be that there are no SNMP agents installed.

  Your SNMP GET- and SET-Community names may not be matching up with the settings on the management station. See "GET- and SET-Community Name and SNMP Port Issues" on page 145 for more information.

- If you have very few SNMP nodes on your network, run `loadhosts` to force `netmon` to find them. See "Use loadhosts" on page 122.

  Or run `netmon` with the jumpstart (`-J`) option. See "Running netmon with the Jumpstart (-J) option" on page 152 for more information.

- Make sure that the appropriate SNMP agent is installed and running on the management station:

  — *Windows:* `SNMP EMANATE Master Agent Service`. The service must be running on the management station for discovery to function correctly. You can verify status in the `Windows NT Services` applet in the Control Panel.

  — *UNIX:* `snmpdm`. An `snmpdm` agent must be running on the management station for discovery to function correctly.

- If you specified a seed file, verify that the seed file exists and that you are using the seed file's correct name in `netmon`'s LRF file. Also, verify that you included all the nodes that you want to use as seeds in the seed file and that all the nodes listed in the seed file support SNMP. Do not use bridges and hubs as seeds, since they do not maintain ARP tables.

- From any submap, select the `Fault:Network Connectivity:Ping` menu item to contact your default router and the closest SNMP-supporting router to start gathering ARP table information.

- Make sure your default route is configured correctly. This information determines how IP packets are routed on nodes. To find the default route, do one of the following:
  - Select your management station's symbol on the NNM map and select the `Configuration:Network Configuration:IP Routing Table` menu item.

TIP You may want to establish a policy for using a standard default route so that only one router needs to maintain the routing table.

  - From the command prompt, issue the following command:
    - *Windows:* `ipconfig /all`
    - *UNIX:* `netstat -r`

All or most of the map is wrong

If all or most of the map database is inaccurate, do the following.

On your NNM map, select the questionable router symbols on the map, then use the `Edit:Object Properties` and select `IP Map` to see the current subnet mask configuration.

If a router's subnet masks are incorrectly configured, correct the configuration (see "Subnet Mask Issues" on page 149) and restart discovery (see "Stop Everything and Start Discovery Over Again" on page 161).

Whole IP networks are missing from my map

NNM isn't yet managing any devices within the missing IP network:

- Routers with addresses in the missing IP networks may not be accessible via SNMP. See "GET- and SET-Community Name and SNMP Port Issues" on page 145.
- See "Interactively Expand/Limit Your Management Domain" on page 117.
- If you have several additional networks that you need to add, consider creating a seed file to set devices within those networks to *managed* all at once. See "Create a Seed File Specifying Multiple IP Networks to Manage" on page 120 for more information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0510
3740
Doc:

Strange networks appeared on my map

The most common cause of this problem is incorrect subnet masks. See "Subnet Mask Issues" on page 149 for more information.

To check the network device's current subnet mask configuration, select the device's symbol on the map and use the map's `Edit:Object Properties` and select `IP Map`.

Router Issues

My default router shows up on the map as a host

If the default router shows up as a host on the map, verify the following:

- The most common reason that `netmon` incorrectly identifies a router as a host is that your SNMP GET- and SET-Community names may not be matching up with the settings on the management station. See "GET- and SET-Community Name and SNMP Port Issues" on page 145 for more information.
- Make sure that IP Forwarding on the router is set to "forwarding" *and* that the router has more than one interface card. From any submap, select the router's symbol and select the `Tools:SNMP MIB Browser` menu item and browse the following information:
  - IP Forwarding configuration (`.1.3.6.1.2.1.4.1`)

    `.iso.org.dod.internet.mgmt.mib-2.ip.ipForwarding`
  - Number of interfaces (`.1.3.6.1.2.1.2.1`)

    `.iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber`

  IP Forwarding is a vendor/device-specific configuration. See your device's documentation for more information.

Some of my routers are missing

If routers are not showing up on your network, check to see if the routers are "backup" routers; that is, routers used in an emergency when another router goes down. `netmon` may not discover backup routers, because `netmon` looks only for nodes on the network that are actually used. Therefore, a backup router will be discovered either as a host or it may not be discovered at all. To solve this problem, follow these steps:

1. Manually add the router to the map. See "Interactively Expand/Limit Your Management Domain" on page 117 for information about manually adding the router.
2. Use the `Fault:Network Connectivity:Ping` to determine the initial status condition of the router and turn its map symbol green (managed).
3. Use the `Fault:Network Connectivity:Poll Node` to get the information that `netmon` needs to connect the router in the proper place on the map.

One router shows up twice on my map as if it were two devices

See "Multi-homed hosts show up as separate devices" on page 141.

Logical interfaces (secondary IP addresses) are missing from my router's interface card submap

Secondary addresses are logical interfaces that are configured in addition to the physical interfaces on a router. Unfortunately, for some agents, these additional interfaces are not included in the IP address table returned through SNMP. Therefore, NNM is unaware that these interfaces exist.

When an IP address is found in an ARP Cache and it resolves to the same official name as a router, the IP address is added as an additional interface. When the router's node submap is displayed, the primary interfaces (the ones returned through SNMP) have labels that contain the first word of the interface description. The secondary addresses (the ones discovered in an ARP Cache) have only their IP addresses as their labels.

NNM can discover secondary addresses only if:

- The secondary address resolves to the same official name as the router.
- The secondary address is connected to an existing subnet.

If NNM fails to discover all the configured secondary addresses, they can be manually added as interface symbols to the router's node submap. If the interface is connected to a new subnet, that subnet must also be manually added. NNM will not automatically add the subnet symbol. See the *netmon* reference page in NNM's online help (or the UNIX manpage) for information about the `-S` parameter.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0511
3740
Doc:

The secondary addresses can be placed in a seed file that will be used by the `netmon` service for discovery (see "Create a Seed File Specifying Multiple IP Networks to Manage" on page 120). In this case, the secondary address interface symbols and the corresponding networks will be added to the map automatically.

NNM's discovery process negatively impacts my router's performance

This can happen when NNM is requesting ARP cache tables or routing tables from the router. You can use the `netmon -R` parameter to stop NNM from polling any routing tables. This cuts down on polling traffic since routing tables can be quite extensive. However, using this option means that NNM cannot discover remote routers over serial WAN links without the help of either a seed file (page 120) or loadhosts (page 122). See the *netmon* reference page in NNM's online help (or the UNIX manpage) for more information about `netmon -R`.

My routers are set to managed but the map doesn't expand

One of the following may be the problem:

- Open the Interface submap for each router by double-clicking on the router symbol and verify that all interface cards are discovered. If any are missing add them manually.
- The missing network may simply be a quiet network; without network traffic, the ARP tables won't be populated to aid NNM in the discovery process. See "Running netmon with the Jumpstart (-J) option" on page 152.
- Your router may have static routes over serial interfaces. NNM can't discover the information it needs to expand discovery because static routes may not have an entry in the routing table with a next hop address. To bypass this issue:
  - — *Windows:* Manually add the corresponding interface card.
  - — *UNIX:* Ping the corresponding interface card.

Problems With Specific Devices

IP addresses are used to identify devices, rather than their hostnames

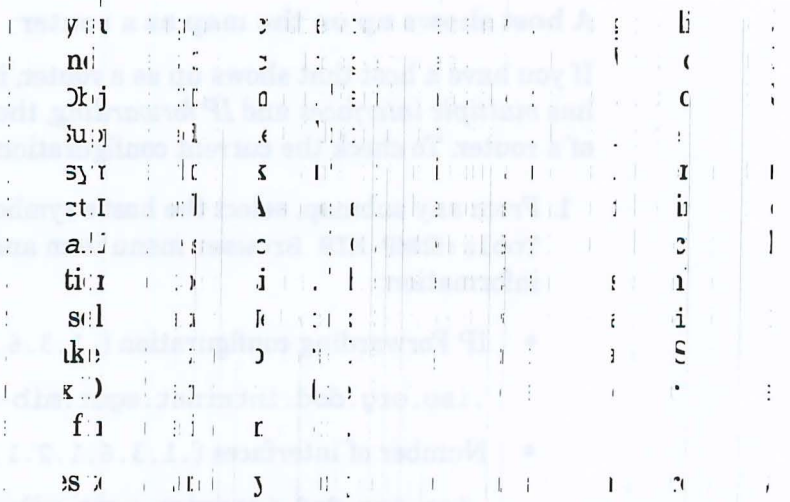
See "Opening NNM takes a long time" on page 133. See "Consistent Name Resolution Scheme" on page 91 for more information.

The map includes devices and routing links that I have never heard of before

This is probably caused by incorrectly configured subnet masks. See "Subnet Mask Issues" on page 149 for information about fixing problems with subnet masks.

A few devices are depicted inaccurately on the map

If isolated information in the map database is inaccurate, check the following:



made, select the device's symbol on any submap, then select the `Fault:Network Connectivity:Poll Node` menu item. This forces an immediate configuration check and updates NNM's databases to reflect your changes. You can also simply wait until the next polling cycle.

An SNMP device shows up on the map as a non-SNMP node

If NNM incorrectly identifies an SNMP node as a non-SNMP node, therefore displaying it as an unmanaged symbol:

- The problem may be that all of `netmon's` SNMP requests to a node failed. During SNMP requests, `netmon` asks for system information, interface table, IP address table, routing table, ARP cache, and possibly Bridge or Repeater MIB tables.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0512
3740
Doc:

If the node does not reply with a `sysObjectID`, `netmon` assumes that the node does not support SNMP. If, however, a configuration check succeeds, `netmon` assumes the node *does* support SNMP. Note that SNMP requests can fail if the transport is very busy. SNMP runs over UDP.

- The most common cause of this problem is that your SNMP GET- and SET-Community names may not be matching up with the settings on the management station. See "GET- and SET-Community Name and SNMP Port Issues" on page 145 for more information.
- Another common reason for failures is that the SNMP agent returns incorrect information. See "GET- and SET-Community Name and SNMP Port Issues" on page 145 for more information.

A host shows up on the map as a router

If you have a host that shows up as a router, it may be because the host has *multiple interfaces* and *IP forwarding,* therefore meeting the criteria of a router. To check the current configuration on the host:

1. From any submap, select the host's symbol and select the `Tools:SNMP MIB Browser` menu item and browse the following information:
   - IP Forwarding configuration (`.1.3.6.1.2.1.4.1`)

     `.iso.org.dod.internet.mgmt.mib-2.ip.ipForwarding`
   - Number of interfaces (`.1.3.6.1.2.1.2.1`)

     `.iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber`
2. From any submap, select the host's symbol and determine the device's System Object ID (`sysObjectID`) by using `Edit:Object Properties` and selecting `IP Map`. Use the `Edit:Find->Object By Attribute` menu item.

   Find all devices with the same `sysObjectID`.

   If all instances of this device are showing the same misbehavior on the map, see the *oid_to_type* reference page in NNM's online help (or the UNIX manpage) for information about the `M` parameter in the `oid_to_type` file that designates a device as a *multi-homed host* (not a gateway).

Some of my devices are missing from the map

There may be a problem with ICMP communication (ping):

- Select the Fault:Network Connectivity:Ping menu item and enter the missing IP address. If you can communicate directly with the device in this manner, it will automatically be added to the map.
- See "Interactively Expand/Limit Your Management Domain" on page 117.
- Check the device itself to ensure that it is not powered down.

The device may be in a network which is not yet *managed* by NNM:

- See "Interactively Expand/Limit Your Management Domain" on page 117.
- If you have several additional networks you need to add, consider creating a seed file to set multiple networks to *managed* all at once. See "Create a Seed File Specifying Multiple IP Networks to Manage" on page 120 for more information.

If initial discovery doesn't find many SNMP objects or if your SNMP community names are in disarray, the netmon jumpstart command (-J option) can force detected SNMP agents to generate ICMP broadcasts to populate their ARP tables, thus aiding the discovery process. See "Running netmon with the Jumpstart (-J) option" on page 152 for more information.

Devices are labeled with the IP address, when I have a name resolution system in place. What happened to the hostname

Check the DNS, NIS, or other name resolution configuration.

Use the nslookup tool that is included in the Windows or UNIX operating system. This utility can easily verify which part of the name-resolution configuration is incorrect. The reverse map must also work (nslookup must be able to resolve an IP address to a hostname, as well as resolve a hostname to an IP address). See your operating system's documentation for more information.

TIP Make sure that the case (use of uppercase and lowercase letters) is consistent in your hostnames.

Multi-homed hosts show up as separate devices

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0513
3740
Doc:

- The most common reason that `netmon` incorrectly identifies a multi-homed host as separate devices is that your SNMP GET- and SET-Community names may not be matching up with the settings on the management station. See "GET- and SET-Community Name and SNMP Port Issues" on page 145 for more information.
- Check the DNS, NIS, or other name resolution configuration.

  See also "Devices are labeled with the IP address, when I have a name resolution system in place. What happened to the hostname" on page 141 and "The name of a system running Windows is incorrect on the map" on page 143 for more information about name resolution.
- See the *oid_to_type* reference page in NNM's online help (or the UNIX manpage) and explore the `M` parameter setting for multi-homes hosts.

How does NNM decide which one of multiple hostnames to use for a device

NNM uses the hostname associated with the lowest numbered IP address which resolves to a name.

Devices have generic icons rather than manufacturer-specific icons

- The most common reason that devices display on the map with generic icons is that your SNMP GET- and SET-Community names may not be matching up with the settings on the management station. See "GET- and SET-Community Name and SNMP Port Issues" on page 145 for more information.
- From any submap, select the inaccurate symbol, right-click with the mouse, and select `Object Properties, IP Map`. Verify that the device supports SNMP (`isSNMPSupported=true`). Write down the `System Object ID` number. Then, open the `oid_to_type` and `oid_to_sym` files to make sure there is an appropriate entry for that `sysObjectID` number. Also, check the registration files included in the *`install_dir`*`\symbols\` (`$OV_SYMBOLS/$LANG`) directory. Make any additions or corrections. Then, select the node's symbol on any submap, select `Fault:Network Connectivity->Capability Poll`. It may take some time before the map symbol updates. See Appendix D, "Changing All the Symbols for a Particular Device," on page 661 for more information.

The name of a system running Windows is incorrect on the map

If an IP address to IP hostname lookup fails, the system attempts to resolve the address via NETBIOS. If the system with the IP address does not have a NETBIOS name that can be resolved back to the IP address in question, the symptoms described above can occur, as well as other communication problems with the target system.

To verify and correct the NETBIOS name on the target system, do the following:

1. On the remote system, access the Windows `Control Panel`.
2. Double-click on the `Network` icon; a dialog box will appear.
3. Correct the configured computer name.

NOTE Changing the name of the target system may affect other network connections for the system.

See also "Devices are labeled with the IP address, when I have a name resolution system in place. What happened to the hostname" on page 141 for more information about name resolution.

Addresses from two distinct nodes within a system running Windows are merged into a single node

See "The name of a system running Windows is incorrect on the map" on page 143 for information about resolving this.

DNS hostname is incorrect on map symbols for a system running Windows

See "The name of a system running Windows is incorrect on the map" on page 143 for information about resolving this.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0514
3740
Doc:

General IP Suggestions

Check NNM's Alarm Browser: Configuration Alarms

NNM's Alarm Browser sorts network alarms into useful categories for you. With your map open, notice the `Alarm Categories` window off to the side of your map. Click on the `Configuration Alarms` button to display the list of problems that NNM has discovered. Fix any problems before continuing. You will find information such as:

- Inconsistent subnet masks discovered on specific nodes (see "Subnet Mask Issues" on page 149).
- Duplicate IP addresses discovered on specific nodes.

Duplicate IP Address Errors

Duplicate IP addresses may cause the following NNM behavior:

- In an effort to keep the map current, NNM may continuously move the device symbol from one submap to a second submap and back again as it discovers the first device using the IP address and then discovers the second device using the same IP address.
- NNM's Alarm Browser may show multiple `Mismatched link-level address` alarms indicating that ARP tables on your network devices are continuously working to update based upon messages received from the two devices using the same IP address.

If within the alarm message NNM identifies the host name of the two devices, correct the problem on one of the two offending devices.

If within the alarm message NNM identifies the MAC address or link-level address of the two devices, use NNM's `Edit:Find->Object by attribute` feature to identify the two offending devices.

Routing Table Configuration

Make sure your network device's routing tables are configured properly. To check the routing table configuration on an SNMP-enabled device, select the device's symbol on any submap, then select `Configuration:Network Configuration->IP Routing Table`.

TIP NNM does not detect proxy ARP (an alternative to defining extensive routing tables). If you receive alarms about misconfigured subnet masks, proxy ARP may be the problem. If you wish to prevent these alarms from posting, highlight one of the alarms in the Alarm Browser and select `Action:Configure Event`. Then modify the event's configuration so that the alarm category is set to `Don't log or display`.

GET- and SET-Community Name and SNMP Port Issues

Community names are a security technique employed by SNMP agent software. If the network management software wants to communicate with the SNMP agent software, both the management station and the SNMP agent must know the current GET-community name and talk over the same port. By default, community names are often set to *public* and the port is set to 161. NNM assumes that these defaults are in use unless you inform it otherwise. Many network administrators change the GET-Community name so that hackers cannot obtain sensitive information about their devices. It is even more common for network administrators to change the SET-Community name, since knowing this community name enables others to make system configuration changes to the device itself.

In order to work, NNM depends upon successful communication with the SNMP agents installed on your network devices. If the GET-community names have been changed from *public* or the port changed from 161, you need to inform NNM of the new ones. (NNM cannot obtain these automatically because that would defeat the security feature.)

NOTE If you do not have access to the GET-Community names, for critical devices in your network, see "If Community Names are Unavailable" on page 148.

To inform NNM of the community naming scheme and ports in use on your network:

1. Open any submap and select the `Options:SNMP Configuration` menu item.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 145
0515
Doc: 3740

2. Enter the specific information about your community naming scheme for IP and IPX devices in this dialog box. For your convenience, you can use wildcard entries when indicating IP addresses. If no SET-Community name is defined, NNM uses the GET-Community name for SNMP SetRequests.

   In this same dialog box, you can indicate any SNMP proxies that you have set up for non-SNMP devices and indicate any nonstandard remote-port configurations that are in use by SNMP agent software on your network (default is port 161). Generally, a remote port is only specified for specialized proxy agents that do not listen to the standard SNMP port.

   Check NNM's online help from this dialog box for more information and directions.

For technical information, see the *ovsnmp.conf* reference page in NNM's online help (or the UNIX manpage).

You can also change these values using a command line interface. For more information, see the *xnmsnmpconf* reference page in NNM's online help (or the UNIX manpage). If you need to know the specific configuration settings for a particular device, use:

```
xnmsnmpconf -resolve device_name
```

For information about configuring SNMP for collection stations and management stations, refer to *A Guide to Scalability and Distribution*.

To determine which GET- and SET-Community name is currently configured in the SNMP agent on each device in your network, refer to the documentation that came with each SNMP agent software package.

If you change the community names on the agent, you also *must* configure the community names for that agent on the management station.

If the settings on both your management station and your SNMP device's agent software are correct and it still does not work, try the following and then contact the vendor of the SNMP agent software.

To verify that the problem resides in the device's SNMP agent, do one of the following. Then see if the information returned to you by the device's SNMP agent makes sense. Make sure common entries in these two tables match:

- On any submap, select the device's symbol and select the `Tools:SNMP MIB Browser` menu item. Then browse the following MIB tables:
  - interface table `.1.3.6.1.2.1.2.2` (`.iso.org.dod.internet.mgmt.mib-2.interfaces`)
  - IP address table `.1.3.6.1.2.1.4.20.1` (`.iso.org.dod.internet.mgmt.mib-2.ip.ipAddrTable`)
- From the command prompt using `snmpget` or `snmpwalk`, type:

```
snmpwalk nodename (or IP address) .1.3.6.1.2.1.2.2
snmpwalk nodename (or IP address) .1.3.6.1.2.1.4.20.1
```

Contact the vendor who supplied the SNMP agent software if the information returned to your request doesn't make sense.

Symptoms of incorrect community names include

- The default router is not discovered.
- Hosts appear to not support SNMP.
- `netmon` incorrectly identifies a router as a host.
- Node that supports SNMP as not supporting SNMP.
- The default router is shown as a host on the map.
- Error messages appear, such as "time-out" or "no such name."
- `netmon` incorrectly identifies a node that supports SNMP as not supporting SNMP.
- Multi-homed hosts show up as separate devices.

If the community name on the default router or the community name on nodes in the seed file does not match the configuration settings in NNM, `netmon` will not be able to get the information that it needs in order to discover the nodes on the network.

TIP If NNM attempts to contact a node using SNMP and the SNMP request times out, NNM looks for a `netmon.cmstr` file that you can configure to contain additional community names for the node. If the `netmon.cmstr` file exists, and contains community names, the first community name from the netmon.cmstr file that results in a successful SNMP response is

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0516
3740
Doc:

stored in the SNMP configuration database for that node. See the *netmon.cmstr* reference page in NNM's online help (or the UNIX manpage) for more information.

If Community Names are Unavailable

If you need to manage critical devices, yet do not have access to their GET-community names, create a `hosts` file. This *optional* file allows NNM to identify multiple IP addresses as being within a single device (without obtaining this information from the device's SNMP agent). This file must be maintained manually, in the following format:

```
IPAddress       hostname       alias(optional)
```

If you are identifying multi-homed devices such as switches, you must implement alias assignments so that the hostnames of all boards within the device resolve to the same IP address.

```
IPAddress_1       hostname_1       hostname_2

IPAddress_2       hostname_1

IPAddress_3       hostname_1       hostname_3
```

Place your new `hosts` file in the following location. Make sure that the file does not have any extension, such as `.txt`:

- *Windows:* `\WinNT\system32\drivers\etc\hosts`
- *UNIX:* `/etc/hosts`

NOTE Name resolution order issues:

Windows: The default behavior is to search the `hosts` file before checking DNS. If you have altered this default order, this technique may not work.

UNIX: Ensure that the hostname resolution order reads your new `hosts` file. Open the `/etc/nsswitch.conf` file and verify the contents.

Subnet Mask Issues

If the subnet masks on the management station or configured on your network devices are incorrect, discovery will fail. If the subnet mask is too restrictive, not enough is discovered. If the subnet mask is not restrictive enough, too much is discovered.

Symptoms of incorrect subnet masks may include:

- `netmon` discovers and adds nodes from the internet that are outside of your administrative domain. This is caused by an un-subnetted or incorrectly subnetted network.
- Nodes in your management domain do not show up on the map. This is caused by incorrect subnet masks on those nodes.
- Strange networks appear on the map, such as a network having a Class A, Class B, or Class C network number when you expect a subnetted network number. This is caused by incorrectly configured subnet masks on the nodes mapped to those strange networks.
- Many `Inconsistent subnet mask` alarms show up in your Alarm Browser. This is caused by incorrect subnet masks on the nodes identified in the alarm messages.

For networks to be discovered correctly, subnet masks must be correctly configured on all IP interfaces on the following:

- The management station
- All gateways
- Any nodes in a seed file for `netmon`
- Any SNMP-enabled node within your management domain

NOTE

Non-contiguous subnet masks are not supported by NNM. Also, in hierarchical subnets, two subnets having the same IP subnet address but different subnet masks are not supported. See the white paper about subnet masks (page 75) for more information.

Proxy ARP (an alternative to defining extensive routing tables) is also not supported and will result in "misconfigured subnet mask" alarms. If you wish to prevent these alarms from posting, highlight one of the

ECT 875 CPMI - CORREIOS
ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0517
3740
Doc:

alarms in the Alarm Browser and select `Action:Configure Event`. Then modify the event's configuration so that the alarm category is set to `Don't log or display`.

To identify the source of the problem caused by incorrect subnet masks, first check the management station to see which subnet masks it knows about, then check the subnet configuration on each network and each device that is causing the problem.

1. *Check the subnet mask information on the Management Station:* Check this information through both SNMP and non-SNMP tools to check for misconfigurations.
   - SNMP check:

     Use the `Edit:Find->Object by Selection Name` to locate the management station's symbol.

     Select the NNM management station's symbol and select `Configuration:Network Configuration->IP Addresses` to see which subnet masks are in use on the management station's interfaces.
   - Non-SNMP check using the tool provided by your operating system:
     - *Windows:* issue the `ipconfig /all` command

       `ipconfig /all` tells you how the system is actually configured; which may not be what the device's SNMP agent returns. For information, see your operating system documentation.
     - *UNIX:* issue the `ifconfig` *`interface`* command, where *`interface`* is usually `lan0`, `lan1`, and so forth. The `interface` command can be found in the `/usr/sbin/ifconfig` file.
2. *Check the subnet mask for each network:* If the subnet masks on the management system are correct (from the previous step), determine the subnet mask currently being used for each network. Do one of the following:

- Select a network symbol on any submap, then right-click on the symbol and select `Object Properties, IP Map`. Check to see that the subnet mask entry is correct. Repeat for each network symbol in question.
- From the command prompt, issue the `ovtopodump` command specifying each network. See the *ovtopodump* reference page in NNM's online help (or the UNIX manpage) for more information.

3. *Check the subnet mask on individual network devices:* To determine what subnet masks are returned to NNM from a device's SNMP agent, do one of the following:
   - On any node-level submap, select an interface board symbol, right-click on the symbol and select `Object Properties, IP Map`. Check the subnet mask entry.
   - On any submap, select the `Fault:Network Connectivity->Poll Node` menu item and type in the offending IP address and look at the results.
   - From the command prompt, type:

     `netstat -I nodename (or IP address)`

     Check the Windows operating system documentation or the UNIX manpage for more information about `netstat`.
4. To solve the subnet masks problems, follow these steps:
   a. Correct the problem with the subnet masks on the network objects that have the problem.

      Log into the network device itself and modify its network configuration to specify the correct subnet masks.
   b. Use the `Fault:Network Connectivity->Poll Node` menu item to verify that the new symbols have the correct subnet masks.

TIP If you discover a large number of inaccuracies, correct the problems and then redo discovery to reset NNM's databases ("Stop Everything and Start Discovery Over Again" on page 161).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0518
3740
Doc:

Running netmon with the Jumpstart (-J) option

The netmon jumpstart command (-J option) can force detected SNMP agents to generate ICMP broadcasts to populate their ARP tables, thus aiding NNM's discovery process. See the *netmon* reference page in NNM's online help (or the UNIX manpage) for more information.

CAUTION Generating ICMP broadcasts can cause a great deal of network traffic. Use this with caution.

netmon's default setting does not use the -J option. By default netmon generates, if necessary, just an ARP Request. There are several factors that determine whether netmon needs to generate an ARP Request:

- For nodes that are up but not on the same subnet with the management station, netmon generates just one ICMP echo request packet and gets back one response. In this case, no ARP Request is generated.

  Because the management station is on a different subnet, a request will go through a gateway. Gateways always have large ARP caches. netmon knows the gateway's link-level address and does not have to broadcast an ARP Request to that gateway. netmon only has to send one ICMP echo request through the gateway and gets back one response.

- For devices that are on the same subnet as the management station, netmon may generate just one ICMP echo request, or it may also generate one ARP Request as well. Because the nodes are on the same subnet, netmon does not have to go through a gateway. Broadcasting an ARP Request will depend on whether or not netmon already has the device's link-level address in the management station's own ARP cache.

- netmon will generate an ARP Request if the address that is being polled for status is not in the ARP cache of your management station.

  The presence of the address in the management station's ARP cache is affected by how many nodes are on the subnet and by how much physical memory is in your management station (some systems will automatically adjust the size of their ARP table).

If netmon is started with the -J option, netmon may cause a broadcast ICMP echo request on each subnet it discovers. These broadcasts will only be issued on a subnet if:

- No broadcast ICMP echo request has ever been issued on this subnet on behalf of this management station.
- An agent capable of issuing a broadcast ICMP echo request on netmon's behalf has been discovered on this subnet. All HP-UX SNMP agents have this capability.

IPX Discovery and Layout (Windows only)

- "General IPX Suggestions" on page 153
- "Network Issues with IPX" on page 154
  - "All IPX nodes are missing from my map" on page 154
  - "IP Network 0.0.0.0 Contains All IPX Nodes" on page 156
- "Router Issues with IPX" on page 156
  - "IPX routers are missing from my map" on page 156
- "Problems with Specific IPX Devices" on page 157
  - "Some IPX nodes are missing from my map" on page 157
  - "IPX nodes have incorrect names or labels" on page 157
  - "Nodes supporting both IP and IPX appear on the map as two separate nodes" on page 159
  - "Duplicate IP Address messages are in the Configuration Alarms list" on page 159

General IPX Suggestions

- Ensure that IPX is configured and installed correctly on the management station. See "Installing IPX Transport Software (Windows only)" on page 100. Pay particular attention to the Frame Type. All IPX nodes on the same IPX network must use the Frame Type configured on the IPX servers and routers.
- Ensure that nodes are running and responding to IPX diagnostic requests *and* SNMP requests. From the command prompt, issue the ipxping -b command. You should receive a response from each

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0519
3740
Doc:

device configured to respond to IPX. If you don't receive any responses, your management station's IPX is probably not configured correctly. If a particular node does not respond, use `snmpget` and `snmpwalk` to check that device's configuration settings. Correct any problems that you discover.

- Ensure that the community name is configured correctly (see "GET- and SET-Community Name and SNMP Port Issues" on page 145).

  It may be necessary to add entries for the IP address and hostname in addition to the IPX address. The format for an IPX address is *<net>*:*<nodeaddr>*; for example, `00000100:080009ABCDEF`. You can drop the leading zeros of the *<net>* portion of the address in most cases. For example: `100:080009ABCDEF`.

- Ensure that the SNMP agent on the node is running.
- Ensure that the IPX objects are *managed* on your map.

Network Issues with IPX

All IPX nodes are missing from my map If NNM does not discover any IPX nodes when run for the first time, check the following:

- Make sure that IPX discovery is enabled via the `Options:Network Polling Configuration:IP/IPX` operation. Click the `IPX Discovery` tab and make sure that `Discover New Nodes` is checked. Also, if IPX discovery is configured for a particular time of day, no nodes will be discovered until that time.
- Make sure that the IPX transport is correctly configured and installed on your system. If `netmon` is started with IPX discovery enabled, but the IPX software is not installed, check the Alarm Browser window under the `Application Alert Alarms` category. You should see an application error event similar to `Could not get IPX RIP socket, disabling IPX discovery.`

  `netmon` will not perform IPX discovery until IPX is correctly configured and `netmon` is restarted.
- Check the Alarm Browser window under the `Application Alert Alarms` category for other errors that may indicate the problem. For example, an invalid license could prevent the system from starting.
- Verify that there is at least one server or router that will respond to the IPX RIP request.

1. Issue the following command at the command prompt:

   Windows: ***install_dir*\bin\ipxping -r -n 1 -d 5**

   This command sends one IPX RIP request and waits five seconds for responses. Responses will include the address of the responding server or router. Adding the -v option will include the IPX networks that can be reached from your management station.

   If you do not see a response and the management station is not also configured as an IPX/NetWare gateway, this indicates that there are either no servers or routers attached to this network, or there is a misconfiguration in your IPX Transport installation. In particular, verify that the IPX transport Frame Type is configured correctly, both on the management system and on the various servers and routers in the network.

   All nodes configured for the same IPX network must run the same Frame Type. For some installations, different IPX networks may be configured for different Frame Types on the same physical cable, but all nodes in the same IPX network must have the same Frame Type, which must match the types configured on the NetWare servers and IPX routers.

2. If the test above succeeded in producing RIP responses, verify that your system receives IPX diagnostic responses by issuing the following command:

   Windows: ***install_dir*\bin\ipxping -n 1**

   This command sends a single IPX diagnostic broadcast request to the local network. All NetWare clients and servers attached to the local network should respond. Lack of response indicates either there are no local NetWare clients, or there is a misconfiguration of the IPX transport on the management station or the target systems. Verify the IPX transport installation and configuration.

3. You can also verify communication with any given network by issuing the following command from the command prompt:

   Windows:
   ***install_dir*\bin\ipxping -n 1 -b <*IPX_net_addr*>**

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 520
Doc: 3740

For example: `bin\ipxping -n 1 -b 00000100` sends a single IPX broadcast diagnostic request to the IPX network 00000100. All NetWare clients and servers configured for the 00000100 network should respond.

IP Network 0.0.0.0 Contains All IPX Nodes If you are running this version of NNM on a collection station that forwards information to a management station running NNM 4.X, you may encounter errors on the management station's display of network information. NNM 4.X does not correctly handle IPX nodes and networks. All nodes with IPX interfaces end up in a single IP network with the IP address 0.0.0.0.

To avoid this, install a topology filter that includes *only* IP objects. You can find details on installing topology filters in *A Guide to Scalability and Distribution*. An example filter, `IPObjectsOnly`, is shipped with the system's filter configuration file for this purpose.

Router Issues with IPX

IPX routers are missing from my map

1. Verify connectivity with the router as described in "Some IPX nodes are missing from my map" on page 157.
2. If the router does not support IPX diagnostic protocols, you can expand the IPX discovery region beyond the router using the `Options:Network Polling Configuration` operation. Click the `IPX Discovery` tab, and use the controls to set the `Maximum Hops` to a larger value. Make sure the value is large enough to expand beyond the router, but not any larger than desired for your discovery purposes. To discover all IPX networks, set the value to 16—the maximum allowed by IPX (however, see note below).

NOTE Setting the maximum hops to 16 can cause a large number of nodes to be discovered rapidly, causing both short-term and long-term system performance problems. Unless you are sure your system is appropriately configured to handle the number of IPX nodes in your environment, Hewlett-Packard recommends that you expand your management domain slowly.

There is no way to add the router manually if it does not respond to IPX diagnostic requests.

3. If you increased your IPX hop count, but no nodes are being discovered in some or all of the IPX networks, check the following:

   - If the IPX networks exist on your map, verify that the target networks are managed. Use `Edit:Manage Objects` to manage the target networks.
   - If you have IPX discovery configured to run only at a certain time of day, new node discovery will not happen on the newly discovered networks until that time. You can verify your IPX discovery configuration using `Options: Network Polling Configuration:IP/IPX`

Problems with Specific IPX Devices

Some IPX nodes are missing from my map If NNM discovers some, but not all nodes that support IPX:

1. Verify the installation and configuration of the IPX transport on the nodes that are not responding. In particular, check the IPX Transport Frame Type, making sure that it is either set to `Auto Detected` or set to match the Frame Type of the management system and servers.
2. Systems must respond to IPX diagnostic requests in order for NNM to add them to the databases and map. The following systems are known not to respond to IPX diagnostic requests:

   - Some dedicated routers (that is, not NetWare servers) do not support IPX diagnostic protocols.
   - Windows systems, including the management station itself.

To verify that a system responds to IPX diagnostic packets, you must know its IPX address, which is a combination of the IPX network number and its node hardware address. Once you know the IPX address, you can test connectivity to that IPX address by issuing the ***install_dir*\bin\ipxping <*IPX_address*>** command. For example: *install_dir*\bin\ipxping 00000100:080009ABCDEF sends an IPX diagnostic packet to the node with a LAN hardware address of 080009ABCDEF in the IPX network 00000100.

IPX nodes have incorrect names or labels NNM uses the following rules to choose the label for an IPX node:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. 0521
3740
Doc:

- If the node has an IP hostname, then truncate the IP hostname to just the basename and use that—preference is given to the IP name of an object.
- If the node is a NetWare server, use the NetWare server name as the label. Otherwise, take the network number of the internal server address (that is, remove the 00000000000, which is the same for every server).
- If the node supports SNMP and reports an SNMP `sysName` value, use that as the label.
- If the node supports IP, use the IP address.
- If the node supports IPX, use the host-address portion of the IPX address, formatted to translate the vendor of the hardware. (For example, `100:080009ABCDEF` gets a label of `HP-ABCDEF`).
- Otherwise, if the node has an LLA/MAC, use the hardware address as the label, formatting the hardware vendor if possible.

Based upon this information, troubleshoot naming problems by doing the following:

- If the node label is an IP address instead of a node name, update the IP address-to-hostname mapping. Verify the DNS configuration under the Network TCP/IP Configuration, and make sure your hostname resolution is configured correctly.
- If the node supports both IP and IPX and the label is incorrect, verify the IP address-to-hostname mapping as above.
- If the node is a Netware Server, verify that the correct server name is being propagated by the IPX network protocols by checking IPX SAP packets that show the server name, server type, and server address. You can check IPX SAP packets by doing either:
  - Listen for the information. Every server on the local network should broadcast a set of SAP packets once per minute. You can see the contents of these packets by typing the following at the command prompt:
    ***install_dir*\bin\ipxping -s -l**
  - Query for the information. You can obtain the information immediately by typing the following at the command prompt:
    ***install_dir*\bin\ipxping -sbgv**

If the name returned via either of the above methods does not match your expectations, you will need to reconfigure the IPX Server name.

- If the node supports SNMP, verify that the SNMP `sysName` is configured correctly on the target node. View the SNMP `sysName`, as determined by netmon, using `Edit: Object Properties`. Select the `IP Map` application and click `Edit Attributes`. The System Name attribute will be the SNMP `sysName` variable. If this name is blank, either the system does not have a `sysName` configured, or the SNMP configuration for the node is incorrect. Many nodes are shipped with a pre-configured SNMP `sysName` which may cause several nodes to have the same label.
- If the discovered label is a hardware address, but no vendor translation is occurring, check the contents of the following file: *`install_dir`*`\conf\physAddr.conf`

  Make sure the vendor is listed correctly; for example: `080009 HP`

Nodes supporting both IP and IPX appear on the map as two separate nodes If nodes that support both IP and IPX are showing up as two separate nodes on the map, verify your SNMP configuration for the IPX addresses of the node. The nodes can only be determined to be the same node if the node supports SNMP over IPX, and reports the MIB-II `ipAddrTable` correctly.

SNMP could be misconfigured over IPX. At the command prompt, type:

`snmpwalk IPXaddress system`

If you do not receive a response, verify the community name configuration (see "GET- and SET-Community Name and SNMP Port Issues" on page 145).

Duplicate IP Address messages are in the Configuration Alarms list Some IPX nodes are shipped with the IP address 192.0.0.192 preconfigured. This normally does not cause problems for IP discovery, but might for IPX discovery. If multiple nodes support SNMP over IPX, and report the 192.0.0.192 address as a valid address, `Duplicate IP Address` alarms will be generated.

To fix this problem, configure a correct IP address on each IPX node in question.

To configure NNM to simply ignore the problem and prevent these particular `Duplicate IP Address` alarms from showing up in your Alarm Browser, do the following:

RQS nº 03/2005 - CN
CPMI - CORREIO
Fls. 0522
Doc: 3740

1. From any submap, select `Options:Event Configuration`. Click the `OpenView` entry in the `Enterprises` section.
2. Select `OV_Duplicate_IP_Addr` from the event list.
3. From the `Event Configuration` window, use `Edit:Events->Copy` to make a copy of the event. A window will be displayed with the event information to be modified.
4. On the `Description` tab, enter a new event name; for example, **`Ignored_Dup_Addrs`**.
5. Click `Only specified sources`.
6. Click the `Sources` tab. Identify each node that is generating duplicate IP address alarms by doing one or more of the following:
   - Select each offending IPX node on the submaps and click the `[Add From Map]` button in the event configuration dialog box.
   - Type each node name or address into the `Source` entry area, and click `Add`. The source name should be the name listed in the `Source` column of the Alarm Browser.
   - Create an ASCII file listing the full host name or IP addresses of each offending IPX source, one per line. (Use of wildcard characters is allowed in this file.)

     Type the full path and name of this file into the `Source` entry area, and click `Add`.

   File names and sources can be intermixed in this list. See NNM's online help for more information.
7. Click the `Event Message` tab.
   a. Select either `Don't log or display`, or `Log only`.
   b. Click `[OK]`.
   c. Click `File:Save` to cause the event configuration to be updated.
   d. Click `File:Exit` to exit the `Event Configuration` window.

Stop Everything and Start Discovery Over Again

If a few aspects of your map do not look right, see "Troubleshooting Discovery" on page 131. However, if the entire map does not accurately represent your network or you decide to try discovering your network in a more limited fashion (page 124) and want to restart initial discovery, repopulate the databases, and generate a new map, do the following:

1. Stop all of NNM's services (background processes):

CAUTION See *A Guide to Scalability and Distribution* for information about shutting down NNM in a distributed environment.

   - *Windows:*
     Select `Start:Programs:HP OpenView:`
     `Network Node Manager Admin->NNM Services - Stop.`
   - *UNIX:* As root, at the command prompt, type **ovstop**.

2. Since this step deletes NNM's topology, object, and map databases and your maps, you may wish to back up your existing databases before proceeding (see "Backup/Restore to Protect Your Investment of Time" on page 165).

   If you have customized NNM's configuration (discovery configuration, SNMP configuration, event configuration, or data collection and threshold monitoring, etc.) none of these configurations are affected by this step.

   Execute the following:

   - *Windows:* Use the Windows Explorer program to highlight the ***install_dir*\databases\openview** directory. Select all of the contents of that directory and delete the contents.
   - *UNIX:* Type

     ```
     cd $OV_DB/openview
     rm -rf $OV_DB/openview/*/*
     ```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0523
3740
Doc:

NOTE If you are using a database other than the one embedded in NNM, see NNM's online manual, *Reporting and Data Analysis*.

3. Optional: To remove the old error messages and start again, execute the following:

   - *Windows:* Use the Windows Explorer program to highlight the ***install_dir*\databases\eventdb** directory. Select all of the contents of that directory and delete the contents.
   - *UNIX:* Type

     ```
     cd $OV_DB/eventdb
     rm -rf $OV_DB/eventdb/*/*
     ```

NOTE If you are using a database other than the one embedded in NNM, see NNM's online manual, *Reporting and Data Analysis*.

4. Restart NNM's services. NNM runs initial discovery, populates the databases, and generates a new map:

   - *Windows:*
     Select `Start:Programs:HP OpenView:`
     `Network Node Manager Admin->NNM Services - Start.`
   - *UNIX:* At the command prompt, type:

     ```
     xnmsnmpconf -clearCache
     $OV_BIN/ovstart ovwdb
     $OV_BIN/ovw -fields
     $OV_BIN/ovstart
     ```

See "Discover the Network... Let NNM Do It" on page 103 to start again.

ECT
DSG
CPL-AC

6 Preserve Your Sanity: Backup and Polling Configuration

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0524
3740
Doc:

Before you begin to configure NNM to meet your team's needs, it is a good idea to make sure that the backup process for NNM is in place and working properly. For information about backing up NNM see page 165.

NNM monitors the devices on your network through standard network protocols. This means that network traffic is generated while accomplishing network management. NNM ships with a generic polling configuration already in place. Take time to learn about and customize the polling configuration to meet your particular business needs. For information about controlling the polling traffic generated by NNM see page 178.

Backup/Restore to Protect Your Investment of Time

Backing up NNM can be integrated into your regularly scheduled network backup scheme. The backup happens in the background while your team continues to monitor alarms on your network. NNM temporarily pauses all services (background processes) whose activities result in changes to the NNM databases (such as the `ovw`, `ovwdb` and `ovtopmd` databases), thus ensuring consistency among the NNM databases and minimizing the potential for database corruption.

After the synchronized files are copied to the backup directory, the services resume normal activity. Then the files that do not require services to be in a paused state are copied to the backup directory.

During the backup of synchronized information, your team's maps are frozen in time, but the Alarm Browser's list and all Data Collection & Threshold information stay current throughout the backup.

NOTE Do not initiate changes to NNM's configuration files from the command line during a backup. It may cause data corruption in the backup copies of the files.

You must ensure that the information copied to the backup directory is archived to the disaster-recovery media of your choice (such as tape).

Add NNM's backup command to your list of regularly scheduled maintenance jobs. This script needs to run prior to your regularly scheduled backup process:

- *Windows:* `install_dir\bin\ovbackup.ovpl`
- *UNIX:* `$OV_BIN/ovbackup.ovpl`

Add NNM's backup directory to the list of items in your regularly-scheduled backup procedure. The backup directory (staging area) on the management station is:

- *Windows:* `install_dir\tmp\ovbackup\`

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0525
Doc: 3740

- *UNIX:* `$OV_TMP/ovbackup/`

See the *ovbackup.ovpl* and/or *ovrestore.ovpl* reference pages in NNM's online help (or the UNIX manpages) for more information.

How Does the Backup Work?

The `ovbackup.ovpl` command encapsulates all the steps needed to create a backup copy of NNM's critical files. In addition, other HP OpenView programs may supply scripts to include their critical files in the backup process.

A backup consists of two phases. The purpose of these phases is to copy the directory structure and data to the backup staging area. Two distinct phases are required in order to ensure that NNM is paused for the shortest possible time.

- **Operational Phase**

  NNM runs each script located in the `pre_pause` directory. Affected applications take preparatory steps. Then, NNM broadcasts an `ovpause` command. *All* services configured to respond to NNM's `ovpause` command take appropriate action. In some cases, the service temporarily becomes inactive. In other cases, such as data collection (`snmpCollect`), the service is not completely inactive; data continues to be recorded in temporary files until the backup is complete.

  Once all services registered to respond to the pause have successfully paused, NNM runs each script located in the `operational` directory. Because all affected services are paused, the data copied during this phase is *synchronized*.

  Once all files are copied to the backup directory structure, NNM broadcasts the `ovresume` command to restart all services. Some services, such as the data collector (`snmpCollect`), then copy their data collected during the paused state from their temporary files to the regular files. In this way, even during a paused state, data collection is not interrupted. Finally, NNM runs each script located in the `post_resume` directory to return affected applications to an operational state.

- **Analytical Phase**



NNM runs each script located in the `analytical` directory. An affected service may or may not be paused and resumed during the backup process, depending on the settings in its local registration file. The backup scripts might also pause and resume affected applications, themselves.

It is your responsibility to ensure that your disaster recovery plan includes archiving NNM's backup directory during your regularly scheduled backup scheme.

CAUTION If you choose to run `ovbackup.ovpl`, you *must* deactivate the default `solid.ini` scheduled backup. Do not do both or neither. Running both programs will result in backups that may not restore properly. Running neither program may cause severe performance problems with the embedded database. See"Problem: Backup failed. SOLID Database Error 10019:Backup is already active" on page 175 or the *Reporting and Data Analysis with HP OpenView Network Node Manager* online manual for more information.

Backing Up and Archiving All Critical Files

Try the backup and archive procedure now, before you spend a lot of time customizing NNM! Then back up and archive NNM files periodically while you configure NNM for your specific site, and back up and archive NNM files regularly as part of your disaster recovery plan.

1. The scripts named `nnm_checkpoint.ovpl` back up all of NNM's critical data. Additional scripts could be provided by other HP OpenView application developers or by you. Backup scripts must be placed in one of the following directories:

   - *Windows:*

     install_dir`\conf\ovbackup\pre_pause` **or**
     install_dir`\conf\ovbackup\checkpoint\operational` **or**
     install_dir`\conf\ovbackup\checkpoint\analytical` **or**
     install_dir`\conf\ovbackup\post_resume`

   - *UNIX:*

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0526
3740
Doc:

```
$OV_CONF/ovbackup/pre_pause or
$OV_CONF/ovbackup/checkpoint/operational or
$OV_CONF/ovbackup/checkpoint/analytical or
$OV_CONF/ovbackup/post_resume
```

TIP To prevent NNM from being paused for longer than necessary, scripts should be placed in the `analytical` directory unless the data needs to be synchronized with the NNM databases. Scripts placed in the `operational` directory are run while all services registered to respond to the `ovpause` command are paused. Scripts placed in the `analytical` directory pause and resume services one at a time or in groups, only if necessary. See "Custom Scripts" on page 176 for information about writing your own backup/restore scripts.

2. Check on disk space availability before backing up the databases.

   At a minimum, the destination directory must have space for the NNM data that `ovbackup.ovpl` copies. If additional scripts have been added by other applications or the administrator, then additional space is needed. To determine the minimum space requirements, calculate the sum of the space used by NNM in the directories listed in the following table.

TIP As soon as you install NNM, data collection begins on certain MIB objects. Data collection consumes disk space. Backing up data collection files consumes additional disk space. Disk space being consumed by any SNMP data collection as well as the back-up of these files needs to be managed. For more information on network performance data collection, see page 447.

Table 6-1 Directories Included in Backup

Windows	UNIX
Operational files: *install_dir*\databases\openview*.* *install_dir*\databases\eventdb*.* *install_dir*\log*.* *install_dir*\conf*.* *install_dir*\registration*.* *install_dir*\lrf*.* *install_dir*\fields*.* *install_dir*\symbols*.*	*Operational files:* $OV_DB/openview/* $OV_DB/eventdb/* $OV_LOG/* $OV_CONF/* $OV_REGISTRATION/* $OV_LRF/* $OV_FIELDS/* $OV_SYMBOLS/*
Analytical files: *install_dir*\databases\snmpCollect*.* *install_dir*\databases\analysis*.*	*Analytical files:* $OV_DB/snmpCollect/* $OV_DB/analysis/*

After the backup, the ovbackup directory contains a duplicate copy of all directory structures as well as individual files. The backup process does not compress data, so depending on the size of the original database, the directory could become very large:

- *Windows:* *install_dir*\tmp\ovbackup\
- *UNIX:* $OV_TMP/ovbackup/

You can specify a different directory with the `ovbackup.ovpl -d` option. See the *ovbackup.ovpl* reference page in NNM's online help (or the UNIX manpage) for more information.

TIP

The following *analytical data* directories are *not* included in NNM's backup scripts:

- *Windows:*

  install_dir\backgrounds
  install_dir\bitmaps
  install_dir\www\htdocs\bitmaps
  install_dir\www\registration

- *UNIX:*

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0527
3740
Doc:

```
$OV_BACKGROUNDS
$OV_BITMAPS
$OV_WWW/htdocs/bitmaps
$OV_WWW_REG
```

If you make changes or additions to map backgrounds, bitmap files, or web registration files ensure that your new files are properly backed up. See "Custom Scripts" on page 176 for information about writing your own backup/restore scripts.

3. Decide how you will archive the backup copy of NNM's critical files. Implement measures to ensure that the files in the *install_dir*\tmp\ovbackup directory (`$OV_TMP/ovbackup`) are archived to the disaster-recovery media of your choice on a regular and timely basis *and NOT during the time that the NNM backup scripts are running*.

CAUTION

If you redirected the Data Warehouse storage from the SOLID database to another database of your choice: The information will not be included by the `ovbackup.ovpl` script. Be sure to back up the database files that are used by NNM's reporting feature and Data Warehouse feature. See your database provider's documentation for directions about backing up your data.

4. At the command line, type **`ovbackup.ovpl`** or create a script that issues the `ovbackup.ovpl` command at the scheduled time of your choice. Refer to the *ovbackup.ovpl* reference page in NNM's online help (or the UNIX manpage) for more information.

NOTE

Do not initiate changes to NNM's configuration files from the command line during a backup. It may cause data corruption in the backup copies of the files.

TIP

UNIX systems only issue: NNM's `ovw`, `ovwdb`, and `ovtopmd` databases use sparse files. Sparse files are RDBM files which are stored to disk with the NULs stripped out. Sparse files usually have the extension `.PAG`. NNM's backup program makes sure that sparse database files are *not* expanded. Do not use `tar` because it expands sparse files.

5. After the backup completes:
   a. Check the ASCII log file to ensure that NNM's critical files were copied successfully:
      - *Windows:* *`install_dir`*`\tmp\ovbackup.log`
      - *UNIX:* `$OV_TMP/ovbackup.log`
   b. At the command line, type **ovstatus** to verify that all NNM services were successfully restarted.
6. Copy the files to the disaster recovery media of your choice.
7. Verify that your archive process successfully ran to completion and that the files on your disaster-recovery media are valid.
8. Optional: to reclaim hard drive space on your management station, delete the archived files from *`install_dir`*`\tmp\ovbackup\*.*` (`$OV_TMP/ovbackup/*`).

Restoring All of NNM (procedures/options)

In the event of a disaster or equipment upgrade, you must restore NNM to the most recently backed up state:

1. Install NNM from the installation CD, if necessary, and install any patches.
2. Stop all of NNM's services (background processes):
   - *Windows:*
     Select `Start:Programs:HP OpenView:`
     `Network Node Manager Admin->NNM Services - Stop`.
   - *UNIX:* As root, at the command prompt, type **ovstop**.
3. Retrieve the latest NNM backup files from your disaster-recovery media and copy them to the management station's backup directory.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0528
3740
Doc:

- *Windows:* *install_dir*\tmp\ovbackup\
- *UNIX:* $OV_TMP/ovbackup/

TIP

UNIX systems only issue: NNM's ovw, ovwdb, and ovtopmd databases use sparse files. Sparse files are RDBM files which are stored to disk with the NULs stripped out. Sparse files usually have the extension .PAG. Make sure that the software being used to copy the files from your disaster-recovery media to the NNM management station does not expand sparse database files. Do not use tar because it expands sparse files.

4. Type **ovrestore.ovpl** from the command line to run the script files that update NNM's databases, log files, and configuration information files.

   The scripts named nnm_restore.ovpl restore all files found in the ovbackup directory. Additional scripts could be provided by other OpenView application developers or by you. See "Custom Scripts" on page 176 for information about writing your own backup/restore scripts. These restore scripts must be placed in one of the following directories:

   - *Windows:*

     install_dir\conf\ovbackup\restore\operational
     install_dir\conf\ovbackup\restore\analytical

   - *UNIX:*

     $OV_CONF/ovbackup/restore/operational
     $OV_CONF/ovbackup/restore/analytical

5. Verify that your files are safely restored.

   Optional: to reclaim hard drive space on your management station, delete the archived files from *install_dir*\tmp\ovbackup*.* ($OV_TMP/ovbackup/*).

6. Start all of NNM's services (background processes):

   - *Windows:*
     Select Start:Programs:HP OpenView:
     Network Node Manager Admin->NNM Services - Start.
   - *UNIX:* As root, at the command prompt, type **ovstart**.

Restoring Part of NNM (procedures/options)

The `ovrestore.ovpl` command allows you to specify that only the operational data (that must remain in a synchronized state) or only the analytical data be restored. It is not recommended that you restore smaller segments of NNM than these two categories. In fact, doing so could introduce data corruption.

See the *ovrestore.ovpl* reference page in NNM's online help (or the UNIX manpage) for more information. Remember that the following steps apply:

1. Stop all of NNM's services (background processes):
   - *Windows:*
     Select `Start:Programs:HP OpenView:`
     `Network Node Manager Admin->NNM Services - Stop`.
   - *UNIX:* As root, at the command prompt, type **`ovstop`**.
2. Retrieve the latest NNM backup information from your disaster-recovery media and copy it to the management station's backup directory:
   - *Windows:* *`install_dir`*`\tmp\ovbackup\`
   - *UNIX:* `$OV_TMP/ovbackup/`

TIP

UNIX systems only issue: NNM's `ovw`, `ovwdb`, and `ovtopmd` databases use sparse files. Sparse files are RDBM files which are stored to disk with the NULs stripped out. Sparse files usually have the extension `.PAG`. Make sure that the software being used to copy the files from your disaster-recovery media to the NNM management station does not expand sparse database files. Do not use `tar` because it expands sparse files.

3. Type **`ovrestore.ovpl`** (along with the parameter specifying either operational or analytical data) from the command line to run the script files that replace NNM's databases, log files, and configuration information files with the backup copy.

   The scripts named `nnm_restore.ovpl` restore NNM-specific data in either the operational or analytical files found in the `ovbackup` directory. Additional scripts could be provided by other HP

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0529
3740
Doc:

OpenView application developers or by you. See "Custom Scripts" on page 176 for information about writing your own backup/restore scripts. These restore scripts must be placed in one of the following directories:

- *Windows:*

  install_dir\conf\ovbackup\restore\operational
  install_dir\conf\ovbackup\restore\analytical

- *UNIX:*

  $OV_CONF/ovbackup/restore/operational
  $OV_CONF/ovbackup/restore/analytical

4. Verify that your files are safely restored.

   Optional: to reclaim hard drive space on your management station, delete the archived files from *install_dir*\tmp\ovbackup*.* ($OV_TMP/ovbackup/*).

5. Start all of NNM's services (background processes):

   - *Windows:*
     Select Start:Programs:HP OpenView:
     Network Node Manager Admin->NNM Services - Start.
   - *UNIX:* As root, at the command prompt, type **ovstart**.

Troubleshooting Information

At the completion of the backup, ensure that the backup completed without the errors. This section describes some errors which can occur. Look at the last entry in NNM's backup log file:

- *Windows:* *install_dir*\tmp\ovbackup.log
- *UNIX:* $OV_TMP/ovbackup.log

Problem: The system is already in a paused state.

Solution: An error occurred while pausing the services. ovpause logs an error and generates a trap. The backup is aborted. From the command line, type **ovresume.ovpl** and then try the backup again. If you are experiencing time-out errors for a particular service during the pause process, double the length of its pause time-out by altering the affected service's lrf file. See the *lrf* reference page in NNM's online help (or the

UNIX manpage) for more information. You must use the `ovaddobj` command to update NNM's configuration, and then use `ovstop` and `ovstart` to force NNM to acknowledge the change.

Problem: `The backup failed due to a file copy error.`

Solution: The original databases are not disturbed; however, the backup files cannot be used for a recovery. Fix the copy failure condition and then restart the backup. If the copy failed due to insufficient space, free up space in the staging area or use the `ovbackup.ovpl -d` option to copy files to a different directory. See the *ovbackup.ovpl* reference page in NNM's online help (or the UNIX manpage) for more information.

Problem: `The system is not in a paused state. ovresume cannot continue.`

Solution: The backup script assumes that there will be no operator interaction during the backup. Should someone on your team execute `ovresume` from the command line prior to the backup completing, the backup process may not run to completion. The original databases are not disturbed; however, the backup files cannot be used for a recovery. Restart the backup.

Problem: `Resume attempt FAILED.`

Solution: Check the backup log file. If you also see "Resume time-out" errors, see the *ovresume* reference page in NNM's online help (or the UNIX manpage) for information about the `-t` parameter to extend the time-out interval. If you see "Resume Error" messages, call HP customer support.

Problem: `Backup failed. SOLID Database Error 10019:Backup is already active`

Solution: If you are using NNM's reporting feature or Data Warehouse feature, historical information about your network is being stored in the SOLID database. By default, the SOLID database conducts a discreet backup of its own at 11 p.m. nightly. If you see this error in the `ovbackup.log` file, it means that the `ovbackup` was scheduled to run shortly after the SOLID database backup began.

To correct this problem you must deactivate the default `solid.ini` scheduled backup. The process for doing this is:

1. Copy the `$OV_DB/analysis/default/solid.ini` file to `$OV_DB/analysis/default/solid.ini.old` file.
2. Edit the `$OV_DB/analysis/default/solid.ini` file.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0530
Doc 3740

3. Comment out the `At=<time> backup` entry, by inserting a semicolon (;) at the beginning of the line. An example would be:

```
;At=23:00 backup
```

4. Save the `$OV_DB/analysis/default/solid.ini` file.

The embedded database will now be backed up only when the `ovbackup.ovpl` command is run. If the use of `ovbackup.ovpl` is stopped at a future time, the default backup should be reinstated by copying the `$OV_DB/analysis/default/solid.ini.old` back to `$OV_DB/analysis/default/solid.ini`.

Windows-only Problem: `WARNING: Could not do 'secure' copy for file <filename>.`

Solution: This is unavoidable when open files on the Windows operating system's NTFS are copied to the staging area. See the WARNINGS section of the *ovbackup.ovpl* reference page in NNM's online help for more information.

UNIX-only Problem: `WARNING: Symbolic link errors or warnings from <directory>.`

Solution: In most cases, this is not a problem and nothing needs to be done. It usually occurs when restore attempts to create a symbolic link for a file that is already there. See the WARNINGS section of the *ovbackup.ovpl(1m)* manpage for more information.

Custom Scripts

NNM's backup procedure and restore procedure are designed so that they can be extended by placing any executable script into the appropriate `operational` or `analytical` directory. The HP-supplied `nnm_checkpoint.ovpl` and `nnm_restore.ovpl` scripts all have the extension `*.ovpl`. The suffix means "OpenView Perl" and refers to a specific subset of the Perl language used to implement NNM automated backup. This subset is not supported for general use by HP customers.

You may use the scripts supplied by HP as a reference or example while creating your own Perl scripts. However, if you create your own Perl scripts, do not use the `*.ovpl` extension in your script's file name and do not invoke HP's unsupported subset of Perl. Instead, ensure that you have a complete version of Perl installed on your system and use that one.

If you have *specific files* that you wish to include in NNM's backup process, the simplest way is to:

- *Windows:* Write a `.BAT` file that copies your files to the backup staging area, *`install_dir`*`\tmp\ovbackup`. Make sure that you duplicate the directory structure to your files, if necessary.
- *UNIX:* Write a shell script that copies your files to the backup staging area, `$OV_TMP/ovbackup`. Make sure that you duplicate the directory structure to your files, if necessary.

After you place your script in the appropriate directory, NNM runs it during the next backup or restore process:

- *Windows:*

```
install_dir\conf\ovbackup\pre_pause or
install_dir\conf\ovbackup\checkpoint\ope:  ti na  or
install_dir\conf\ovbackup\checkpoint\ana:  ti a  or
install_dir\conf\ovbackup\post_resume or
install_dir\conf\ovbackup\restore\operat:  a.
install_dir\conf\ovbackup\restore\analyt:  l
```

- *UNIX:*

```
$OV_CONF/ovbackup/pre_pause or
$OV_CONF/ovbackup/checkpoint/operational
$OV_CONF/ovbackup/checkpoint/analytical
$OV_CONF/ovbackup/post_resume or
$OV_CONF/ovbackup/restore/operational or
$OV_CONF/ovbackup/restore/analytical
```

CAUTION

If you write scripts to copy *specific files* to the backup staging area, you must either:

- Create scripts that restore those specific files to the correct location (upon execution of `ovrestore.ovpl`). Place the scripts in the appropriate restore directories.
- Remember to copy the files to their original locations after running `ovrestore.ovpl`.

Refer to the *ovbackup.ovpl* or *ovrestore.ovpl* reference page in NNM's online help (or the UNIX manpage) for more information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0531
3740
Doc:

Controlling the Amount of Traffic Generated by NNM

NOTE When you configure performance reports using the NNM web Reporting interface, the data collector starts collecting data. This data collection increases network traffic. You cannot control when or how frequently the collections are taken. If you need to reduce the amount of network traffic, you can suspend the generation of the report. See the NNM online help for more information.

Network Node Manager software automatically generates intense polling traffic at first as the network monitoring process is discovering your network.

After NNM's initial discovery of you network, *you* are in control of NNM's polling based upon your business needs. There are five types of polling in NNM that you need to know about. You can customize polling, or you can turn polling off completely. There are benefits and consequences to your decisions: less polling means less network traffic; however, reducing the amount of polling traffic by lengthening polling intervals may delay real-tim map updates, resulting in a less accurate map and less timely alarm logs. Turning polling off completely disables proactive management of you network.

You adjust NNM's polling through two dialog boxes accessed with the map menu's `Options:SNMP Configuration` and `Options:Network Polling Configuration` menu items.

Figure 6-1 Options:SNMP Configuration Dialog Box

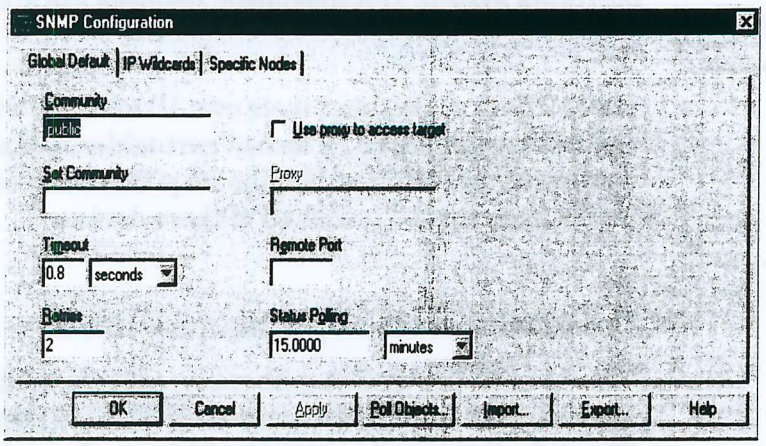
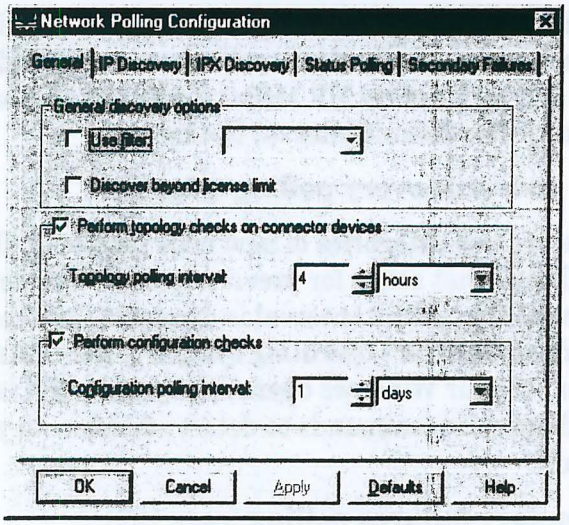


Figure 6-2 Options:Network Polling Configuration Dialog Box



Check the online help from these dialog boxes for more detailed information than you will find in this chapter. The five types of polling are:

- **Status polling** (See "Status Polling" on page 181)

  This is an ICMP `ping` sent to each interface of each managed device to verify if it is still accessible by the management station. In addition, a direct SNMP poll checks cached port tables on hubs and bridges to find the physical address listings of non-SNMP supported

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0532
3740
Doc:

devices, and a direct SNMP poll updates the designated list of DHCP addresses. Status polling intervals are configurable as described in this section. *Only management stations running a Windows operating system:* IPX diagnostic requests are also sent.

TIP

Level-2 devices (without their own IP address) whose physical addresses were found in cached port tables are included in NNM's databases and displayed on the map. However, no network polling traffic is generated on behalf of these devices.

- **Configuration check polling** (page 183)

  This is an SNMP poll to gather current information about managed devices. This information is used by NNM to keep the maps current. The default interval is once-per-24-hours for each managed device.

- **Topology check polling of connecting devices** (page 184)

  This is an SNMP poll to verify the manner in which managed connective devices (bridges and hubs via the Bridge MIB, Repeater MIB, and proprietary HP MIBs) service other devices on the network. The default interval is 4 hours.

- **New node discovery polling** (page 184)

  There are two categories of new node discovery, IP and IPX. IP is an SNMP poll that scans for previously unknown devices and updates the map. The default interval is dynamic. *Only management stations running a Windows operating system:* if the IPX stack is configured as part of your Windows operating system, IPX issues RIP, SAP, and IPX diagnostic commands to detect additions to your management domain.

- **Secondary failures polling** (page 192)

  This status polling works in conjunction with the Event-Correlation feature provided with NNM. During a network failure, NNM now identifies the device causing the problem and correlates failure messages from all other affected devices. Through this setting, you control how long NNM ignores devices other than the primary failure. You can also instruct NNM to never ignore certain critical devices, even if they are a secondary failure in an event stream.

- Also see suggestions for fine-tuning all of these polling settings on page 193.

Status Polling

For each managed IP device, an ICMP `ping` is issued to verify if it is still accessible by the management station. The `Global Default` interval for IP devices is once every 15 minutes. Often, the `Global Default` interval setting for every device is not optimal. Refer to the list of mission-critical devices that you developed in Chapter 4, "Planning Your NNM Configuration." You will probably want to poll mission-critical devices more frequently. Some customers decide not to poll certain devices at all, such as end-user PCs or certain printers.

Dynamic Host Configuration Protocol (DHCP) allows IP addresses to be allocated on a temporary basis (a lease). When the lease for an IP address expires, the address can be reused by a different node. This is useful in environments supporting mobile users who connect to the network with a laptop from many different places.

You can specify the range of IP addresses that your network is configured to assign dynamically for mobile devices. The default is OFF (no filter in use). If this filter is enabled, NNM keeps the map clean and the Alarm Browser list free of unnecessary messages about devices within this address range as they are repeatedly attached and detached from your network. Addresses are defined through a *filter* that you write using Boolean logic. See *A Guide to Scalability and Distribution* for information about writing, testing, and implementing the DHCP filter.

You can control status polling in the following ways.

In the Options:SNMP Configuration dialog box

- Set polling intervals on specific nodes by IP address, IPX address, or hostname.

  For IP addresses only, you can set polling intervals using IP address wildcards for a group of IP nodes (for example, `15.122.*.*`). You can also import a file that contains your configuration preferences; see the online help in this dialog box for information about using a file. The IP address wildcard is useful; for example, when you want to configure different values for time-outs or the number of retries for Wide Area Networks (WANs).

RQS nº 03/2005 - CN - CPMI - CORREIOS 0533
Fls. Nº
3740
Doc:

- Set the status polling interval to be used for any device not specifically listed. If you set it to 24-hours, polling begins at the time that you enter the setting. The actual time may drift depending on network conditions.
- Specify time-out and retry values. For example, you may want to increase the time-out and retry count values to prevent the management station from a premature time-out when making requests across a WAN because latency times are greater over WANs than LANs. Note that the time-out value is set in tenths of a second, and the time-out value doubles with each retry.
- Use filters to configure status polling by object classes. To view the current object class status polling interval configurations, click `Poll Objects` to open the `Status Polling Interval Configuration` dialog box. See the *OVfilterIntro* reference page (or the UNIX manpage) in NNM's online help for more information about defining filters. See the *netmon.statusIntervals* reference page (or the UNIX manpage) about modifying object-based status polling definitions.

NOTE You may want to view or edit the current object class status polling interval configurations from a remote computer. To do this, use the following procedure:

1. Edit, as `root` (UNIX) or `Administrator` (Windows), the following file and follow the instructions contained in the file.
   - *Windows*:*install_dir*`\conf\remoteConfAllow.conf`
   - *UNIX*: `$OV_CONF/remoteConfAllow.conf`
2. From your remote computer, point your web browser to the following location:
   `http://`*hostname*`:3443/OvCgi/statusIntervalConf.ovpl`

In the Options:Network Polling Configuration dialog box

- Turn OFF/ON both IP and IPX status polling.
- Specify the interval of time that NNM should wait before deleting a "down node" from your maps. The default is 1 week.

- Identify your DHCP node list filter to specify a group of IP addresses that NNM should use for laptop computers. NNM handles this group of IP addresses differently, since devices will be connected and disconnected often from these addresses. Also specify the time interval that NNM should wait before deleting a disconnected node from your map.
- Designate your Discovery filter (if you created a filter of devices that should be excluded from polling). See "Create a Discovery Filter Identifying Which Devices to Include" on page 128.

NOTE One other status polling method, **SNMP status polling**, is used only in special cases to obtain device status information using SNMP queries. SNMP status polling is not configured to run automatically at installation and does not generate any network traffic until you configure it to run. SNMP status polling is covered in more detail on page 273.

Configuration-Check Polling

This type of polling gathers SNMP information about all currently managed devices for NNM's exclusive use. Configuration-check polling gathers information such as:

- Contact and location change
- Forwarding IP packets change
- Interface added
- Interface deleted
- Incorrect routing by a node
- Link address change
- Mismatch of link address
- Network mask change
- Node name change
- Object Identifier change
- Mismatches in link addresses
- World wide web capabilities

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0534
3740
Doc.

This information is used by NNM to keep the maps and databases current. The default interval is once-per-24-hours. This setting applies to all managed devices; it cannot be customized per node.

You can control configuration-check polling in the following ways.

In the Options:Network Polling Configuration dialog box

- Turn OFF/ON all configuration polling.
- Set the interval of time to wait between configuration polling, starting from the time that you set it. The time may drift depending on network conditions.

TIP To monitor status of devices outside your firewall, see "SNMP Status Polling" on page 273.

Connector Topology Polling

Connector topology polling monitors how hubs and bridges are connected in a network. All hubs and bridges are polled based upon the Bridge MIB (RFC1493), Repeater MIB (RFC2108), MAU MIB (RFC1515), and proprietary HP MIBs. You cannot set this polling on a per node basis. This setting helps keep your map current when you are moving devices around.

You can control connector topology polling in the following ways.

In the Options:Network Polling Configuration dialog box

- Turn it OFF/ON.
- Specify the interval of time. The default is 4 hours.

New Node Discovery Polling (IP, Level-2, and IPX)

New node discovery polling checks available ARP caches and Routing tables. This information is used to keep your maps current. This setting applies to all managed devices. It cannot be customized per node.

If you are running NNM on a Windows management station: For each managed IPX network, the following broadcasts occur for each discovery interval. The default interval is 6 hours:

- A single broadcast IPX Routing Information Protocol (RIP) request
- Two broadcast Service Advertising Protocol (SAP) requests
- Two broadcast IPX diagnostic requests per network, 10 seconds apart

You can control new node discovery polling in the following ways.

In the Options:Network Polling Configuration dialog box

For IP and Level-2 devices:

- Turn new node discovery polling OFF/ON. The default is ON for both IP and Level-2 devices. See "Controlling Level-2 Device Discovery and Layout" for more information about configuring NNM to discover level-2 devices.
- Select either the auto-adjust discovery interval or set your own polling interval. The default is auto-adjust, which is based upon the number of new nodes discovered. The range is between 15 minutes and 24 hours.

For IPX devices:

- Turn new-node discovery polling OFF/ON. The default is OFF.
- Set your polling interval or the desired specific time of day for polling.
- Specify the maximum number of sequential routers through which to poll. The default hop count is zero.

Controlling Level-2 Device Discovery and Layout

NNM discovers level 2 devices on both LANs and WANs and presents this information in a graphical format in the NNM map.

Table 6-2 on page 186 and Table 6-3 on page 190 summarize the information contained in this section. Table 6-2 shows the `netmon -k` keyword options and how these options work with the `Discover Level-2 Objects` check box to deliver the resulting NNM behaviors.

Table 6-3 shows how the `Discover New IP Nodes` check box and the `Discover Level-2 Objects` check box works with the `loadhosts` command to deliver the resulting NNM behaviors.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 02535
Doc: 3740

See "Controlling Level-2 Discovery: Detailed Information" on page 188 for more in-depth information about controlling level-2 discovery and layout.

Table 6-2 Controlling Level 2 Discovery and Layout

netmon -k Option	Discover Level2 Object Check Box Status	NNM Behavior
bridgeMIB=true	Checked	Level 2 nodes and interfaces are discovered and added to the topology database. Bridge MIB layout is done. Existing level 2 interfaces in the topology are unaffected.
bridgeMIB=false	Checked	Level 2 nodes and interfaces are discovered and added to the topology database. No Bridge MIB layout is done. Existing level 2 interfaces in the topology are unaffected.
bridgeMIB=true	Not checked	Level 2 interfaces are discovered and added to the topology database. Level 2 nodes are not discovered. Bridge MIB layout is done. Existing level 2 interfaces in the topology are unaffected.
bridgeMIB=false	Not Checked	Level 2 nodes and interfaces are not discovered. No Bridge MIB layout is done. Existing level 2 interfaces in topology are unaffected.

Table 6-2 Controlling Level 2 Discovery and Layout (Continued)

netmon -k Option	Discover Level2 Object Check Box Status	NNM Behavior
discoverLevel2Nets=true	Checked	L2Nets are created between pairs of routers with such routes. All level 2 interfaces on routers are discovered and added to the topology db. Existing level 2 interfaces in the topology are unaffected.
discoverLevel2Nets=false	Checked	L2Nets are not created between pairs of routers with such routes. All level 2 interfaces on routers are discovered and added to the topology db. Existing level 2 interfaces in the topology are unaffected.
discoverLevel2Nets=true	Not checked	Routers are examined for non-IP interfaces. L2Nets are created between pairs of routers with such routes. All level 2 interfaces on routers are discovered. Only level 2 interfaces on routers needed for L2Nets are added to the topology. Existing level 2 interfaces in the topology are unaffected.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0536
3740
Doc:

Table 6-2 Controlling Level 2 Discovery and Layout (Continued)

netmon -k Option	Discover Level2 Object Check Box Status	NNM Behavior
discoverLevel2Nets=false	Not Checked	Routers are not examined for non-IP interfaces. L2Nets are not created. No level 2 interfaces on routers are discovered. Existing level 2 interfaces in the topology are unaffected.

Controlling Level-2 Discovery: Detailed Information

NNM controls the discovery and layout of level 2 devices in the following manner:

- NNM discovers and adds views of level 2 devices that support the Bridge MIB (RFC 1493).
- NNM examines routers for non-IP interfaces and adds views of level 2 networks that exist between pairs of routers to the NNM map.

You can control the discovery and map layout of level 2 devices by using of the following NNM controls:

- Using the `netmon -k` options.
- By selecting the `Discover Level2 Objects` check box in the `IP Discovery` area of the `Network Polling Configuration` user interface.

You can use the `Discover Level2 Objects` check box together with the `netmon -k bridgeMIB` options to configure the following discovery and layout behaviors:

- If the `bridgeMIB` keyword is set to true (the default value) and the `Discover Level-2 Objects` check box is checked, the `netmon` process discovers level 2 interfaces and adds these interfaces to the topology database. The `netmon` process attempts to create new

segments for bridges and switches supporting the bridge MIB and places the devices on the NNM map. In some cases the netmon process creates and places level 2 nodes on the NNM map. The `netmon` process changes the names of these newly created level 2 nodes from MAC layer addresses to IP or IPX name references if it determines that the level 2 nodes are IP or IPX nodes. Existing level 2 interfaces in the topology are unaffected.

- If you change the `bridgeMIB` keyword to `false` and the `Discover Level-2 Objects` check box is checked, the `netmon` process discovers level 2 interfaces and adds these interfaces to the topology database. The `netmon` process will not attempt to create new segments for the bridges and switches supporting the bridge MIB nor will it place the devices on the NNM map. Existing level 2 interfaces in the topology are unaffected.
- If the `bridgeMIB` keyword is set to true and the `Discover Level-2 Objects` check box is not checked, the `netmon` process discovers level 2 interfaces and adds these interfaces to the topology database. The `netmon` process attempts to create new segments for bridges and switches supporting the bridge MIB and places the devices on the NNM map. The `netmon` process will not create nor will it place level 2 nodes on the NNM map. Existing level 2 interfaces in the topology are unaffected.
- If you change the `bridgeMIB` keyword to false and the `Discover Level-2 Objects` check box is not checked, the `netmon` process will not discover level 2 interfaces nor will it add these interfaces to the topology database. The `netmon` process will not create nor will it place level 2 nodes on the NNM map. The `netmon` process will not attempt to create new segments for bridges and switches supporting the bridge MIB, nor will it place the devices on the NNM map. Existing level 2 interfaces in the topology are unaffected.

See the `ovtopofix` reference page in NNM's online help (or the UNIX manpage) for information on reversing the effects of the `bridgeMIB` keyword. Look for information on the `ovtopofix -l` (el) and `-I` options.

You can use the `Discover Level2 Objects` check box together with the `netmon -k discoverLevel2Nets` options to configure the following discovery and layout behaviors:

- If the `discoverLevel2Nets` keyword is set to true (the default value) and the `Discover Level-2 Objects` check box is checked, the `netmon` process examines routers for non-IP interfaces and creates

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 189 0537
3740
Doc:

L2Nets between pairs of routers with non-IP interfaces. All level 2 interfaces on routers are discovered and added to the topology database.

- If you change the `discoverLevel2Nets` keyword to false and the `Discover Level-2 Objects` check box is checked, the `netmon` process will not examine routers for non-IP interfaces nor will it create L2Nets between pairs of routers with non-IP interfaces. All level 2 interfaces on routers are discovered and added to the topology database.
- If the `discoverLevel2Nets` keyword is set to true and the `Discover Level-2 Objects` check box is not checked, the `netmon` process examines routers for non-IP interfaces and creates L2Nets between pairs of routers with non-IP interfaces. All level 2 interfaces on routers are discovered. Only level 2 interfaces on routers needed for L2Nets are added to the topology. Existing level 2 interfaces in the topology are unaffected.
- If you change the `discoverLevel2Nets` keyword to false and the `Discover Level-2 Objects` check box is not checked, the `netmon` process will not examine routers for non-IP interfaces nor will it create L2Nets between pairs of routers with non-IP interfaces. No level 2 interfaces on routers are discovered. Existing level 2 interfaces in the topology are unaffected.

When the `Discover New IP Nodes` check box is not checked, the `Discover Level-2 Objects` check box is grayed-out, but still impacts NNM behavior. Table 6-3 shows the resulting NNM behavior when the `Discover New IP Nodes` check box is not checked and new nodes are added by using the `$OV_BIN/loadhosts` command, netmon's seedfile, or when manually adding symbols to the map. The discovery of level 2 interfaces on these nodes is still controlled by the `Discover Level-2 Objects` check box.

Table 6-3 **Discovery Impact of Using `loadhosts` Command or a Seed File**

Discover Level-2 Objects Check Box Status	Discover New IP Nodes Check Box Status	NNM Behavior
Checked	Not checked	Adds both IP interfaces and level 2 interfaces

Table 6-3 **Discovery Impact of Using `loadhosts` Command or a Seed File (Continued)**

Discover Level-2 Objects Check Box Status	Discover New IP Nodes Check Box Status	NNM Behavior
Not checked	Not checked	Adds only IP interfaces

Changing `netmon -k` Options

You can use the following procedure to modify the netmon -k options:

1. Log in as:
   - *Windows*: Administrator
   - *UNIX*: root
2. Open the netmon local registration file in the ASCII editing software of your choice:
   - *Windows*: *install_dir*\lrf\netmon.lrf
   - *UNIX*: $OV_LRF/netmon.lrf
3. Add the text shown in bold to set the keyword to the stated value:
   - To set bridgeMIB= true:

```
netmon:netmon:

OVs_YES_START:ovtopmd,pmd,ovwdb:-P -k segRedux=true -k
bridgeMIB=true:OVs_WELL_BEHAVED:15:PAUSE::
```

   - To set bridgeMIB=false:

```
netmon:netmon:

OVs_YES_START:ovtopmd,pmd,ovwdb:-P -k segRedux=true -k
bridgeMIB=false:OVs_WELL_BEHAVED:15:PAUSE::
```

   - To set DiscoverL2Nets=true:

```
netmon:netmon:

OVs_YES_START:ovtopmd,pmd,ovwdb:-P -k segRedux=true -k
discoverLevel2Nets=true:OVs_WELL_BEHAVED:15:PAUSE::
```

   - To set DiscoverL2Nets=false;

```
netmon:netmon:
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0538
3740
Doc:

```
OVs_YES_START:ovtopmd,pmd,ovwdb:-P -k segRedux=true -k discoverLevel2Nets=false:
OVs_WELL_BEHAVED:15:PAUSE::
```

4. Turn off the netmon service (background process). At the command prompt, run **ovstop -c netmon.**
5. Force NNM to acknowledge the change. At the command prompt, run:
   - *Windows*: **ovaddobj *install_dir*\lrf\netmon.lrf**
   - *UNIX*: **ovaddobj $OV_BIN/ovaddobj $OV_LRF/netmon.lrf**
6. Turn on the netmon service (background process): At the command prompt, run: **ovstart -c netmon**

See the *netmon* reference page in NNM's online help (or the UNIX manpage) for more information; look for the -k keyword parameter and the bridgeMIB and discoverLevel2Nets keyword arguments.

Secondary Failure Polling

This setting allows you to fine-tune the behavior of the connector-down correlation circuit. The default is ON. See "NNM's Event Reduction Capabilities" on page 352 and "Connector Down Correlation" on page 361 for more information about the event correlation feature.

You can control secondary failure polling in the following ways.

In the Options:Network Polling Configuration dialog box

- Turn secondary failure polling OFF/ON.
- Specify the factor by which the normal polling interval should be extended for secondary devices during a failure.
- Designate the section that you wrote in the `filters` file that specifies which critical devices should always be excluded from the secondary status list regardless of their location during a failure event.

  See the *OVfilterIntro* reference page (or the UNIX manpage) in NNM's online help for more information about defining filters. See also *A Guide to Scalability and Distribution* for information about creating filters.
- Control the behavior of the map and event log during a failure event.

Fine-Tuning the Polling Services

The amount of network management traffic generated by status polling depends on your network's configuration, including:

- How many nodes are up and how many are down?
- How many nodes are on the same subnet?
- How many nodes are on other subnets?
- How large is the permanent ARP cache?
- How probable is it that a particular IP address can be found in the permanent ARP cache?

Polling is controlled by NNM's `netmon` service (background process). Because automatic polling is based upon managed nodes, you can reduce the amount of network-management traffic by unmanaging nodes. Simply select the node or nodes on the map, and then select the `Edit:Unmanage Objects` menu item. You can add nodes and change nodes from unmanaged to managed. It may take a while for polling changes to take effect. Polling is scheduled on a per node basis, but the `netmon` service can fall behind schedule if its polling load exceeds capacity limits.

TIP

To automatically set specific types of devices to unmanaged, such as all printers or all end-user systems, see the *oid_to_type* reference page in NNM's online help (or the UNIX manpage). See also "Modify the oid_to_type File to Unmanage Devices by Type" on page 129.

To determine if the polling process is overloaded, select the `Performance:Network Polling Statistics` menu item. If "Seconds until next status poll" or "Seconds until next SNMP poll" is a negative number, then the polling queue is overloaded and running behind.

If polling is continually running behind, you may want to change the startup parameter settings in the `netmon.lrf` file for queue length (`-q` controls the ICMP queue length, `-Q` controls the SNMP queue length, and -x controls the IPX queue length). The default queue setting is 3 on a management station running the Windows operating system and 20 on a management station running a UNIX operating system. Increasing queue length affects the management station's use of system resources and use of network bandwidth for network management.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0539
3740
Doc:

For information about parameter choices available to you for configuring NNM's polling service:

- See the *netmon* reference page in NNM's online help (or the UNIX manpage) for a wealth of choices about controlling polling from the command line and start-up parameter settings. The information in this reference page lists the parameters allowed in the `netmon.lrf` file. See "Create a Seed File Specifying Multiple IP Networks to Manage" on page 120 for information about the process of changing the `netmon.lrf` file (the seed file requires a modification to the `netmon.lrf` file).
- See the *xnmpolling* reference page in NNM's online help (or the UNIX manpage) for information about how to change polling configuration from the command line.
- See NNM's online help available from within the `Options:SNMP Configuration` dialog box and the `Options:Network Polling Configuration` dialog box for more information.

Information that is gathered during polling is stored in NNM's `ovsnmp.conf_db` database.

Watching NNM's Polling Queue

You can automate NNM to notify you whenever the `netmon` service is falling behind in the polling queue.

Use NNM's Data Collection & Thresholds feature (see page 447) to monitor two MIB values from HP's netmon MIB (provided on NNM's installation CD; use Load/Unload MIBs to access the `netmon` MIB):

- `nnmICMPSecsUntilNextPoll ( 1.3.6.1.4.1.11.2.17.4.4.1.1.3)` and
- `nnmSNMPSecsUntilNext Poll (.1.3.6.1.4.1.11.2.17.4.4.1.2.3)`

Set the threshold configuration to generate a trap each time the polling queue falls behind to the negative amount that you specify.

Then use NNM's Event Configuration feature (page 422) to set up Automatic Action instructions for that trap instructing NNM to email a message to you or to page you each time that trap is received.

Running NNM Without Network Polling

It is possible to run NNM without the netmon service (background process) that polls your network to generate the map and detect changes. This may be useful if the only applications you have running under NNM do not rely on netmon's discovery functionality or if you are relying on collection stations to perform discovery and monitoring.

NOTE See *A Guide to Scalability and Distribution* for information about collection stations and how to proceed with this step when using collection stations.

To run NNM without automatic IP discovery, configuration checking, and polling by netmon, follow these steps:

1. Stop the currently running netmon service (background process). From the command line, type **ovstop -v netmon**
2. Remove netmon from NNM's start-up options. At the command prompt, type:

   Windows: **ovdelobj *install_dir*\lrf\netmon.lrf**

   UNIX: **ovdelobj $OV_LRF/netmon.lrf**

NOTE If you change your mind and want to restart netmon at a later time:

1. Add netmon to NNM's start-up options. At the command prompt, type:

   Windows: **ovaddobj *install_dir*\lrf\netmon.lrf**

   UNIX: **ovaddobj $OV_LRF/netmon.lrf**

2. Start the netmon service (background process):

   Windows: Select `Start:Programs:HP OpenView:Network Node Manager Admin->NNM Services - Start`.

   UNIX: As root, at the command prompt, type **ovstart**.

The pmd, ovwdb, and ovtopmd services must also be running before netmon can work properly. To generate a list showing the status of each of NNM's services:

RQS nº 03/2005 - CN - CPMI CORREIOS
Fls. Nº 0540
3740
Doc:

- *Windows:* Select `Start:Programs:HP OpenView:Network Node Manager Admin->NNM Services - Status`.
- *UNIX:* At the command line prompt, type **`ovstatus -c`**.

If any of the processes are not successfully running, see Appendix A, "NNM Services and Files," on page 539 for information about troubleshooting NNM's services before continuing.

PREGÃO 118/2003

PASTA 04

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0541
3740
Doc:

DGECIDECAM FLS. Nº 3196

RESULTADO DO PREGÃO Nº 29/2003

A FUNASA, através de sua Pregoeira e equipe de apoio, declara vencedora do certame a Empresa JOSE FRANCISCO DE SOUZA O IPORA.

MARIA DAS NEVES DE LIZ HENDERSON

(SIDEC - 31/12/2003) 255000-36211-2003NE900006

COORDENAÇÃO REGIONAL NO PIAUÍ

EXTRATO DE CONTRATO Nº 1/2004

Nº Processo: 25235004867200362. Contratante: FUNDACAO NACIONAL DE SAUDE. CNPJ Contratado: 12190625000142. Contratado : OPEN-TOUR VIAGENS E TURISMO LTDA. Objeto: Fornecimento de passagens aéreas nacionais, com o percentual de desconto de 5,00% (cinco, por cento), sobre o volume de vendas. Fundamento Legal: Decreto 3555/2000 Vigência: 02/01/2004 a 31/12/2004. Valor Total: R$137.295,90. Fonte: 151000000 - 2003NE900920 Fonte: 151000000 - 2003NE900921 Fonte: 153000000 - 2003NE900922. Data de Assinatura: 22/12/2003.

(SICON - 31/12/2003) 255018-36211-2003NE000006

EXTRATO DE TERMO ADITIVO Nº 3/2003

Número do Contrato: 1/2002. Nº Processo: 25235001618200153. Contratante: FUNDACAO NACIONAL DE SAUDE. CNPJ Contratado: 12066015000131. Contratado : SERVI SAN VIGILANCIA E TRANSPORTEDE VALORES LTDA. Objeto: Repactuação de preço do Contrato nr.01/2002 e prorrogação do prazo de vigência, referente Serviço de Vigilância Armada prédio sede da FUNASA/CORE-PI. Fundamento Legal: Decreto nr. 3555/2000 Vigência: 02/01/2004 a 01/01/2005. Valor Total: R$66.972,00. Fonte: 151000000 - 2001NE900897. Data de Assinatura: 05/11/2003.

(SICON - 31/12/2003) 255018-36211-2003NE000006

EXTRATO DE TERMO ADITIVO Nº 1/2003

Número do Contrato: 24/2002. Nº Processo: 25235006987200213. Contratante: FUNDACAO NACIONAL DE SAUDE. CNPJ Contratado: 23651284000181. Contratado : TECDATA TECNOLOGIA EM DADOS LTDA. Objeto: Prorrogação do prazo de vigência do contrato nr. 24/2002 - Prestação de Serviços de manutenção preventiva e corretiva no Parque Computacional da FUNASA/CORE-PI, valor mensal R$2.585,00, valor total anual R$31.020,00. Fundamento Legal: Decreto nr. 3555/2000 Vigência: 02/01/2004 a 01/01/2005. Data de Assinatura: 03/12/2003.

(SICON - 31/12/2003) 255018-36211-2003NE000006

COORDENAÇÃO REGIONAL NO RIO DE JANEIRO

EXTRATO DE TERMO ADITIVO Nº 3/2003

Número do Contrato: 42/2001. Nº Processo: 25245001213/01-43. Contratante: FUNDACAO NACIONAL DE SAUDE. CNPJ Contratado: 33530486000129. Contratado : EMPRESA BRASILEIRA DETELECOMUNICACOES S A EMBRATEL. Objeto: Constitui objeto deste termo aditivo a inclusão de dotação orçamentária, referente às despesas decorrentes do segundo termo aditivo. Fundamento Legal: 8.666/93. Vigência: 15/12/2003 a 04/12/2004. Valor Total: R$[illegible]2,90. Fonte: 151000000 - 2003NE900974. Data de Assinatura: [illegible]/12/2003.

(SICON - 31/12/2003) 255019-36211-2003NE900001

COORDENAÇÃO REGIONAL NO RIO GRANDE DO NORTE

EXTRATO DE DOAÇÃO

Processo nº 25100.003.408/1996-05.ESPECIE: Termo de Doação nº 3/2003. DONATARIO: Fundação Nacional de Saude, Coordenação Regional do Rio Grande do Norte. BENEFICIARIO: Secretaria Estadual de Saude Publica RN.OBJETO: Bens Patrimoniais conforme consta na Relação de Bens Adquiridos do referido processo. Valor total da aquisição R$ 85.720,66, conforme consta no processo supracitado. Fundamento Legal: Artigos 538 a 564 do Codigo Civil Lei nº 10.406/2002, Inciso IV do Art. 15º do Decreto nº 99.658/90, Lei nº 8.666/93 e alterações posteriores e a Lei nº 9.784/99. Data da Doação: 30/12/2003. SIGNITARIOS: Lauro Gonçalves Bezerra, CPF nº 002.669.574-04, Coordenador Regional FUNASA RN, e Ivis Alberto Lourenço de Andrade, CPF nº 003.458.734-91, Secretario Estadual de Saude Publica RN.

RESULTADO DO PREGÃO Nº 14/2003

A FUNASA CORE/RN, através do seu Pregoeiro e equipe de apoio, torna publico o Resultado de Julgamento do Pregão Presencial nr. 14/2003, declarando vencedoras as empresas: LEDIMAR AUTOPEÇASE SERVIÇOS LTDA-ME,item 01,no valor de R$ 15,30(Quinze Reais e Trinta Centavos) hora/homem e a empresa FLASH CAR PEÇAS E SERVIÇOS LTDA-ME,item03, no valor de R$ 44,50 (Quarenta e Quatro Reais e Cinquenta Centavos) hora/homem. O item 02 foi cancelado.Os autos do processo encontram-se a disposição dos interessados a partir desta publicação.

CICERO ALVES TEIXEIRA NETO

(SIDEC - 31/12/2003) 255020-36211-2003NE900006

FUNDAÇÃO OSWALDO CRUZ
CENTRO DE INFORMAÇÕES CIENTÍFICAS E TECNOLÓGICAS

EXTRATO DE CONTRATO Nº 29/2003

Nº Processo: 25380006797200311. Contratante: FUNDACAO OSWALDO CRUZ. CNPJ Contratado: 08758264744. Contratado : CRISTOVAO LIBERATO MONTEIRO. Objeto: Contratacao de prestador de servico emprogramacao em Web no processo de informatizacao do CICT. Fundamento Legal: Artigo 24 Inciso II da Lei nº 8666/93 Vigência: 23/12/2003 a 23/03/2004. Valor Total: R$7.800,00. Fonte: 151000000 - 2003NE909445. Data de Assinatura: 23/12/2003.

(SICON - 31/12/2003) 254431-25201-2003NE900811

EXTRATO DE CONTRATO Nº 30/2003

Nº Processo: 25380007247200310. Contratante: FUNDACAO OSWALDO CRUZ. CNPJ Contratado: 27173399734. Contratado : SERGIO GALVES PINTO DA COSTA. Objeto: Contratacao de prestador de servico emanalise e Programacao Delphi no processo de informatizacao da gestão do CICT Fundamento Legal: Art. 24 Inciso II da Lei 8666Vigência: 23/12/2003 a 23/03/2004. Valor Total: R$7.900,00. Fonte: 151000000 - 2003NE909423. Data de Assinatura: 23/12/2003.

(SICON - 31/12/2003) 254420-25201-2003NE909445

SECRETARIA DE VIGILÂNCIA EM SAÚDE
CENTRO DE REFERÊNCIA PROFESSOR HELIO FRAGA

EXTRATO DE TERMO ADITIVO Nº 4/2003

Número do Contrato: 00008/2000, subrogado pelaUASG: 255030 - FNS/CRP.HELIO FRAGA. Nº Processo: 25246000238199951. Contratante: FUNDACAO NACIONAL DE SAUDE. CNPJ Contratado: 32260390000125. Contratado : ELETRONICA GUTERRES LTDA ME. Objeto: Por força do decreto nº 4726/03, fica alterado no preambulo do contrato originario, a situaçao juridica, o nº de inscriçao do CNPJ/MF, a indicaçao do ato designativo e da competencia do representante legal do CRPHF, fazendo constar o teor da redaçao do preambulo do presentetermo aditivo no contrato nº 08 de 2000,celebrado em 01/03/2000 entre o CRPHF e a empresa Eletronica Guterres Ltda. - ME. Fundamento Legal: Lei nº 8666/93 e suas alteraçoes posteriores. Vigência: 26/12/2003 a 28/02/2004. Valor Total: R$975,00. Data de Assinatura: 26/12/2003.

(SICON - 31/12/2003) 255000-36211-2003NE900023

EXTRATO DE TERMO ADITIVO Nº 1/2003

Número do Contrato: 00008/2003, subrogado pelaUASG: 255030 - FNS/CRP.HELIO FRAGA. Nº Processo: 25246000410200350. Contratante: FUNDACAO NACIONAL DE SAUDE. CNPJ Contratado: 27859008000164. Contratado : ULTRAPEL COMERCIO DE MATERIAIS DE ESCRITORIO LTDA. Objeto: Por força do Decreto nº 4726/03,fica alterado no preambulo do contrato originario, a situaçao juridica, o nº de inscriçao do CNPJ/MF,a indicaçao do ato designativo e da competencia do representante legal do CRPHF, fazendo constar o teor da redaçao do preambulo do presente termo aditivo e prorrogado com fundamento no incisoII do art. 57, da Lei nº 8666/93 e suas alteraçoes posteriores de 01/01/04 a 31/12/04, o prazo de vigencia originalmente estabelecido na Clausula VI do contrato nº 08/03. Fundamento Legal: Lei 8666/93 e suas alteraçoes posteriores. Vigencia: 01/01/2004 a 31/12/2004. Valor Total: R$44.880,00. Data de Assinatura: 26/12/2003.

(SICON - 31/12/2003) 255000-36211-2003NE900023

EXTRATO DE TERMO ADITIVO Nº 2/2003

Numero do Contrato: 00009/2002, subrogado pelaUASG: 255030 - FNS/CRP.HELIO FRAGA. Nº Processo: 25246000628200171. Contratante: FUNDACAO NACIONAL DE SAUDE. CNPJ Contratado: 36529998000163. Contratado : UNIRIO MANUTENCAO E SERVICOS LTDAME. Objeto: Por força do Decreto nº 4726/03, fica alterado no preambulo do contrato originario, asituaçao juridica, o nº de inscriçao do CNPJ/MF,a indicaçao do ato designativo e da competencia do representante legal do CRPHF, fazendo constar o teor da redaçao do preambulo do presente termo aditivo e prorrogado com fundamento no inciso II do art.57, da Lei nº 8666/93 e suas alteraçoes posteriores, de 01/01/04 a 31/12/04, o prazo de vigencia originalmente estabelecido na clausula VI do contrato nº 09/02 de 16/02/02. Fundamento Legal: Lei nº 8666/93 e suas alteraçoes posteriores. Vigencia: 01/01/2004 a 31/12/2004. Valor Total: R$25.908,72. Data de Assinatura: 20/12/2003.

(SICON - 31/12/2003) 255000-36211-2003NE900023

Ministério das Cidades

GABINETE DO MINISTRO

EXTRATO DE ACORDO DE COOPERAÇÃO TÉCNICA Nº 1/2003

Processo n. º 80000.016850/2003-10
Partícipes: Ministério das Cidades, CNPJ nº 05.465.986/0001-99 e Caixa Econômica Federal - CEF - CNPJ/MF 00.360.305/0001-04. Objeto do Acordo: Promover a operacionalização da execução orçamentária e financeira dos programas Nosso Bairro, Saneamento e Vida, Morar Melhor, Gestão Urbana e Metropolitana, Infra-Estrutura Urbana, Gestão de Resíduo Sólido Urbano e Programas relativos a transporte e Mobilidade Urbana, bem como a implementação de outras ações e programas geridos pelo Ministério... Signatários: Olívio de Oliveira Dutra, Ministro de Estado das Cidades - CPF/MF n. º 050.126.430-20, Jorge Eduardo Levi Mattoso, Presidente da Caixa Econômica Federal - CEF - CPF/MF n. º 010.118.868-47.

SECRETARIA NACIONAL DE HABITAÇÃO

EXTRATO DE CONTRATO

nº 2003/003041
Espécie: Contratação de serviços técnicos especializados e de consultoria. Partícipes: MINISTÉRIO DAS CIDADES, CNPJ/MF n.º 05.465.986/0001-99, Programa das Nações Unidas para o Desenvolvimento - PNUD - BRA/00/019 - Habitar Brasil/BID e ELZIRA MARQUES LEÃO Objeto do contrato: realizar levantamento de dados e confecção de relatório semestral. Identificação do Signatário: ELZIRA MARQUES LEÃO, Consultora - Serviços não continuados, na modalidade por Produto (conforme está no TOR e na SAP). Valor Total da Contratação: 6.500,00 (seis mil e quinhentos reais), correspondente ao percentual de 100% (cem por cento). Período: 08/12/03 à 31/12/03. Recursos Orçamentários: Os recursos serão disponibilizados pelo PNUD, através do Contrato BRA/00/019. Notas de Assinaturas: CARLOS LOPES - Representante Residente do Programa das Nações Unidas para o Desenvolvimento - PNUD, Inscrição Genérica n. º X3621302 e ELZIRA MARQUES LEÃO, CPF/MF n.º 022.859.672-68

Ministério das Comunicações

GABINETE DO MINISTRO

EXTRATO DE CONTRATO

PARTES: União e a Rádio Comunicação Pitangui Ltda.
ESPECIE: Contrato de Adesão de Permissão outorgada por meio da Portaria nº 363, de 5 de julho de 2001, publicada no Diário Oficial da União de 11 de julho de 2001.
OBJETO: Execução do serviço de radiodifusão sonora em freqüência modulada, na localidade de Pitangui, Estado de Minas Gerais.
VIGENCIA: O contrato tem vigência de 10 (dez) anos e entra em vigor na data de publicação deste extrato no Diário Oficial da União.
DATA E ASSINATURA: 16 de dezembro de 2003. Miro Teixeira - Ministro de Estado das Comunicações, e Marcilio Valadares - Procurador da Rádio Comunicação Pitangui Ltda.

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS
ADMINISTRAÇÃO CENTRAL

EXTRATO DE CONTRATO

1.ESPÉCIE: Contrato nº 12.416/03; 2. CONTRATANTE: EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS - ECT; 3. CONTRATADA: HEWLETT-PACKARD BRASIL LTDA.; 4. DATA DA ASSINATURA: 26/12/2003; 5. VALOR GLOBAL: 418.500,00 (quatrocentos e dezoito mil e quinhentos reais); 6. RECURSOS ORÇAMENTÁRIOS: Conta: 9.02, Atividade: 17.1.01; 7. VIGENCIA: Inicia-se na data de assinatura e termina com a emissão do Termo de Aceitação Final - TAF dos softwares, limitado ao prazo de 12 meses; 8. OBJETO: Aquisição de 5 (cinco) licenças do software HP OPEN VIEW NETWORK NODE MANAGER ENTERPRISE - versão 6.2 ou superior, incluindo serviços de atendimento e suporte técnico; 9. ORIGEM: Pregão nº 118/2003- CPL/AC; 10. SIGNATÁRIOS: Eduardo Medeiros de Morais - Diretor de Tecnologia e de Infra-estrutura da Contratante e Ana Lucia Leitão Nunes - Chefe do Departamento de Rede Corporativa da Contratante, e Paulo César Rossigneux Vieira - Gerente de Contas da HEWLETT-PACKARD e José Eduardo Pires do Rio Ribeiro - Gerente de Contas da HEWLETT-PACKARD

EXTRATOS DE TERMOS ADITIVOS

1.ESPECIE: Primeiro Termo Aditivo ao Contrato nº 11.390/02, 2.CONTRATANTE: EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS - ECT, CONTRATADA: INTELIG TELECOMUNICAÇÕES LTDA; DATA DA ASSINATURA: 10/09/2003; OBJETO: Prorrogação da vigência do contrato, por mais 12 (doze) meses, período de 11/09/2003 a 11/09/2004, e supressão de 57,1497% do valor global inicialmente contratado; RECURSOS ORÇAMENTÁRIOS: Atividade: 00.8.00 - Conta: 04.01; SIGNATÁRIOS: Airton Langaro Dipp - Presidente da Contratante e Gabriel Pauli Fadel - Diretor de Administração da Contratante, João Humberto Mazimi Soler e Moacir Alves da Conceição - Procuradores da Contratada

RQS nº 03/2005 - CN CPMI - CORREIOS Fls. Nº 0542 3740

CORREIOS

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS

DGECIDECAM
FLS. Nº 315

CONTRATO DE AQUISIÇÃO DE LICENÇAS HP OPEN VIEW NETWORK NODE MANAGER ENTERPRISE - VERSÃO 6.2 OU SUPERIOR

CONTRATANTE: EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS

CNPJ: 34.028.316/0001-03
INSCRIÇÃO ESTADUAL: 07.333.821/002-05
ENDEREÇO: SBN QUADRA 1, BLOCO "A", CONJ. 3 – ED. SEDE DA ECT
CEP: 70.002-900 - BRASÍLIA/DF
TELEFONE: (61) 426-2794
FAX: (61) 426-2807

DEPARTAMENTO JURÍDICO
E C T
30 DEZ 2003
Contrato nº 12416
BRASÍLIA - DF

REPRESENTANTE (S):

DIRETOR DE ÁREA: EDUARDO MEDEIROS DE MORAIS
DOCUMENTO DE IDENTIDADE: 453.609 – SSP/DF
CPF: 150.199.771-87

CHEFE DE DEPARTAMENTO: ANA LÚCIA LEITÃO NUNES
DOCUMENTO DE IDENTIDADE: 1.279.946 – SSP/DF
CPF: 339.526.397-53

CONTRATADA: HEWLETT-PACKARD BRASIL LTDA
CNPJ : 61.797.924/0001-55
INSCRIÇÃO ESTADUAL: 206.203.572.117
ENDEREÇO: AL. RIO NEGRO, 750 – ALPHAVILLE – BARUERI -/SP
CEP: 06454-000
TELEFONE: (11) 4197-8000
FAX: (11) 4197-8432

REPRESENTANTE(S):

GERENTE CONTAS: PAULO CESAR ROSSIGNEUX VIEIRA
CARTEIRA DE IDENTIDADE: 703.633 – SSP/DF
CPF: 903.621.798-91

GERENTE CONTAS: JOSÉ EDUARDO PIRES DO RIO RIBEIRO
CARTEIRA DE IDENTIDADE: 15.319.247 –SSP/SP
CPF: 071.885.858-14
E-MAIL: jose-eduardo.ribeiro@ hp.com

DEPARTAMENTO JURÍDICO E C T

Conforme NJ/DEJUR/DJTEC 12/11/03

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0543

3740
Doc:

DGEC/DECAM
FLS. Nº 3194

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. O presente Contrato temo como objeto a aquisição de *05 (cinco) Licenças do software* HP OPEN VIEW NETWORK NODE MANAGER ENTERPRISE, VERSÃO 6.2. OU SUPERIOR, incluindo os serviços de atendimento e suporte técnico, conforme condições e especificações constantes deste Contrato e seu Anexo 01.

CLÁUSULA SEGUNDA - DAS OBRIGAÇÕES DA CONTRATADA

2.1. Manter todas as condições de habilitação e qualificação exigidas na licitação, durante todo o período do Contrato.

2.2. Efetuar a entrega do objeto contratado e emitir Nota Fiscal, em nome da **CONTRATANTE**, de acordo com as quantidades, especificações e endereço(s) constante(s) do **ANEXO 1** deste contrato.

2.3. Discriminar, no documento fiscal, o número deste Contrato e o seu objeto, de acordo com o estabelecido no **subitem 1.1.** deste Contrato.

2.4. Aceitar, nas mesmas condições contratuais, acréscimos ou supressões que se fizerem necessárias, em até **25% (vinte e cinco por cento)** do valor inicial atualizado do Contrato, previsto no **subitem 5.1.** da Cláusula Quinta, facultada a supressão além desse limite, mediante acordo a ser celebrado entre as partes.

2.5. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, os objetos em que se verificarem vícios, defeitos ou incorreções.

2.6. Responder, diretamente por quaisquer perdas, danos ou prejuízos que vierem a causar à **CONTRATANTE** ou a terceiros, decorrentes de sua ação ou omissão, dolosa ou culposa, na execução deste Contrato, independentemente, de outras cominações contratuais ou legais a que estiver sujeita.

2.7. São de inteira responsabilidade da **CONTRATADA** todas as obrigações pelos encargos previdenciários, fiscais, trabalhistas e comerciais resultantes da execução deste Contrato.

2.8. Fornecer as licenças dos softwares acompanhadas da documentação técnica do fabricante, bem como da documentação das parametrizações (customizações) realizadas nas ferramentas no processo de instalação e configuração e ainda, da documentação referente a instalação, configuração e operação e prestar esclarecimentos e informações técnicas que venham a ser solicitada pela **CONTRATANTE**.

2.9. Prestar atendimento de suporte técnico à ECT, conforme estabelecido no subitem 3.6 do Anexo 2 deste Contrato.

CLÁUSULA TERCEIRA - DAS OBRIGAÇÕES DA CONTRATANTE

3.1. Efetuar os pagamentos devidos à **CONTRATADA** no prazo estabelecido no **subitem 6.1** deste Contrato.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0544
3748
Doc:
DEPARTAMENTO JURÍDICO
E C T
Conforme
AJ/DEJOR/DJTEC

DGECIDECAN
FLS Nº 319

3.2. Fiscalizar a execução deste Contrato, e subsidiar a **CONTRATADA** com informações e/ou comunicações úteis ou necessárias ao melhor e fiel cumprimento deste Instrumento.

3.3. Comunicar à **CONTRATADA** toda e qualquer ocorrência que interfira na execução deste Contrato.

CLÁUSULA QUARTA – DAS CONDIÇÕES GERAIS

4.1. Não havendo expediente na **CONTRATANTE** no dia da entrega do material, do pagamento ou outro evento, a data para o adimplemento da obrigação será prorrogada para o primeiro dia útil imediato.

4.2. O material recusado/rejeitado será considerado como não entregue.

4.3. A aceitação do objeto não exclui a responsabilidade civil, por vícios de forma, quantidade, qualidade ou técnicos ou por desacordo com as correspondentes especificações, verificadas posteriormente.

CLÁUSULA QUINTA – DO VALOR E DOS PREÇOS

5.1. O valor global do presente Contrato é de R$ 418.500,00 (quatrocentos e dezoito mil e quinhentos reais), conforme preço(s) unitário(s) abaixo:

ITEM	DESCRIÇÃO DO MATERIAL	UNID	QTDE	PREÇO UNITÁRIO R$
01	Licenças do Software **HP OPEN VIEW NETWORK NODE ENTERPRISE VERSÃO 6.2 OU SUPERIOR**	UM	05	83.700,00

5.2. No preço estão contidos todos os custos e despesas diretas e indiretas, tributos incidentes, encargos sociais, previdenciários, trabalhistas e comerciais, taxa de administração e lucro, materiais e mão-de-obra a serem empregados, seguros, frete, embalagens e quaisquer outros obrigatórios ou necessários à composição do preço do material, objeto deste Contrato.

5.3. O preço é fixo e irreajustável durante a vigência deste Contrato, salvo se houver determinação do Poder Executivo em contrário e de acordo com as regras definidas à época.

CLÁUSULA SEXTA - DO PAGAMENTO

6.1. Em parcela única, mediante entrega das ferramentas, no prazo de **15 (quinze) dias** após a emissão do **Termo de Aceitação Final - TAF**.

6.1.1. Havendo disponibilidade e interesse da **CONTRATANTE**, bem como solicitação da **CONTRATADA**, o pagamento, eventualmente, poderá ser antecipado, mediante desconto, nos termos do Art. 40, Inciso XIV, letra "d" da Lei 8.666/93 e nas regras estabelecidas no site da ECT, acessando http://www.correios.com.br/institucional/licit_compras_contratos/SPFVP/default.cfm.

RQS nº 03/2005 - CN - CPMI - CORREIOS
0545
Fls. Nº

Conforme
RJ DEJOR/DITEC/SEDOC 2
3740

DGECIDECAM
FLS. Nº 3199

6.1.2. A **CONTRATADA** deverá apresentar, por ocasião do pagamento, a Certidão Negativa de Débito do INSS, devidamente atualizada.

6.1.3. A não-apresentação da Certidão Negativa de Débito do INSS (CND) ou sua irregularidade, não acarretará retenção do pagamento. Entretanto, a **CONTRATADA** será comunicada a apresentar tal documento em até **30 (trinta) dias**, sob pena de rescisão contratual e demais penalidades cabíveis.

6.1.4. Decorrido o prazo acima, persistindo a irregularidade, o Contrato poderá ser rescindido, sem prejuízo das demais penalidades cabíveis.

6.1.5. Concomitantemente à comunicação à **CONTRATADA,** a **CONTRATANTE** oficiará a ocorrência ao INSS.

6.1.6. Caso o objeto deste Contrato seja recusado e/ou o documento fiscal apresente alguma incorreção, será considerado como não entregue e o prazo de pagamento será contado a partir da data de regularização, observado o disposto no **subitem 6.1.** deste Contrato.

6.1.7. O(s) pagamento(s) será(ão) efetuado(s) por meio de depósito bancário, conforme dados a seguir:

- **BANCO:** 341 ITAU
- **AGÊNCIA:** 0912
- **CONTA CORRENTE:** 08067-8

6.1.8. Quaisquer alterações nos dados bancários deverão ser comunicadas à **CONTRATANTE**, por meio de Carta, ficando sob inteira responsabilidade da **CONTRATADA** os prejuízos decorrentes de pagamentos incorretos devido à falta de informação.

6.1.9. Correrão por conta da **CONTRATADA** o ônus do prazo de compensação e todas as despesas bancárias decorrentes da transferência de crédito.

6.2. Ocorrendo atraso de pagamento por culpa da **CONTRATANTE**, será procedida a atualização monetária decorrente desse atraso, com base na variação *pro rata tempore* do IGPM (FGV), verificada entre a data prevista para o pagamento e a data em que o mesmo for efetivado.

6.3. A **CONTRATANTE** não acatará a cobrança por meio de duplicatas ou qualquer outro título, em bancos ou outras instituições do gênero.

6.4. Os pagamentos efetuados pela **CONTRATANTE** não isentam a **CONTRATADA** de suas obrigações e responsabilidades assumidas.

CLÁUSULA SÉTIMA – DAS ALTERAÇÕES CONTRATUAIS

7.1. Este Contrato poderá ser alterado, com as devidas justificativas, nos seguintes casos:

7.1.1. ***Unilateralmente***, pela **CONTRATANTE**, quando:

RQS nº 03/2005 - CI
CPMI - CORREIOS
Fls. Nº 0546
Conforme
3740
Doc: 1391 03

DGEC/DECAM
FLS. Nº 3191

a) houver modificação do projeto ou das especificações, para melhor adequação técnica aos seus objetivos;
b) necessária a modificação do valor contratual em decorrência de acréscimo ou diminuição quantitativa de seu objeto, nos limites previstos neste Contrato.

7.1.2. ***Por acordo entre as partes***, quando:

a) necessária a modificação do modo e/ou do cronograma de fornecimento, em face de verificação técnica da inaplicabilidade dos termos contratuais originários;

b) necessária a modificação da forma de pagamento, por imposição de circunstâncias supervenientes, mantido o valor inicial atualizado, vedada a antecipação do pagamento, com relação ao cronograma financeiro fixado, sem a correspondente contraprestação de fornecimento;

c) para restabelecer a relação que as partes pactuaram inicialmente entre os encargos da **CONTRATADA** e a retribuição da **CONTRATANTE** para a justa remuneração do fornecimento, objetivando a manutenção do equilíbrio econômico-financeiro inicial deste Contrato, na hipótese de sobrevirem fatos imprevisíveis ou previsíveis, porém de conseqüências incalculáveis, retardadores ou impeditivos da execução do ajustado, ou ainda, em caso de força maior, caso fortuito ou fato do príncipe, configurando álea econômica extraordinária e extracontratual.

d) conveniente a substituição da garantia de execução contratual;

7.2. As alterações serão procedidas mediante os seguintes instrumentos:

7.2.1. APOSTILAMENTO: para as alterações que envolverem as seguintes situações:

a) as atualizações, compensações ou penalizações financeiras decorrentes das condições de pagamento aqui previstas;

b) o empenho de dotações orçamentárias suplementares, até o limite do seu valor corrigido;

c) ajustes nas especificações técnicas, no cronograma de entrega ou na execução dos serviços, desde que não impactem nos encargos contratados e não afetem a isonomia do processo licitatório, situações estas previamente reconhecidas por autoridade competente da **CONTRATANTE**.

7.2.2. TERMO ADITIVO: alterações não abrangidas pelo apostilamento, que ensejarem modificações deste Contrato ou do seu valor.

7.3. Os Termos Aditivos ou Apostilas farão parte do Contrato, como se nele estivessem transcritos.

CLÁUSULA OITAVA - DAS PENALIDADES

8.1. Pela inexecução total ou parcial deste Contrato, a **CONTRATANTE** poderá aplicar à **CONTRATADA** as seguintes sanções, sem prejuízo da reparação dos danos causados à **CONTRATANTE**:

RQS nº 03/2005 - CI
CPMI - CORREIO
Fls. Nº 0547
Conforme 3740
NJ/DEJUR/DJTEC/591/03

DGEC/DECAM
FLS. Nº 3190

8.1.1. Advertência: será aplicada quando ocorrer o descumprimento das obrigações assumidas, desde que sua gravidade, devidamente analisada e justificada pela **CONTRATANTE**, não recomende a aplicação de outra penalidade.

8.1.2. Multa: será aplicada nos seguintes casos:

8.1.2.1. O atraso injustificado na execução deste Contrato sujeitará a **CONTRATADA** à **multa de mora**, na forma a seguir:

a) atraso na entrega das ferramentas, em relação ao prazo estipulado no **ANEXO 1** deste Contrato: **1% (um por cento)** do valor da entrega, por dia de atraso, até o limite de **15 (quinze)** dias;

b) atraso na entrega das ferramentas, a partir do **16° (décimo sexto) dia: 3% (três por cento)** do valor da entrega questionada, por dia de atraso, quando poderá ensejar a rescisão contratual.

c) atraso na apresentação/atualização ou ainda da renovação da garantia de execução contratual, estabelecida neste Contrato: **1% (um por cento)** do valor total da garantia prestada, por dia de atraso, conforme **subitem 14.1.** deste Contrato.

d) não atualização de versão e/ou não atendimento do suporte técnico e solução dos problemas à **CONTRATANTE**, dentro dos prazos estabelecidos nos itens 3.10, 3.11 e 4 do Termo de Garantia – Anexo 2 deste Contrato;

8.1.2.2. Pela inexecução total ou parcial serão aplicadas multas na forma a seguir, garantida a prévia defesa:

a) entrega das ferramentas em desconformidade com o especificado: multa de **10% (dez por cento)** sobre o valor global atualizado;

b) pela não entrega das ferramentas: multa de **20% (vinte por cento)** sobre o valor total do contrato e ainda a rescisão contratual, conforme previsto no subitem 9.1.1., alínea deste Contrato.

c) pela não-manutenção das condições de habilitação e qualificação exigidas na licitação: **20% (vinte por cento)** sobre o valor global atualizado deste Contrato, sem prejuízo da rescisão contratual e demais penalidades previstas na Cláusula Oitava deste Contrato;

d) ocorrência de quaisquer outros tipos de descumprimento contratual não abrangidos pelas alíneas anteriores: **1% (um por cento)** do valor global atualizado deste Contrato para cada evento, por dia corrido;

e) quando a **CONTRATADA**, incorrer em alguma das hipóteses das alíneas "**a**" a "**j**" do **subitem 9.1.1.** deste Contrato: **20% (vinte por cento)** do valor global atualizado deste Contrato.

8.1.2.3. As penalidades referentes ao atendimento e suporte técnico encontram-se elencadas no Termo de Garantia Técnica, anexo deste Contrato.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0548
3740
Doc.
DEPARTAMENTO JURÍDICO
Conforme
NJ/DEJUR/DJTEC/1398/03

DGECIDEC
FLS. Nº 358

8.1.2.4. As multas previstas nos **subitens 8.1.2.1.** e **8.1.2.2.** são independentes entre si, podendo ser aplicadas isoladas ou cumulativamente, ficando, porém, o total das multas elencadas do subitem **8.1.2.1.** limitado a **20% (vinte por cento)** do valor total atualizado deste Contrato.

8.1.2.5. Em caso de descumprimento deste Contrato, além das multas de mora, a **CONTRATADA** responderá por quaisquer danos e prejuízos sofridos pela **CONTRATANTE.**

8.1.2.6. Não serão aplicadas multas decorrentes de casos fortuitos, ou força maior, ou razões de interesse público, devidamente comprovado.

8.1.2.7. O valor da multa e os prejuízos causados pela **CONTRATADA,** serão executados pela **CONTRATANTE** nos termos das alíneas **"a", "b"** e **"c"** do **subitem 9.6.** deste Contrato.

8.1.3. Suspensão temporária de participação em licitação e impedimento de contratar com a CONTRATANTE, pelo período não superior a **5 (cinco) anos**, poderá ser aplicada especialmente nos seguintes casos:

a) não-manutenção de situação regular em relação à Documentação de Habilitação;

b) se a **CONTRATADA** der causa à rescisão unilateral deste Contrato, por descumprimento de suas obrigações;

c) apresentação de documentos falsos ou falsificados;

d) cometimento reiterado de falhas ou fraudes na execução deste Contrato.

8.1.3.1. A suspensão temporária de participação em licitação e impedimento de contratar com a **CONTRATANTE** também poderá ser aplicada nos casos previstos nas alíneas do **subitem 8.1.4.** deste Contrato.

8.1.4. Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a **CONTRATADA** ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo previsto no § 3º do Art. 87 da Lei 8.666/93, que será aplicada, também, nos seguintes casos:

a) tenha sofrido condenação definitiva por praticar, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;

b) tenha praticado atos ilícitos, visando a frustrar os objetivos da contratação;

c) demonstre não possuir idoneidade para contratar com a Administração Pública;

8.2. As penalidades serão aplicadas com observância dos princípios da ampla defesa e do contraditório.

DEPARTAMENTO JURÍDICO DECT
Conforme
RJ/DEJUR/DITEC 2 XXX
RQS nº 03/2005 - CN - CPMI - CORREIOS
0549
Fls. Nº
3740
Doc.

DGECIDECAM
FLS. Nº 3188

8.3. No caso do **subitem 8.1.2.1.**, a multa será aplicada de imediato, sendo deduzida do valor da Nota Fiscal/Fatura.

8.4. As sanções previstas nos **subitens 8.1.1., 8.1.3.** e **8.1.4.** poderão ser aplicadas juntamente com a do **subitem 8.1.2.**, facultada a defesa prévia da **CONTRATADA**, no prazo de **5 (cinco) dias úteis**, cujas razões, em sendo procedentes, poderão isentá-la das penalidades; caso contrário, aplicar-se-á a sanção cabível.

8.5. Da aplicação das penalidades previstas nesta Cláusula caberá recurso.

8.5.1. O recurso será dirigido à autoridade superior, por intermédio da que praticou o ato recorrido, a qual poderá reconsiderar sua decisão, no prazo de **5 (cinco) dias úteis**, ou, neste mesmo prazo, fazê-lo subir, devidamente informado, devendo, neste caso, a decisão ser proferida em **5 (cinco) dias úteis** contados do recebimento do recurso, pela autoridade superior, sob pena de responsabilidade.

CLÁUSULA NONA - DA RESCISÃO

9.1. O presente Contrato poderá ser rescindido, sem prejuízo das penalidades previstas na Cláusula Oitava:

9.1.1. ***Por ato unilateral*** da **CONTRATANTE**, quando ocorrer:

a) o não cumprimento ou cumprimento irregular de Cláusulas contratuais, especificações técnicas, projetos ou prazos, tais como;

a1) não-manutenção das condições de habilitação exigidas na licitação;

a2) descumprimento do disposto no Inciso V do Art. 27 da Lei 8.666/93, sem prejuízo das sanções penais cabíveis;

b) a lentidão do seu cumprimento, levando a **CONTRATANTE** a comprovar a impossibilidade da conclusão do fornecimento, nos prazos estipulados.

c) atraso injustificado na entrega do material;

d) paralisação do fornecimento, sem justa causa e prévia comunicação à **CONTRATANTE**;

e) subcontratação total ou parcial do objeto deste Contrato, ou associação da **CONTRATADA** com outrem, cessão ou transferência, total ou parcial, bem como a fusão, cisão ou incorporação, sem a expressa anuência da **CONTRATANTE**;

f) desatendimento das determinações regulares da autoridade designada para acompanhar e fiscalizar a sua execução, assim como, a de seus superiores;

g) cometimento reiterado de falhas na execução deste Contrato;

RQS nº 03/2005 / CPMI - CORREIOS
Fls. Nº 0550
Conforme
Doc:

DGECIDEC
FLS. Nº 328

h) decretação de falência da **CONTRATADA**;

i) dissolução da sociedade da **CONTRATADA**;

j) alteração social ou a modificação da finalidade ou da estrutura da **CONTRATADA**, que prejudique a execução deste Contrato;

k) razões de interesse público, de alta relevância e amplo conhecimento, justificadas e determinadas pela máxima autoridade da esfera administrativa a que está subordinada a **CONTRATANTE** e exaradas no processo administrativo a que se refere este Contrato;

l) caso fortuito ou força maior, regularmente comprovados, impeditiva da execução do Contrato.

9.1.2. Amigavelmente, por acordo entre as partes, desde que haja conveniência para a **CONTRATANTE**, reduzida a termo no Processo Administrativo;

9.1.3. Judicialmente, nos termos da legislação.

9.2. É prevista a rescisão, ainda, nos seguintes casos:

a) supressão, por parte da **CONTRATANTE**, acarretando modificação além do limite de **25% (vinte e cinco por cento)** do valor inicial atualizado deste Contrato, estabelecido à época da celebração deste Instrumento, devidamente corrigido até a data da supressão, ressalvados os casos de concordância da **CONTRATADA**;

b) suspensão de sua execução, por ordem escrita da **CONTRATANTE**, por prazo superior a **120 (cento e vinte) dias**, salvo em caso de calamidade pública, grave perturbação da ordem interna ou guerra, ou ainda, por repetidas suspensões que totalizem o mesmo prazo, independentemente do pagamento obrigatório de indenização pelas sucessivas e contratualmente imprevistas desmobilizações e mobilizações e outras previstas, assegurado à **CONTRATADA**, nesses casos, o direito de optar pela suspensão do cumprimento das obrigações assumidas até que seja normalizada a situação;

c) ocorrendo atraso superior a **90 (noventa) dias** dos pagamentos devidos pela **CONTRATANTE**, salvo em caso de calamidade pública, grave perturbação da ordem interna ou guerra, assegurado à **CONTRATADA** o direito de optar pela suspensão do cumprimento de suas obrigações, até que seja normalizada a situação.

9.3. Os casos de rescisão contratual serão formalmente motivados nos autos do Processo Administrativo, assegurado o contraditório e a ampla defesa.

9.4. A rescisão unilateral ou amigável deverá ser precedida de autorização escrita e fundamentada da autoridade competente.

9.5. Quando a rescisão ocorrer com base nas **alíneas "k"** e **"l"** do **subitem 9.1.1.** desta Cláusula e **alíneas "a"**, **"b"** e **"c"** do **subitem 9.2.**, sem que haja culpa da **CONTRATADA**, será esta ressarcida dos prejuízos regularmente comprovados que houver sofrido.

ROS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 0551

DEPARTAMENTO JURÍDICO
Conforme
NJ/DEJUR/DITEC
Doc: 3746/05

DGEC/DECAM
FLS. Nº 3186

9.6. A rescisão de que trata o **subitem 9.1.1.**, exceto quando se tratar de casos fortuitos, ou força maior ou razões de interesse público, acarretará as seguintes conseqüências, sem prejuízo das sanções previstas em lei ou neste instrumento:

a) retenção dos créditos decorrentes deste Contrato, até o limite dos prejuízos causados à **CONTRATANTE;**

b) retenção dos créditos existentes em outros Contratos, porventura vigentes entre a **CONTRATANTE** e a **CONTRATADA**, até o limite dos prejuízos causados;

c) retenção/execução da garantia contratual, para ressarcimento da **CONTRATANTE** dos valores das multas e indenizações a ela devidas.

9.7 Caso a retenção não possa ser efetuada, no todo ou em parte, na forma prevista nas alíneas do **subitem 9.6.**, a **CONTRATADA** será notificada para, no prazo de **5 (cinco) dias úteis,** a contar do recebimento da notificação, recolher o respectivo valor, em Agência indicada pela **CONTRATANTE**, sob pena de imediata aplicação das medidas judiciais cabíveis.

CLÁUSULA DÉCIMA – DOS RECURSOS ORÇAMENTÁRIOS

10.1. As despesas decorrentes da aquisição do objeto deste Contrato correrão por conta da seguinte classificação orçamentária: **CONTA: 9.02. - PROJETO: 17.1.01.**

CLÁUSULA DÉCIMA-PRIMEIRA - DA VIGÊNCIA

11.1. Este Contrato tem vigência a partir da data de sua assinatura e termina com a emissão do **Termo de Aceite Final – TAF** dos softwares, limitado ao prazo máximo de **12 (doze) meses**.

CLÁUSULA DÉCIMA-SEGUNDA - DA LICITAÇÃO E SUBORDINAÇÃO LEGAL

12.1. Este Contrato é oriundo do Pregão nº 118/2003, homologado por meio do Relatório Homologação/CPL/AC 065 de 19/12/2003.

12.2. As partes contratantes submetem-se às condições ora acordadas e aos ditames da Lei 10.520/02, do Decreto nº 3.555/00, 3.697/00 e 3.784/2001 e supletivamente aos da Lei nº 8.666/93.

12.3. Constituirão partes integrantes deste Contrato, seu **Anexo 1 e Anexo 2**, o Edital, seus Anexos, e a Proposta econômica da **CONTRATADA**.

12.4. A **CONTRATANTE** providenciará a publicação do extrato do presente Contrato na imprensa oficial, nos termos da legislação vigente.

CLÁUSULA DÉCIMA-TERCEIRA – DA GESTÃO DO CONTRATO

13.1. A gestão deste Contrato será feita:

RQS nº 03/2005 - CN - CPMI - CORREIOS
0552
FLS. Nº
Conforme 3740
NJ/DEJUR/DJTEC 29/11/03
Doc.

DGEC/DEC
FLS. Nº 3385

13.1.1. Por parte da **CONTRATANTE:**

ÁREA GESTORA ADMINISTRATIVA: DERCO - Departamento de Rede Corporativa
TELEFONE: (061)426-1963
FAX: (061)426-1964
e-mail: derco@correios.com.br

13.1.2. Por parte da **CONTRATADA:**

NOME DO GESTOR:. JOSÉ EDUARDO PIRES DO RIO RIBEIRO
TELEFONE: (61).329-6055
FAX: (61) 329-6199
E-MAIL: jose-eduardo.ribeiro@hp.com

CLÁUSULA DÉCIMA-QUARTA – DA GARANTIA DE EXECUÇÃO CONTRATUAL

14.1. A **CONTRATADA** comprovará no prazo de **05 (cinco) dias úteis** da data de assinatura deste Contrato, a efetivação da garantia de execução contratual, em percentual equivalente a **5% (cinco por cento)** do valor global, correspondente a R$ 20.925,00 (vinte mil e novecentos e vinte cinco reais), podendo optar pelas seguintes modalidades:

a) caução em dinheiro ou títulos da dívida pública;
b) seguro-garantia;
c) fiança bancária.

14.2. Em caso de garantia em dinheiro, a **CONTRATADA** deverá depositar o valor em nome da **CONTRATANTE**, conforme dados abaixo:

- **BANCO:** 001 – Banco do Brasil S/A
- **AGÊNCIA:** 3307-3
- **CONTA CORRENTE: 195.159-9**

14.3. No caso de apresentação de fiança bancária, a Carta de Fiança deverá registrar expressa renúncia do fiador aos benefícios dos artigos 827 e 835 do Novo Código Civil Brasileiro.

14.4. Se a opção da garantia recair em seguro garantia ou fiança bancária, deverá conter expressamente cláusulas de atualização financeira, de imprescritibilidade, de inalienabilidade e de irrevogabilidade.

14.5. Se o valor da garantia for utilizado em pagamento de quaisquer obrigações, inclusive indenização a terceiros, a **CONTRATADA** se obriga a fazer a respectiva reposição, no prazo máximo e improrrogável de **72 (setenta e duas) horas**, a contar da data que for notificada pela **CONTRATANTE**.

14.6. A garantia prestada será liberada ou restituída após cessadas todas obrigações assumidas pela CONTRATADA, inclusive aquelas previstas no Termo de Garantia Técnica, anexo deste Contrato.

ROS nº 002/2005 CN - CPMI - CORREIOS
Fls. Nº 0553
DEPARTAMENTO JURÍDICO
Conforme
NJ/DEJUR/DITEC 24/03
Doc:

DGECIDECAM
FLS. Nº 3184

CLÁUSULA DÉCIMA-QUINTA - DO FORO

15.1. É competente o Foro da Justiça Federal, Seção Judiciária do Distrito Federal, para dirimir quaisquer dúvidas, porventura oriundas do presente Contrato.

E, por estarem justas e contratadas, assinam as partes o presente Contrato, em 02 (duas) vias de igual teor e forma e para um só efeito de direito, na presença de 02 (duas) testemunhas abaixo assinadas.

Brasília/DF, 26 de Dezembro de 2003

Pela Contratante

Eduardo de Medeiros
Diretor DITEC
Eduardo Medeiros de Morais
Diretor de Tecnologia e de Infra-Estrutura
Mat. 8.010.051-1

Ana Lúcia Leitão Nunes
Chefe de Departamento
Ana Lúcia Leitão Nunes
Chefe/Deptº. de Rede Corporativa
Mat. 8.007.888-5

Pela Contratada

Paulo César Rossigneux Vieira
Gerente de Contas

José Eduardo Pires do Rio Ribeiro
Gerente de Contas

TESTEMUNHAS:

1) Hugo Viana da Silva Junior
Nome
CPF: 953 655 324-49

2) _____
Nome MARCO ANTONIO GIANINI
CPF: 296.850.101-10

DEPARTAMENTO JURÍDICO
DEJUR
Conforme
NJ/DEJUR/DJTEC/391/07

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0554
Doc: 3740

CORREIOS

Protocolo

9754
30.12.03
14:36 HS

FL. Nº 3183

De: CHEFE DO DERCO

Ao: CHEFE DO DECAM

CI / DIADR/DERCO - 3.499/2003

Ref.:

Assunto: Contratato HP.

Brasília, 30 de dezembro de 2003.

Encaminhamos, em anexo, 02 (duas) cópias do contrato 12416/03, para as providências cabíveis.

Atenciosamente,

Ana Lúcia Leitão Nunes
Chefe do Derco

Anexo: citado no texto

ALLN/nmf – DERCO 5º Andar Ala Norte – fone/fax: (61) 426-1963 – 426-1964

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0555
Doc: 3740

CORREIOS

09820

Protocolo

De: PREGOEIRA AC

Ao: CHEFE DO DMARK

CI / CPL/AC - 1468/2003

Ref.: Pregão 118/2003 - CPL/AC

FL. Nº 3189 DECAM

Assunto: Publicação no DOU - Aviso de Retificação

Brasília, 29 de dezembro de 2003.

Solicitamos a V.Sª. veicular mensagem, cujo texto anexamos à presente, de acordo com a especificação a seguir:

- Pregão nº 118/2003 -CPL/AC (AVISO DE RETIFICAÇÃO)
- **Data de veiculação: 30/12/2003**

Salientamos que tal veiculação deverá ser feita de acordo com a Lei n.º 10.520/2002, Decreto n.º 3.784/2001 e Lei n.º 8.666/93, republicada em 06/07/94.

Atenciosamente,

MARTA MARIA COELHO
Pregoeira/AC

GILBERTO FERREIRA DO AMARAL
Membro da CPL/AC
Mat. 8.008.347-1

C/Anexo: Publicação
FCAR/fcar

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0556
Doc: 3740

CORREIOS

9681

Protocolo

FL. Nº 3381 DECAM

De: PREGOEIRA/AC

Ao: CHEFE DO DECAM

CI / CPL/AC -1462/2003

Ref.: Pregão 118/2003 - CPL/AC

Assunto: Encaminha processo para emissão de Contrato - Pregão-118/2003

.Brasília, 26 de dezembro de 2003.

Encaminhamos a V.Sª., em anexo, 04 pastas pertinentes ao processo licitatório sob referência ***(aquisição de licenças de Software HP Open View Network Node Manage Enteroruse V. 620 ou superior)***, para as providências cabíveis desse órgão em relação à gestão do contrato.

Informamos que a minuta do contrato foi encaminhada ao DEJUR para chancela, conforme CI/GAB/DITEC – 3052/2003, de 17/12/2003, constante nos autos do processo.

Comunicamos ainda, que foi providenciada a veiculação do resultado de julgamento (homologação/adjudicação) no Diário Oficial da União do dia 23 de dezembro de 2003.

Atenciosamente,

MARTA MARIA COELHO
Pregoeira/AC

GILBERTO FERREIRA DO AMARAL
Membro da CPL/AC
Mat. 8.008.347-1

DOEL
Providencia
26/12/03

Antônio Francisco da Silva Filho
Subchefe/DECAM
Mat. 8.010.819-9

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0557
Doc: 3740

C/ANEXO: 04 pastas do Pregão-118/2003
FCAR/fcar

FW0010

FL. Nº 3180 DECAM

PREGÃO 118/2003
AQUISIÇÃO DE LICENÇAS DE SOFTWARE HO OPEN VIEW NETWORK NODE MANAGER ENTERPRISE V.620,OU SUPERIOR
TIPO: Menor Preço

INÍCIO: 15/09/2003 ABERTURA: 16/12/2003	ORIGEM: CI/CAS/DCON/DECAM – 4.737/2003	CLASSIFICAÇÃO ORÇAMENTÁRIA: 09.02/17.1.01
REQUISITANTE(S): DECAM	DESTINATÁRIO: BSB E SP	
VALOR ESTIMADO:R$ 423.058,58 QUANTIDADE: 05	VALOR ADJUCADO: R$ 418.500,00	PUBLICAÇÃO DO RESULTADO: 23/12/2003

DESENVOLVIMENTO

Na CPL elaborando edital.

08/10/2003 – CPL encaminha ao DEJUR edital para chancela.
03/11/2003 – CPL reencaminha o edital ao DEJUR para chancela após correções.
04/11/2003 – CPL encaminha a DIRAD anexos 01 e 06 do edital para o "de acordo" do diretor.
05/11/2003 – CPL recebe da DIRAD o expediente com a assinatura do diretor.
05/11/2003 – CPL encaminha ao DEJUR a especificação técnica anexos 01 e 06 para substituição no edital e chancela.
05/11/2003 – CPL recebe do DECAM parecer técnico sobre o edital.
01/12/2003 – CPL recebe do DEJUR edital chancelado.
02/12/2003 – CPL publica no DOU aviso de licitação com data de abertura para o dia 16/12/2003 às 9:30h.
16/12/2003 – Abertura da Licitação
19/12/2003 – CPL recebe o relatório homologado da DITEC.
19/12/2003 – CPL solicita publicação no DOU do aviso de homologação/adjudicação, para veiculação no dia 23/12/2003.
26/12/2003 – CPL encaminha ao DECAM o processo para gestão do contrato.

(PROCESSO CONCLUÍDO)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls/Nº 0558
Doc: 3740

DOCUMENTAÇÃO DE PROCESSO LICITATÓRIO- PREGÃO

FL. Nº 3179

		S/N(*)	Página
01	Portaria		
02	Requisição de Material/Serviço, devidamente fundamentada, especificação ou projeto básico do órgão inicial/requisitante		
03	Pesquisa de preço no mercado		
04	Tabela de Bloqueio		
05	Autorização da Licitação		
06	Instrução Processo: DECAM/DESAD/DITEC/DIOPE		
07	CI´S das áreas técnicas e jurídicas		
08	Edital e Anexos chancelados pelo DEJUR		
09	Comprovante / publicação no DOU		
10	Recibos referente às retiradas do Edital de licitação		
11	Perguntas e respostas sobre o Edital de licitação		
12	Impugnação aos termos do Art12 e Decreto 3.555/00, Decisão e conhecimento à Impugnante (o AR deve constar no processo).		
13	Credenciamento e Declaração		
14	Propostas econômicas		
15	Documentos de Habilitação		
16	Ata de Reunião de Adjudicação do Pregoeiro		
17	Recursos		
18	Envio dos Recursos para Impugnação /DEJUR		
19	Decisão dos Recursos		
20	Reabertura do Pregão: se o Recurso for procedente		
21	Documentos de Habilitação do vencedor da rodada de lances		
22	Ata de Reunião e ato de Adjudicação do Pregoeiro		
23	Recursos		
24	Impugnação/DEJUR		
25	Relatório homologação		
26	Publicação no DOU		
27	Termo de Contrato		
28	Demais Documentos		
29	Paginação do Processo		

OBS: *(*) S- aplicável*
N- não aplicável

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0559
3740
Doc:

PAGINAÇÃO DO PROCESSO

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0560
3740
Doc:

DEMAIS DOCUMENTOS

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0561
3740
Doc:

TERMO DE CONTRATO

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0562
3740
Doc:

CORREIOS

Protocolo

3.178 CAG

De: PREGOEIRA/AC

Ao: CHEFE DO DECAM

CI / CPL/AC -1462/2003

Ref.: Pregão 118/2003 - CPL/AC

Assunto: Encaminha processo para emissão de Contrato - Pregão-118/2003

.Brasília, 26 de dezembro de 2003.

Encaminhamos a V.Sª., em anexo, 04 pastas pertinentes ao processo licitatório sob referência ***(aquisição de licenças de Software HP Open View Network Node Manage Enteroruse V. 620 ou superior)***, para as providências cabíveis desse órgão em relação à gestão do contrato.

Informamos que a minuta do contrato foi encaminhada ao DEJUR para chancela, conforme CI/GAB/DITEC – 3052/2003, de 17/12/2003, constante nos autos do processo.

Comunicamos ainda, que foi providenciada a veiculação do resultado de julgamento (homologação/adjudicação) no Diário Oficial da União do dia 23 de dezembro de 2003.

Atenciosamente,

P MARTA MARIA COELHO
Pregoeira/AC

GILBERTO FERREIRA DO AMARAL
Membro da CPL/AC
Mat. 8.008.347-1

C/ANEXO: 04 pastas do Pregão-118/2003
FCAR/fcar

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0563
Doc: 3740

FW0010

CORREIOS

Protocolo

De: DIRETOR DE TECNOLOGIA E DE INFRA-ESTRUTURA

Ao: CHEFE DO DEJUR

CI / GAB/DITEC 3059/2003

Ref.:

3.177

DEPARTAMENTO JURÍDICO E.C.T.

Assunto: Pregão-118/2003-CPL/AC

Brasília, 17 de dezembro de 2003.

Solicitamos a V.Sa. a análise e chancela do Contrato para aquisição de 05 (cinco) licenças HP Open View Network Node Manager Enterprise, com a empresa Hewlett Packard Ltda, vencedora do Pregão-118/2003-CPL/AC em 16/12/2003, em anexo.

Atenciosamente,

Eduardo Medeiros de Morais
Diretor de Tecnologia e Infra-Estrutura

C\Anexo

- Minuta de Contrato

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0564
3740
Doc:

PUBLICAÇÃO NO DOU

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0565
3740
Doc:

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS
ADMINISTRAÇÃO CENTRAL

EXTRATOS DE CONTRATOS

Espécie: Terceiro Termo Aditivo nº 12406/03 ao Contrato nº 10835/01; Contratada: Siemens Ltda; Objeto: Substituir a empresa Contratada, SIEMENS DEMATIC LTDA, em razão de processo de incorporação societária, que passa a ser a incorporadora SIEMENS LTDA, proceder ao ajuste no fornecimento e no cronograma de execução, decorrente das adaptações no leiaute (configuração física) de instalação, incluir no Contrato o ANEXO 6 - "Lista de Ferramentas e Instrumentos", bem como fixar o valor e estabelecer as condições de pagamento da multa por atraso no cumprimento dos prazos estipulados no cronograma de execução; Origem: Concorrência nº 016/99; Classificação Orçamentária: Atividade: 14.1.01 e Conta 3.02; Valor Total do Contrato: R$9.798.888,72 (nove milhões, setecentos e noventa e oito mil, oitocentos e oitenta e oito reais e setenta e dois centavos) e R$ 8.220.342,07 (oito milhões, duzentos e vinte mil, trezentos e quarenta e dois euros e sete centavos), correspondendo a uma redução de 0,38% (trinta e oito centésimos por cento) em relação ao valor original do Contrato nº 10835/01.

A Empresa Brasileira de Correios e Telégrafos celebrou o Contrato nº 12409/03 - Contratada: PREFEITURA MUNICIPAL DE FLORES, assinado em 28/11/03 com vigência de 02 meses a partir da data de sua assinatura. Objeto: Contrato de Patrocínio Não-Incentivado. Origem: Inexigibilidade de Licitação nº 214/03. Conta orçamentária 00.8.00/5.02. Valor total da contratação: R$ 10.000,00 (dez mil reais). Signatários: Airton Langaro Dipp - Presidente da Contratante e Gabriel Pauli Fadel - Diretor de Administração da Contratante; Arnaldo Pedro da Silva - Prefeito da Contratada.

1. ESPÉCIE: Contrato nº 12.398/2003; 2. CONTRATADA: CAVIGLIA & CIA LTDA.; 3. OBJETO: aquisição de mesas para carteiro; 4. VALOR GLOBAL R$ 2.727.607,00; 5. DATA DE ASSINATURA: 23/12/2003; 6. VIGÊNCIA: do Fornecimento: A partir da data de sua assinatura e termina com a entrega do último pedido, limitado ao prazo máximo de 12 meses; da Prestação da Garantia: 12 meses a partir da emissão do Termo de Aceitação do material; 7. RECURSOS ORÇAMENTÁRIOS: Projeto: 14.1.03 e Conta 9.02; 8. ORIGEM: Pregão nº 080/2003 - CPL/AC; 9. SIGNATÁRIOS: Airton Langaro Dipp - Presidente da Contratante, Gabriel Pauli Fadel - Diretor de Administração da Contratante, e Aline de Lacerda Rios - Procurador da Contratada.

A Empresa Brasileira de Correios e Telégrafos celebrou o Contrato nº 12407/03 - Contratado: Cinética Filmes e Produções Ltda: assinado em 15/12/03 com vigência de 18 meses a partir da data de sua assinatura. Objeto: Contrato de Patrocínio Incentivado. Origem: Inexigibilidade de Licitação nº 116/03. Conta orçamentária 00.8.00/5.02. Valor total da contratação: R$100.000,00 (cem mil reais). Signatários: Airton Langaro Dipp - Presidente da Contratante e Gabriel Pauli Fadel - Diretor de Administração da Contratante; Wagner de Assis - Sócio da Contratada.

AVISO DE REVOGAÇÃO
PREGÃO Nº 101/2003

Comunicamos a todos os interessados que o Pregão n.º 101/2003 - CPL/AC - aquisição de 600.000 rótulos internacionais, publicado no DOU do dia 30/10/2003, página 77, foi revogado por interesse público com base no art. 49 da Lei n.º 8.666/93.

MARTA MARIA COELHO
Pregoeira

AVISOS DE RETIFICAÇÃO
PREGÃO Nº 107/2003

Retificamos o aviso de homologação e adjudicação publicado no DOU do dia 24/12/2003, Seção 3, página 172, conforme a seguir: no título, onde se lê Pregão 107/2002 - CPL/AC, leia-se Pregão n.º 107/2003-CPL/AC; no corpo do aviso, onde se lê: Comunicamos a todos os interessados que o objeto do Pregão 107/2002 - CPL/AC..., leia-se: Comunicamos a todos os interessados que o objeto do Pregão n.º 107/2003 - CPL/AC, foi homologada a adjudicação à empresa HHP Brasil Ltda., para o fornecimento de 3.577 equipamentos destinados ao Sistema de Rastreamento de Objetos - SRO, no valor total de R$ 14.569.998,93 (quatorze milhões, quinhentos e sessenta e nove mil, novecentos e noventa e oito reais e noventa e três centavos)

PREGÃO Nº 118/2003

Retificamos o aviso de homologação e adjudicação publicado no DOU do dia 23/12/2003, página 102. Onde se lê: Pregão 118/2002, leia-se: Pregão 118/2003.

MARTA MARIA COELHO
Pregoeira da CPI

DIRETORIA REGIONAL NO AMAZONAS

EXTRATO DE INSTRUMENTOS CONTRATUAIS

. Contrato n.º 163/2003; Assinado em: 20/10/2003; Contratada: Antares Distribuidora de Motos Ltda; Objeto: prestação dos serviços técnicos de manutenção corretiva e preventiva em 88 motocicletas Honda CG e XL-125,na cidade de Manaus; Origem: Pregão 017/2003; Vigência: 12 (doze) meses, a partir da data de sua assinatura; Classificação Orçamentária - Atividade: 00.800 Conta/sub-conta 317/02; Valor Global: R$ 2.340,80; Signatário: Rodolfo Manoel Marques do Amaral - Diretor Regional da Contratante, Jayme Aranha Chacon Junior; Gerente de Administratação da Contratante e Aldemir da Silva Gorayebe, Represente da Contratada.

. Contrato n.º 166/2003; Assinado em: 22/12/2003; Contratada: Amazonas Copiadoras Ltda; Objeto: Locação de 07 Máquinas reprográficas em preto e branco em Manaus e Boa Vista/RR com instalação dos equipamentos; Origem: Pregão 027/2003; Vigência: 01 (um) ano, a partir de 22/12/2003; Classificação Orçamentária - Atividade: 00800; Conta/sub-conta 705; Valor Global: R$ 82.195,20; Signatário: Rodolfo Manoel Marques do Amaral - Diretor Regional da Contratante, Jayme Aranha Chacon Junior; Gerente de Administração da Contratante e Cláudio Antônio Cestaro, Representante da contratada.
. Contrato nº 167/2003; Assinado em 15/12/2003; Contratada: Rollis Equipamentos Ltda - Objeto: Locação de 01 (uma) Empilhadeira, com e 03 (três) Paleteiras; Origem: CV 049/2003; Vigência: 03 (três) meses, com início a partir de 17/12/2003; Classificação Orçamentária - Atividade: 00800; Conta 704; Valor Global: R$ 14.546,40; Signatário: Rodolfo Manoel Marques Amaral - Diretor Regional da Contratante, Jayme Aranha Chacon Junior, Gerente Administração da Contratante, Rômulo Lima dos Santos, Representante da contratada.

DIRETORIA REGIONAL NA BAHIA

EXTRATO DE DISPENSA DE LICITAÇÃO

DL-0366/03 - Data aut. 23.12.03 - Contratado: Rozinete Rita dos Santos - Prazo Vigência: 01.12.2003 à 01.12.2008 - Objeto: Locação de Imóvel não residencial, visando proposição onde funcionamento da AC/Piatã/Ba - Justificativa: Por necessidade operacional. Enquadramento Legal: Com base Art. 24, inciso X da Lei 8.666/93 Classificação orçamentária:11.444.040.10002 - Valor contratual: R$24.000,00.

AVISO DE HOMOLOGAÇÃO
PREGÃO Nº 20/2003

OBJETO: Contratação de empresa para prestação de serviços de emissão e entrega de passagens aéreas regionais e nacionais, com adjudicação à Turismo Pinheiro Ltda, no valor global estimado de R$ 583.800,00 (quinhentos e oitenta e três mil e oitocentos reais), e desconto sobre o Valor Bruto do faturamento de 2,70%.

EDLENA MARIA S. S. MACIEL
Pregoeira

DIRETORIA REGIONAL EM BRASÍLIA

AVISO DE HOMOLOGAÇÃO
PREGÃO Nº 16/2003

A ECT, por intermédio da Diretoria Regional de Brasília, comunica aos interessados, a homologação do Pregão supracitado (registro de preços para aquisição de materiais de limpeza e higiene), para a empresa Lucan Comercial e Representações Ltda , itens 01 (R$ 0,55), 02 (R$ 0,85), 05 (R$ 0,43), 08 (R$ 1,70), 09 (R$ 1,50), 11 (R$ 0,53), 12 (R$ 1,59) e 13 (R$ 0,17), perfazendo o valor mensal estimado de R$ 7.626,50 (sete mil, seiscentos e vinte e seis reais e cinqüenta centavos) e anual de R$ 91.518,00 (noventa e um mil quinhentos e dezoito reais). Os itens 3, 4, 6, 7 e 10 foram revogados, tendo em vista que não foram cotados.

EDSON PEREIRA DE CARVALHO
Pregoeiro

DIRETORIA REGIONAL EM GOIÁS E TOCANTINS

EXTRATOS DE CONTRATOS

Contrato nº 761/03; Data de Assinatura: 16/12/2003; Contratada: ECO Engenharia Ltda; CNPJ: 02.858.942/0001-30 - Vigência: 60 (sessenta) dias corridos; Objeto: obra de adaptação da AC Almas - TO; Classificação Orçamentária: Conta/atividade - 001.02/16.1.01.; Valor da Contratação: R$ 48.870,38; Signatários: Sérgio Douglas Repolho Negri - Diretor Regional da Contratante, Valdblan Peres de Freitas - Presidente da CEL/DR/GT da Contratante e Geraldo Vasconcelos Valadares - representante da Contratada. Contrato nº 762/03; Data de Assinatura: 16/12/2003; Contratada: ECO Engenharia Ltda; CNPJ: 02.858.942/0001-30 - Vigência: 60 (sessenta) dias corridos; Objeto: obra de adaptação da AC Palmeirópolis - TO; Classificação Orçamentária: Conta/atividade - 001.02/16.1.01.; Valor da Contratação: R$ 54.949,03; Signatários: Sérgio Douglas Repolho Negri - Diretor Regional da Contratante, Valdblan Peres de Freitas - Presidente da CEL/DR/GT da Contratante e Geraldo Vasconcelos Valadares - representante da Contratada. Contrato nº 763/03; Data de Assinatura: 17/12/2003; Contratada: PHP Construções e Terraplenagem Ltda; CNPJ: 05.634.058/0001-00 - Vigência: 60 (sessenta) dias corridos; Objeto: obra de adaptação da AC Vicentinópolis - GO; Classificação Orçamentária: Conta/atividade - 001.02/16.1.01.; Valor da Contratação: R$ 34.380,67; Signatários: Sérgio Douglas Repolho Negri - Diretor Regional da Contratante, Valdblan Peres de Freitas - Presidente da CEL/DR/GT da Contratante e Paulo Mendonça Alves - representante da Contratada. Contrato nº 768/03; Data de Assinatura: 09/12/2003; Contratado: Jackson Jesus da Costa - Vigência: inicia-se em 01/01/2004 e termina em 01/01/2005; Objeto: Locação de imóvel para funcionamento AC São Miguel do Passa Quatro/GO; Classificação Orçamentária: Atividade - 0800702.01; Valor da Contratação: R$ 4.800,00; Signatários: Sérgio Douglas Repolho Negri - Diretor Regional da Contratante, Valdblan Peres de Freitas - Presidente da CEL/DR/GT e Jackson Jesus da Costa - Locador. Contrato nº 769/03; Data de Assinatura: 24/11/2003; Contratada: Altha Construções Ltda; CNPJ: 01.703.770/0001-63 - Vigência: 60 (sessenta) dias corridos; Objeto: obra de adaptação da AC Aliança do Tocantins - TO; Classificação Orçamentária: Conta/atividade - 001.02/16.1.01.; Valor da Contratação: R$ 38.913,94; Signatários: Sérgio Douglas Repolho Negri - Diretor Regional da Contratante, Valdblan Peres de Freitas - Presidente da CEL/DR/GT da Contratante e Edaman Rodrigues Nóbrega - representante da Contratada. Contrato nº 770/03; Data de Assinatura: 22/12/2003; Contratada: AMCC Engenharia Ltda; CNPJ: 03.420.632/0001-00 - Vigência: 60 (sessenta) dias corridos; Objeto: obra de adaptação da AC Praia Norte - TO; Classificação Orçamentária: Conta/atividade - 001.02/16.1.01.; Valor da Contratação: R$ 54.249,89; Signatários: Sérgio Douglas Repolho Negri - Diretor Regional da Contratante, Valdblan Peres de Freitas - Presidente da CEL/DR/GT da Contratante e André Martins da Costa Côdo - representante da Contratada. Contrato nº 771/03; Data de Assinatura: 22/12/2003; Contratada: Milênio Engenharia Ltda; CNPJ: 03.420.632/0001-00 - Vigência: 90 (noventa) dias corridos; Objeto: obra de adaptação da AC Caiapônia - GO; Classificação Orçamentária: Conta/atividade - 001.02/16.1.01.; Valor da Contratação: R$ 80.000,00; Signatários: Sérgio Douglas Repolho Negri - Diretor Regional da Contratante, Valdblan Peres de Freitas - Presidente da CEL/DR/GT da Contratante e Rommel Maia Sarmento - representante da Contratada.

EXTRATOS DE TERMOS ADITIVOS

Terceiro Termo Aditivo ao Contrato 022/2001; DATA DA ASSINATURA: 11/11/2003; CONTRATADA: ACF TRANSPORTES LTDA - VIGÊNCIA: Inicia-se em 01/02/2003 e termina em 31/01/04; OBJETO: Prestação de serviços de transporte de cargas postais LCE-CALDAS NOVAS; CLASSIFICAÇÃO ORÇAMENTÁRIA: Atividade: 00800 Conta: 311.06; VALOR DA ALTERAÇÃO: R$ 0; SIGNATÁRIOS: Sérgio Douglas Repolho Negri - Diretor Regional da Contratante - Charles Martins Borges - Gerente de Operações da Contratante e Alexandre Costa Ferro - Diretor da Contratada.

1º Termo Aditivo ao Contrato nº 678/03; Data de Assinatura: 01/12/2003; Contratada: Altha Construções Ltda; CNPJ: 01.703.770/0001-63 - alteração do parágrafo segundo da Cláusula Quarta - número da conta bancária; Signatários: Sérgio Douglas Repolho Negri - Diretor Regional da Contratante, Valdblan Peres de Freitas - Presidente da CEL/DR/GT da Contratante e Edman Rodrigues Nóbrega - representante da Contratada.

DIRETORIA REGIONAL EM MATO GROSSO

EXTRATO DE CONTRATO

Contrato n.º 105/2003. Assinado em : 10/12/03. Contratado : AFPL-Agência Fiscalizadora de Propaganda Ltda. Objeto : Prestação de serviços de clipagem eletrônica e gravações jornalísticas .Vigência : 10/12/03 à 09/12/04, prorrogável até o limite de 60 (sessenta) meses. Valor Global (estimado) : R$ 9.000,00 (Nove mil reais). Classificação Orçamentária : 00800.315.03/02144403.070021. Origem : Convite n.º 060/2003.

EXTRATO DE TERMO ADITIVO

1) Segundo Termo Aditivo n.º 122/2003 ao Contrato de n.º 237/2000. Contratado : Domani Distribuidora de Veículos Ltda. Objeto : Prorrogar a Vigência do Contrato por até 60 (sessenta) dias, período de 12/12/03 à 09/02/03. Valor Global do período: R$ 6.250,00 (seis mil duzentos e cinqüenta reais) .

DIRETORIA REGIONAL EM MINAS GERAIS

AVISO DE RETIFICAÇÃO
PREGÃO Nº 142/2003

A Diretoria Regional da ECT, em Minas Gerais, retifica o Aviso de Licitação, publicado no DOU nº 252, de 29/12/2003, Seção 3, página 300, referente ao Pregão nº 142/2003 a aquisição de combustíveis - (gasolina comum e óleo diesel) para abastecimento dos veículos da ECT localizados em Uberlândia-MG, conforme a seguir: A reunião de abertura ocorrerá às 14:30 horas do dia 15/01/2004, na Rua Rivalino Pereira, 846, Bairro: Martins, CEP: 38400-000 - Uberlândia - MG. Outras informações e retirada de Edital: Rua Boaventura, nº 401 - Sala M-302 - Bairro Indaiá - Belo Horizonte/MG, fones: (31)3249-2515 / 2505 e fax: (31)3249-2512.

JOIMAR LÚCIO MARTINS
Pregoeiro

DIRETORIA REGIONAL NO PARANÁ

AVISO DE HOMOLOGAÇÃO
PREGÃO Nº 68/2003

TIPO: MENOR PREÇO
Em relação ao Pregão nº . 068/2003, que tem por objeto a Contratação de Empresa para prestar o serviço de Auditoria Médica na cidade de Curitiba/PR informamos que o mesmo foi homologado à empresa CLINICA MÉDICA RICHTER LTDA. Esclarecemos que o valor total a contratar é de R$ 82.200,00 (oitenta e dois mil e duzentos reais).

ELIZANDRO ROBERTO MACIEL BENECK
Pregoeiro

RQS nº 03/2005 - CN
CPMI - CORREIO
FIS: Nº 056
3740
Doc:

SUPERINTENDÊNCIA DE RADIOFREQUÊNCIA E FISCALIZAÇÃO
GERÊNCIA-GERAL DE FISCALIZAÇÃO
ESCRITÓRIO REGIONAL DO CEARÁ

EXTRATOS DE TERMOS ADITIVOS

Primeiro Termo Aditivo ao Contrato ER-9-N º 12/2002-ANATEL
Data da Assinatura: 30.09.2003
Contratada: PRIMARE ENGENHARIA LTDA.
Vigência: 01.10.2003 a 30.09.2004
Objeto: Prorrogação do prazo de vigência, cujo objeto é a prestação de serviços de manutenção preventiva e corretiva dos equipamentos de ar-condicionado para as instalações do Escritório Regional da Anatel no Ceará, pelo período de 12(doze) meses, contados a partir de 01.10.2003.
Fundamento Legal: Artigo 57, Inciso II da Lei 8.666/93, de 21/06/93.
Programas de Trabalho: 24.722.0750.2000.0001
Elemento de Despesa: 339039.00
Valor do Contrato: R$ 13.740,00 (treze mil e setecentos e quarenta reais)

Quarto Termo Aditivo ao Contrato ER-9(UO 9.2)-N º 013/99-ANATEL
Data da Assinatura: 02 de novembro de 2003
Contratado: MIGUEL MENDES ARCOVERDE
Vigência: 03.11.2003 a 02.11.2004
Objeto: Prorrogação do prazo de vigência, cujo objeto é a locação de imóvel, situado na Av. Frei Serafim, nº 2786 - Centro - Teresina/PI, para instalação da Unidade Operacional da Anatel no Piauí, pelo período de 12 (doze) meses, contados a partir de 03.11.2003.
Fundamento Legal : Artigo 57, Inciso II, da Lei 8.666/93, de 21/06/93.
Programas de Trabalho: 24.722.0750.2000.0001
Elemento de Despesa: 339036.00
Valor Anual do Contrato: R$ 48.000,00 (quarenta e oito mil reais)

EDITAIS DE NOTIFICAÇÃO DE 22 DE DEZEMBRO DE 2003

Edital nº: 090-0009/2003

A Agencia Nacional de Telecomunicações - Anatel, por meio do presente Edital, NOTIFICA DO(S) LANÇAMENTO(S) do(s) crédito(s) da(s) receita(s) em nome do(s) devedor(es) que se encontra(m) ao final relacionado(s), por se encontrar(em) em local incerto e não sabido. Fica(m), portanto, ciente(s) que poderá(ao) apresentar IMPUGNAÇÃO, a ser dirigida à (ao) Escritório Regional da Anatel no Ceará, Endereço: Av. Senador Virgílio Távora 2500 - Dionísio Torres - Fortaleza/CE CEP: 60170-251, no prazo de 30 (trinta) dias, a partir da data da publicação deste Edital, e que o não pagamento do débito ou a rejeição da impugnação implicará a inscrição do débito em Dívida Ativa, assim como, transcorrido o prazo especificado a seguir, a instauração de procedimento de apuração de descumprimento de obrigação que poderá resultar em caducidade, no prazo de 60 (sessenta) dias, e a inclusão do devedor no Cadastro Informativo de créditos não quitados do Setor Público Federal - CADIN, no prazo de 75 (setenta e cinco) dias. O pagamento poderá ser realizado junto ao Banco do Brasil S/A com a utilização do Documento de Arrecadação das Receitas do FISTEL - boleto bancário, obtido na Anatel ou na internet, no endereço: www.anatel.gov.br/boleto, que informará o valor atualizado e a data para pagamento. E para que chegue ao conhecimento dos interessados, foi expedido o presente edital, que será publicado pela Imprensa Oficial, e, ainda, afixado no local.

CNPJ/CPF	Nome do Devedor	Número Fistel	Receita	Ano
07859234000138	LOSEL - LOCADORA DE SERVIÇOS E COMERCIAL LTDA	10020294220	TFF	1998, 1999, 2000

Edital nº: 090-0010/2003

A Agencia Nacional de Telecomunicações - Anatel, por meio do presente Edital, NOTIFICA DO(S) LANÇAMENTO(S) do(s) crédito(s) da(s) receita(s) em nome do(s) devedor(es) que se encontra(m) ao final relacionado(s), por se encontrar(em) em local incerto e não sabido. Fica(m), portanto, ciente(s) que poderá(ao) apresentar IMPUGNAÇÃO, a ser dirigida à (ao) Escritório Regional da Anatel no Ceará, Endereço: Av. Senador Virgílio Távora 2500 - Dionísio Torres - Fortaleza/CE CEP: 60170-251, no prazo de 30 (trinta) dias, a partir da data da publicação deste Edital, e que o não pagamento do débito ou a rejeição da impugnação implicará a inscrição do débito em Dívida Ativa, assim como, transcorrido o prazo especificado a seguir, a instauração de procedimento de apuração de descumprimento de obrigação que poderá resultar em caducidade, no prazo de 60 (sessenta) dias, e a inclusão do devedor no Cadastro Informativo de créditos não quitados do Setor Público Federal - CADIN, no prazo de 75 (setenta e cinco) dias. O pagamento poderá ser realizado junto ao Banco do Brasil S/A com a utilização do Documento de Arrecadação das Receitas do FISTEL - boleto bancário, obtido na Anatel ou na internet, no endereço: www.anatel.gov.br/boleto, que informará o valor atualizado e a data para pagamento. E para que chegue ao conhecimento dos interessados, foi expedido o presente edital, que será publicado pela Imprensa Oficial, e, ainda, afixado no local.

JOSÉ EVERARDO DE SOUSA LEITE
Gerente do Escritório

CNPJ/CPF	Nome do Devedor	Número Fistel	Receita	Ano
35658368000126	SANTA JULIA AGRO-COMERCIAL-EXPORTADORA DE FRUTAS TROPICAIS LTDA	50000468541	TFF	1998, 1999, 2000

ESCRITÓRIO REGIONAL EM SÃO PAULO
APOIO ADMINISTRATIVO E FINANXEIRO

EXTRATOS DE NOTAS DE EMPENHO

[illegible]nto - ANATEL
[illegible]e Processo: 53504.004528/2003.
[illegible]tante: Agência Nacional de Telecomunicações - ANATEL
Contratada: César Reis Office Products Ltda.
Data assinatura: 19 de dezembro de 2003
Objeto: Este Contrato tem por objeto a aquisição de Suprimentos de Informática, relacionada, de acordo com as especificações constantes deste Contrato, em conformidade com a documentação constante do mesmo processo.
Modalidade de Licitação: Pregão Amplo
Nota de Empenho: 2003NE000596 de 13/12/2003
Valor do Contrato: R$9.000,00 (nove mil reais).

Descrição	Qtd.	Unitário	Total
Cilindro Okipage 4068701	04	R$1.250,00	R$5.000,00
Toner Okipage 40468801	16	R$ 250,00	R$4.000,00

Programa de Trabalho: n. º 24.722.0250.2424.0001
Elemento de Despesa: n. º 33.90.30.17

Contrato - ANATEL
N. º de Processo: 53504.004528/2003
Contratante: Agência Nacional de Telecomunicações - ANATEL
Contratada: Sixpel Informática e Material de Escritório Ltda
Data assinatura: 19 de dezembro de 2003
Objeto: Este Contrato, tem por objeto a aquisição de Suprimentos de Informática, relacionada, de acordo com as especificações constantes deste Contrato, em conformidade com a documentação constante do mesmo processo.
Modalidade de Licitação: Pregão Amplo
Nota de Empenho: 2003NE000601 de 13/12/2003
Valor do Contrato: R$ 4.518,00 (quatro mil, quinhentos e dezoito reais)

Descrição	Qtd.	Unitário	Total
Cart.EpsonS20108 Extralife	150	R$ 11,50	R$1.725,00
Cart.Epson S20189 Extralife	150	R$11,70	R$1.755,00
[illegible]Kyocera TK12	02	R$519,00	R$1.038,00

[illegible]rograma de Trabalho: n. º 24.722.0250.2424.0001
Elemento de Despesa: n. º 33.90.30.17

Contrato - ANATEL
N. º de Processo: 53504.004527/2003.
Contratante: Agência Nacional de Telecomunicações - ANATEL
Contratada: Sixpel Informática e Material de Escritório Ltda
Data assinatura: 19 de dezembro de 2003
Objeto: Este Contrato tem por objeto a aquisição de Suprimentos de Informática, relacionada, de acordo com as especificações constantes deste Contrato, em conformidade com a documentação constante do mesmo processo.

Descrição	Qtd.	Unitário	Total
Bobina para fax Brother	40	R$ 25,50	R$ 1.020,00
Clips Galvanizado nº 0/0	30	R$ 2,80	R$ 84,00
Clips Galvanizado nº 6/0	30	R$ 2,80	R$ 84,00
Clips Galvanizado nº 4/0	20	R$ 2,80	R$ 56,00
Elástico látex nº 18 25 grs	300	R$ 0,39	R$ 117,00
Lápis sextavado preto	576	R$ 0,29	R$ 167,04
Pasta Registr. AZ L.Larga	300	R$ 2,26	R$ 678,00
Pasta com aba elástica	200	R$ 0,47	R$ 94,00
Pilha alcalina pequena AA	500	R$ 0,95	R$ 475,00

Programa de Trabalho: n. º 24.722.0250.2424.0001
Elemento de Despesa: n. º 33.90.30.17

Contrato - ANATEL
N. º de Processo: 53504.004528/2003.
Contratante: Agência Nacional de Telecomunicações - ANATEL
Contratada: Xerox Comércio e Indústria Ltda.
Data assinatura: 19 de dezembro de 2003
Objeto: Este Contrato tem por objeto a aquisição de Suprimentos de Informática, relacionada, de acordo com as especificações constantes deste Contrato, em conformidade com a documentação constante do mesmo processo.
Modalidade de Licitação: Pregão Amplo
Nota de Empenho: 2003NE000603 de 13/12/2003
Valor do Contrato: R$12.500,00 (doze mil e quinhentos reais)

Descrição	Quant	Unitário	Total
Cartucho preto 8R12728	200	R$ 62,50	R$12.500,00

Programa de Trabalho: n. º 24.722.0250.2424.0001
Elemento de Despesa: n. º 33.90.30.17

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS
ADMINISTRAÇÃO CENTRAL

EXTRATO DE CONTRATO

A Empresa Brasileira de Correios e Telégrafos celebrou o Contrato nº 12386/03 - Contratado: INSTITUTO CULTURAL AMILCAR MARTINS, assinado em 09/12/03 com vigência de 10 meses a partir da data de sua assinatura. Objeto: Contrato de Patrocínio Incentivado. Origem: Inexigibilidade de Licitação nº 182/03. Conta orçamentária 00.8.00/5.02. Valor total da contratação: R$50.000,00 (cinqüenta mil reais). Signatários: Airton Langaro Dipp - Presidente da Contratante e Gabriel Pauli Fadel - Diretor de Administração da Contratante; Lucia Martins Flecha de Lima - Presidente da Contratada.

[redacted]

Comunicamos a todos os interessados que o objeto do Pregão n.º 118/2002 - CPL/AC, foi homologada a adjudicação à empresa HEWLETT-PACKARD BRASIL LTDA, para o fornecimento de 05 (cinco) licenças do software HP Open View Network Node Enterprise, versão 6.2 ou superior, incluindo os serviços de atendimento e suporte técnico, no valor global de

AVISOS DE LICITAÇÃO
PREGÃO ELETRÔNICO Nº 130/2003

Objeto: Pregão Eletrônico nº 130/2003 - Aquisição de 08 veículos 04 portas - tipo sedan ou tipo perua. Recebimento das Propostas: no endereço: http://www.correios.com.br até 12/01/2004 às 09:30 horas. Obtenção do Edital: No endereço eletrônico acima. Informações pelo Fax: (0xx61) 426-2759 e telefone: (0xx61) 426-2770, no horário de 08 ás 17:30horas.

PREGÃO ELETRÔNICO Nº 131/2003

Objeto: Pregão Eletrônico nº 131/2003 - Prestação de Serviços de Locação - Copiadora Digital. Recebimento das Propostas: no endereço: http://www.correios.com.br até 12/01/2004 às 14:15 horas. Obtenção do Edital: No endereço eletrônico acima. Informações pelo Fax: (0xx61) 426-2759 e telefone: (0xx61) 426-2770, no horário de 08 ás 17:30horas.

MARTA MARIA COELHO
Pregoeira

DIRETORIA REGIONAL DO AMAZONAS

EXTRATOS DE INSTRUMENTOS CONTRATUAIS

Contrato n.º 164/2003; Assinado em: 29/10/2003; Contratada: Diana Paolucci S/A Industria e Comércio; Objeto: Fornecimento regular e parcelado, pela CONTRATADA, de sacos de ráfia, conforme especificações, consumo médio mensal e cronograma de entrega contidos no Anexo 1 deste Contrato; Origem: Pregão 018/2003; Vigência: 01 (um) ano, a partir de 03/11/2003; Classificação Orçamentária - Atividade: 00.800 Conta/sub-conta 202.27; Valor Global: R$ 42.0000,00; Signatário: Rodolfo Manoel Marques do Amaral - Diretor Regional da Contratante, Jayme Aranha Chacon Junior; Gerente de Administratação da Contratante e Cláudio Roberto da Silva Represente da Contratada.

Contrato nº 149/2003; Assinado em 29/10/2003; Contratada: J. F. de S Teles Comercial - Objeto: Fornecimento regular e parcelado, pela CONTRATADA, de sacos de ráfia, conforme especificações, consumo médio mensal e cronograma de entrega contidos no Anexo 1 deste Contrato;. Origem: Pregão 018/2003; Vigência: 01 (um) ano, com início a partir de 03/11/2003; Classificação Orçamentária - Atividade: 00800; Conta 202.27; Valor Global: R$ 122.400,00; Signatário: Rodolfo Manoel Marques Amaral - Diretor Regional da Contratante, Jayme Aranha Chacon Junior, Gerente Administração da Contratante, José Francisco de Souza Teles Representante da contratada.

Contrato nº 156//2003; Assinado em 20/10/2003; Contratada: Antares Distribuidora de Motos Ltda. Objeto: Fornecimento de peças originais de reposição para 88 motocicletas Honda CG e XL-125, na cidade de Manaus/AM: Origem: Pregão - 017/2003; Vigência: 01 (um) ano, iniciando na data de sua assinatura.; Classificação Orçamentária - Atividade: 00800; Conta 204.02; Valor Global: R$ 26.400,00; Signatários: Rodolfo Manoel Marques Amaral - Diretor Regional da Contratante, Jayme Aranha Chacon Junior, Gerente Administração da Contratante, Aldemir da Silva Gorayeb Representante da contratada.

Contrato nº 158//2003; Assinado em 20/10/2003; Contratada: Auto Peças Manaus Mercedes Ltda. Objeto: Serviços técnicos de manutenção

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 0567
3740
Doc:

CORREIOS

De: PREGOEIRA AC

Protocolo

Ao: CHEFE DO DMARK

CI / CPL/AC - 1468/2003

Ref.: Pregão 118/2003 - CPL/AC

Assunto: Publicação no DOU - Aviso de Retificação

Brasília, 29 de dezembro de 2003.

Solicitamos a V.Sª. veicular mensagem, cujo texto anexamos à presente, de acordo com a especificação a seguir:

- Pregão nº 118/2003 -CPL/AC (AVISO DE RETIFICAÇÃO)
- **Data de veiculação: 30/12/2003**

Salientamos que tal veiculação deverá ser feita de acordo com a Lei n.º 10.520/2002, Decreto n.º 3.784/2001 e Lei n.º 8.666/93, republicada em 06/07/94.

Atenciosamente,

MARTA MARIA COELHO
Pregoeira/AC

GILBERTO FERREIRA DO AMARAL
Membro da CPL/AC
Mat. 8.008.347-1

C/Anexo: Publicação
FCAR/fcar

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0568
3740
Doc:

MINISTÉRIO DAS COMUNICAÇÕES
EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS
ADMINISTRAÇÃO CENTRAL

AVISO DE RETIFICAÇÃO
PREGÃO N.º 118/2003- CPL/AC

Retificamos o aviso de homologação e adjudicação publicado no DOU do dia 23/12/2003, página 102. Onde se lê: Pregão 118/2002, leia-se: Pregão 118/2003.

MARTA MARIA COELHO
Pregoeira CPL/AC

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0569
Doc.
L 3740

RELATORIO ULTIMA TRANSMISSÃO

N. Act	0430	
Tipo	TRANSM. MCE	
N. DOC		
Numero discado	2042	
Nome		
Identificação recebida		
Data/Hora	29-12-03	12:39
Duração	00:35	
Pags.	02	
Resul.	OK	

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0570
Doc: 3740

SUPERINTENDÊNCIA DE RADIOFREQUÊNCIA E FISCALIZAÇÃO
GERÊNCIA-GERAL DE FISCALIZAÇÃO
ESCRITÓRIO REGIONAL DO CEARÁ

EXTRATOS DE TERMOS ADITIVOS

Primeiro Termo Aditivo ao Contrato ER-9-N º 12/2002-ANATEL
Data da Assinatura: 30.09.2003
Contratada: PRIMARE ENGENHARIA LTDA.
Vigência: 01.10.2003 a 30.09.2004
Objeto: Prorrogação do prazo de vigência, cujo objeto é a prestação de serviços de manutenção preventiva e corretiva dos equipamentos de ar-condicionado para as instalações do Escritório Regional da Anatel no Ceará, pelo período de 12(doze) meses, contados a partir de 01.10.2003.
Fundamento Legal: Artigo 57, Inciso II da Lei 8.666/93, de 21/06/93.
Programas de Trabalho: 24.722.0750.2000.0001
Elemento de Despesa: 339039.00
Valor do Contrato: R$ 13.740,00 (treze mil e setecentos e quarenta reais)

Quarto Termo Aditivo ao Contrato ER-9(UO 9.2)-N º 013/99-ANATEL
Data da Assinatura: 02 de novembro de 2003
Contratado: MIGUEL MENDES ARCOVERDE
Vigência: 03.11.2003 a 02.11.2004
Objeto: Prorrogação do prazo de vigência, cujo objeto é a locação de imóvel, situado na Av. Frei Serafim, nº 2786 - Centro - Teresina/PI, para instalação da Unidade Operacional da Anatel no Piauí, pelo período de 12 (doze) meses, contados a partir de 03.11.2003.
Fundamento Legal : Artigo 57, Inciso II, da Lei 8.666/93, de 21/06/93.
Programas de Trabalho: 24.722.0750.2000.0001
Elemento de Despesa: 339036.00
Valor Anual do Contrato: R$ 48.000,00 (quarenta e oito mil reais)

EDITAIS DE NOTIFICAÇÃO DE 22 DE DEZEMBRO DE 2003

Edital nº: 090-0009/2003

A Agencia Nacional de Telecomunicações - Anatel, por meio do presente Edital, NOTIFICA DO(S) LANÇAMENTO(S) do(s) crédito(s) da(s) receita(s) em nome do(s) devedor(es) que se encontra(m) ao final relacionado(s), por se encontrar(em) em local incerto e não sabido. Fica(m), portanto, ciente(s) que poderá(ao) apresentar IMPUGNAÇÃO, a ser dirigida à (ao) Escritório Regional da Anatel no Ceará, Endereço: Av. Senador Virgílio Távora 2500 - Dionísio Torres - Fortaleza/CE CEP: 60170-251, no prazo de 30 (trinta) dias, a partir da data da publicação deste Edital, e que o não pagamento do débito ou a rejeição da impugnação implicará a inscrição do débito em Dívida Ativa, assim como, transcorrido o prazo especificado a seguir, a instauração de procedimento de apuração de descumprimento de obrigação que poderá resultar em caducidade, no prazo de 60 (sessenta) dias, e a inclusão do devedor no Cadastro Informativo de créditos não quitados do Setor Público Federal - CADIN, no prazo de 75 (setenta e cinco) dias. O pagamento poderá ser realizado junto ao Banco do Brasil S/A com a utilização do Documento de Arrecadação das Receitas do FISTEL - boleto bancário, obtido na Anatel ou na internet, no endereço: www.anatel.gov.br/boleto, que informará o valor atualizado e a data para pagamento. E para que chegue ao conhecimento dos interessados, foi expedido o presente edital, que será publicado pela Imprensa Oficial, e, ainda, afixado no local.

CNPJ/CPF	Nome do Devedor	Número Fistel	Receita	Ano
07859234000138	LOSEL - LOCADORA DE SERVIÇOS E COMERCIAL LTDA	10020294220	TFF	1998, 1999, 2000

Edital nº: 090-0010/2003

A Agencia Nacional de Telecomunicações - Anatel, por meio do presente Edital, NOTIFICA DO(S) LANÇAMENTO(S) do(s) crédito(s) da(s) receita(s) em nome do(s) devedor(es) que se encontra(m) ao final relacionado(s), por se encontrar(em) em local incerto e não sabido. Fica(m), portanto, ciente(s) que poderá(ao) apresentar IMPUGNAÇÃO, a ser dirigida à (ao) Escritório Regional da Anatel no Ceará, Endereço: Av. Senador Virgílio Távora 2500 - Dionísio Torres - Fortaleza/CE CEP: 60170-251, no prazo de 30 (trinta) dias, a partir da data da publicação deste Edital, e que o não pagamento do débito ou a rejeição da impugnação implicará a inscrição do débito em Dívida Ativa, assim como, transcorrido o prazo especificado a seguir, a instauração de procedimento de apuração de descumprimento de obrigação que poderá resultar em caducidade, no prazo de 60 (sessenta) dias, e a inclusão do devedor no Cadastro Informativo de créditos não quitados do Setor Público Federal - CADIN, no prazo de 75 (setenta e cinco) dias. O pagamento poderá ser realizado junto ao Banco do Brasil S/A com a utilização do Documento de Arrecadação das Receitas do FISTEL - boleto bancário, obtido na Anatel ou na internet, no endereço: www.anatel.gov.br/boleto, que informará o valor atualizado e a data para pagamento. E para que chegue ao conhecimento dos interessados, foi expedido o presente edital, que será publicado pela Imprensa Oficial, e, ainda, afixado no local.

JOSÉ EVERARDO DE SOUSA LEITE
Gerente do Escritório

CNPJ/CPF	Nome do Devedor	Número Fistel	Receita	Ano
35658368000126	SANTA JULIA AGRO-COMERCIAL-EXPORTADORA DE FRUTAS TROPICAIS LTDA	50000468541	TFF	1998, 1999, 2000

ESCRITÓRIO REGIONAL EM SÃO PAULO
APOIO ADMINISTRATIVO E FINANXEIRO

EXTRATOS DE NOTAS DE EMPENHO

Contrato - ANATEL
Nº de Processo: 53504.004528/2003.
Contratante: Agência Nacional de Telecomunicações - ANATEL
Contratada: César Reis Office Products Ltda.
Data assinatura: 19 de dezembro de 2003
Objeto: Este Contrato tem por objeto a aquisição de Suprimentos de Informática, relacionada, de acordo com as especificações constantes deste Contrato, em conformidade com a documentação constante do mesmo processo.
Modalidade de Licitação: Pregão Amplo
Nota de Empenho: 2003NE000596 de 13/12/2003
Valor do Contrato: R$9.000,00 (nove mil reais).

Descrição	Qtd.	Unitário	Total
Cilindro Okipage 4068701	04	R$1.250,00	R$5.000,00
Toner Okipage 40468801	16	R$ 250,00	R$4.000,00

Programa de Trabalho: n. º 24.722.0250.2424.0001
Elemento de Despesa: n. º 33.90.30.17

Contrato - ANATEL
N. º de Processo: 53504.004528/2003
Contratante: Agência Nacional de Telecomunicações - ANATEL
Contratada: Sixpel Informática e Material de Escritório Ltda
Data assinatura: 19 de dezembro de 2003
Objeto: Este Contrato, tem por objeto a aquisição de Suprimentos de Informática, relacionada, de acordo com as especificações constantes deste Contrato, em conformidade com a documentação constante do mesmo processo.
Modalidade de Licitação: Pregão Amplo
Nota de Empenho: 2003NE000601 de 13/12/2003
Valor do Contrato: R$ 4.518,00 (quatro mil, quinhentos e dezoito reais)

Descrição	Qtd.	Unitário	Total
Cart.EpsonS20108 Extralife	150	R$ 11,50	R$1.725,00
Cart.Epson S20189 Extralife	150	R$11,70	R$1.755,00
Kyocera TK12	02	R$519,00	R$1.038,00

Programa de Trabalho: n. º 24.722.0250.2424.0001
Elemento de Despesa: n. º 33.90.30.17

Contrato - ANATEL
N. º de Processo: 53504.004527/2003.
Contratante: Agência Nacional de Telecomunicações - ANATEL
Contratada: Sixpel Informática e Material de Escritório Ltda
Data assinatura: 19 de dezembro de 2003
Objeto: Este Contrato tem por objeto a aquisição de Suprimentos de Informática, relacionada, de acordo com as especificações constantes deste Contrato, em conformidade com a documentação constante do mesmo processo.

Descrição	Qtd.	Unitário	Total
Bobina para fax Brother	40	R$ 25,50	R$ 1.020,00
Clips Galvanizado nº 0/0	30	R$ 2,80	R$ 84,00
Clips Galvanizado nº 6/0	30	R$ 2,80	R$ 84,00
Clips Galvanizado nº 4/0	20	R$ 2,80	R$ 56,00
Elástico látex nº 18 25 grs	300	R$ 0,39	R$ 117,00
Lápis sextavado preto	576	R$ 0,29	R$ 167,04
Pasta Registr. AZ L.Larga	300	R$ 2,26	R$ 678,00
Pasta com aba elástica	200	R$ 0,47	R$ 94,00
Pilha alcalina pequena AA	500	R$ 0,95	R$ 475,00

Programa de Trabalho: n. º 24.722.0250.2424.0001
Elemento de Despesa: n. º 33.90.30.17

Contrato - ANATEL
N. º de Processo: 53504.004528/2003.
Contratante: Agência Nacional de Telecomunicações - ANATEL
Contratada: Xerox Comércio e Indústria Ltda.
Data assinatura: 19 de dezembro de 2003
Objeto: Este Contrato tem por objeto a aquisição de Suprimentos de Informática, relacionada, de acordo com as especificações constantes deste Contrato, em conformidade com a documentação constante do mesmo processo.
Modalidade de Licitação: Pregão Amplo
Nota de Empenho: 2003NE000603 de 13/12/2003
Valor do Contrato: R$12.500,00 (doze mil e quinhentos reais)

Descrição	Quant	Unitário	Total
Cartucho preto 8R12728	200	R$ 62,50	R$12.500,00

Programa de Trabalho: n. º 24.722.0250.2424.0001
Elemento de Despesa: n. º 33.90.30.17

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS
ADMINISTRAÇÃO CENTRAL

EXTRATO DE CONTRATO

A Empresa Brasileira de Correios e Telégrafos celebrou o Contrato nº 12386/03 - Contratado: INSTITUTO CULTURAL AMILCAR MARTINS, assinado em 09/12/03 com vigência de 10 meses a partir da data de sua assinatura. Objeto: Contrato de Patrocínio Incentivado. Origem: Inexigibilidade de Licitação nº 182/03. Conta orçamentária 00.8.00/5.02. Valor total da contratação: R$50.000,00 (cinqüenta mil reais). Signatários: Airton Langaro Dipp - Presidente da Contratante e Gabriel Pauli Fadel - Diretor de Administração da Contratante; Lucia Martins Flecha de Lima - Presidente da Contratada.

AVISO DE HOMOLOGAÇÃO E ADJUDICAÇÃO PREGÃO Nº 118/2002

Comunicamos a todos os interessados que o objeto do Pregão n.º 118/2002 - CPL/AC, foi homologada a adjudicação à empresa HEWLETT-PACKARD BRASIL LTDA, para o fornecimento de 05 (cinco) licenças do software HP Open View Network Node Enterprise, versão 6.2 ou superior, incluindo os serviços de atendimento e suporte técnico, no valor global de

AVISOS DE LICITAÇÃO PREGÃO ELETRÔNICO Nº 130/2003

Objeto: Pregão Eletrônico nº 130/2003 - Aquisição de 08 veículos 04 portas - tipo sedan ou tipo perua. Recebimento das Propostas: no endereço: http://www.correios.com.br até 12/01/2004 às 09:30 horas. Obtenção do Edital: No endereço eletrônico acima. Informações pelo Fax: (0xx61) 426-2759 e telefone: (0xx61) 426-2770, no horário de 08 ás 17:30horas.

PREGÃO ELETRÔNICO Nº 131/2003

Objeto: Pregão Eletrônico nº 131/2003 - Prestação de Serviços de Locação - Copiadora Digital. Recebimento das Propostas: no endereço: http://www.correios.com.br até 12/01/2004 às 14:15 horas. Obtenção do Edital: No endereço eletrônico acima. Informações pelo Fax: (0xx61) 426-2759 e telefone: (0xx61) 426-2770, no horário de 08 ás 17:30horas.

MARTA MARIA COELHO
Pregoeira

DIRETORIA REGIONAL DO AMAZONAS

EXTRATOS DE INSTRUMENTOS CONTRATUAIS

Contrato nº 164/2003; Assinado em: 29/10/2003; Contratada: Diana Paolucci S/A Industria e Comércio; Objeto: Fornecimento regular e parcelado, pela CONTRATADA, de sacos de ráfia, conforme especificações, consumo médio mensal e cronograma de entrega contidos no Anexo 1 deste Contrato; Origem: Pregão 018/2003; Vigência: 01 (um) ano, a partir de 03/11/2003; Classificação Orçamentária - Atividade: 00.800 Conta/sub-conta 202.27; Valor Global: R$ 42.0000,00; Signatário: Rodolfo Manoel Marques do Amaral - Diretor Regional da Contratante, Jayme Aranha Chacon Junior; Gerente de Administratação da Contratante e Cláudio Roberto da Silva Represente da Contratada.

Contrato nº 149/2003; Assinado em 29/10/2003; Contratada: J. F. de S Teles Comercial - Objeto: Fornecimento regular e parcelado, pela CONTRATADA, de sacos de ráfia, conforme especificações, consumo médio mensal e cronograma de entrega contidos no Anexo 1 deste Contrato;. Origem: Pregão 018/2003; Vigência: 01 (um) ano, com início a partir de 03/11/2003; Classificação Orçamentária - Atividade: 00800; Conta 202.27; Valor Global: R$ 122.400,00; Signatário: Rodolfo Manoel Marques Amaral - Diretor Regional da Contratante, Jayme Aranha Chacon Junior, Gerente Administração da Contratante, José Francisco de Souza Teles Representante da contratada.

Contrato nº 156//2003; Assinado em 20/10/2003; Contratada: Antares Distribuidora de Motos Ltda. Objeto: Fornecimento de peças originais de reposição para 88 motocicletas Honda CG e XL-125, na cidade de Manaus/AM: Origem: Pregão - 017/2003; Vigência: 01 (um) ano, iniciando na data de sua assinatura.; Classificação Orçamentária - Atividade: 00800; Conta 204.02; Valor Global: R$ 26.400,00; Signatários: Rodolfo Manoel Marques Amaral - Diretor Regional da Contratante, Jayme Aranha Chacon Junior, Gerente Administração da Contratante, Aldemir da Silva Gorayeb Representante da contratada.

Contrato nº 158//2003; Assinado em 20/10/2003; Contratada: Auto Peças Manaus Mercedes Ltda. Objeto: Serviços técnicos de manutenção

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº: 0571
3740
Doc:

CORREIOS

De: PREGOEIRA AC

Ao: CHEFE DO DMARK

CI / CPL/AC - 1443/2003

Ref.: Pregão 118/2003 - CPL/AC

Protocolo

3.176

Assunto: Publicação no DOU - Aviso de Homologação da Adjudicação

Brasília, 19 de dezembro de 2003.

Solicitamos a V.Sª. veicular mensagem, cujo texto anexamos à presente, de acordo com a especificação a seguir:

- Pregão nº 118/2003 -CPL/AC (AVISO DE HOMOLOGAÇÃO DA ADJUDICAÇÃO)
- **Data de veiculação: 23/12/2003**

Salientamos que tal veiculação deverá ser feita de acordo com a Lei n.º 10.520/2002, Decreto n.º 3.784/2001 e Lei n.º 8.666/93, republicada em 06/07/94.

Homologação: Relatório/CPL/AC – 065/2003.

Atenciosamente,

MARTA MARIA COELHO
Pregoeira/AC

C/Anexo: Publicação
FCAR/fcar

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 0572
Doc: 3740

FW0010

MINISTÉRIO DAS COMUNICAÇÕES
EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS
ADMINISTRAÇÃO CENTRAL

AVISO DE HOMOLOGAÇÃO E ADJUDICAÇÃO
PREGÃO N.º 118/2002- CPL/AC

Comunicamos a todos os interessados que o objeto do Pregão n.º 118/2002 – CPL/AC, foi homologada a adjudicação à empresa HEWLETT-PACKARD BRASIL LTDA, para o fornecimento de 05 (cinco) licenças do software HP Open View Network Node Enterprise, versão 6.2 ou superior, incluindo os serviços de atendimento e suporte técnico. no valor global de R$ 418.500,00 (quatrocentos e dezoito mil e quinhentos reais).

MARTA MARIA COELHO
Pregoeira

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0573
3740
Doc:

RELATORIO ULTIMA TRANSMISSÃO

N. Act	0392	
Tipo	TRANSM. MCE	
N. DOC		
Numero discado	2042	
Nome		
Identificação recebida		
Data/Hora	19-12-03	16:13
Duração	00:33	
Pags.	01	
Resul.	OK	

3.174

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0574
3740
Doc:

RELATÓRIO HOMOLOGAÇÃO

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: Nº 0575
3740
Doc:

CORREIOS SISBLOQ Web

Diretoria Econômico-Financeira
Departamento de Orçamento e Custo

Emissão de Bloqueio Orçamentário
- Autorizado -

Diretoria Regional:	**01 - Administração Central**
No do Bloqueio:	**73236/2003**
Área Solicitante:	01340000 - DPTO DE REDE CORPORATIVA
Solicitado em:	04/09/2003
Projeto/Atividade:	17101 - Rede Corporativa
Conta:	80009020000 - EQUIPAMENTOS/MATERIAL PERMAMENTE
Finalidade:	Contratação de 5 licenças do SW HP OpenView referente ao projeto de Administração da Rede.
Bloqueio Ajustado:	68384
Data da Autorização:	10/09/2003

Cronograma de Execução

Mês	Ano	Valor - R$
12	2003	423.059,00

Valor Total do Bloqueio - R$ 423.059,00

DEORC
Jameson Reinaux da Cunha
80111157

Voltar

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0576
3740
Doc:

IDENTIFICAÇÃO: Relatório/Homologação/CPL/AC-065/2003

ASSUNTO: Homologação do Pregão-118/2003 - CPL/AC - Aquisição de licenças do software HP.

I. PROPOSTA

Homologar o Pregão nº 118/2003-CPL/AC, no valor global de R$ 418.500,00 (quatrocentos e dezoito mil e quinhentos reais), com adjudicação à empresa HEWLETT-PACKARD BRASIL LTDA., para fornecimento de 05 (cinco) licenças do software HP Open View Network Node Enterprise, versão 6.2 ou superior, incluindo os serviços de atendimento e suporte técnico.

APLICAÇÃO/META: Garantir e expandir a gerência de ambientes da ECT

ÓRGÃO REQUISITANTE: DITEC (CI/ASS/DERCO-1781/2003).

EMPRESA A CONTRATAR:

- HEWLETT-PACKARD BRASIL LTDA.

OBJETO: Aquisição de 05 licenças do Software HP Open View Network Node Manager Enterprise v.620 ou superior.

VALOR CONTRATUAL: R$ 418.500,00 (quatrocentos e dezoito mil e quinhentos reais).

PERIODICIDADE DE REAJUSTE: Não se aplica.

ÍNDICE DE REAJUSTE: Não se aplica.

PRAZO DE EXECUÇÃO/ENTREGA: Em até 10 dias, contados a partir da data da assinatura do Contrato.

FORMA DE PAGAMENTO: Em parcela única, no prazo de até 15 dias após a emissão do Termo de Aceitação Final

CONTA/PROJETO: 9.02/17.1.01

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0577
3740
Doc: 1

CORREIOS

II. INDICATIVO DE COMPETÊNCIA

Diretor de Tecnologia e de Infra-Estrutura da ECT, conforme disposto no Relatório/PR-067/2003, 15ª REDIR de 16/04/2003.

3/71

III. PROCESSO LICITATÓRIO

Modalidade da Licitação: Pregão

Empresas:

- retiraram o edital: 09
- participaram da licitação: 03
- classificadas a dar lances: 03
- inabilitada: 00

Propostas:

ITEM 01: 05 LICENÇAS DO SOFTWARE HP OPEN VIEW NETWORK NODE ENTERPRISE, VERSÃO 6.2 OU SUPERIOR, INCLUINDO OS SERVIÇOS DE ATENDIMENTO E SUPORTE TÉCNICO:

Empresas	Valor Unitário (R$)		Valor Total/ Com base melhor lance (R$)	Posição (%)
	Proposta escrita	Com base melhor lance		
Hewlett-Packard	**95.000,00**	**83.700,00**	**418.500,00**	**100,00**
TM Solutions	99.000,00	87.200,00	436.000,00	104,19
E-TAILOR	101.000,00	87.600,00	438.000,00	104,66
Valor de Referência *	**84.611,71**		**423.058,55**	**101,09**

(*) Valor de Referência fornecido pelo DCAMP, baseado na média composta pelo preço da pesquisa de mercado.

IV. ÚLTIMAS AQUISIÇÕES

Não foram encontrados registros de aquisições anteriores, com especificações e critérios de julgamento similares ao adotado na presente licitação, tornando-se, pois, inviável uma análise comparativa de preços.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0578
3740
Doc:

V. HISTÓRICO DO PROCESSO LICITATÓRIO

Autorização para licitar	28/08/2003
Recebido na CPL/AC para licitar	01/09/2003
Veiculação do edital em D.O.U.	02/12/2003
Reunião de abertura	16/12/2003

3.170

VI. FUNDAMENTAÇÃO LEGAL

- Lei nº 8.666/1993;
- Lei nº 10.520/2002;
- Decreto nº 3.555/2000;
- Decreto nº 3.784/2001;
- MANLIC (Manual de Licitação e Contratação).

VII. INFORMAÇÕES COMPLEMENTARES

Em cumprimento às orientações da CI/CAS/DCON/DECAM-4.641/2003 e do Comitê de Avaliação de Contratações Estratégicas (Parecer CACE-077/2003), foi deflagrada a presente licitação, tipo menor preço, objetivando a aquisição da ferramenta HP Openview Network Node Manger Enterprise, versão 6.2 ou superior, objeto da CI/ASS/DERCO-1781/2003.

As licenças serão instaladas em 05 servidores, integradas ao ambiente de gerenciamento de rede já implantado na ECT, permitindo a monitoração de aproximadamente mais de 5000 elementos de rede e consequentemente obtendo um maior controle sobre os serviços que fazem uso dos recursos de rede.

Conforme disposto no Parecer CACE, atualmente a ECT necessita ampliar a quantidade de licenças da ferramenta atual de gerência pró-ativa, que tem a finalidade de verificar a disponibilidade dos elementos de rede que correspondem aos rodeadores e antenas satélites instaladas nas unidades de atendimento (Agências), unidades administrativas e operacionais e, ainda, os servidores, rodeadores e switches, localizados nos Centros Corporativos de Dados (CCD) em Brasília e em São Paulo.

Ainda no Parecer, cada licença é instalada em um servidor do ambiente de gerência e propicia a visibilidade do "status" de responsabilidade de aproximadamente 1000 elementos de rede. Com estas informações é possível

CPMI - CORREIOS
Fls. Nº 0579
Doc: 3740

agilizar a tomada de decisão para a correção dos problemas referentes a elementos de rede, minimizando ao máximo o impacto de indisponibilidade dos serviços e dos negócios da ECT.

Cumpre assinalar, que na ECT existem duas licenças do HP Open View Network Node Manager instaladas em dois servidores, uma adquirida no projeto do ERP e outra no projeto do Banco Postal. Um servidor gerência aproximadamente mil agências do Banco Postal e o outro servidor possibilita gerenciar vários elementos dos Centros Corporativos de Dados/AC e SPM, além dos Projetos SRO, ERP e MECTRI.

A aquisição das licenças apresenta também as seguintes vantagens :

- Monitoração dos elementos de rede instalados nos diversos projetos da ECT, de forma a gerar alarmes instantâneos de falhas, permitindo a atuação imediata após o incidente, minimizando o tempo de reparo e aumentando o tempo de disponibilidade desses sistemas.
- Monitoração dos elementos de rede instalados nas agências, onde são realizados os negócios da empresa, permitindo a geração de alarmes instantâneos de falhas e favorecendo à redução do tempo de reparo e ao aumento do tempo de disponibilidade dos serviços de rede;
- Redução dos gastos com deslocamentos de profissionais técnicos, mão-de-obra e telefonia; e
- Melhoria do processo de diagnóstico de falhas.

Dessa forma, consoante disposto no item 7 do edital e com base no melhor preço ofertado, está sendo proposta a homologação da adjudicação à empresa HEWLETT PACKARD LTDA., CNPJ n.º 61.797.924/0001-55, para o respectivo fornecimento.

VIII. ANEXOS

1. CI/ASS/DERCO-1781/2003;
2. Autorização para licitar (Parecer do Comitê – CACE-077/2003);

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0580
3740
Doc:

3. CI/CAS/DCON/DECAM-4.641/2003;
4. Mapa Comparativo de Preços;
5. Ata da Sessão do Pregão;
6. Tabela de Bloqueio.

3.168

Brasília, 19 de dezembro de 2003.

Marta Maria Coelho
Pregoeira

Decisão superior:

Homologo a Licitação, Pregão-0118/2003, conforme proposto no **item I da Proposta** deste Relatório.

Brasília, 19 de dezembro de 2003.

Eduardo Medeiros de Morais
Diretor de Tecnologia e de Infra-Estrutura

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0581
3740
Doc:

ANEXO 1. DO RELATÓRIO/HOMOLOGAÇÃO/CPL/AC-065/2003

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS

Área Reservada ao Protocolo

URGENTE

DE: DERCO

AO: DECAM

CI/ASS/DERCO- 1781/2003

Ref.: CI/CPL/AC-0726/2003

Assunto: Solicitação de Abertura de Licitação

Brasília-DF, 29 de julho de 2003

Estamos encaminhando a V.Sª., em anexo, relatório DERCO-1780/2003, solicitando a abertura de licitação para aquisição de licenças de software de gerenciamento HP OpenView Network Node Manager Enterprise, bem como toda documentação da tramitação do processo.

Atenciosamente,

Ana Lúcia Leitão Nunes
Chefe do DERCO

C/ ANEXOS: Relatorio DERCO-1780 e Documentacao do Processo

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0582
3740
Doc:

CORREIOS

PARECER/CACE-077/2003

Assunto: Abertura de Licitação para a Aquisição de 5 licenças do Software HP OpenView Network Node Manager Enterprise v.620 ou superior.

Referência: 28ª Reunião do Comitê, de 26/08/2003.

3166

1. Dados da **Contratação:**

⇒ **Modalidade:** Pregão

⇒ **Objeto:** Aquisição de 5 licenças do Software HP OpenView Network Node Manager Enterprise v.620 ou superior para instalação em 5 Servidores para gerenciamento pró-ativo de elementos da Rede Corporativa.

⇒ **Valor Estimado:** R$ 423.054,55

⇒ **Classificação Orçamentária**: Projeto: 17.1.01 – Conta 9.02

⇒ **Justificativa da Contratação**: Necessidade da ECT ampliar a quantidade de licenças da ferramenta atual de gerência pró-ativa, que verifica a disponibilidade dos elementos de rede que correspondem aos roteadores e antenas satélites instaladas nas Unidades de Atendimento (Agências), Unidades Administrativas e Operacionais e, ainda, os servidores, roteadores e switches localizados nos Centros Corporativos de Dados (CCD) em Brasília e em São Paulo.

Cada licença é instalada em um servidor do ambiente de gerência e propicia a visibilidade do "status" de disponibilidade de aproximadamente 1000 elementos de rede. Com estas informações é possível agilizar a tomada de decisão para a correção dos problemas referentes a elementos de rede, minimizando ao máximo o impacto de indisponibilidade dos serviços e dos negócios dos Correios. Ou seja, é possível agrupar os elementos de rede de um determinado Projeto Corporativo, por exemplo Banco Postal, fornecendo, em tempo real, alarmes de falhas identificando o elemento causador do problema.

Estas licenças serão instaladas em 5 (cinco) servidores, integradas ao ambiente de gerenciamento de rede já implantado nos Correios, permitindo a monitoração de aproximadamente mais 5000 elementos de rede e consequentemente obtendo um maior controle sobre os serviços que fazem uso dos recursos de rede.

⇒ **Situação Atual**: Atualmente, o ambiente de gerência de rede possui 2 licenças instaladas em 2 servidores, uma adquirida no projeto ERP e outra no projeto do Banco Postal. Um servidor possibilita gerenciar aproximadamente 1000 agências do Banco Postal e o outro servidor, possibilita gerenciar vários elementos de rede dos Centros Corporativos de Dados/AC e SPM, Projetos SRO, ERP e MECTRI.

Na expansão do CCD (pregão recente) serão disponibilizados mais 5 servidores para a gerência dos demais elementos da rede, para tal serão necessárias 5 licenças dessa ferramenta.

De acordo com o informado pelo DERCO, atualmente possuímos, conforme descriminados a seguir, 6.853 elementos de rede para serem gerenciados, sendo que dessa total apenas 2.000, aproximadamente, estão sendo gerenciados de forma pró-ativa:

- 2.949 (apenas mil estão sendo gerenciadas on-line) são agências com Banco Postal;

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0583
Doc: 3740

- ✓ 2.350 são agências onde será implantado o Banco Postal até dezembro/03, segundo o gestor do projeto;
- ✓ 1.554 (apenas mil estão sendo gerenciadas on-line) são elementos de rede dos Centros Corporativos de Dados/AC e SPM, Projetos SRO, ERP e MECTRI e outras unidades de atendimento sem Banco Postal.

3.166

2. Informações Gerais:

⇒ **Política Interna de contratação para o objeto a ser contratado:** Conforme definido no contrato de aquisição do Banco Postal (fase 1), foi especificado o fornecimento de ferramentas de gerenciamento da infra-estrutura, aderentes ao modelo já utilizado nos Correios. A fim de evitar desperdício e subutilização de recursos de gerência, o DERCO utiliza a política de incorporar, em cada novo projeto básico, as especificações das licenças de softwares já existentes e, tecnicamente já aprovadas pela equipe técnica.

⇒ **Compatibilização da contratação com as Diretrizes do Plano Estratégico da ECT**: O Plano Diretor de Tecnologia da Informação (PDTI), definiu as estratégias da área de Tecnologia e de Infra-estrutura da ECT, para o pleno atendimento aos planos de negócios, às automações operacionais e administrativas da Empresa. No PDTI estão previstas ações estratégicas para o gerenciamento integrado dos ambientes, que possibilitará o maior controle sobre toda estrutura de TI e consequentemente maior agilidade na tomada de decisões.

⇒ **Viabilidade Técnica:** Esta aquisição é compatível com o modelo de gerenciamento adotado nos Correios e trata-se de expansão de quantidade de licenças de um produto que já é amplamente utilizado no ambiente de gerenciamento.

⇒ **Expectativa de Economicidade e Eficiência**: O gerenciamento pró-ativo e on-line dos elementos de rede permitirá a redução de gastos com deslocamento de profissionais (transporte, hospedagem, passagens), com mão-de-obra e telefonia, além de dar maior eficiência ao processo.

3. Benefícios e/ou Impactos

⇒ **Operacional:** Estas licenças permitirão que os elementos de rede instalados nos projetos SRO (Sistema de Rastreamento de Objetos) e MECTRI (Mecanização da Triagem), sejam monitorados, de modo que sejam gerados alarmes instantâneos em determinadas circunstâncias de falha, propiciando à área de rede atuar imediatamente após o incidente, minimizando o tempo de reparo e consequentemente aumentando o tempo de disponibilidade desses sistemas, essenciais aos processos da área operacional.

⇒ **Comercial:** Estas licenças permitirão que os elementos de rede instalados nas agências, onde os negócios são realizados, sejam monitorados, de modo que sejam gerados alarmes instantâneos em determinadas circunstâncias de falha, propiciando à área de rede atuar imediatamente após o incidente, minimizando o tempo de reparo e consequentemente aumentando o tempo de disponibilidade dos serviços que estão sendo executados na rede.

⇒ **Administrativo:** redução de gastos com deslocamento de profissionais (transporte, hospedagem, passagens), com mão-de-obra e telefonia.

⇒ **Tecnológico:** melhoria na qualidade do suporte técnico;

⇒ **Recursos Humanos:** A melhoria do processo de diagnóstico de falhas permitirá uma melhor produtividade dos recursos humanos envolvidos.

⇒ **Financeiro:** a aquisição das licenças está prevista na programação orçamentária da ECT, conforme Bloqueio Orçamentário DORC/DEORC-68384/2003.

RQS II 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0584
3740
Doc:

4. Conclusão:

Diante do exposto, somos de parecer favorável ao desencadeamento da licitação em tela.

Ressaltamos que a proposta de aquisição originalmente submetida ao Comitê previa a compra de 8 licenças, sendo posteriormente reavaliada pelo DERCO, em função das ponderações deste Comitê.

Brasília, 28 de agosto de 2003.

Marcos Gomes da Silva
Coordenador do Comitê

Sr. Presidente,

O DERCO propõe a abertura de licitação para a aquisição de 5 (cinco) licenças do Software HP OpenView Network Node Manager Enterprise v.620 ou superior, pelo valor total de R$ 423.054,55. Com base nas informações disponibilizadas, o Comitê se posicionou favorável à contratação. Sendo assim, submeto a sua apreciação a presente proposta, sugerindo que seja autorizada a abertura da licitação, conforme disposto no Parecer-077/2003.

Brasília, 28 / 08 /2003.

Eduardo Medeiros de Morais
Diretor de Tecnologia e de Infra-Estrutura

Autorizo a abertura da licitação, conforme proposto pelo DERCO e de acordo com o estabelecido no Parecer-077/2003.

Brasília, 28 / 08 /2003.

Airton Langaro Dipp
Presidente da ECT

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0585
3740
Doc:

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS

3/64

De: DECAM

PROTOCOLO

Ao: COMITÊ DE AVALIAÇÃO DE CONTRATAÇÕES ESTRATÉGICAS

Diretoria de Administração / DIRAD
Protocolo nº 1630
Recebido em: 05 / 08 / 2003
Assinatura:

CI/CAS.DCON/DECAM – 4.641/2003

Ref. CI ASS/DERCO – 1781/2003

ASSUNTO: Análise de pedido de abertura de licitação.

Brasília, 05 de agosto de 2003

Estamos encaminhando o processo abaixo, para análise desse Comitê, haja vista que em função do valor estimado, depende de autorização do Presidente, conforme orientação contida na CI/DIRAD – 243/2003 – Circular.

ÓRGÃO REQUISITANTE	OBJETO	VALOR MÉDIO ESTIMADO
DERCO	AQUISIÇÃO DE LICENÇA DE SOFTWARE – HP OPEN VIEW NETWORK	R$ 676.887,28

Seguem. em anexo, Termo de Referência nº 078/2003, Quadro de Estimativa de Preços nº 091/03. Propostas Fornecedores, Tabela de Bloqueio Orçamentário DORC/DEORC nº 68384/2003, e demais documentos pertinentes ao assunto.

Atenciosamente.

Adauto Tameirão Machado
Chefe do Departamento de Contratação e
Administração de Material – DECAM

RQS nº 03/2005 - CN -
CPMI - CORREIOS
-5
FLS. Nº 0586
3740
Doc:

CORREIOS/ECT -15-Set-2003-15:08-00744-2/6

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS

De:DECAM

PROTOCOLO

A(o) :CPL/AC

CI/CAS/DCON/DECAM – 4.737/2003

Ref.: CI/ASS/DERCO-1781/2003

Assunto: Aquisição de Licenças de Software HP Open View Network Node Manager Enterprise v.620, ou superior .

Brasília-DF, 15 de setembro de 2003.

Estamos enviando em anexo, o processo para a prestação de serviços técnicos de Contratação de empresa para aquisição de 5 licenças de Software HP Open View Network Node Manager Enterprise v.620, ou superior, devidamente autorizado pelo Comitê de Avaliação das Contratações Estratégicas, conforme Parecer/CACE 077/2003, para as providências dessa CPL/AC com vistas à abertura de processo licitatório, na modalidade Pregão.

O DERCO informa que, a presente contratação faz-se necessária, tendo em vista o objetivo de ampliar a quantidade de licenças da ferramenta atual de gerência pró-ativa, que verifica a disponibilidade dos elementos de rede que correspondem aos roteadores e antenas satélites instaladas nas Unidades de Atendimento (agencias, Unidades Administrativas e Operacionais e, ainda, os servidores, roteadores e switches localizados nos Centros Corporativos de Dados (CCD) em Brasília e em São Paulo.

O valor estimado da contratação é de R$ 423.058,58 (quatrocentos e vinte e três mil, cinqüenta e oito reais e cinqüenta e oito centavos), resultado da pesquisa de mercado realizada pelo DERCO, conforme demonstrado no quadro de estimativa de preços, em anexo.

Relativamente ao bloqueio orçamentário, informamos que o mesmo está sendo retificado pelo DERCO, na Conta: 09.02., Atividade: 17.1.01 e será encaminhado posteriormente.

Seguem em anexo: Parecer/CACE – 077/2003, Quadro de Estimativa de Preços, Termo de Referência, Proposta e demais documentos pertinentes ao assunto em questão.

Atenciosamente,

Adauto Tameirão Machado
Chefe do Departamento de Contratação e Administração de Material - DECAM

Antônio Francisco da Silva Filho
Subchefe/DECAM
Mat. 8.010.819-9

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0587
3740
Doc:

\\sac0424\ac\dirad\decam\dcon\documentos 2003\ci\ci4.737_03 licenças software hp open view_cpl_ac.doc
Anexos
TT/tt

CORREIOS

Comissão Permanente de Licitação da Administração Central - CPL/AC

CPL/AC RCT

MAPA COMPARATIVO DE PREÇOS

Licitação: Pregão n.º 118/2003 - CPL/AC **Data de Abertura**: 16/12/2003

ITEM	DESCRIÇÃO	UNID.	QTDE.	EMPRESA/MELHOR LANCE /UNITÁRIO (R$)			VALOR TOTAL REFERÊNCIA (R$) *	VALOR TOTAL CONTRATAÇÃO (R$)
				E-TAILOR	TM SOLUTIONS	HP		
01	Licenças do software HP Open View Network Node Enterprise Versão 6.2 ou superior, incluindo os serviços de atendimento e suporte técnico.	Um	05	87.600,00	87.200,00	**83.700,00**	84..611,71	**83.700,00**
							423.058,55	**418.500,00**

(*) *Valor de Referência fornecido pelo DECAM, com base na média dos valores da pesquisa de mercado.*

Empresa Vencedora

Validade da Proposta: 60 dias a contar da data de reunião de abertura da licitação.
Prazo de Execução/Entrega: Em até 10 dias, contados a partir da data da assinatura do contrato.
Condições de Pagamento: Em parcela única, no prazo de até dias após a emissão do Termo de Aceitação Final.

Maria Maria Coelho
Pregoeira

Equipe de Apoio

Gilberto Ferreira do Amaral

Cláudio Nunes Barbosa

Hélio Flauzino Garcia

Pedro Alberto da Silva Oliveira

Marise da Consolação Cerqueira Capella

João Batista Vieira de Carvalho

CPMI - CORREIOS
Fls. Nº 0588
3740
Doc.

ANEXO 4. DO RELATÓRIO/HOMOLOGAÇÃO/CPL/AC-065/2003

CORREIOS

Comissão Permanente de Licitação da Administração Central - CPL/AC

ATA DE REUNIÃO DE LICITAÇÃO
PREGÃO N.º 0118/2003 - CPL/AC

OBJETO: Aquisição de 05 licenças do software HP OPEN VIEW NET WORK NODE ENTERPRISE VERSÃO 6.2. OU SUPERIOR.

DIA/HORA: 16/12/2003 das 09:30 às 11:10 horas.

ASSUNTO: Esta Sessão destinou–se a abertura do Pregão n.º 0118/2003 objetivando a obtenção das propostas mais vantajosas para a Administração, por meio de lances verbais disputados entre os licitantes. Foram recebidos e abertos os envelopes das propostas econômicas e o envelope de habilitação da firma vencedora.

LOCAL: Sala de Reunião – CPL/AC, localizada no SBN, Quadra 01, Bloco "A" 4º andar, do Ed. Sede da ECT, em Brasília.

QUANTIDADE DE EDITAIS RETIRADOS: Foram retirados 09 (nove) exemplares do Edital, todos através do sistema magnético, via Internet.

CREDENCIADOS: Compareceram à Sessão 03(três) empresas relacionadas nesta ata.

ABERTURA DAS PROPOSTAS ECONÔMICAS: Após o credenciamento das participantes, procedeu-se a abertura dos envelopes e análise das propostas econômicas. Os preços unitários e totais cotados foram lidos para que os presentes tomassem conhecimento, conforme discriminado a seguir:

AQUISIÇÃO DE 05 LICENÇAS DO SOFTWARE HP OPEN VIEW NET WORK NODE ENTERPRISE VERSÃO 6.2. OU SUPERIOR, INCLUINDO SERVIÇOS DE ATENDIMENTO E SUPORTE TÉCNICO:

EMPRESAS	PREÇO UNITÁRIO (R$)	PREÇO TOTAL (R$)
E-TAILOR	**101.000,00**	**505.000,00**
TM Solutions	**99.000,00**	**495.000,00**
Hewlett-Packard	**95.000,00**	**475.000,00**

CLASSIFICAÇÃO DAS PROPOSTAS/RODADAS DE LANCES: Após a conferência das propostas, foram classificadas e autorizadas a dar lances, de acordo com a alínea "d-1" do subitem 7.3 do edital as empresas relacionadas a seguir, iniciando-se com a empresa **E-TAILOR E-TAILOR** e terminando com a empresa **Hewlett-Packard** vencedora deste do Pregão, com o preço unitário negociado de R$ 83.700,00.

EMPRESA	PROPOSTA ESCRITA	RODADAS DE LANCES				
		1ª	2ª	3ª	4ª	5ª
HP	95.000,00	93.600,00	91.800,00	87.800,00	83.800,00	83.700,00
TM	99.000,00	93.800,00	92.800,00	90.600,00	87.200,00	
E-TAILOR	101.000,00	94.800,00	93.000,00	90.800,00	87.600,00	

(*) Desistência de Lance.

PROS nº 03/2005 - CN - 1
CPMI - CORREIOS
0589
Fls. Nº
3740
Doc:

CORREIOS

Comissão Permanente de Licitação da Administração Central - CPL/AC

HABILITAÇÃO DA VENCEDORA: Após conferência de toda a documentação da empresa **HEWLETT-PACKARD BRASIL LTDA.** vencedora deste Pregão, a mesma foi considerada habilitada. Os envelopes das empresas **TM Solutions Tecnologia da Informação Ltda.** e **E-TAILOR Soluções em Tecnologia da Informática Ltda.** 2ª e 3ª colocadas ficarão em poder do Pregoeiro até a assinatura do contrato.

ADJUDICAÇÃO: O Pregoeiro declarou vencedora e adjudicou o objeto deste Pregão à empresa **HEWLETT-PACKARD BRASIL LTDA.**, CNPJ n.º 61.797.927/0001-55, com o preço unitário de R$ 83.700,00 e total de .R$ 418.500,00 (quatrocentos e dezoito mil e quinhentos reais). Para efeito de desembolso financeiro este valor não sofrerá alteração, tendo em vista que os softwares não são tributados pelo ICMS.

ENCERRAMENTO DA REUNIÃO: Nada mais havendo a tratar foi dada como encerrada a reunião, lavrada a presente Ata, que após lida e achada conforme, vai assinada pelo Pregoeiro e sua equipe e pelos representantes credenciados presentes ao ato.

Gilberto Ferreira do Amaral
Pregoeiro

3.160

Equipe de Apoio:

Pedro Alberto da Silva Oliveira

Hélio Flauzino Garcia

Cláudio Nunes Barbosa

Marise da Consolação Cerqueira Capella

João Batista Vieira de Carvalho

Ana Maria Santos
DERCO

Representantes credenciados e as respectivas Empresas:

1) Empresa: E-TAILOR Soluções em Tecnologia da Informática Ltda.
Nome Representante: Ítalo Eligio Togni
Telefax.: (61) 347-2610 Cel: (61) 8124-9611

2) Empresa: TM Solutions Tecnologia da Informação Ltda
Nome Representante: Mario Roberto Gimenes Silva
Tel: (11) 3887-8896 Fax: (11) 3884-4466

3) Empresa:. Hewlett-Packard Brasil Ltda
Nome Representante: José Eduardo Pires do Rio Ribeiro
Fone: (61) 329-6055 Fax: (61) 329-6055

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0590
3740
Doc:

ANEXO 6. DO RELATÓRIO/HOMOLOGAÇÃO/CPL/AC-065/2003

CORREIOS SISBLOQ Web

Diretoria Econômico-Financeira
Departamento de Orçamento e Custo

300
3.159

Emissão de Bloqueio Orçamentário
- Autorizado -

Diretoria Regional:	**01 - Administração Central**
No do Bloqueio:	**73236/2003**
Área Solicitante:	01340000 - DPTO DE REDE CORPORATIVA
Solicitado em:	04/09/2003
Projeto/Atividade:	17101 - Rede Corporativa
Conta:	80009020000 - EQUIPAMENTOS/MATERIAL PERMAMENTE
Finalidade:	Contratação de 5 licenças do SW HP OpenView referente ao projeto de Administração da Rede.
Bloqueio Ajustado:	68384
Data da Autorização:	10/09/2003

onograma de Execução

Mês	Ano	Valor - R$
12	2003	423.059,00

Valor Total do Bloqueio - R$ 423.059,00

DEORC
Jameson Reinaux da Cunha
80111157

Voltar

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0591
3740
Doc:

ATA DE REUNIÃO DE ADJUDICAÇÃO DO PREGOEIRO

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0592
3740
Doc:

CORREIOS

Comissão Permanente de Licitação da Administração Central - CPL/AC

CPL/AC ACT

MAPA COMPARATIVO DE PREÇOS

Licitação: Pregão n.º 118/2003 - CPL/AC **Data de Abertura**: 16/12/2003

ITEM	DESCRIÇÃO	UNID.	QTDE.	EMPRESA/MELHOR LANCE /UNITÁRIO (R$)			VALOR TOTAL REFERÊNCIA (R$) *	VALOR TOTAL CONTRATAÇÃO (R$)
				E-TAILOR	TM SOLUTIONS	HP		
01	Licenças do software HP Open View Network Node Enterprise Versão 6.2 ou superior, incluindo os serviços de atendimento e suporte técnico.	Um	05	87.600,00	87.200,00	**83.700,00**	84..611,71	**83.700,00**
							423.058,55	**418.500,00**

(*) *Valor de Referência fornecido pelo DECAM, com base na média dos valores da pesquisa de mercado.*

Empresa Vencedora

Validade da Proposta: 60 dias a contar da data de reunião de abertura da licitação.
Prazo de Execução/Entrega: Em até 10 dias, contados a partir da data da assinatura do contrato.
Condições de Pagamento: Em parcela única, no prazo de até dias após a emissão do Termo de Aceitação Final.

Maria Maria Coelho
Pregoeira

Equipe de Apoio

Gilberto Ferreira do Amaral

Cláudio Nunes Barbosa

Hélio Flauzino Garcia

Pedro Alberto da Silva Oliveira

Marise da Consolação Cerqueira Capella

João Batista Vieira de Carvalho

PROT.Nº 03/2005 - CA
CPMI - CORREIO
Fls. Nº 0593
Doc: 3740

3.157

ATA DE REUNIÃO DE LICITAÇÃO
PREGÃO N.º 0118/2003 - CPL/AC

OBJETO: Aquisição de 05 licenças do software HP OPEN VIEW NET WORK NODE ENTERPRISE VERSÃO 6.2. OU SUPERIOR.

DIA/HORA: 16/12/2003 das 09:30 às 11:10 horas.

ASSUNTO: Esta Sessão destinou–se a abertura do Pregão n.º 0118/2003 objetivando a obtenção das propostas mais vantajosas para a Administração, por meio de lances verbais disputados entre os licitantes. Foram recebidos e abertos os envelopes das propostas econômicas e o envelope de habilitação da firma vencedora.

LOCAL: Sala de Reunião – CPL/AC, localizada no SBN, Quadra 01, Bloco "A" 4º andar, do Ed. Sede da ECT, em Brasília.

QUANTIDADE DE EDITAIS RETIRADOS: Foram retirados 09 (nove) exemplares do Edital, todos através do sistema magnético, via Internet.

CREDENCIADOS: Compareceram à Sessão 03(três) empresas relacionadas nesta ata.

ABERTURA DAS PROPOSTAS ECONÔMICAS: Após o credenciamento das participantes, procedeu-se a abertura dos envelopes e análise das propostas econômicas. Os preços unitários e totais cotados foram lidos para que os presentes tomassem conhecimento, conforme discriminado a seguir:

AQUISIÇÃO DE 05 LICENÇAS DO SOFTWARE HP OPEN VIEW NET WORK NODE ENTERPRISE VERSÃO 6.2. OU SUPERIOR, INCLUINDO SERVIÇOS DE ATENDIMENTO E SUPORTE TÉCNICO:

EMPRESAS	PREÇO UNITÁRIO (R$)	PREÇO TOTAL (R$)
E-TAILOR	**101.000,00**	**505.000,00**
TM Solutions	**99.000,00**	**495.000,00**
Hewlett-Packard	**95.000,00**	**475.000,00**

CLASSIFICAÇÃO DAS PROPOSTAS/RODADAS DE LANCES: Após a conferência das propostas, foram classificadas e autorizadas a dar lances, de acordo com a alínea "d-1" do subitem 7.3 do edital as empresas relacionadas a seguir, iniciando-se com a empresa **E-TAILOR E-TAILOR** e terminando com a empresa **Hewlett-Packard** vencedora deste do Pregão, com o preço unitário negociado de R$ 83.700,00.

EMPRESA	PROPOSTA ESCRITA	RODADAS DE LANCES				
		1ª	2ª	3ª	4ª	5ª
HP	95.000,00	93.600,00	91.800,00	87.800,00	83.800,00	83.700,00
TM	99.000,00	93.800,00	92.800,00	90.600,00	87.200,00	
E-TAILOR	101.000,00	94.800,00	93.000,00	90.800,00	87.600,00	

(*) Desistência de Lance.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0594
Doc: 3740

3156

297 A

HABILITAÇÃO DA VENCEDORA: Após conferência de toda a documentação da empresa **HEWLETT-PACKARD BRASIL LTDA.** vencedora deste Pregão, a mesma foi considerada habilitada. Os envelopes das empresas **TM Solutions Tecnologia da Informação Ltda.** e **E-TAILOR Soluções em Tecnologia da Informática Ltda.** 2ª e 3ª colocadas ficarão em poder do Pregoeiro até a assinatura do contrato.

ADJUDICAÇÃO: O Pregoeiro declarou vencedora e adjudicou o objeto deste Pregão à empresa **HEWLETT-PACKARD BRASIL LTDA.**, CNPJ n.º 61.797.927/0001-55, com o preço unitário de R$ 83.700,00 e total de .R$ 418.500,00 (quatrocentos e dezoito mil e quinhentos reais). Para efeito de desembolso financeiro este valor não sofrerá alteração, tendo em vista que os softwares não são tributados pelo ICMS.

ENCERRAMENTO DA REUNIÃO: Nada mais havendo a tratar foi dada como encerrada a reunião, lavrada a presente Ata, que após lida e achada conforme, vai assinada pelo Pregoeiro e sua equipe e pelos representantes credenciados presentes ao ato.

Gilberto Ferreira do Amaral
Pregoeiro

Equipe de Apoio:

Pedro Alberto da Silva Oliveira

Hélio Flauzino Garcia

Cláudio Nunes Barbosa

Marise da Consolação Cerqueira Capella

João Batista Vieira de Carvalho

Ana Maria Santos
DERCO

Representantes credenciados e as respectivas Empresas:

1) Empresa: E-TAILOR Soluções em Tecnologia da Informática Ltda.
Nome Representante: Ítalo Eligio Togni
Telefax.: (61) 347-2610 Cel: (61) 8124-9611

2) Empresa: TM Solutions Tecnologia da Informação Ltda
Nome Representante: Mario Roberto Gimenes Silva
Tel: (11) 3887-8896 Fax: (11) 3884-4466

3) Empresa:. Hewlett-Packard Brasil Ltda
Nome Representante: José Eduardo Pires do Rio Ribeiro
Fone: (61) 329-6055 Fax: (61) 329-6055

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0595
3740
Doc:

DOCUMENTOS DE HABILITAÇÃO

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0596
3740
Doc:

CORREIOS

Comissão Permanente de Licitação da Administração Central - CPL / AC

3.155

2946

OBJETO	
Pregão n.º 0118/2003	Aquisição de 05 licenças do softwares HP OPEN VIEW NTE WORK NODE ENTERPRISE VERSÃO 6.2. OU SUPERIOR.
PATRIMÔNIO LÍQUIDO	
Exigido	R$ 30.000,00 (trinta mil reais)
Licitante	R$ 134.002.000,00
LICITANTE	
Nome / Razão Social	HEWLETT PACKARD BRASIL LTDA
CNPJ n.º	61.797.924/0001-55

Sim	Não	Documento	Data Expedição	Validade
X		**CRC / ECT**	20 / 03 / 2003	19 / 03 / 2004
–	–	**Contrato Social**	– – –	– – –
–	–	**Cadastro Geral de Contribuintes**	– / – / –	– / – / –
–	–	**Cadastro de Contribuintes Estadual**	– / – / –	– / – / –
–	–	**Cadastro de Contribuintes Municipal**	– / – / –	– / – / –
–	–	**Balanço Patrimonial**	– / – / –	– / – / –
X		**Certidão de Falência e Concordata**	17 / 11 / 2003	16 / 05 / 2004
X		**Certidão de Quitação de Tributos e Contribuições Federais**	19 / 11 / 2003	19 / 05 / 2004
X		**Certidão quanto a Dívida Ativa da União**	27 / 11 / 2003	26 / 05 / 2004
X		**Regularidade para com a Fazenda Estadual**	01 / 08 / 2003	01 / 02 / 2004
X		**Regularidade para com a Fazenda Municipal**	14 / 10 / 2003	13 / 04 / 2004
X		**CND (INSS)**	03 / 10 / 2003	02 / 01 / 2004
X		**FGTS**	17 / 11 / 2003	16 / 12 / 2004
X		**Atestado de Capacidade Técnica**		
X		**Declaração de cumprimento ao Disposto inciso XXXIII do Art. 7ª da Constituição Federal**		

Brasília/DF, 16 de dezembro de 2003.

DE ACORDO

(Assinatura do Representante da Licitante)

Assinatura do Membro da Equipe - responsável pela análise dos documentos

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0597
Doc 3740

JBVC/jbvc
F:\DIRAD\CPL\Documentos2003\Ficha de Análise\Ficha de Análise PR0118_2003 Aquisição de software HP OPEN VIEW.doc

PROPOSTAS ECONÔMICAS

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0598
3740
Doc:



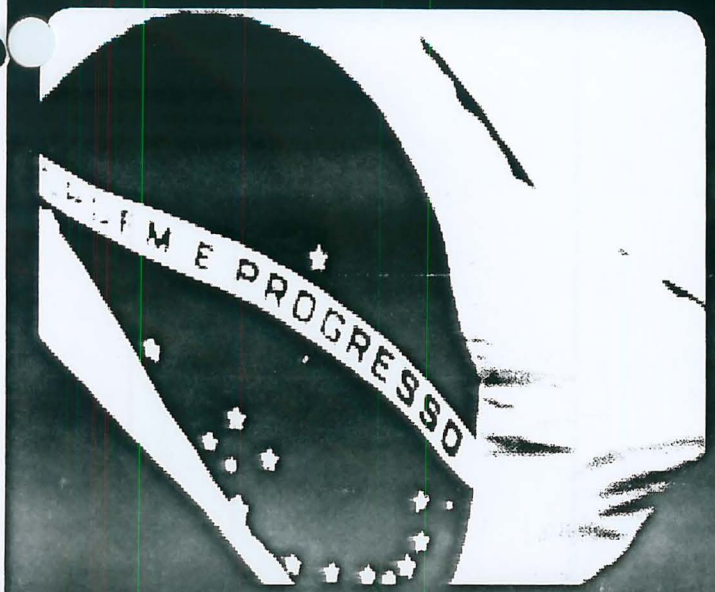
invent

Pregão nº 118/2003 – CPL/AC

Habilitação

16 de dezembro de 2003





CORREIOS

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0599
3740
Doc:

3.153

invent

habilitação

Hewlett-Packard Brasil Ltda.

CORREIOS

Pregão nº 118/2003 - CPL/AC

16 de dezembro de 2003

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0600
3740
Doc:

293

Hewlett-Packard Brasil Ltda.
Alameda Rio Negro, 750
Alphaville - 06454-000
Barueri - SP
Brasil

3.152

José Eduardo Ribeiro
Representante Legal
Tel.: (61) 329-6055
Cel.: (61) 9974-6565
josé-eduardo_ribeiro@hp.com

São Paulo, 16 de dezembro de 2003

Áos
CORREIOS

Ref.: Pregão nº 118/2003 – CPL/AC

Prezados Senhores,

A Hewlett-Packard Brasil Ltda. está honrada em responder sua solicitação. Estamos encaminhando para apreciação nossa habilitação para Pregão nº 118/2003 - CPL/AC

Estamos confiantes que a nossa proposta atenderá suas necessidades atuais e futuras. Para maiores esclarecimentos e informações, não hesite em contatar-nos.

A Hewlett-Packard Brasil Ltda. possui pessoal, tecnologia, experiência e comprometimento que resultarão em uma parceria perfeita com vocês.

Atenciosamente,

José Eduardo Ribeiro

Representante Legal

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0601
3740
Doc:

Índice

1. Certificado de Registro Cadastral
2. Regularidade Fiscal
3. Qualificação Técnica

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0602
3740
Doc:

3.150

291

1. Certificado de Registro Cadastral

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0603
3740
Doc:

CORREIOS

EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS
DIRETORIA REGIONAL DE SÃO PAULO - METROPOLITANA

290

GERAD DR SPM

CERTIFICADO DE REGISTRO CADASTRAL

3149

Código	7201158
Razão Social	HEWLETT-PACKARD BRASIL LTDA
Endereço	ALAMEDA RIO NEGRO, 750 FUNDOS 1º ANDAR SALA 4
Bairro	ALPHAVILLE
Cidade/UF	BARUERI / SP
CEP	06454000

CNPJ	61.797.924/0001-55	Inscrição Estadual	206203572117
Capital Social	370.601.469,00	Patrimônio Líquido	134.002.000,00

Colégio Notarial do Brasil-SP
AUTENTICAÇÃO
0109 ... 0023
Oficial de Registro Civil das Pessoas Naturais e Tabel... de Notas do Distrito de Aldeia - Comarca de Barueri - R. Pe. Donizete T. de Lima, 3... - Vila São Francis... Telefones: (011) 4198-2164 / 3076 Fax: 4198-32...
AUTENTICAÇÃO
Aldeia 15 JUL. 2003
(Válido somente c... o selo de autenticidad...
Autentico a presente cópia reprográfica conforme ao original... mim apresentado do que dou fé.
Ivo Trevizano - Oficial / Tabelião
Alessandro de Souza Matos - Escr. Autorizado
Adriano Pereira da Silva - Escr. Autorizado
Roseli de Lurdes Honda e Castro - Escr. Autorizada
Larissa Fieri Trevizano - Escr. Autorizada
1,10

RAMO DE ATIVIDADE

96	- SERVIÇOS DE CABEAÇÃO ESTRUTURADA
204	- SOFTWARE
205	- MÁQUINAS/EQUIPAMENTO INFORMÁTICA
207	- MANUT MÁQ/EQUIP INFORMÁTICA
212	- SERVIÇOS DE INFORMÁTICA - DIVERSOS

CERTIDÕES DO FORNECEDOR

CERTIDÃO	EMISSÃO	VENCIMENTO
CRC - CERTIFICADO DE REGISTRO CADASTRAL	20/03/2003	19/03/2004

OBSERVAÇÕES

1. OS PEDIDOS DE ALTERAÇÃO E DE SEGUNDA VIA, QUE PODERÃO SER REQUERIDOS A QUALQUER TEMPO, SERÃO ATENDIDOS NO PRAZO MÁXIMO DE 3 (TRES) DIAS ÚTEIS, DESDE QUE SOLICITADOS POR ESCRITO, DEVIDAMENTE JUSTIFICADOS.
2. A RENOVAÇÃO DA INSCRIÇÃO DEVERÁ SER SOLICITADA COM ANTECEDÊNCIA DE 05 (CINCO) DIAS ÚTEIS DO TÉRMINO DA VALIDADE DESTE CERTIFICADO.
2.1. A NÃO MANIFESTAÇÃO DA FIRMA ATÉ O PRAZO LIMITE, RESULTARÁ NA EXCLUSÃO AUTOMÁTICA DO REGISTRO CADASTRAL.
2.2. TRANSCORRIDOS 60 (SESSENTA) DIAS APÓS O VENCIMENTO DESTE CERTIFICADO, NÃO HAVENDO QUALQUER PRONUNCIAMENTO DA FIRMA CADASTRADA, A DOCUMENTAÇÃO PERTINENTE SERÁ DESTRUÍDA, SEM QUE CAIBA QUALQUER RECLAMAÇÃO POSTERIOR.
3. O REGISTRO CADASTRAL SERÁ CANCELADO NOS SEGUINTES CASOS:
a) QUANDO A FIRMA FOR IMPEDIDA DE PARTICIPAR DE LICITAÇÃO E CONTRATAR COM A ECT;
b) QUANDO FOR DECRETADA INIDÔNEA POR QUALQUER ÓRGÃO PÚBLICO DA ADMINISTRAÇÃO DIRETA OU INDIRETA;
c) QUANDO TIVER REQUERIDO OU DECRETADO PROCESSO DE FALÊNCIA OU DE CONCORDATA;
d) QUANDO A FIRMA ENCERRAR SUAS ATIVIDADES.
4. CRC EMITIDO DE ACORDO COM A LEI NÚMERO 8.666/93.

Certificamos que o fornecedor acima qualificado está inscrito no cadastro de fornecedores da ECT estando habilitado a participar das Licitações promovidas por qualquer de suas dependências para os ramos de atividades indicados desde que satisfaçam também, as condições estabelecidas nos respectivos editais.

SAO PAULO/SP, 20 DE MARÇO DE 2003.

Ass: _____
Etelvina Rodrigues Nascimento
Ch. SPCD/SUCON/GERAD/DR/SPM

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0604
3740
Doc: _____

3148
209

2. Qualificação Econômica

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0605
Doc: 3740

PASSAR COLA AQUI

288

PODER JUDICIÁRIO
SÃO PAULO
CERTIDÃO DE DISTRIBUIÇÕES CÍVEIS NA COMARCA

BARUERI

Nº 926667

INSTRUÇÕES DE PREENCHIMENTO NO VERSO

1 - Nome
HEWLETT PACKARD BRASIL LTDA

CNPJ/CPF 61.797.924/0001-55 RG

2 - Esta certidão corresponde à existência ou não de ações cíveis, de família, execuções estaduais e municipais, no período de:

| | 5 anos	|X| 10 anos	| | 20 anos	| | acima de 20 anos

3 - Opções:

		Prazo para entrega da Certidão
| |	A - Processos em Andamento	05 Dias
| |	B - Inventário/Arrolamento/Testamento	05 Dias
|X|	C - Falência/Concordata	05 Dias
| |	D - Processos Extintos e em Andamento	10 Dias

E FAZ. FEDERAL

3.147

Observação: Conforme item 47 Capítulo VII das NSCGJ: Nas Certidões expedidas pelos Distribuidores Cíveis não constarão os processos extintos, salvo se houver autorização do Juiz Corregedor Permanente do respectivo Ofício ou Seção.

4 - CERTIDÃO NEGATIVA - Pesquisada até 13 NOV 2003

NADA CONSTA nos fichários, contra o nome pesquisado tal como grafado acima.

Pesquisador

São Paulo, 17 NOV 2003

5 - CERTIDÃO POSITIVA - Pesquisada até

contra o nome pesquisado, tal como grafado acima, **CONSTA(M)** nos fichários a(s) seguinte(s) distribuição(ões):

Ana Aparecida Baldi
Escr. Técnico Jud.
Matr. nº 319.918

OFÍCIO DO DISTRIBUIDOR DA COM. DE BARUERI
OBS: a pesquisa exclui o município de Carapicuíba a partir de 11/83 e de Jandira a partir de 08/89.

Chancela da Escrivã Diretora
Isabel Cristina H. W. Araujo
Matr. 310.637

Esta certidão não aponta, ordinariamente, os processos em que a pessoa, cujo nome foi pesquisado, figura como autor.

Colégio Notarial do Brasil - SP
AUTENTICAÇÃO
0109AA29...
VALIDA SOMENTE COM A AUTENTICAÇÃO DO ANVERSO

Pesquisador

São Paulo,

6 - SERVIÇO TÉCNICO DE INFORMAÇÕES CÍVEIS - Pretendo receber a Certidão

| | NO GUICHÊ - Forum Cível (Pça. João Mendes Jr. - Térreo - São Paulo)	| | PELO CORREIO - Preencha o Verso e não destaque o protocolo

ATENÇÃO: Esta Certidão somente terá valor mediante

a) A chancela do Diretor; e

b) Autenticação de recebimento das custas

Autenticação Mecânica	Carimbo do Órgão Arrecadador
ENC 0761 12Nov2003 159 9,00RD 018	Esta certidão só terá validade se for Original, rasurada ou com prazo vencido. Da Lei 8666/93 (Lei de Licitações).

10/02 - 10/0414-- DISTRIBUIÇÃO GRATUITA - PROIBIDA A VENDA

CRMI CORREIOS
Fls. Nº 0606
Doc: 3740

ATENÇÃO: QUALQUER RASURA TORNARÁ NULO ESTE DOCUMENTO

DOBRA

PODER JUDICIÁRIO

São Paulo

SELO

Nome _____

Endereço _____

☐☐☐☐☐-☐☐☐ _____ Cidade _____ Estado

REMETENTE: SERVIÇO TÉCNICO DE INFORMAÇÕES CIVEIS

ENDEREÇO: Praça João Mendes Jr. - Térreo - São Paulo

CEP: 01501-020

Colegio Notarial do Brasil SP

AUTENTICAÇÃO

0109AA29356[illegible]

Oficial de Registro Civil das Pessoas Naturais e Tabelião de Notas do Distrito de Aldeia [illegible] Barueri
R. Pe. Donizete T. de Lima, 3[illegible] - Vila São Francisco
Telefones: (011) 4198-2164 / 3078 Fax: 4198-3284
AUTENTICAÇÃO

26 NOV. 2003

(Válido somente com o selo de autenticidade)

Autentico a presente cópia reprográfica conforme ao original a mim apresentado do que dou fé. 1,10
Ivo Trevizano - Oficial / Tabelião
Larissa Fiori Trevizano - Escr. Autorizada

INSTRUÇÕES DE PREENCHIMENTO

Campo 1: - O pedido de certidão deverá ser preenchido a máquina, ou em letra de forma, legível, com tinta indelével azul ou preta. Válido apenas um nome por pedido;
- Não deverão ser abreviados nomes;
- Entre cada nome será deixado um campo em branco;
- Indicar, sempre que possível, o CNPJ, CPF ou RG do nome a ser pesquisado.

Campo 2: - O interessado poderá optar por 5, 10, 20 e acima de 20 anos como período para pesquisa. No silêncio, entender-se-á pesquisa por 10 anos.

Campo 3: - A certidão poderá ser expedida nas seguintes opções: Processos em Andamento; Inventário/Arrolamento/Testamento; Falência/Concordata e Processos Extintos e em Andamento. No silêncio enterder-se-á opção por Processos em Andamento.
VÁLIDA APENAS UMA OPÇÃO POR PEDIDO.
a) Na opção **A - Processos em Andamento**, serão certificadas todas as distribuições em andamento, quando existentes.
b) Na opção **B - Inventário/Arrolamento/Testamento**, serão certificadas apenas as distribuições dessa natureza em nome da pessoa falecida, quando existentes;
c) Na opção **C - Falência/Concordata**, serão certificados apenas os feitos dessa natureza, quando existentes.
d) Na opção **D - Processos Extintos e em Andamento**, o pedido será submetido à autorização judicial, caso em que prazo de expedição da Certidão será de 10 (dez) dias.

Campo 6: - A certidão será entregue no andar Térreo do Forum Central, Pça. João Mendes, ou remetida pelo correio, se o interessado assinalar o campo específico;
- As certidões não retiradas depois de 30 (trinta) dias, contados do prazo marcado para a entrega, poderão ser inutilizadas com perda das custas;
- A inobservância de qualquer dos itens previstos no CAMPO 1 importará na impossibilidade de atendimento ao pedido.

3.145
RH

284
A.

3. Regaularidade Fiscal

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0607
3740
Doc:

MINISTERIO DA FAZENDA
SECRETARIA DA RECEITA FEDERAL

CERTIDAO POSITIVA DE DEBITOS DE TRIBUTOS E CONTRIBUICOES FEDERAIS, COM EFEITOS DE NEGATIVA

285

(SUJEITA A CONFIRMACAO DE AUTENTICIDADE NA PAGINA DA SRF NA INTERNET, NO ENDERECO <HTTP://WWW.RECEITA.FAZENDA.GOV.BR>)

VALIDA ATE: 19/05/2004 - EMITIDA EM: 19/11/2003 NRO.: 6.507.377

3.144

CNPJ: 61.797.924/0001-55
HEWLETT-PACKARD BRASIL LTDA
AL RIO NEGRO 750 FUNDOS 1 AND S 4 ALPHAVILLE
CEP: 06454-000 BARUERI SP

CONFORME DISPOSTO NO ART. 206 DA LEI NRO 5.172, DE 25 DE OUTUBRO DE 1966, (CODIGO TRIBUTARIO NACIONAL), ESTE DOCUMENTO TEM OS MESMOS EFEITOS DA CERTIDAO NEGATIVA EXPEDIDA DE ACORDO COM O ART. 205 DO REFERIDO CODIGO, POR EXISTIREM EM NOME DO CONTRIBUINTE ACIMA IDENTIFICADO SOMENTE DEBITOS EM RELACAO AOS TRIBUTOS E CONTRIBUICOES FEDERAIS NA CONDICAO ABAIXO ESPECIFICADA:

EXIGIBILIDADE ESTA SUSPENSA NOS TERMOS DO ART. 151 DO CTN:
- CONTENCIOSO ADMINISTRATIVO:
  IRPJ, CONTRIBUICAO SOCIAL, COFINS, PIS/PASEP, IPI, FONTE, II, MULTAS
- MEDIDA JUDICIAL:
  PIS/PASEP, MULTAS

ESTA CERTIDAO REFERE-SE EXCLUSIVAMENTE A SITUACAO DO CONTRIBUINTE NO AMBITO DA SECRETARIA DA RECEITA FEDERAL, NAO CONSTITUINDO, POR CONSEGUINTE, PROVA DE INEXISTENCIA DE DEBITOS INSCRITOS EM DIVIDA ATIVA DA UNIAO, ADMINISTRADOS PELA PROCURADORIA GERAL DA FAZENDA NACIONAL.

ESTA CERTIDAO ABRANGE SOMENTE O ESTABELECIMENTO ACIMA IDENTIFICADO

EMITIDA GRATUITAMENTE

CARIMBO,DATA E ASSINATURA

ARF BARUERI 19/11/03
SERGIO SANT'ANNA MELHEM
Agente - TRF SIAPECAD 60.353
Delegação de Competência
Portaria nº 148 de 25/10/2001

Oficial de Registro Civil das Pessoas Naturais e Tabelião de Notas do Distrito de Aldeia - Comarca de Barueri
R. Pe. Donizete T. de Lima, 39 - Vila São Francisco
Telefones: (011) 4198-2164 / 3076 Fax: 4198-3284
Aldeia 20 NOV 2003 (Válido somente com o selo de autenticidade)
Autentico a presente cópia/reprodução conforme o original a mim apresentado do(a)
Ivo Trevizano - Oficial/Tabelião
Larissa Fieri Trevizano - Escrevente Autorizada

Colégio Notarial do Brasil - SP
AUTENTICAÇÃO
0109AA282393

EMITIDA COM BASE NA IN/SRF 93, DE 23/11/2001

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0608
3740
Doc:

MINISTÉRIO DA FAZENDA
PROCURADORIA-GERAL DA FAZENDA NACIONAL

3143

CERTIDÃO QUANTO À DÍVIDA ATIVA DA UNIÃO

NEGATIVA

CNPJ
61.797.924/0001-55

Nome Completo
HEWLETT-PACKARD BRASIL LTDA

Ressalvado o direito de a Fazenda Nacional inscrever e cobrar as dívidas que venham a ser apuradas, certifica-se, para os fins de direito, que, analisados os registros da Dívida Ativa da União, verificou-se a **NÃO EXISTÊNCIA de INSCRIÇÕES** em nome do contribuinte acima identificado. E, para constar, foi extraída, por intermédio da Internet (rede mundial de computadores), esta certidão **NEGATIVA**.

ASPECTOS JURÍDICOS DE VALIDADE

Esta certidão é fornecida gratuitamente tendo validade por 30 dias (Portaria PGFN nº 22, de 19 de janeiro de 2001), não prevalecendo sobre certidões emitidas posteriormente.

Decreto-lei nº 147, de 03 de fevereiro de 1967: "Art. 62. Em todos os casos em que a lei exigir a apresentação de provas de quitação de tributos federais, incluir-se-á, obrigatoriamente, dentre aquelas, a certidão negativa de inscrição de dívida ativa da União, fornecida pela Procuradoria da Fazenda Nacional competente."

ASPECTOS TÉCNICOS DE VALIDADE

Emissão às 16:55:45 do dia 27/11/2003

Código de Controle da Certidão: 2649.1088.54D5.DC87

Tanto a veracidade da informação quanto a manutenção da condição de não devedor poderá ser verificada na seguinte página na Internet: **http://www.pgfn.fazenda.gov.br**

Atenção: Qualquer rasura ou emenda INVALIDARÁ este documento.

Colegio Notarial do Brasil - SP
AUTENTICAÇÃO
0109AA297906

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0609
Doc: 3740

FOLHA UNICA

GOVERNO DO ESTADO DE SAO PAULO

SECRETARIA DE ESTADO DOS NEGOCIOS DA FAZENDA

COORDENACAO DA ADMINISTRACAO TRIBUTARIA

DIRETORIA DE ARRECADACAO

N. CERTIDAO

2.972/03

283

3142

C E R T I D A O

CONTRIBUINTE - HEWLETT-PACKARD BRASIL LTDA
ENDERECO - ALM RIO NEGRO, 00750 - FUN 4 CEP - 06.454-000
BAIRRO - INDUSTRIA MUNICIPIO - BARUERI
INSCRICAO ESTADUAL - 206.203.572.117
C.G.C. - 61797924/0001-55 C.N.A.E - 5163-2/02

INEXISTEM DEBITOS FISCAIS RELATIVOS AO ICM/ICMS E OUTROS TRIBUTOS (IPVA, AIR, ITBI-CAUSA MORTIS/ITCMD), INSCRITOS NA DIVIDA ATIVA ATE A DATA DE EMISSAO DESTE DOCUMENTO.

..*.*.*.*.*.*.*.*.

*.
*.
*.
*.
*.
*.
*.
*.
*.
*.
..*.*.*.*.*.*.*.*.*

FINALIDADE: CONCORRENCIA PUBLICA

1- A PRESENTE CERTIDAO SO E VALIDA EM RELACAO AO INTERESSADO E DEMAIS DADOS INDICADOS.

2- FICA RESSALVADO O DIREITO DA FAZENDA DO ESTADO DE EXIGIR, A QUALQUER TEMPO, CREDITOS TRIBUTARIOS QUE VENHAM A SER APURADOS.

3- A TAXA DE FISCALIZACAO E SERVICOS DEVIDA FOI RECOLHIDA NOS TERMOS DA LEGISLACAO VIGENTE.

4- PRAZO DE VALIDADE DA CERTIDAO: 06 (SEIS) MESES CONFORME PORTARIA CAT NR. 20 DE 01/04/98 (DOE DE 02/04/98)

LOCAL DE EMISSAO:	DATA DE EMISSAO:
DRT/14-CRA-OSASCO	01/08/2003
EMITIDO POR:	RESPONSAVEL:
JOAO JOSE DE FREITAS FILHO	ROSA MARIA PINTO

DSCF81

Colegio Notarial do Brasil SP
AUTENTICADA
0109AA284589

REGISTRO CIVIL E TABELIONATO
BARUERI - SP

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0610
3740
Doc:

PREFEITURA MUNICIPAL DE BARUERI

Estado de São Paulo

182

SECRETARIA DE FINANÇAS
Departamento de Arrecadação
Coordenadoria de Fiscalização de Tributos Mobiliários

Certidão n.º 02454/2003

3.141

JOSÉ ANTONIO G. DA SILVA, Diretor de Arrecadação da Prefeitura Municipal de Barueri, Estado de São Paulo, no uso de suas atribuições legais, **CERTIFICA**, de acordo com o despacho exarado no requerimento protocolado sob o nº **36860/2003 em 13/10/2003**, que revendo os livros de registro a cargo do **Departamento de Arrecadação (I.S.S.Q.N. TAXAS MOBILIÁRIAS) e Tributos Imobiliários (IPTU, TAXAS DE SERVIÇOS URBANOS, TAXAS DE COMBATE E EXTINÇÃO DE INCÊNDIO)**, verificou que a empresa **HEWLETT-PACKARD BRASIL LTDA, CNPJ N.º 61797924000155**, estabelecida na **ALAMEDA RIO NEGRO,750 - 01ºANDAR - FUNDOS - SALA: 04 -ALPHAVILLE CENTRO INDUSTR E EMPRESARIAL - BARUERI - SP**, inscrito sob n.º **5.00878-8**, não tem débito junto à Fazenda Municipal, inscrita ou não em **Dívida Ativa**. O referido é verdade e dou fé. **Certifico, outrossim, que fica ressalvado o direito da Fazenda Pública do Município na cobrança de débitos que venham a ser apurados ou que se verifiquem a qualquer tempo, inclusive em relação aos tributos e períodos referidos nesta certidão.**

CERTIDÃO VÁLIDA POR NOVENTA DIAS.

Prefeitura Municipal de Barueri, 14 de outubro de 2003

JOSÉ ANTONIO G. DA SILVA
Diretor de Arrecadação

Colégio Notarial do Brasil - SP
AUTENTICAÇÃO
01 09AA284650

REGISTRO CIVIL DE BELIONATO ALDEIA BARUERI - SP

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0611
Doc: 3740

PREVIDÊNCIA SOCIAL
A seguradora do trabalhador brasileiro

PREVNet

281
A.

CERTIDÃO POSITIVA DE DÉBITO COM EFEITOS DE NEGATIVA

3.140
CH

Nº 125622003-21028040

DADOS DO SUJEITO PASSIVO:

CNPJ: 61.797.924/0001-55
NOME: HEWLETT-PACKARD BRASIL LTDA.
ENDERECO: AL RIO NEGRO 750 2. ANDAR , SALA 4
BAIRRO OU DISTRITO: ALPHAVILLE
MUNICIPIO: BARUERI
ESTADO: SP
CEP: 06454-000

Colégio Notarial do Brasil - SP
AUTENTICA CAD
0109AA298619
04 DEZ. 2003

FINALIDADE DA CERTIDÃO:

QUAISQUER DAS FINALIDADES PREVISTAS NAS LEIS 8.212, DE 24 DE JULHO DE 1991, E ALTERACOES, EXCETO PARA:

- AVERBACAO DE CONSTRUCAO CIVIL EM IMOVEL;
- REDUCAO DE CAPITAL SOCIAL E TRANSFERENCIA DE CONTROLE DE COTAS DE SOCIEDADES DE RESPONSABILIDADE LIMITADA;
- BAIXA DE FIRMA INDIVIDUAL, CISAO TOTAL OU PARCIAL, TRANSFORMACAO OU EXTINCAO DE ENTIDADE OU SOCIEDADE COMERCIAL OU CIVIL.

E CERTIFICADO, NA FORMA DO DISPOSTO NA LEI No 8.212/91 E ALTERACOES E NO CODIGO TRIBUTARIO NACIONAL, LEI 5.172/66, QUE, EM NOME DO SUJEITO PASSIVO ACIMA IDENTIFICADO, CONSTA A EXISTENCIA DOS DEBITOS A SEGUIR RELACIONADOS, CUJA EXIGIBILIDADE ENCONTRA-SE SUSPENSA, NAO SENDO IMPEDITIVOS A EMISSAO DESTA CERTIDAO, PARA A FINALIDADE DISCRIMINADA:

320525996 320526003 325938296 325938407 352306106 352306114 352306149

VALIDA PARA TODOS OS ESTABELECIMENTOS DA EMPRESA, MATRIZ E FILIAIS.

A ACEITACAO DA PRESENTE CERTIDAO ESTA CONDICIONADA A VERIFICACAO DE SUA VALIDADE NA INTERNET, NO ENDERECO www.previdenciasocial.gov.br, OU EM QUALQUER AGENCIA DA PREVIDENCIA SOCIAL OU UNIDADE AVANCADA DE ATENDIMENTO DA PREVIDENCIA SOCIAL.
DEVERA SER OBSERVADA A FINALIDADE PARA A QUAL FOI EMITIDA.

EMITIDA EM, 03 DE OUTUBRO DE 2003.
COM VALIDADE ATE 01/01/2004 .
VALIDA POR 90 DIAS DA DATA DA SUA EMISSAO.

PREVIDÊNCIA SOCIAL. A SEGURADORA DO TRABALHADOR BRASILEIRO.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0612
3740
Doc:

CAIXA
CAIXA ECONÔMICA FEDERAL

Certificado de Regularidade do FGTS - CRF

280
CA.

3.139
Pf

Inscrição: 61797924/0001-55
Razão Social: HEWLETT PACKARD BRASIL LTDA
Endereço: AL RIO NEGRO 750 750 1º ANDAR / ALPHAVILLE / BARUERI / SP / 6454-000

A Caixa Econômica Federal, no uso da atribuição que lhe confere o Art. 7, da Lei 8.036, de 11 de maio de 1990, certifica que, nesta data, a empresa acima identificada encontra-se em situação regular perante o Fundo de Garantia do Tempo de Serviço - FGTS.

O presente Certificado não servirá de prova contra cobrança de quaisquer débitos referentes a contribuições e/ou encargos devidos, decorrentes das obrigações com o FGTS.

Emitido em atendimento a determinação judicial.

Validade: 17/11/2003 a 16/12/2003

Certificação Número: 2003111709173423557998

Informação obtida em 17/11/2003, às 09:30.

Utilização deste Certificado para os fins previstos em Lei está condicionada à verificação de autenticidade no site da Caixa: **www.caixa.gov.br**

Colégio Notarial do Brasil - SP
AUTENTICAÇÃO
0109AA279468

Oficial de Registro Civil das Pessoas Naturais e Tabelião
Distrito de Aldeia - Comarca de Barueri
Rua da Lima, 35 - Vila São Francisco
4198-2164 / 3078 Fax: 4198-3284
AUTENTICAÇÃO
Aldeia 17 NOV. 2003
(Válido somente com o selo de autenticidade)
Autentico a presente cópia reprográfica conforme ao original a mim apresentado do que dou fé. 1,10
Ivo Trevizano - Oficial / Tabelião
Larissa Fieri Trevizano - Escr. Autorizada

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0613
Doc: 3740

279

3.138

Governo do Estado de São Paulo

POSTO FISCAL ELETRÔNICO

SECRETARIA DA FAZENDA DE SÃO PAULO

Simplificando a vida do Contribuinte

Serviços Contribuinte | Sugestões | Voltar

Deca . Consulta . Contribuinte

Estabelecimento

Inscrição Estadual	Situação	Data da Situação
206.203.572.117	CONTRIBUINTE ATIVO	11/11/2002

Posto Fiscal	DRT
PF: 206 - BARUERI	DRT: 14 - OSASCO

Nome ou Razão Social
HEWLETT-PACKARD BRASIL LTDA

Nome Fantasia

CNPJ	NIRE	Início Atividade
61.797.924/0001-55	35.217.669.190	11/11/2002

Capital Social	Tipo de Estabelecimento	Franquia
370.601.469,00	MATRIZ	NENHUMA

Tipo Jurídico
Sociedade por Quotas de Responsabilidade

Início de Regime	Regime de Apuração	Substituição Tributária
11/11/2002	NORMAL RPA	NÃO

Endereço

Tipo	Logradouro	Número
ALAMEDA	RIO NEGRO	750

Complemento	Bairro	CEP
FUNDOS 1º AND SALA 4	ALPHAVILLE INDUSTRIA	06.454-000

Município	UF
BARUERI	SP

Comunicações

DDD Fone	Telefone	DDD Fax	Fax
(011)	4197-8332	(011)	41978219

e-mail
jose-carlos.cordeiro@hp.com

Colégio Notarial do Brasil - SP
REGISTRO CIVIL E TABELIONATO
AUTENTICAÇÃO
ALDEIA BARUERI - SP
0109AA284721

CNAE

Início CNAE	CNAE	Descrição do CNAE
01/08/2003	5165-9/01	Comércio atacadista de equipamentos de informática, partes e peças

Data CPR	CPR Normal	CPR-ST

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0614
3740
Doc:

278
A.

3.137
9

01/08/2003	1031	

Contabilista

Tipo CRC	CRC	Documento
Contabilista	1SP148957/O-0	178.502.581-34

Participante 1

Situação	Data da Situação
Ativo	11/11/2002

Tipo de Participação	Assina pela Empresa
Gerente Delegado (contrato social)	SIM

Nome
CARLOS ROCHA RIBEIRO DA SILVA

Documento	RG
405.086.097-04	17817822SP

Tipo	Logradouro	Número
AVENIDA	PROF RUBENS GOMES G DE SOUZA	1359

Complemento	Bairro	CEP
	BROOKLYN	04.640-000

Município	UF
SÃO PAULO	SP

DDD Fone	Telefone	DDD Fax	Fax
(011)	4197-8332	(011)	4197-8332

e-mail

Participante 2

Situação	Data da Situação
Ativo	11/11/2002

Tipo de Participação	Assina pela Empresa
Gerente Delegado (contrato social)	SIM

Nome
IVO ROMANI

Documento	RG
903.621.798-91	7187356-9 SP

Tipo	Logradouro	Número
RUA	SERGIPE	309

Complemento	Bairro	CEP
APTO 3	HIGIENOPOLIS	01.243-001

Município	UF
SÃO PAULO	SP

DDD Fone	Telefone	DDD Fax	Fax
(011)	4197-8332	(011)	4197-8219

e-mail

Colégio Notarial do Brasil - SP
AUTENTICAÇÃO
REGISTRO CIVIL E TABELIONATO
ALDEIA BARUERI - SP
0109AA284722

PCS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0615
Doc. 3740

3.136
04

Participante 3

Situação	Data da Situação
Ativo	31/01/2003

Tipo de Participação	Assina pela Empresa
Gerente Delegado (contrato social)	SIM

Nome
DÉCIO DOS SANTOS ALARCON

Documento	RG
012.139.148-50	78111316SP

Tipo	Logradouro	Número
RUA	GUARARAPES	78

Complemento	Bairro	CEP
AP 15	BROOKLIN PAULISTA	04.561-000

Município	UF
SÃO PAULO	SP

DDD Fone	Telefone	DDD Fax	Fax

e-mail

Sócio Estrangeiro 1

Situação	Data da Situação
Ativo	26/05/2003

Tipo de Participação
Socio P. Juridica com Sede no Exterior

Nome
HEWLETT-PACKARD EUROPE B.V.

CPF Representante	País
01213914850	PAÍSES BAIXOS (HOLANDA)

Sócio Estrangeiro 2

Situação	Data da Situação
Ativo	26/05/2003

Tipo de Participação
Socio P. Juridica com Sede no Exterior

Nome
HEWLETT-PACKARD CAPELLE B.V.

CPF Representante	País
90362179891	PAÍSES BAIXOS (HOLANDA)

Sócio Estrangeiro 3

Situação	Data da Situação
Ativo	26/05/2003

Colegio Notarial do Brasil - SP
REGISTRO CIVIL E TABELIONATO
ALDEIA BARUERI - SP
AUTENTICAÇÃO
0109AA284723

RQS nº 03/2005 - CN - CPMI - CORREIOS
0616
3740
Doc:

3135

276

Tipo de Participação	
Socio P. Juridica com Sede no Exterior	
Nome	
HEWLETT-PACKARD INTER-AMERICAS	
CPF Representante	País
01213914850	**ESTADOS UNIDOS**

Esta Declaração corresponde a expressão da verdade, sujeitando-se o infrator em crime de falsidade ideológica previsto no Código Penal.

Colegio Notarial do Brasil SP
REGISTRO CIVIL E TABELIONATO
ALDEIA BARUERI - SP

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0617
3740
Doc:

Prefeitura Municipal de Barueri

ESTADO DE SÃO PAULO

Secretaria de Finanças - Departamento Técnico de Arrecadação

DECLARAÇÃO PARA FINS DE INSCRIÇÃO

3.134

275

5-00.878-8

Inscrição

PESSOA JURÍDICA

Razão Social: HEWLETT PACKARD BRASIL LTDA.			
Nome Fantasia:			
Endereço: (Rua, Av., Etc...) ALAMEDA RIO NEGRO	Nº 750	Andar 1ºAnd. Fund	Sala 4
Bairro: Alphaville	Inscrição Cadastral do Imóvel: 002325142160001000001		
Fone:	Estabelecido: [X] Sim [ ] Não		

	CNPJ	Inscrição Estadual	Espécie de Estabelecimento
PESSOA JURÍDICA	61.797.924/0001-55	206.203.572.117	[ ] Único [ ] Filial c/ Matriz do Município [ ] Matriz [ ] Filial c/ Matriz fora do Município
SOCIEDADE DE PROFISSIONAIS	CNPJ	Quantidade de Sócios	Quantidade de assalariados na mesma categoria profissional

ATIVIDADES EXERCIDAS NO MUNICÍPIO:

[illegible]bricação, comercialização e locação de equipamentos periférico e eletrônicos em geral, computadores, bem como suas peças e componentes, a produção, locação e comercialização e locação de programas de computador, serviços de consultoria, assistência técnica e manutenção de atinentes ao ramo.

ATIVIDADE PRINCIPAL:

RELACIONAR OS SERVIÇOS PRESTADOS INICIANDO PELO PRINCIPAL

ATIVIDADE	CÓDIGO	ATIVIDADE	CÓDIGO
1) Locação de Equipamentos	160221211	11)	
2) Locação de Equip. Perifé	160221211	12)	
3) [illegible]ção de Elet. em gera	160221211	13)	
4) Locação de Prog. de Comp	040620819	14)	
5) Serviços de Consultoria	040521310	15)	
6) Assistência Técnica	150421318	16)	
7) Manutenção	150421416	17)	
8) Conserto equio. inf.	150421318	18)	
9) Manutenção equip. inf.	150421416	19)	
10)		20)	

AUTENTICAÇÃO MECÂNICA

Mod 184

Cartório Registro Civil das Pessoas Naturais e Tabelião [illegible] Comarca de Barueri [illegible] Francisco [illegible] Fax: 4190 [illegible]

AUTENTICAÇÃO

Aldeia

04 DEZ. 2003

(Válido somente com a data de autenticidade)

Colégio Notarial do Brasil - SP

AUTENTICAÇÃO

0109AA298735

RQS nº 03

CPMI - CORRE

Fls. Nº 0618

Doc. 3740

PREFEITURA MUNICIPAL DE BARUERI

Estado de São Paulo

273
A

SECRETARIA DE FINANÇAS
Departamento de Arrecadação
Divisão Especializada de Licença de Funcionamento

ALVARÁ DE LIBERAÇÃO FISCAL nº 01236/2003

3.132
9

Pelo presente Alvará fica **HEWLETT-PACKARD BRASIL LTDA**

Situada na: **ALAMEDA RIO NEGRO** Nº **750** Andar: **01** Sl.: **04** Compl.
Bairro: **ALPHAVILLE CENTRO INDUSTR E EMPRESARIAL - BARUERI - SP**
Distrito: **SEDE**

Inscrição Municipal nº **5.00878-8** autorizada no aspecto tributário a funcionar com o ramo de: **FABRICAÇÃO, COMERCIALIZAÇÃO E LOCAÇÃO DE EQUIPAMENTOS PERIFÉRICOS E ELETRÔNICOS, COMPUTADORES, BEM COMO SUAS PEÇAS E COMPONENTES, A PRODUÇÃO, LOCAÇÃO E COMERCIALIZAÇÃO E LOCAÇÃO DE PROGRAMAS DE COMPUTADOR, SERVÇOS DE CONSULTORIA, ASSISTÊNCIA TÉCNICA E MANUTENÇÃO DE ATINENTES AO RAMO** de acordo com o despacho exarado no requerimento protocolado sob o nº **26326/2003** em **22/07/2003**, respeitando o Código Tributário Municipal em vigor.

Horário de Funcionamento: SEGUNDA Á SEXTA DAS 08:00 ÀS 18:00 HORAS

A emissão do Alvará de Liberação Fiscal, conforme § 1º do artigo 3º do Decreto nº 5.091 de 13/11/2002, não dispensa o contribuinte da observação das normas e exigências da Secretaria de Planejamento e Controle Urbanístico e da Diretoria de Vigilância Sanitária.

Validade até 21 de julho de 2004

Barueri, em 24 de julho de 2003

Maria Cristina M. T. Juliani
Assessora de Depto

José Antonio Gonçalves da Silva
Diretor de Arrecadação

Colégio Notarial do Brasil - SP
AUTENTICAÇÃO
0109AA29873
04 DEZ. 2003

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0619
3740
Doc:

PREFEITURA MUNICIPAL DE BARUERI

Estado de São Paulo

SECRETARIA DE FINANÇAS
Divisão Especializada de licença de Funcionamento

272
A

ANEXO A INSCRIÇÃO MUNICIPAL

3131
9

Razão Social : HEWLETT-PACKARD BRASIL LTDA

Endereço : ALAMEDA RIO NEGRO, 750 Andar: 01 Sala: 04

Bairro : ALPHAVILLE CENTRO INDUSTR E EMPRESARIAL BARUERI-SP

Dia de Recolhimento: 09

Relação das atividades de serviços desenvolvidas pela empresa com os respectivos códigos e alíquotas, conforme o Decreto 5124/2002.

Descrição	Código	Alíquota
CONSULTORIA	04.05.2.13.1-0	2,00
PROGRAMACAO	04.06.2.08.1-9	2,00
CONSERTO DE EQUIPAMENTOS PARA INFORMATICA E AUTOMACAO	15.04.2.13.1-8	2,00
MANUTENCAO DE EQUIP. PARA INFORMATICA E AUTOMACAO	15.04.2.14.1-6	2,00
LOCACAO DE MAQUINAS, APARELHOS E EQUIPAMENTOS	16.02.2.12.1-1	2,00

Colégio Notarial do Brasil - SP
AUTENTICAÇÃO
0109AA298737
AUTENTICAÇÃO
04 DEZ. 2003

MARIA CRISTINA M.T. JULIANI
ASSESSORA DE DEPARTAMENTO

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0620
3740
Doc:

Data de Emissão: 23/07/2003 16:33:26

1.130
9

271

Prefeitura Municipal de Barueri

PROTOCOLO CENTRAL

Nº Protocolo **026326/2003**
Data: 22/07/2003 Hora: 16:23:27

Requerente - HEWLETT-PACKARD BRASIL LTDA		
Endereço - ALAMEDA RIO NEGRO, 750		
Bairro/Cidade - ALPHAVILLE CENTRO INDUSTR E EMPRESARIAL/BARUERI		
Cep 06454000	**Documento** 61797924000155	**Telefone** 41974963
Destinatário - ARRECADAÇAO		
Fone - 4199-8090 /4199-8060 /		
Assunto - ALTERAÇAO REFERENTE A INSCRIÇAO MUNICIPAL		
Observação OBJETIVO		

Acompanhe as ações de governo de nossa cidade acessando o site www.barueri.sp.gov.br

1ª. via - Solicitante

Colégio Notarial do Brasil-SP
AUTENTICAÇÃO
0109AA298738

04 DEZ. 2003

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0621
Doc: 3740

Receita Federal

Comprovante de Inscrição e de Situação Cadastral

Contribuinte,

Confira os dados de Identificação da Pessoa Jurídica e, se houver qualquer divergência, providencie junto à SRF a sua atualização cadastral.

REPÚBLICA FEDERATIVA DO BRASIL

CADASTRO NACIONAL DA PESSOA JURÍDICA

NÚMERO DE INSCRIÇÃO	COMPROVANTE DE INSCRIÇÃO E DE SITUAÇÃO CADASTRAL	DATA DE ABERTURA
61.797.924/0001-55		**22/10/1970**

NOME EMPRESARIAL **HEWLETT-PACKARD BRASIL LTDA**			
TÍTULO DO ESTABELECIMENTO (NOME DE FANTASIA) ********			
CÓDIGO E DESCRIÇÃO DA ATIVIDADE ECONÔMICA PRINCIPAL **51.65-9-01 - Comércio atacadista de equipamentos de informática; partes e peças**			
CÓDIGO E DESCRIÇÃO DA NATUREZA JURÍDICA **206-2 - SOCIEDADE EMPRESARIA LIMITADA**			
LOGRADOURO **AL RIO NEGRO**	NÚMERO **750**	COMPLEMENTO **FUNDOS 1 AND S 4**	
CEP **06.454-000**	BAIRRO/DISTRITO **ALPHAVILLE**	MUNICÍPIO **BARUERI**	UF **SP**
SITUAÇÃO CADASTRAL **ATIVA**		DATA DA SITUAÇÃO CADASTRAL **15/05/2003**	
SITUAÇÃO ESPECIAL ********		DATA DA SITUAÇÃO ESPECIAL ********	

Aprovado pela Instrução Normativa SRF nº 200, de 13 de setembro de 2002.

Emitido no dia **10/11/2003** às **14:37:04** (data e hora de Brasília).

Voltar

12 NOV. 2003

AUTENTICAÇÃO

0109AA277938

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls.: 0622
3740
Doc:

3.128
9

~~269~~
~~A.~~

4. Qualificação Técnica

RQS nº 03/2003
CPMI - CORREIOS
Fls. Nº 0623
3740
Doc:

CASSI

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos para os devidos fins que a empresa Hewlett Packard Brasil Ltda e CNPJ nr. 61.797.924/0001-55 estabelecida na Alameda Rio Negro, 750 – Alphaville – Barueri - SP, forneceu e executou para a CASSI – Caixa de Assistência aos Funcionários do Banco do Brasil CNPJ Nº 33.719.485/0001-27, situada no endereço SBS Qd 02 Bloco "N" Ed Sede II do Banco do Brasil, o(s) material(ais), abaixo especificados, no período de (3/março/2003 a 12/agosto/2003):

•HP Openview Network Node Manager Enterprise e outros produtos da família Openview, realizando o serviço de implementação e customização

Atestamos ainda, que tais fornecimentos estão sendo/foram executados satisfatoriamente, não existindo, em nossos registros, até a presente data, fatos que desabonem sua conduta e responsabilidade com as obrigações assumidas.

Brasília. - DF, 10 de Dezembro de 2003.

Ruver Muci **Damasio** de Sousa
Gerente de Área de Rede e Atendimento

Ruver Muci Damasio de Souza
Gerente de Área de Rede e Atendimento

Colégio Notarial do Brasil - SP
AUTENTICAÇÃO
01109AA303767
1º TABELIONATO DE NOTAS E DE PROTESTO CIVIL
ALDEIA BARUERI - SP

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0624
3740
Doc:

0.27.170-5 - Mai/99

3.126
P

267
A

5. Declaração

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0625
Doc: 3740

declaração

Hewlett Packard Brasil Ltda.
Alameda Rio Negro, 750 - Alphaville
06454-000 - Barueri - SP
CNPJ: 61.797.924/0001-55
Fone: (11) 4197 8000
Fax: (11) 4197 8432

www.hp.com.br

690469-BR

ANEXO 3

(MODELO III)

DECLARAÇÃO DE ATENDIMENTO AO ART. 27, INCISO V DA LEI 8666/93

À

EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS - ECT

SBN, Quadra 01 – Bloco "A" – 4º andar – Ala Norte – Ed. Sede/ECT – CEP 70002-900 – Brasília/DF

Fax.: 61. 426.2759

REF.: PREGÃO Nº 118/2003 – CPL/AC

Hewlett-Packard Brasil Ltda., CNPJ nº 61.797.924/0001-55, por intermédio de seu representante legal o Sr. Jose Eduardo Pires do Rio Ribeiro, portador da Carteira de Identidade nº 15.319.247 (SSP/SP) e do CPF nº 071.885.858-14, DECLARA, para fins do disposto no inciso V do Art. 27 da Lei 8666/93, que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos.

Ressalva: emprega menor, a partir de quatorze anos, na condição de aprendiz(X).

Barueri, 15 de dezembro de 2003.

Jose Eduardo Pires do Rio Ribeiro
Gerente Contas Governo
Hewlett Packard Brasil Ltda
CNPJ Nº 61.797.924/0001-55

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0626
Doc: 3740

E-TAILOR
ENTERPRISE

3124

E–Tailor Soluções em Tecnologia da Informação Ltda.

CORREIOS

Pregão nº 118/2003 - CPL/AC

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0627
3740
Doc:

E-TAILOR
ENTERPRISE

São Paulo, 16 de dezembro de 2003

Aos
CORREIOS

Ref.: Pregão nº 118/2003 – CPL/AC

Prezados Senhores,

A E-Tailor Enterprise está honrada em responder sua solicitação. Estamos encaminhando para apreciação nossa proposta para Pregão nº 118/2003 - CPL/AC.

Estamos confiantes que a nossa proposta atenderá suas necessidades atuais e futuras. Para maiores esclarecimentos e informações, não hesite em contatar-nos.

A E-Tailor Enterprise possui pessoal, tecnologia, experiência e comprometimento que resultarão em uma parceria perfeita com vocês.

Atenciosamente,

Ítalo Togni
Representante Legal

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0628
3740
Doc:

E-TAILOR ENTERPRISE

PROPOSTA ECONÔMICA

PREGÃO Nº 118/2003.

3122

1. Razão Social da Empresa: .E–Tailor Soluções em Tecnologia da Informação Ltda.
2. CNPJ Nº: 04.525.751/0001-82
3. Inscrição Estadual: Isenta
4. Inscrição Municipal: .0004655-9
5. Endereço Completo: .R. Getúlio Vargas, 64 – sala 212-parte – Centro – Rio Bonito - RJ
6. Telefone: (021).2225-4847 Fax: ..(021) 2225-4847.. E-mail: .comercial@etailor.com.br
7. Validade da Proposta: ..60. *(sessenta)* dias
8. Prazo de Pagamento: Em parcela única, mediante entrega das ferramentas, no prazo de 15 (quinze) dias após a emissão do Termo de Aceitação Final – TAF.
9. Banco: .Boston Agência: .0068. Conta Corrente: .00009680
10. Representante da Empresa: .Itálo Togni
11. Cargo: ..Representante de Vendas . RG: .4.569.457 (SSP-SP). CPF: .043.818.748-20
12. Unidade da Federação de emissão da Nota Fiscal: .Rio de Janeiro

Apresentamos nossa Proposta para fornecimento do material do objeto do Pregão nº /2003, acatando todas as estipulações consignadas no Edital, conforme abaixo:

ITEM	DESCRIÇÃO	UNID.	QTDE.	PREÇO UNITÁRIO (R$)	PREÇO TOTAL (R$)
01	Licença do Software HP OPEN VIEW NETWORK NODE MANAGER ENTERPRISE VERSÃO 6.2 OU SUPERIOR.	UM.	05	101.000,00	505.000,00 ✓

(Quinhentos e cinco mil reais)

Garantia do objeto: (01 ano)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0629
3740
Doc:

E-TAILOR ENTERPRISE

MODELO DE PLANILHA DE CUSTOS DE FORMAÇÃO DO PREÇO

ITEM	PERCENTUAL
1. MATÉRIA PRIMA/INSUMOS:	
Licenças de Software e Serviços	85%
Subtotal	85%
2. TRIBUTOS	
ISSQN	5%
Subtotal	5%
3. TRASPORTES	
Frete	1.5%
Subtotal	1.5%
4. DESPESAS ADMINISTRATIVAS	
	2%
Subtotal	2%
5. LUCRO	
	5%
Subtotal	5%
6. OUTROS	
	1.5%
Subtotal	1.5%
TOTAL	100%

Declaramos que tomamos conhecimento de todas as informações e condições para o cumprimento das obrigações objeto desta licitação e que atendemos todas as condições do Edital.

Data: .16./ 12./ .2003

Ítalo Togni
Representante Legal

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0630
Doc: 3740

Especificação Técnica
Licenças de Software para Gerenciamento



	Características Mínimas
1. Descrição	Software HPOpenView Network Node Manager Enterprise v. 6.20 ou superior
2. Quantidade de Licenças	5 (cinco)
3. Garantia	- 12 (doze) meses a contar do Termo de Aceite Final -A garantia deve compreender a correção de falhas no produto, independentemente de correções tornadas públicas, desde que tenham sido detectadas e formalmente comunicadas à contratada. - Caso seja detectado bugs ou falhas no software, a empresa contratada deverá fornecer atualizações necessárias à correção do problema. Os produtos devem ser isentos de back doors. - A versão deve ser a última disponível no mercado na data de entrega do produto.
4. Compatibilidade	O produto deve ser compatível com o sistema operacional SUN SOLARIS e HP-UX.
5. Documentação Técnica	O produto deve ser entregue com documentação técnica do fabricante. Deverá ser fornecida documentação: – das parametrizações (customizações) realizadas nas ferramentas no processo de instalação e configuração; e – de instalação, configuração e operação.
6. Outros	O produto deve: – Ser fornecido em CD/ROM; – Ser fornecido, instalado, configurado e integrado às ferramentas HP OpenView NNM e VP/O já existentes no ambiente de gerência da ECT, mantendo a padronização existente; – A instalação compreende, dentre outros, a preparação dos servidores SUN e/ou HP, instalação e parametrização dos respectivos Sistemas Operacionais (Solaris e/ou HP UX). Os servidores e sistemas operacionais serão fornecidos pela ECT. – A instalação compreende, dentre outros, a implementação de alarmes definidos segundo padronização da ECT, integração com as consoles do HP-VP/O e descoberta (discovery) dos elementos a serem gerenciados.
7. Prazos	Entrega: até 10 (dez) dias, após a assinatura do contrato; Instalação e Configuração Final: até 40 (quarenta) dias após a Entrega; Termo de Aceite Final: até 5 (cinco) dias após a Instalação e Configuração Final; Pagamento: até 15 (quinze) dias após o Termo de Aceite Final.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0631
Doc: 3740

Especificação Técnica
Licenças de Software para Gerenciamento

8. Atendimento e Suporte	- Deve ser fornecido a referência completa do canal de atendimento e suporte técnico do produto ofertado, com a nomeação e o telefone do(s) responsável(eis) técnicos que possa(m) responder questionamentos sobre todas as características do produto em pauta. - O atendimento e suporte ao produto deve compreender o acesso a help-desk para atendimento e abertura de chamados em língua portuguesa (durante horário comercial), incluindo o atendimento telefônico e o atendimento via e-mail. - Na descrição dos requisitos técnicos constantes de proposta referente ao produto devem ser apresentadas as demais modalidades de suporte técnico disponibilizadas, com detalhamento dos seus meios de acesso, quando existentes. -O atendimento a chamadas deve ocorrer, se necessário, nos dias úteis da semana no horário comercial, no esquema 8 x 5, até 4 (quatro) horas da abertura dos chamados por uma central de atendimento 0800 do fabricante. - O prazo de Atendimento e Suporte é de 12 (doze) meses a contar do Termo de Aceite Final.
9. Garantia Contratual	5% (cinco porcento) do valor global do contrato. Vigência: até o prazo final do Atendimento e Suporte.
10. Atualização	-A contratada deverá prover toda e qualquer atualização pertinente ao produto pelo período mínimo de um ano. -Em caso de upgrades, quando a aplicação da nova versão resultar em perda de dados, incapacidade de abertura ou gravação de arquivos ou qualquer outra incompatibilidade relativamente às versões anteriores, tais restrições deverão estar claramente relatadas na descrição dos requisitos de natureza técnica das propostas -Para fins desta especificação técnica, entende-se como atualização o provimento de toda e qualquer evolução do produto, incluindo: - patches, fixes, correções, updates e service packs; - novas releases, builds e funcionalidades; - o provimento de upgrades para novas versões de mercado ou lançamentos (tal como ocorre, por exemplo, na migração de *Produto* 6 para *Produto* 7 e similares); e, - o provimento de upgrades englobando, inclusive, versões não sucessivas, caso a disponibilização de tais versões ocorra durante o período da garantia (como exemplo, a migração de *Produto* 5 para *Produto* 7, 8 ou posterior). -A contratada deverá fornecer tais atualizações independentemente de solicitação expressa da contratante.

(X) Atende ( ) Não atende

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 0632
Doc. 3740

3. Documentos

E-TAILOR ENTERPRISE

3118

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0633
Doc: 3740

declaração

Hewlett Packard Brasil Ltda.
Alameda Rio Negro, 750 - Alphaville
06454-000 - Barueri - SP
CNPJ: 61.797.924/0001-55
Fone: (11) 4197 8000
Fax: (11) 4197 8432

www.hp.com.br

690469-BR

ANEXO 3

(MODELO VI)

DECLARAÇÃO DE SOLIDARIEDADE

EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS - ECT

SBN, Quadra 01 – Bloco "A" – 4º andar – Ala Norte – Ed. Sede/ECT – CEP 70002-900 – Brasília/DF

Fax.: 61. 426.2759

REF.: PREGÃO Nº 118/2003 – CPL/AC

Hewlett-Packard Brasil Ltda., CNPJ nº 61.797.924/0001-55, situada na Al. Rio Negro, 750 – Alphaville – Barueri/SP, na condição de fabricante, declara ser responsável solidária com a ETAILOR SOLUÇÕES EM TECNOLOGIA DA INFORMAÇÃO LTDA., CNPJ 04.525.751/0001-82, situada Rua Getulio Vargas, nº 64 – Sala 212 – Parte – Centro – Rio Bonito/RJ, no atendimento ao Edital em epígrafe, no que diz respeito ao prazo de fornecimento, atendimento e suporte técnico e prestação de garantia, relativos aos produtos indicados em sua Proposta Econômica.

Barueri, 15 de dezembro de 2003.

Ieda T. Viana Batista
Representante Legal
Tel. 11.4197.8749
Hewlett Packard Brasil Ltda.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0634
3740
Doc.

3116

E-TAILOR ENTERPRISE

DECLARAÇÃO DE ATENDIMENTO DE CERTIFICAÇÃO TÉCNICA

À

EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS - ECT

SBN, Quadra 01 – Bloco "A" – 4º andar – Ala Norte – Ed. Sede/ECT – CEP 70002-900 – Brasília/DF

Fax.: 61. 426.2759

REF.: PREGÃO Nº 118/2003 – CPL/AC

E-TAILOR Soluções em Tecnologia da Informação Ltda., CNPJ nº CNPJ nº 04.525.751/0001-82, por intermédio de seu representante legal o Sr. Ítalo Eligio Togni,, portador da Carteira de Identidade nº 4569457 (SSP/SP) e do CPF nº 043.818.748-20, DECLARA, para os devidos fins que, possui Certificação Técnica para prestação de suporte, manutenção e garantia.

Barueri, 15 de dezembro de 2003.

Ítalo Eligio Togni
Representante Legal
E-TAILOR Soluções em Tecnologia da Informação Ltda
CNPJ Nº 04.525.751/0001-82

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0635
3740
Doc:

690469-BR

ANEXO 6

TERMO DE GARANTIA TECNICA

Inicio de Vigência:

As empresas abaixo descritas, firmam entre si o presente Instrumento, doravante denominado simplesmente de TERMO DE GARANTIA TECNICA.

DESIGNAÇÃO DAS PARTES DORAVANTE NO TERMO	ECT	FORNECEDORA
Razão Social	EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS	E-TAILOR SOLUÇÕES EM TECNOLOGIA LTDA
Endereço	SBN, Qd. 01 – Bloco "A" – 4º andar – Ala Norte – Ed.Sede/ECT	Rua Getulio Vargas, 64 – Sala 212 - Parte
CEP	70002-900	28800-000
Cidade	Brasília	Rio Bonito
Estado	DF	RJ
CNPJ		04.525.751/0001-82
I.E.		

1. **OBJETO**: Garantia Técnica do software HPOpen View Network Node Manager Enterprise v.6.20 ou superior, englobando o atendimento e suporte.
2. **PRAZO DE GARANTIA:** a partir da data de emissão do Termo de Aceite Final, encerrando-se 12 (doze) meses após a emissão deste Termo de aceite final.
3. RESPONSABILIDADE DA FORNECEDORA:

3.1 – Corrigir falhas no produto, independentemente de correções tornadas públicas, desde que tenham sido detectadas e formalmente comunicadas à FORNECEDORA.

3.2 – Fornecer atualizações necessárias à correção de problemas como bugs ou falhas no software. Os produtos devem ser isentos de back doors.

3.3 – entregar a última versão disponível no mercado na data de entrega do produto.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0636
3740
Doc:

3114

E-TAILOR ENTERPRISE

3.4 – Comprometemo-nos a fornecer à ECT todas as atualizações de versões do software adquirido durante a vigência deste TERMO.

3.5 Forneceremos a referência completa do canal de atendimento e suporte técnico do produto ofertado, com a nomeação e o telefone dos responsáveis técnicos que possam responder questionamentos sobre todas as características do produto em pauta.

3.6 Prestar atendimento de suporte técnico a ECT, pelo período de 1(um) ano, visando sanar eventuais problemas, observando-se os seguintes prazos:

a) atendimento: no prazo de 04(quatro) horas corridas; e
b) solução do problema: 12(doze) horas corridas.

3.6.1. Define-se como tempo de atendimento o período compreendido entre o horário de comunicação do chamado feito pela ECT e o horário de chegada ao local de atendimento.

3.6.2. Define-se como tempo de solução do problema, o período compreendido entre o horário de comunicação do chamado feito pela ECT e o horário de término da solução, deixando o software em condições normais de operação.

3.7. o atendimento e suporte ao produto devem compreender o acesso a help-desk para atendimento e abertura de chamados em língua portuguesa(durante horário comercial), incluindo o atendimento telefônico e o atendimento via e-mail.

3.8 – Na descrição dos requisitos técnicos constantes da proposta referente ao produto serão apresentadas as demais modalidades de suporte técnico disponibilizadas, com detalhamento dos seus meios de acesso, quando existentes.

3.9. o atendimento a chamados deve ocorrer, se necessário, nos dias úteis da semana no horário comercial, no esquema 8 x 5, até (quatro) horas da abertura dos chamados por uma central de atendimento nº 0800.130.999 da HP.

3.10. o prazo de atendimento e suporte é de 12(doze) mesesa contar da data de emissão do termo de aceite final – TAF, pela ECT.

3.11. a E-TAILOR proverá toda e qualquer atualização pertinente ao produto pelo período mínimo de um ano.

3.12. em caso de upgrades, quando a aplicação da nova versão resultar em perda de dados, incapacidade de abertura ou gravação de arquivos ou qualquer outra incompatibilidade relativamente às versões anteriores, tais restrições estarão claramente relatadas na descrição dos requisitos de natureza técnica das palavras.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0637
Doc: 3740

3112

E-TAILOR ENTERPRISE

3.13. – Para fins da especificação técnica constante neste contrato, entende-se como atualização o provimento de toda e qualquer evolução do produto, incluindo:
- patches, fixes, correções, updates e serviços packs
- novas releases, builds e funcionalidades;
- o provimento de upgrades para novas versões de mercado ou lançamentos (tal como ocorre, por exemplo, na migração de produto 6 para Produto 7 e similares); e
- o provimento de upgrades englobando, inclusive, versões não sucessivas, caso a disponibilização de tais versões ocorra durante o período da garantia(como exemplo, a migração de Produto 5 para Produto 7, 8 ou posterior).

3.14. A HP fornecerá tais atualizações independentemente de solicitação expressa da ECT.

4. – DAS PENALIDADES:

4.1. 0 não atendimento do suporte técnico e solução de problemas à ECT, dentro dos prazos estabelecidos no subitem 3.4. deste Termo: 1% (um por cento) sobre o valor unitário da ferramenta, cujo atendimento foi reclamado, por hora de atraso.

4.2. – o não atendimento de qualquer item descrito neste Termo de Garantia Técnica : 1% (um por cento) sobre o valor unitário da ferramenta.

Barueri, 15 de dezembro de 2003.

CONTRATADA: CONTRATANTE:

Representante LegaL.: Carlos Alberto dos Santos Teixeira Representante Legal

Testemunha: Testemunha:

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0638
3740
Doc:

declaração

Hewlett Packard Brasil Ltda.
Alameda Rio Negro, 750 - Alphaville
06454-000 - Barueri - SP
CNPJ: 61.797.924/0001-55
Fone: (11) 4197 8000
Fax: (11) 4197 8432

www.hp.com.br

690469-BR

3112

ANEXO 3

(MODELO VI)

DECLARAÇÃO DE SOLIDARIEDADE

EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS - ECT

SBN, Quadra 01 – Bloco "A" – 4º andar – Ala Norte – Ed. Sede/ECT – CEP 70002-900 – Brasília/DF

Fax.: 61. 426.2759

REF.: PREGÃO Nº 118/2003 – CPL/AC

Hewlett-Packard Brasil Ltda., CNPJ nº 61.797.924/0001-55, situada na Al. Rio Negro, 750 – Alphaville – Barueri/SP, na condição de fabricante, declara ser responsável solidária com a ETAILOR SOLUÇÕES EM TECNOLOGIA DA INFORMAÇÃO LTDA., CNPJ 04.525.751/0001-82, situada Rua Getulio Vargas, nº 64 – Sala 212 – Parte – Centro – Rio Bonito/RJ, no atendimento ao Edital em epígrafe, no que diz respeito ao prazo de fornecimento, atendimento e suporte técnico e prestação de garantia, relativos aos produtos indicados em sua Proposta Econômica.

Barueri, 15 de dezembro de 2003.

Ieda T. Viana Batista
Representante Legal
Tel. 11.4197.8749
Hewlett Packard Brasil Ltda.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0639
3740
Doc:

4. Anexos

E-TAILOR ENTERPRISE

3111

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0640
3740
Doc:

3110

HP OpenView Network Node Manager

A Guide to Scalability and Distribution

HP-UX, Solaris, and Windows operating systems



Manufacturing Part Number: J5323-90001

January, 2003

© Copyright 2003 Hewlett-Packard Company.

ECT/ECOS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0641
3740
Doc.

Legal Notices

Warranty.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices.

©Copyright 1983-2003 Hewlett-Packard Company.

No part of this document may be copied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

Contains software from AirMedia, Inc.

© Copyright 1996 AirMedia, Inc.

Trademark Notices

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

Windows® and MS Windows® are U.S. registered trademarks of Microsoft Corporation.

Windows® 2000 is a U.S. registered trademark of Microsoft Corporation.

Windows NT® is a U.S. registered trademark of Microsoft Corporation.

Netscape and Netscape Navigator are U.S. trademarks of Netscape Communications Corporation

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

Oracle7TM is a trademark of Oracle Corporation, Redwood City, California.

OSF/Motif® and Open Software Foundation® are trademarks of the Open Software Foundation, Inc. in the U.S. and other countries.

Pentium® is a U.S. registered trademark of Intel Corporation.

UNIX® is a registered trademark of The Open Group.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0642
Doc 3740

3102

Support

1. Overview of Scalability and Distribution in NNM

Scalability and Distribution in NNM 15
Benefits of Scalability 15
What Makes NNM a Scalable Solution for Network Management? 16
Network, System, and Operator Efficiency via Filtering 19
Distributed Internet Discovery and Monitoring 20
Capacity Planning 21
About Management Stations and Collection Stations 22
Management Consoles 24
On-Demand Submaps 26
Distributed Threshold Monitoring and Event Forwarding 27
General Events 27
Threshold Events 28
Trend Data Collection in a Distributed NNM Solution 28
Large-Map Viewing Support 29
The Panner 30
The Quick Navigator 30

2. The Scalable Architecture of Network Node Manager

The Distribution Model for Network Node Manager 33
Network Connections between Distributed Components 36
Filters 37
Discovery Filtering 40
Topology Filtering 41
Map Filtering 42
Defining New Filters 43
Filter Utilities 45
Distributed Internet Discovery and Monitoring 46
About Collection Domains 46
Distributed Services Architecture 48
High Availability Management Information 50
Overlapping Collection Domains 52
Configuration Concepts 56
Distributed Threshold Monitoring and Event Forwarding 59

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0643
3740
Doc:

Event Correlation for "Connector Down" 60
Data Collection for Distributed Threshold Monitoring 62
On-Demand Submaps 64
Transient Submaps and the Submap List Dialog 67
Persistence Filtering 68
Comparing Map Filters and Persistence Filters 69
Management Consoles 70
Management Consoles and On-Demand Submaps 72
Customized Views of the Network 72
Management Consoles and X-Terminals 73
Interface Managed-state Automation 74
Microsoft Terminal Server Access 75
Accessing a Single NNM Station From Multiple Terminal Server Clients 75
Accessing Multiple NNM Stations From a Single Terminal Server Client 77
Accessing Multiple NNM Stations From Multiple Terminal Server Clients 78

3. Strategies for Deploying Network Node Manager

Planning the Right Approach 83
General Considerations about Scalability and Distribution 84
General Strategies for Deployment 87
Deployment Strategies for NNM 89
Use of Scalability Features in NNM Deployment 89
Fully Centralized Management 92
Implementation Tactics 93
Implications of Using the Fully Centralized Management Model 94
Centralized-Hierarchical Management 95
Implementation Tactics 96
Implications of Using Centralized-Hierarchical Management 97
Hierarchical Management 98
Implementation Tactics 100
Implications of Using the Hierarchical Management Model 101
Cooperative Independent Management 103
Implementation Tactics 104
Implications of Using the Cooperative Independent Model 105

4. Procedures for Scaling NNM

Configuring Management Consoles 109
Configuring a Windows System Console Server 111
Installing a Management Console on Windows for an NNM Server on Windows . 111
UNIX System Server Configuration 112
Installing Management Consoles on Windows for UNIX System Management Servers 115
UNIX System Console Configuration 117
Increasing Security for Management Consoles 119
Undoing a Management Console 120
Configuring On-Demand Submaps 121
Configuring Demand Level 121
Specifying a Persistence Filter 124
Integrating Applications With On-Demand Submaps 125
Configuring a Map Filter 127
Configuring Data Collection for a Station 128
Configuring a Discovery Filter 128
Managing and Unmanaging Locally Monitored Objects 132
Configuring Collection Stations 133
Configuring Security for a Collection Station 133
Configuring a Topology Filter for a Collection Station 134
Changing the Topology Filter for a Collection Station 135
Configuring IPX on a Collection Station under Windows 136
Configuring Management Stations 137
Determining if a Node is a Collection Station 137
Determining All Objects Monitored by a Collection Station 138
Configuring for a Specific Collection Station 138
Unmanaging a Collection Station 140
Removing a Collection Station from a Management Station 141
Configuring a Remote Communication Timeout and Retry Count 141
Performing a Full Topology Synchronization 144
Identifying Collection Station Communication Problems 145
Troubleshooting Collection Station Communication 147
Configuring Domain Overlaps and Failover 150
Determining the Primary Collection Station for an Object 150
Changing the Primary Collection Station for an Object 151
Changing the Overlap Mode 152

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0644
3740
Doc:

Collection Station Failover 153
Configuring Event Forwarding and Correlation 154
Forwarding an Event 154
Using Distributed Data Collection 159

5. Dynamic Views and Distributed Management

Dynamic Views and Distributed Management 163
NNM Neighbor View 164
NNM Path View 165

A. The Filter Definition Language

The Filter Definition File 169
Filters and Filter-Expressions 170
Sets 171
Attribute Value Assertions 172
Valid Operators for AVAs 173
Boolean AVAs 174
Integer AVAs 175
Enumerated (Enum) AVAs 175
String AVAs 175
Excluding a Node 180
Relationships Between Nodes and Interfaces 180
Valid Operators for Logical Combinations of AVAs or Filters 180
Filterable Objects and Attributes 181
Filter File Grammar 187
Filter File Example 189
Setting Up Collection Domains 190
Excluding Nodes 192
Failover Filters 193
Important Node Filters 193
Topology Filters 194
Map Filters 195
Using the Network Presenter 195
Default Filter File 197

B. Using NNM Under a Mixed Codeset Environment

3103

Glossary **209**

Index **213**

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: Nº 0645
3740
Doc:

Support

Please visit the HP OpenView web site at:

`http://openview.hp.com/`

There you will find contact information and details about the products, services, and support that HP OpenView offers.

The support area of the HP OpenView web site includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

RQS nº 03/2005 - CN
CPMI - CORREIOS
FIS. Nº 0646
3740

1 Overview of Scalability and Distribution in NNM

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0647
3740
Doc:

Scalability and Distribution in NNM

You can configure NNM to perform well for a wide range of network sizes and degrees of complexity. This attribute is commonly referred to as the **scalability** of NNM. Scalability gives NNM the potential to handle almost any size network, in both local and wide-area environments.

One approach to making a product like NNM scalable, and an important feature of NNM, is to distribute the network management workload to multiple, usually remote, systems. NNM makes **distribution** possible, so you can monitor and manage much larger networks while minimizing the management resources required.

In summary, the scalability and distribution of NNM optimizes the use of two key resources:

- First, NNM includes features that help you use the *system resources* at the management station very efficiently.
- Second, other features of NNM, especially distribution, reduce the amount of management traffic over your *network*, most importantly, over congested or expensive links.

Benefits of Scalability

Having a scalable network management platform, implemented in part through distribution, provides you with many benefits in your application of NNM as a network management solution.

First, scalability gives your network management solution the ability to evolve with your organization. Networks are dynamic entities that reflect the changing structures and needs of the organizations they serve. As your network changes and grows, the scalable features of NNM make it easier to adapt your network management to handle new networking landscapes.

Second, a distributed network management solution can dramatically reduce the traffic overhead that network management can impose on congested or expensive network links. Most large (enterprise) networks include serial or wide-area (WAN) links. Such links are both relatively slow and expensive. Without a distributed network management solution, it is simply impractical to monitor tens of thousands of nodes from a single workstation; the networking load emanating from the

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0648
3740
Doc:

management station becomes a bottle neck. Distribution minimizes the amount of network management traffic on these links, freeing bandwidth for business purposes.

Third, a distributed solution makes it possible to share network management responsibility and resource requirements among multiple sites. By spreading the resources and responsibilities out, you reduce the risk of losing all network management in the event of an unexpected shutdown of your management station. Distribution also makes it easier to perform maintenance shutdowns without losing your overall network management.

Fourth, a scalable network management solution, sensibly deployed and properly configured, results in faster response times and better performance. You spend less time waiting for data and more time acting on it. Furthermore, it improves network reliability by allowing local management actions even when contact is lost with a remote central management site.

Finally, deploying a scalable network management platform means everyone in your organization can share a single customizable tool. This naturally leads to a common vocabulary, common experiences, sharable expertise, and the ability to more easily articulate and implement standard processes and procedures in your organization.

All together, NNM's scalability and distribution gives you the power to manage the large and geographically dispersed enterprise networks that are critical to key business or organizational processes. You can use common applications at every level to create a more integrated, consistent solution to the complex problems in these environments.

What Makes NNM a Scalable Solution for Network Management?

The idea of "scalability" is abstract, but HP OpenView Network Node Manager has several broad categories of features that make scalability a concrete reality.

Distributed Internet Discovery and Monitoring

> Distributed Internet Discovery and Monitoring lets remote collection stations monitor their part of the network and inform the central management station about it. This reduces network traffic, and also reduces the load on the central station.

Management Consoles

Management consoles off-load display processing from the management station to a display station. With management consoles, you can have more operators monitoring and managing your network without loss of performance; these operators can handle larger environments.

Web Browser Interface

Accessing network management functions from your web browser lets you monitor your network from any location with a web browser installed, even if it is not a management console. See *Managing Your Network with HP OpenView Network Node Manager* for more information.

Large-Map Viewing Support

NNM gives you two essential features for examining large maps:

- The panner, which makes it easy to navigate submaps with hundreds of symbols.
- The quick navigator, which gives you instant access to your most critical or frequently visited submaps.

On-Demand Submaps

The on-demand submap feature provides a very significant boost in the performance of NNM, allowing it to manage many more objects (up to ten times) than with persistent submaps. Enabling the on-demand submap feature lets your management station use less memory to perform the same tasks.

Filtering

Filters let you reduce the amount of extraneous data being handled by the system, or presented to the operator. This provides improved performance, and reduces visual clutter for the operator.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0649
Doc. 3740

Event Forwarding

You can configure your remote stations so that events from managed nodes, or from non-NNM applications on the collection station, get forwarded to interested management stations. This can be set up to occur whether or not the event triggers local actions, or has already been correlated.

Important events generated internally to NNM, such as topology or status change events, are automatically forwarded from a collection station to the interested management stations, without additional configuration steps.

Distributed Threshold Monitoring

Distributed threshold monitoring reduces management traffic on the network by allowing remote stations, instead of the management station, to collect SNMP trend data and trigger threshold events based on that data.

Interface Managed-state Automation

NNM lets you automatically manage or unmanage interfaces based on filters. Interface managed-state automation makes it easier to manage large environments, where frequently many discovered interfaces do not require active status polling.

High Availability and Fault Tolerance

NNM stations can be run on HP Service Guard clusters to provide continuous availability. Also, if a collection station fails, you can configure its status polling duties to transfer over to a management station. You can also perform backup of your network management data without losing incoming information during that time.

Your practical limits in using all the above depend on the size of your network environment, your management strategy, and the resources available on the management and collection stations. For the most current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide*, available at `http://openview.hp.com/`.

NOTE The upper limits of operators and managed devices depends very heavily on the level of monitoring and data collection you require. In general, increasing the polling intervals on noncritical nodes increases the number of nodes that can be handled.

Network, System, and Operator Efficiency via Filtering

For NNM to manage very large environments, all resources (network, system, and human) must be used as efficiently as possible. To maximize the efficient use of these resources, NNM employs a strategy of data reduction via filters.

A **filter** is essentially just a way to remove unneeded data from consideration for further processing. The result of less data in the system is higher performance for NNM, and improved usability for the operators.

For example, you may have an operator whose only concern is the routers and hubs in your environment. For that operator, any other objects on his map are merely clutter. With NNM, you can apply a filter to the map, so that only routers and hubs appear.

See "Filters" on page 37 for more details about filtering in NNM.

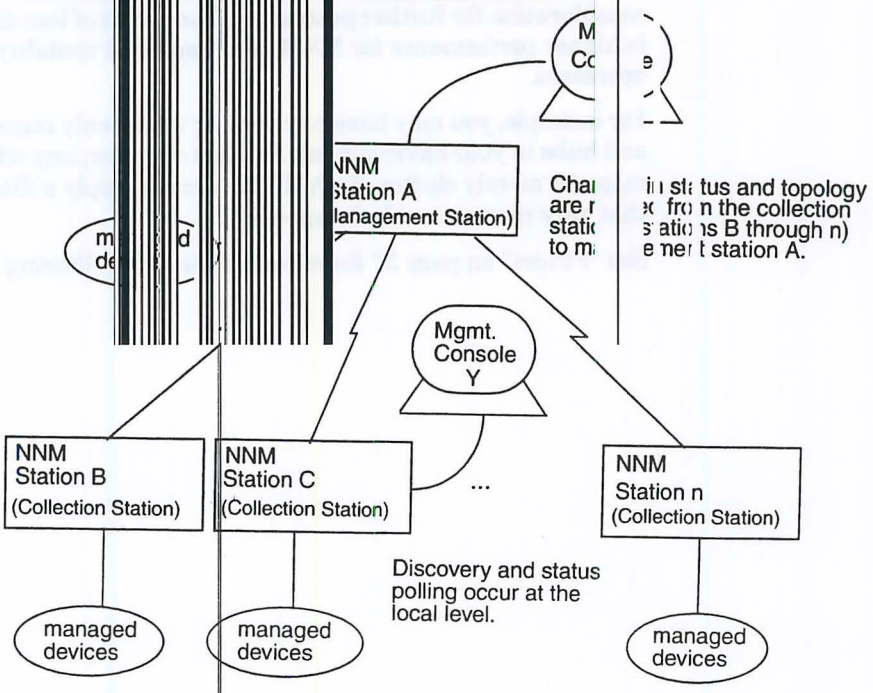
RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0650
Doc: 3740

Distributed Internet Discovery and Monitoring

A network management system can consume significant resources while performing discovery, topology monitoring, and status polling. One feature of HP OpenView Network Node Manager is the ability to move much of this load from the management station to one or more remote machines.

This capability is called **Distributed Internet Discovery and Monitoring**, and is illustrated in Figure 1-1. The device count for this model assumes one interface per device, on average. Note that the management console at Station C indicates that it also serves as a manag[illegible] the objects it monitors; [illegible]s the usual configu[illegible]n f[illegible]

Figure 1-1 **Simpl[illegible] L[illegible] Model for NNM**



To use distributed internet discovery and monitoring, you designate one or more remote machines as **collection station**s. Each collection station takes over the task of monitoring some portion of the network, while informing all interested management stations of any changes in the status or topology of the network it monitors.

Capacity Planning

Because distributed management partitions the work of discovery and status polling, it also dramatically reduces traffic on the network, most importantly on expensive or congested links.

When considering performance and configuration issues, you must distinguish between nodes and objects. There is a one to many relationship between the number of nodes and the number of objects in the database. Even though a network model is typically described in terms of the number of nodes the application manages, it is the total number of managed objects that is the most important consideration in predicting how the application will scale and perform.

Knowing the exact number of managed objects is especially critical when considering, for example, the size of a database, the load on network's bandwidth, or the load imposed on a management station when communicating with a collection station. You'll want to determine the typical node to object multiplier for your environment.

Not all environments conform to the typical environment we describe. In some environments, the ratio of objects to nodes is higher. Large enterprise routers tend to have more than two physical interfaces. For example a network center responsible for monitoring only backbone routers would have a higher ratio. In some cases nodes may have additional virtual interfaces. Secondary addresses, for example, increase the number of objects associated with that particular managed node.

There is no concrete limit to the number of objects or devices you can manage, or to the management stations you can deploy. Your practical limits depend on the size of your network environment, your management strategy, and the resources available on the management and collection stations. For the most current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide*, available at `http://openview.hp.com/`.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0651
3740
Doc:

About Management Stations and Collection Stations

In the previous section (including Figure 1-1), two terms were introduced:

- Management station
- Collection station

It is important to recognize that these labels state the *roles* of the machines involved, and do not refer to different software on them. In this vein, you should note that a single NNM station can perform either role, or both at once. Regardless of the role it is playing (as a collection or management station, or both), every NNM station has the full capabilities of NNM[1]. HP Service Guard clusters for UNIX systems may be used for any type of management station to ensure constant availability.

The role of a management station is to make the network management functionality available to users, either directly or via one or more management consoles.[2]

The role of a collection station is to be a collection point in the overall network management system. A collection station typically performs topology and IP status monitoring, threshold data collection, local event correlation, and event forwarding or handling on behalf of one or more management stations.

When changes occur in topology or status, or when a configured threshold is crossed, the necessary information is forwarded from the collection station to any interested management stations, so that the end-user at a management console is informed. The set of objects for which topology and status information is forwarded can be controlled via filtering.[3]

1. Only NNM Enterprise nodes (unlimited license) can receive information from collection stations.
2. See "Management Consoles" on page 24.
3. See "Use of Scalability Features in NNM Deployment" on page 89 for introductory information, and "Filters" on page 37 for more details about filtering.

Management and collection stations alike have all components of the HP OpenView NNM software running on them. The only difference is that a collection station has been designated and configured to serve one role, and a management station has been designated and configured to serve another.

Stated another way, every NNM station (regardless of operating system or license limit) is inherently a management station, but it must be configured to use the management resources of a remote collection station. Likewise, every NNM station is *also* inherently a collection station, but it must be configured to provide its data to a remote management station.

In Network Node Manager, a computer acting as a collection station is generally also a management station in its own right, with local users performing network monitoring and management, either independently or in cooperation with the users at a remote management station.

This is illustrated in Figure 1-1. In that illustration, the operator at Management Console Y can see only the nodes directly managed by NNM Station C. On the other hand, the operator at Management Console X can (depending on how the collection stations are configured) see all the objects in the entire scope of management for NNM Station A.

NNM Station View

The NNM Station view is useful in a distributed management environment. It shows you a graphical representation of the collection stations and management stations in your topology. You can use this view to troubleshoot communications between collection stations and management stations. See "Identifying Collection Station Communication Problems" on page 145 for detailed information.

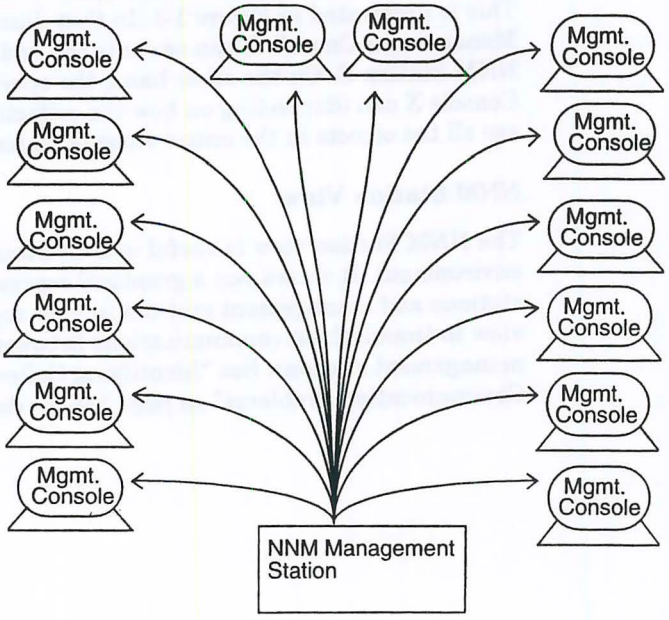
RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0652
Doc 3740

Management Consoles

One of the main problems associated with managing large networks is providing access to enough operators to handle all the objects in the map.

With HP OpenView Network Node Manager, you can have many operators simultaneously monitoring your network, as shown in Figure 1-2, operating from the same topology database and sharing common discovery and monitoring processes at the management station. Operators can share one map, or have individual maps. The limit on how many again depends on the size of your environment and the resources available to the management solution. For the most current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide*, available at `http://openview.hp.com/`.

Figure 1-2 Multiple Management Consoles



Consoles run on UNIX[4] or Windows[5] operating systems work with management stations on a UNIX system. These management consoles communicate with the UNIX system management station via NFS and socket connections on a LAN link. Management stations on the Windows operating system only support consoles run on Windows, not consoles run on UNIX. This is because a management station on a Windows operating system uses Windows file sharing, not NFS.

Web browsers using Network Presenter may reside on any system, including the same system as a management console. However, the web server must reside on a full management station, not a console.

4. In this manual, the term UNIX, when used without other qualifications, refers to the supported UNIX operating systems, as described in the Release Notes.
5. in this manual, the term Windows, when used without other qualifications, refers to the supported Windows operating systems, as described in the Release Notes.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0653
3740
Doc:

On-Demand Submaps

One of the potential problems with having maps that contain thousands of nodes involves the use of available memory.

The `ipmap` application[6] typically creates a hierarchy of several levels of submaps (root, Internet, segment, node). An interesting and important point is that many of these submaps are rarely, if ever, visited by an operator.

Imagine if NNM kept every submap in the map in memory at all times. In a large map, with literally thousands of submaps, this approach would create a substantial requirement for memory.

However, NNM makes it possible to specify that only *some* of the submaps be kept persistently in memory; any *other* submap is created if and only if a user requests it. This means that for a management station with a given amount of memory, you can manage maps with many more submaps containing many more objects.

The main benefit of the on-demand submap feature is a dramatic improvement in performance, especially during synchronization. Meanwhile, the features and functionality of NNM are essentially identical whether or not on-demand submaps are enabled. Whenever you double-click on an explodable object in `ipmap`, the submap opens promptly (though submaps with many objects may take several seconds to open). Furthermore, all features of NNM, including "find" and IP status propagation, work as usual.

Some applications that were created before this feature was part of NNM may not be compatible with the on-demand submap feature. They may expect certain objects to be available in memory at all times. In this case, you can use **persistence filtering** to make those objects persistent.[7] Persistence filtering provides per-object exceptions to the on-demand feature, so that certain objects and their submaps are always present in memory even if on-demand submaps are enabled.

6. See *Managing Your Network with HP OpenView Network Node Manager* for information about this and other key NNM processes.
7. See "Persistence Filtering" on page 68 for details.

Distributed Threshold Monitoring and Event Forwarding

In an NNM distributed environment, it is necessary that operators at the management console be aware of critical events wherever they occur. This is commonly called "management by exception." For this reason, NNM has the ability to forward events, typically from collection stations to management stations.

Using the graphical `Event Configuration` window, you can configure any event, on a case-by-case basis, to be forwarded to any or all of the following:

- All managers currently using the NNM station as a collection station.
- Particular hosts, identified by hostname or IP address.
- Hosts listed (by hostname or IP address) in a specific file.

All configurable events, including threshold events, can be configured for forwarding. Internal NNM events are automatically forwarded to management stations as needed.

When defining new events, we recommend that you use multiple varbinds with individual pieces of data rather than using a full string. This allows the receiving machine to specify the formatting. Refer to the reference page in NNM online help (or the UNIX system manpage) for *trapd.conf* more information.

General Events

You can forward any or all events from collection stations to management stations. This is most useful when a collection station receives little or no local attention, or when you have applications that issue events which you want to have forwarded to the management station.

For example, suppose you have a collection station that monitors an agent that generates an event called `FuseIsLit`. At the collection station, you can configure that event to be forwarded to the management station, and thereby alert the operator that the device is not functioning properly.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0654
3740
Doc:

Threshold Events

Threshold events give you a way to be notified of traffic patterns that are outside normal expectations. For example, you could set a threshold to monitor disk utilization on a server. If the amount of free disk falls below the threshold you set, NNM can notify an operator, or take other predetermined actions (such as mailing a message). Threshold events help operators detect and isolate problems as they arise, before users experience difficulty.

In the context of a distributed network management solution, the ability to forward threshold events means that the management station does not itself have to perform data-collection on all the objects that need thresholds monitored. That effort, and the associated network traffic, is delegated to the various collection stations that the manager uses.

Trend Data Collection in a Distributed NNM Solution

Some users may be interested in having trend data collected at remote locations and forwarded back to a central point, such as an NNM management station, for trend analysis.

Distributed data collection doesn't reduce the load on a management station if the data is sent back to the management station in real time. Therefore, in NNM the remote station stores any trend data in its own database. Data can then be transferred to a relational database if that is available.[8]

NNM does not provide a way to automatically synchronize data back to the management station. It does, however, offer some basic tools that you can use to create custom solutions. For example, you can transfer NNM's data files from the collection stations to the management station (via FTP or a similar utility) during off-peak periods. Then you can use NNM's data-merging tool (see the *ovcoltosql* reference page in NNM online help (or the UNIX system manpage)) to merge the data into an SQL database. Then you can use database tools to create reports on the data.

8. See *Reporting and Data Analysis with HP OpenView Network Node Manager* for information on supported database.

Large-Map Viewing Support

When a submap contains hundreds of nodes, the symbols and connections get smaller, and it becomes difficult to make sense of the graphical picture. Also, changes in status are not as noticeable.

HP OpenView Network Node Manager has two features that make it easy to use maps that contain hundreds, even thousands, of nodes:

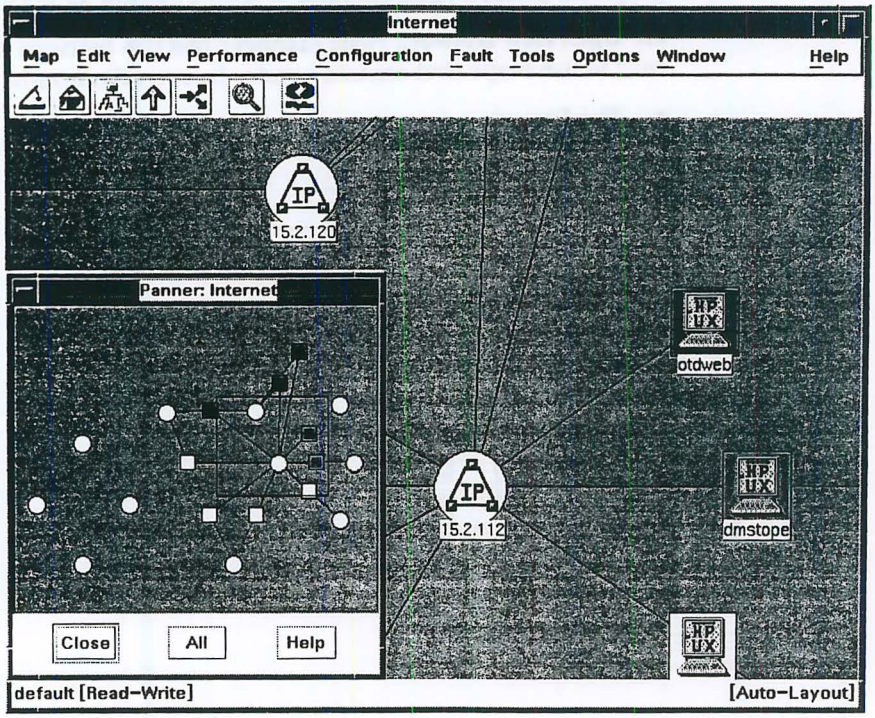
- The Panner
- The Quick Navigator

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0655
3740
Doc:

The Panner

The panner, shown in Figure 1-3, provides a way to zoom in on regions of a submap, and drag the zoomed region around. See *Managing Your Network with HP OpenView Network Node Manager*, or NNM's online help, for details.

Figure 1-3 The Panner



The Quick Navigator

The Quick Navigator is a special window that you can customize easily for quick access to your most frequently visited submaps. Your tool bar has a Quick Navigator button, which is described in the online help.

Each operator can customize their own Quick Navigator window by following the simple directions in the online help.

2 The Scalable Architecture of Network Node Manager

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0656
3740
Doc:

This chapter contains more detailed information about the distribution and scalability features of HP OpenView Network Node Manager (NNM). It includes diagrams and descriptions of the major elements of the distributed, scalable NNM architecture, and shows how data moves through the system.

NOTE

The information in this chapter is not introductory; readers are assumed to have read the previous chapter. Readers are also assumed to be conversant with NNM's key features for network monitoring, data collection, event handling, and so on. This includes a functional understanding of some key services (background processes on UNIX systems) in non-distributed NNM, including `ovw`, `ipmap`, `snmpCollect`, `ovtopmd`, and `netmon`. See *Managing Your Network with HP OpenView Network Node Manager* for details about the key services in Network Node Manager.

Later chapters contain guidelines on how to deploy NNM effectively in your organization, and specific configuration procedures to use with the scaling and distribution features of NNM.

The Distribution Model for Network Node Manager

Figure 2-1 illustrates the key components of the distribution scheme implemented by NNM. This diagram is fairly complex, and much of the remainder of this chapter is devoted to explaining many of the concepts it illustrates.

The diagram shows several components that can, and often do, run on different systems. These include full NNM management stations, NNM 250 management stations, NNM stations in the role of collection stations, and management consoles. These components can be run in any combination of supported operating systems (except for management consoles: Windows operating system servers can only serve Windows operating system clients).

NOTE The Windows operating system workstation provides status and topology information on IP and IPX devices. The IPX information exported by the Windows operating system collection station is passed to the UNIX system management station, thus providing a graphical representation of the IPX network topology and status of the individual devices.

In Figure 2-1, stations with no local management console are labeled as collection stations; stations that do have a local management console are labeled as management stations.

NOTE The labelling of management and collection stations in Figure 2-1 is for illustrative purposes only; most (if not all) collection stations also serve as management stations. See "About Management Stations and Collection Stations" on page 22.

Again, whether a particular system is a management station or collection station may be a matter of whose point of view one has at the moment. From the point of view of an operator at Management Console

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0657
3740
Doc:

1, it appears that NNM Station C is a collection station (just like NNM Station D). But from the point of view of an operator at Management Console 4, NNM Station C is the management station he is using.

Each management station can support approximately 15 management consoles via a LAN connection. The management consoles run the per-operator services, freeing up resources on the management station. A later section of this chapter covers this in more detail.[1] As shown in Figure 2-1 at NNM station A, it is still possible to run the per-operator services on the management station, routing the display to an X terminal, or, for NNM on a Windows operating system, a Windows operating system console connected to a Windows operating system collection station.[2]

The number of devices that a full NNM management station can manage in a distributed configuration varies with several different factors:

- The management station's resources (CPU, memory, and disk storage)
- Network performance
- Status and discovery polling intervals
- The level of data collection and threshold monitoring you have configured
- The number of collection stations being managed
- The number of nodes being managed by each collection station

For more information on selecting and sizing the correct computer system for your NNM management station, see the latest version of the *NNM Performance and Configuration Guide*.

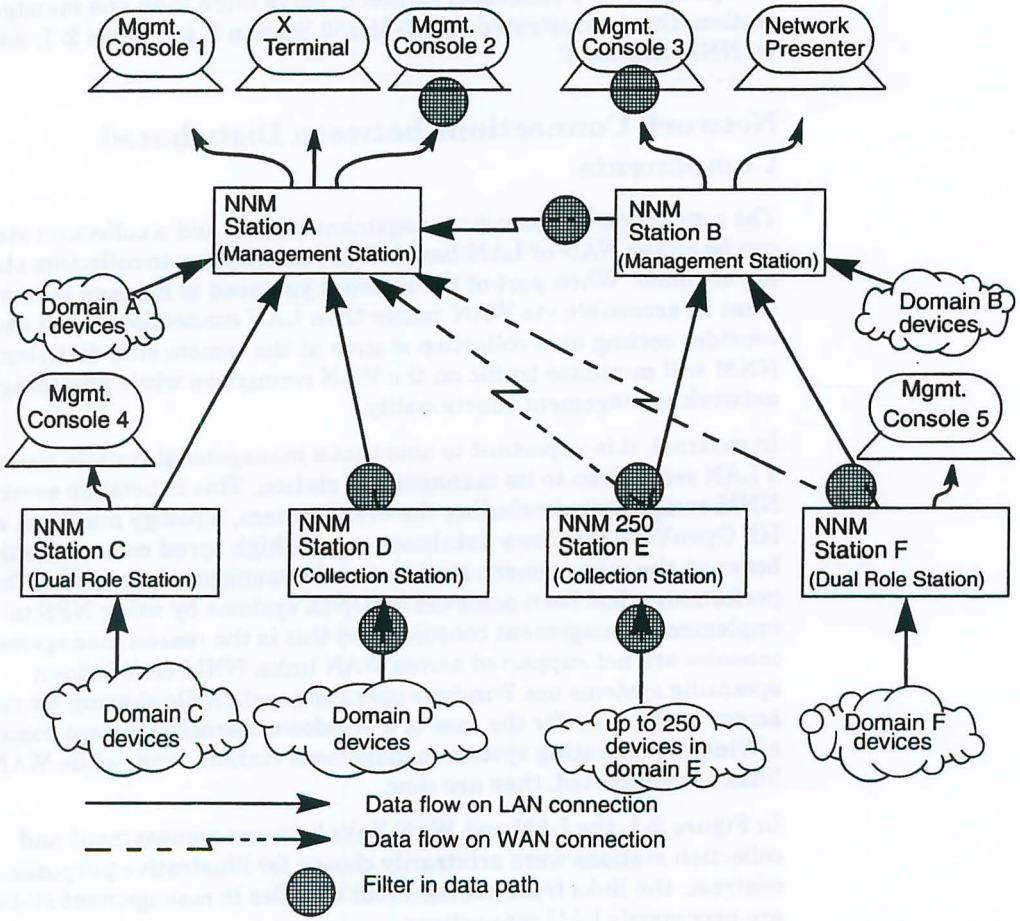
To attain your desired IP monitoring response times, you need to maximize the management station resources and set polling intervals to the maximums you can tolerate.

The only differences between a full NNM management station and an NNM 250 management station are that the NNM 250 management stations can manage only up to 250 nodes per license and cannot manage collection stations.

---

1. See "Management Consoles" on page 70
2. See also "Management Consoles and X-Terminals" on page 73

Figure 2-1 The Distribution Model for Network Node Manager



With NNM, it is also possible to obtain management information from one or more NNM stations acting as collection stations. In Figure 2-1, most of the NNM stations (Stations B, C, D, E, and F) are operating in the role of collection stations.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0658
3740
Doc:

Stations C and F illustrate how an NNM station can have the role of a management station (possibly making use of collection stations), a collection station (serving one or more management stations), or both roles at once.[3]

It is possible for a collection station to serve more than one management station; this is illustrated by NNM 250 Station E in Figure 2-1, and also by NNM Station F.

Network Connections between Distributed Components

The connection between a management station and a collection station can be either WAN or LAN-based. WAN connections to collection stations are common. When part of the network you need to manage is remote (that is, accessible via WAN rather than LAN connections), you should consider setting up a collection station at the remote site; distributing NNM will minimize traffic on the WAN connection while providing full network management functionality.

In contrast, it is important to note that a management console must have a LAN connection to its management station. This is because several NNM components (including the event system, topology manager, and HP OpenView Windows database) require high speed communication between the management station and the management console. This performance has been achieved on UNIX systems by using NFS to implement management consoles, and this is the reason management consoles are not supported across WAN links. NNM on Windows operating systems use Windows operating system file sharing for remote access to the files (for the case of a Windows operating system console to a Windows operating system management station), and, while WAN links are supported, they are slow.

In Figure 2-1, the LAN and WAN links between management and collection stations were arbitrarily chosen for illustrative purposes. In contrast, the links from management consoles to management stations are necessarily LAN connections.

3. See "About Management Stations and Collection Stations" on page 22.

Filters

The function of most filters is to select network management data that is of sufficient value to be kept, and to eliminate other data.[4] Data that is useful at one point (say, a site management station) can be filtered out before it gets sent to another (say, regional management station) where it is unneeded.

NNM uses two basic types of filters:

- A **data-stream filter** acts as a sieve through which objects flow. This type of filter contains criteria that permit some objects to proceed, and blocks other objects. Downstream from a data-stream filter, the data stream includes only those objects that the filter passed; other objects are blocked, and thus eliminated from the data at the point of the filter.

  Note that once an object has passed a data-stream filter, later changes to the filter have no effect on it. It remains in the data stream.

- A **set-defining filter** is applied to a pool of candidate objects, and determines which objects belong in the final set based on the criteria contained in the filter. Before a new object can be added to the set, it is tested by the set-defining filter to determine if it is a valid member or not.

  If a set-defining filter is changed, all candidate objects are reevaluated to determine which ones belong in the new set and which do not. Then the set is reconstituted out of valid members.

The difference may seem abstract at first. As an analogy, you can compare a data-stream filter to a wire-mesh sieve, of the kind used to sort stones. Once a large stone has passed through the sieve, it is in the sorted pile beneath regardless of whether you later switch to a finer mesh in the sieve.

Imagine, on the other hand, that your sieve behaved like a set-defining filter. In that case, changing to a finer mesh in the sieve would cause all the source material to be refiltered, yielding a sorted pile of uniformly smaller stones.

4. See "Persistence Filtering" on page 68 for an important exception.

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0659
3740
Doc:

In either case, remember that a filter specifies or describes the objects you want it to pass, *not* the objects you want it to reject. When the filter is applied, it passes the selected objects through, eliminating the rest from the data stream. As a user, you can apply filters only to object data; however, applications can filter events also.[5]

Filtering is based on the information contained in a subset of the fields of the object database (ovwdb).[6] These fields are candidates to be all or part of the criteria by which objects are assessed in a filter.

Filters can eliminate unnecessary data at different points in the system:

- Discovery filtering at any NNM station.
- Exported topology filtering at the collection station.
- Map filtering at the management station.
- Failover filtering on the management station.

Table 2-1, Comparing Types of Filters, compares the types of filters. See "Filter File Example" on page 189 for more information.

Table 2-1 Comparing Types of Filters

Filter Type	Apply on Incoming Data	Reevaluate If Filter Changes	Purpose	Applied So Data Is	Reference
Discovery	X		Limit scope of objects added to database.	Excluded	page 40
Topology	X	X	Limit information forwarded from collection station to management station.	Excluded	page 41

5. Interested application developers should see the *HP OpenView Integration Series: SNMP Developer's Guide*.
6. See "Filterable Objects and Attributes" on page 181 for specifics.

Table 2-1 Comparing Types of Filters (Continued)

Filter Type	Apply on Incoming Data	Reevaluate If Filter Changes	Purpose	Applied So Data Is	Reference
Map	X	X	Show only items of interest to operator on map.	Excluded	page 42
Persistence	X	X	Disable on-demand submaps for third party applications.	Included	page 68
Failover	X	X	Limit nodes polled by management station when collection station fails.	Included	page 52
Important Nodes	X	X	List unreachable important nodes as primary alarms in the Alarm Browser rather than children of a connector down event.	Included	*Managing Your Network with HP OpenView Network Node Manager*
DHCP Range	X		Identify DHCP (shared or floating) IP addresses	Included	*Managing Your Network with HP OpenView Network Node Manager*

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0660
Doc. 3740

Discovery Filtering

Discovery filters specify which devices an NNM station is actively discovering and monitoring. The purpose of discovery filtering is to reduce the discovery and monitoring effort of the station. Different stations have independent (though possibly identical) discovery filters.

Discovery filtering limits the scope of objects that `netmon` adds to the collection station topology database. To unmanage objects and limit the set of nodes that are polled at all, refer to *Managing Your Network with HP OpenView Network Node Manager*. The filter may be set to pass, for example:[6]

- Gateways.
- Bridges, routers, and hubs.
- All devices.
- Nodes based on their `sysObjectID`.
- Objects inside or outside of a particular range of IP addresses.

By default, Segments and Networks pass the discovery filter.

Discovery filtering is achieved by configuring the `netmon` service[7]; the filter is then applied to all newly discovered objects. Objects that are rejected by the discovery filter never appear in any topology or object database.

Discovery filters are data-stream filters; changes to a discovery filter affect new data *only*. All objects that previously passed the filter remain in the data stream, regardless of whether they would currently pass or not, and polling is still done on all previously discovered objects whether or not they would now pass the filter. You can, however, use the `ovtopofix` command to change the set of previously discovered objects.[8]

7. See "Configuring a Discovery Filter" on page 128, for details, *netmon* and *xnmpolling* reference pages in NNM online help (or the manpages on UNIX systems), the NNM online help, and "Distributed Services Architecture" on page 48.
8. See the *ovtopofix* reference page in NNM online help (or the UNIX system manpage) for details.

Implement any discovery filtering on an NNM station before you begin using it as a collection station; this will improve overall performance, by reducing the amount of synchronization effort.

Topology Filtering

Topology filters specify which topology data gets forwarded to a management station. The result is less management traffic on the network and lower data storage requirements at the management station. By default, the topology filter does not pass Networks and Segments.

A topology filter at a collection station defines the subset of topology data that management stations can see. The idea is to have the topology filter at the collection station pass information about only those objects in which the manager is interested. Data about objects outside the manager's interest doesn't clog up the link to the management station.

Objects rejected by a topology filter remain in the collection station's topology database. They are not, however, provided to a higher-level management station. Each collection station has only one topology filter in place. Note that this means the topology filter of a collection station must meet the needs of all management stations.Through topology filtering, you can choose to provide the following kinds of topology data to interested managers (many other choices exist):[9]

- All topology data, by using no filter at all.
- Nodes with (or specifically without) a certain `sysObjectID`.
- Objects inside or outside of a particular range of IP addresses.
- Nodes from a particular vendor.
- Objects with particular physical address.
- All token ring segments.

Topology filtering is achieved by configuring the `ovtopmd` service.[10] You should test topology filters at the collection station before the station goes into service.[11]

9. See "Filterable Objects and Attributes" on page 181 for specifics.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0661
3740
Doc:

Topology filters are, technically, data-stream filters. However, in effect, any change to a topology filter affects new and old data *alike*. When a topology filter is changed, the topology database of the management station is resynchronized with the filtered collection station topology database. Some objects may be deleted from the management station topology (if they do not pass the new topology filter), and some objects may be added (if they were previously rejected, but now pass the topology filter). As a result, the database of the management station ends up reflecting the topology being passed by the new topology filter, so the effect is that of a set-defining filter.

NOTE Topology filters do not affect the events that are passed from collection stations to management stations. This means that any events that you have configured to be forwarded are in fact forwarded from the collection station to the management stations, regardless of whether the objects to which the events refer pass the topology filter or not. Listing particular event sources in the event configuration at the management station can reduce the likelihood of operator confusion.

Map Filtering

The purpose of map filtering is to give the operator visibility of only those objects in which he or she has interest. By default, Networks and Segments do not pass the map filter.

Map filtering occurs on a per-map basis, not a per-display basis. All operators who use a particular map have the same filtered view. Additional maps can be created and separately filtered for specific purposes.

10. See "Distributed Internet Discovery and Monitoring" on page 46, Chapter 4, Procedures for Scaling NNM, and the *ovtopmd* reference page in NNM online help (or the UNIX system manpage), for further details.
11. See the reference page in NNM online help (or the UNIX system manpage) for *ovtopodump*, especially the `-f` option, for instructions on testing topology filters.

Objects that are rejected by a map filter remain in the management station's topology database, and are still subject to status polling. Events from these objects pass through and are visible in the event subsystem, but this can be changed to show only events from objects on the operator's current map.[12]

Like the previously discussed types of filtering, map filtering can be configured so that (regardless of how much other topology data exists in the database) the map seen by the operator displays only the objects of interest to that operator. In general, this means objects that match some combination of attributes and attribute values; among the many choices, this can include:[13]

- All objects, by using no filter at all.
- Connectors, networks, and segments only.
- Nodes with specific `sysObjectIDs`.
- Bridges, hubs, and their segments.
- Objects inside or outside of a particular range of IP addresses.
- Only nodes that support SNMP.

Map filtering is generally configured in the NNM interface.[14]

Map filters are set-defining filters. When you change a map filter, all the objects currently in the map are reevaluated to see if they pass the new filter; new objects must also pass the filter before being added to the map.

Defining New Filters

All filters, discovery, topology, map, and persistence, are configured by creating a text file in which you use a special filter definition language to define filters that pass and reject objects in the ways you want.[15]

---

12. See the *xnmevents* reference page for details on the "filter by map" feature.
13. See "Filterable Objects and Attributes" on page 181 for specifics.
14. See the online help and Chapter 4, Procedures for Scaling NNM, for further details.
15. See Appendix A, The Filter Definition Language, for details on the syntax, semantics, and mechanics of filter definition.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0662
3740
Doc:

NOTE While you can create multiple filter definition files, you can use only one at any given time. Hence, only the filters defined in the currently in-use filter definition file are available.

You can give each filter you define a sensible name. For example, a map filter that would pass only routers might be named `Routers`.

Effective use of filtering lets you monitor a broader domain with a given management station. For example, suppose you have a site with 5000 workstations and PCs connected by 300 hubs and routers.

If you are only interested in the connecting devices, you might be able to use a single collection station with filters configured to discover and monitor only the 300 hubs and routers. Without such filtering, monitoring all 5300 nodes might require three or more collection stations to maintain equivalent performance.

NOTE As a rule, the sooner you can filter out a particular object, the better overall performance of the network management solution will be. For example, by using discovery filtering to discover and monitor exactly and only those objects of interest, you can dramatically reduce the amount of data that all other parts of the system have to handle. The next-best type of filter, to reduce the data load on the distributed management system, is a topology filter. While a local collection station may need broader discovery for its own management domain, the management stations that use the collection station frequently do not require a full copy of the topology at the collection station; topology filtering is the way to prevent unnecessary data from being exported to the management station.

Filter Utilities

NNM provides the utilities shown in Table 2-2, Filter Utilities, to help you build filters that do what you want and expect.

Table 2-2 Filter Utilities

Utility Name	Description
On Windows operating systems: *install_dir*\bin\ovfiltercheck On UNIX systems: $OV_BIN/ovfiltercheck	Provides syntax validation for a filter file. Can also be used to check individual Set, Filter, and Filter-Expression statements for correct syntax.
On Windows operating systems: *install_dir*\bin\ovfiltertest On UNIX systems: $OV_BIN/ovfiltertest	Tests all or part of a specific object database (ovwdb) against a filter. Objects that pass the filter are reported to the output. Use the -c option to specify a collection station to determine which objects the management station polls on failover.
On Windows operating systems: *install_dir*\bin\ovtopodump On UNIX systems: $OV_BIN/ovtopodump	Use the -f option to compare a filter against the current topology database.

See the reference pages in NNM's online help (or the UNIX system manpages) for these commands to obtain details on their syntax and use.

RQS nº 03/2005 - CNPJ
CPMI - CORREIOS
Fls. Nº 0663
Doc 3740

Distributed Internet Discovery and Monitoring

Distributed Internet Discovery and Monitoring is one of NNM's keys to providing a scalable network management solution. The purpose of this section is to give you a picture of exactly which parts of NNM are distributed, and how data flows through the distributed solution. With this knowledge, you will be able to better understand what is occurring as you deploy NNM.

About Collection Domains

Within the NNM model of distribution outlined in "The Distribution Model for Network Node Manager" on page 33, it is useful to distinguish these two sets of objects:

Management domain

This is the set of all objects that are of interest to the user. In Figure 2-1, the management domain of the operator at Management Console 1 contains all the objects in the whole network (except objects that are removed by intervening filters). On the other hand, the management domain of the operator at Management Console 6 consists of only the objects directly monitored by Station F; no other objects are visible from that station.

Keep in mind that the management domain is an attribute of the management station, not the operator. Different operators might deal with different subsets of the management domain, based on map definitions and map filters.

Collection domain

This is the set of objects that are directly discovered and monitored by an NNM station. This typically includes any objects on which data collection (for trends or thresholds) is occurring.

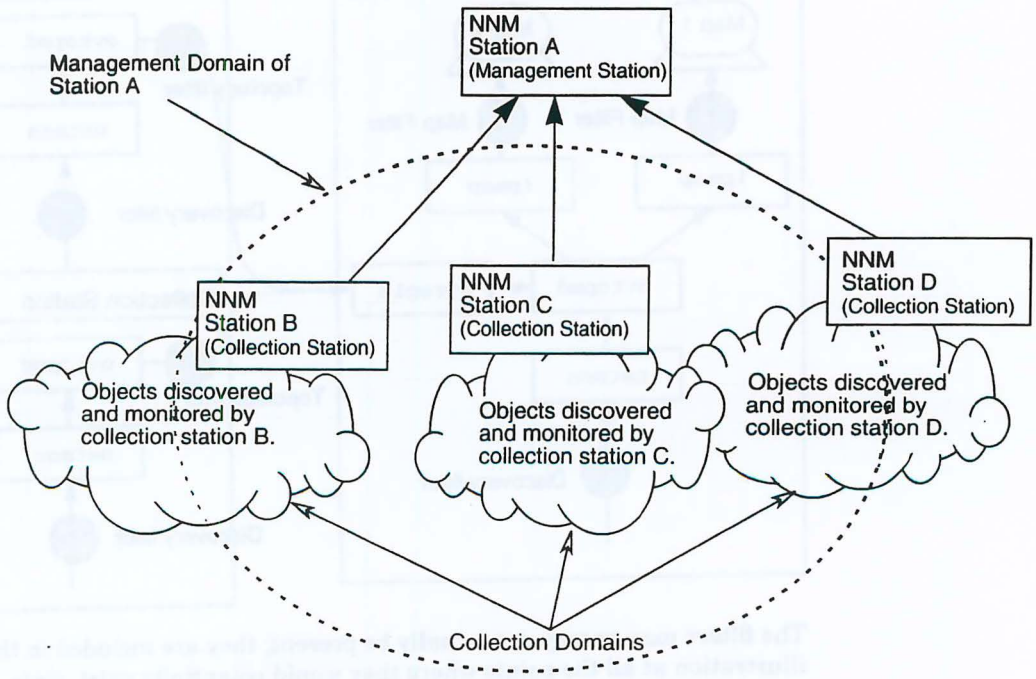
At a high level, these definitions can be depicted as in Figure 2-2.

In the diagram, the management domain of station A does not include all the objects in the collection domains of all the collection stations. Remember, the collection stations are probably management stations too. For each of these, the management domain is coincident with the collection domain.

However, the administrator of the overall network, working from Management Station A, is quite possibly very selective about which objects within the various collection domains of the collection stations are of interest to operators at the management station.

You can use filtering to select exactly those objects, and thus constrain your management domain to those objects that make the most sense for you.

Figure 2-2 Management and Collection Domains



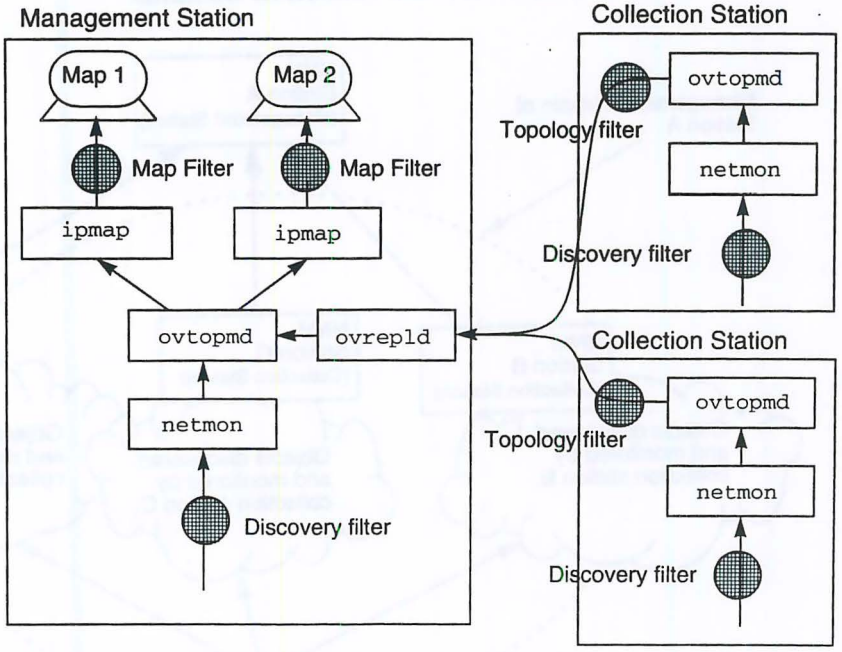
RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0664
3740
Doc:

Distributed Services Architecture

Network Node Manager relies on the complex interplay of several different services (background processes on UNIX systems) to provide the level of functionality and performance you need. In making NNM a scalable solution, several of these services appear in locations remote from the management station.

Figure 2-3 is a diagram of the key services involved in a distributed deployment of NNM. Of these, the `ovrepld` service is central to the distribution of network topology; the others have other, stand-alone functionality. The `ovrepld` service is the "replicator" of the topology, responsible for integrating topology data from multiple collection stations into the management station's topology database.

Figure 2-3 **Service Components in Distributed Internet Monitoring**



The filters may or may not actually be present; they are included in the illustration at all the points where they would potentially exist. Note also that when a collection station is also fulfilling a local management

role, it runs local ipmap and ovw services too. And finally, understand that in the interest of simplicity, Figure 2-3 omits the role of the event system, which is illustrated in Figure 2-4.

How Distributed Internet Discovery and Monitoring Works

Figure 2-3, shows two collection stations working on behalf of the management station. Each collection station has its own collection domain, which is the responsibility of the local netmon service. You can set discovery filters to minimize unnecessary discovery and monitoring.

Having a station take the role of a collection station, or make use of collection stations, requires several other configuration steps. "Configuration Concepts" on page 56 introduces these configurations steps, and "Configuring Collection Stations" on page 133 gives complete details.

After the stations have been configured correctly, start the collection station as usual. The netmon service begins IP and level-2 discovery, and (along with the ovtopmd service) populates the local topology database.[16] It takes time for this process to finish, but to minimize management traffic on the network, you should allow NNM to finish (or nearly finish) discovery before you begin to use it as a collection station. The Performance:Network Polling Statistics tool can help you determine when the collection station has reached a steady state.[17]

After waiting for the collection station to build its topology database and reach a steady state, the management station administrator uses the xnmtopoconf command to begin using the discovery and monitoring services of the collection station.[18]

At this point, the management station obtains access to the topology data at the collection station. It requests the collection station to send the objects in the collection station's topology database across the network. If the collection station has a topology filter configured, only those objects that pass the filter are provided to the management station.

16. See *Managing Your Network with HP OpenView Network Node Manager* for details about these and other services (background processes on UNIX systems) in Network Node Manager.
17. See the online help about this tool for more information about the procedure.
18. See the reference page in NNM online help (or the UNIX system manpage) for *xnmtopoconf*.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0665
3740
Doc:

Topology data that is not derived from a local `netmon` service is not sent to the management station. This precludes the possibility of cycles (where station "A" discovers and reports "B," which discovers and reports "C," which again discovers and reports "A," ...). It also precludes indirect multiple-level hierarchical management.[19]

The `ovrepld` service on the management station replicates the topology data from the collection station in the local topology database. "Replication" does not imply a 100% mirroring of the collection station topology database at the management station. Remember that topology filtering at the collection station means that some of the objects present in the collection station's topology database may *not* be present at the management station. The topology data that *does* pass the topology filter is kept synchronized between the collection station and the management station.

NOTE

The `ovrepld` service provides synchronization of the topology data *only*. It does not affect any other databases (such as `ovwdb`, `snmpCollect`, or `ovw`).

Once the topology merging is done, the `ovtopmd` service treats the new objects just like objects obtained from the local `netmon` service.

After the synchronization phase is complete, only *changes* in status and topology get sent to the management station. The `ovrepld` service updates the topology database of the management station to reflect the changes.

High Availability Management Information

One way to ensure your network management information is always available is to run your management stations on HP Service Guard clusters. If the primary processor goes down, processing automatically and transparently rolls over to another processor in the cluster. Configure Service Guard NNM stations using the `ov.conf` configuration file parameter `HOSTNAME=`. See the *ov.conf* reference page in NNM online help (or the UNIX system manpage) for more information.

19. See "Hierarchical Management" on page 98, especially Figure 3-4 and Figure 3-5, for more information on multilevel hierarchical management.

As part of the Service Guard interface, NNM offers `ovwrs` (self-restarting `ovw`). This interface runs `ovw` while monitoring the status of the console server process on the management station. If the connection to the server is lost, the it informs the user and re-establishes its connection to the server. See the reference page in NNM online help (or the UNIX system manpage) for *ovwrs* for more information.

Collection Station Failover

NNM also provides capability to continue data collection when a collection station goes down. The management station's `ovrepld` service performs periodic status checks to verify the status and state of the currently managed collections stations. When a status check fails, the status of the collection station is downgraded one level. The default interval between checks is five minutes (but this can be reconfigured via the `xnmtopoconf` command). Thus, it will take 20 minutes before a "Collection Station Critical" event is generated; an event confirmation popup dialog is presented to the operator. The nodes affected by the failure are left with the status they had at the time the collection station stopped responding.

Collection Station failover enables a management station to take over status polling responsibilities for a collection station which is temporarily unreachable. When the collection station returns to normal, the management station returns to its previous state, delegating discovery and monitoring of those objects to the collection station. This feature is not intended to provide support for collection stations which will be down for a long time or which have been permanently removed from service.

In order to prevent `netmon` from being overloaded, failover only takes over status polling, not the full responsibilities of the collection station. Discovery and SNMP configuration polling are not picked up.

When the collection station returns to normal operation, the management station removes the failed over topology list from its polling queue and resynchronizes with the collection station. The status from the collection station is considered to be current, which means it takes priority and overwrites the status for the objects where were stored in the management station database.

IP and IPX (Windows operating systems) collection stations can failover to a management station. IPX interfaces from a Windows operating system collection station are not polled by a UNIX system management station.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº
3740
Doc:

You control failover operations through the management station's `Options:Network Polling Configuration:IP` menu selection, "`Status Polling`" tab; or through the `xnmtopoconf` flags "`failover`," "`nofailover`," and "`failoverFilter`." Refer to the reference page in NNM online help (or the UNIX system manpage) for more information.

Failover Filtering

The default operation is for the management station to pick up status polling responsibility for all nodes loaded in the management station's topology from that collection station. However, you can control the load on the management station by providing a failover filter that lists specifically which nodes should be polled. The failover filter behaves like a discovery filter which loads networks and segments, and then filters on nodes and interfaces before the data is given to `netmon`. The interfaces and the node to which they are attached are considered a unit. If one interface on the node passes the filter, then the entire node and all of its interfaces that the collection station polls pass the filter as well. You determine which objects are picked up on failover on a collection station by collection station basis.

Failover Considerations

The management station must have access to the interfaces which are to be picked up in a failover situation. A route needs to exist to the interface to be polled.

The possibility of overloading the management station is a consideration when configuring failover. The devices for which continuous status polling is especially important, such as routers and gateways, are good candidates for inclusion in a failover filter. The management station needs information about connection devices in order to detect secondary failures.

Overlapping Collection Domains

Reexamine Figure 2-2, and notice that sometimes the objects in the collection domain of one collection station are *also* within the collection domain of a different collection station.

For example, in Figure 2-2 the collection domain of Station C overlaps that of Station D, and both serve as collection stations for Station A. Such instances are not uncommon in practice. It is easy to imagine a

router that Stations C and D both care about and monitor. At Station A, that one router will appear in the topology data arriving from both collection stations.

When a management station receives multiple versions of the same object from different collection stations, it uses the rules described in the next section to automatically choose one version as the "primary" version; it then treats all other versions as "secondary."

The station that provides the primary version of an object's data is called the **primary collection station** for the object; any other station that provides information about that object is a **secondary collection station** for the object.

Note that a collection station can be a primary for one object, and a secondary for another object. In other words, the choice of primary vs. secondary is on a per object basis, not a per station basis. Furthermore, a collection station does not know or care whether it is the primary or secondary station for a given object.

Only the primary version of data is displayed in the operator's map. Unless you specifically request information from a secondary version, all topology queries return information from the primary version.

Overlapping collection domains cause redundancy and can therefore waste memory, processing and network resources. In order to reduce the overlap, set the DeleteSecondary mode via `xnmtopoconf` on the management station.

The Selection of Primary and Secondary Collection Stations

NNM uses several rules to decide which of several versions of an object is primary (and by implication, which collection station is the primary collection station). The rules are evaluated in order, and the first rule that distinguishes a primary collection station is applied and the process terminates; remaining rules are ignored.

The rules NNM uses to establish the primary collection station for an object are as follows:

1. If only one station is reporting the object, that station is the primary collection station for the object.
2. If the object is an interface (`isInterface == TRUE`), skip to rule 7.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0667
3740
Doc:

3. If only one station reporting the object is *a.)* managed (meaning currently in active use as a collection station), and *b.)* has noncritical status or has failed over, that station is the primary collection station for the object.
4. If the user has expressed a preferred primary collection station for the object[20], that station is the primary collection station for the object.
5. If only one station reporting the object is managing the object (meaning actively managing it, either by default or via `Edit:Manage/Unmanage Objects`, that station is the primary collection station for the object.
6. If one station reporting the object is a gateway, that station is the primary collection station for the object. (A gateway is a node with multiple interfaces performing IP routing functions.)
7. If the object (A) is completely contained in another object (B), the collection station for the container object (B) is the primary collection station for the object (A). For example, a non-gateway node should have the same primary collection station as the network that contains it.
8. If one of only two stations reporting the object is non-local, the non-local station is the primary collection station for the object.
9. The first station to report the object is the primary collection station for it.

You can express a preferred primary collection station for an object.[21] However, you should be aware that if conditions force NNM to reevaluate the primary collection station, your preference may be temporarily overridden, according to the preceding rules.

---

20. See the *xnmtopoconf* reference page in NNM online help (or the UNIX system manpage), especially the `-preferred` and `-clearPreferred` options.
21. See the *xnmtopoconf* reference page in NNM online help (or the UNIX system manpage).

For example, suppose the preferred primary collection station you selected for an object goes down and you have configured `nofailover`. If a secondary collection station can pick up reporting for that object, that station becomes the primary collection station for the object until the preferred primary station is again available.

If the down primary collection station has failed over to the management station, the management station does not make its local version of the object the primary. Where failed over objects were in overlapping domains with the management station, `netmon` handles the duplicate objects by only polling the device once and updating all of the objects with the status.

A management station will not pick up status polling on secondary objects during failover. There is already a primary collection station still providing information for those objects.

Overlaps with the Collection Domain of the Management Station

In some cases, particularly when an existing large collection domain is partitioned by collection stations, the collection domain of the management station overlaps the collection domain of a collection station. The question then arises, what should be done with the secondary (local) version of information about objects in the overlap?

You have three choices:

1. "`Allow Overlap`", which means that the `netmon` running on the management station should continue polling the node even though a collection station is also polling the node. This would also accept the associated resource consumption caused by duplicate monitoring (potentially over an expensive link) and duplicate information in the topology database.
2. "`Unmanage Secondary`", which unmanages the local version of objects (networks, segments, and nodes) in the overlap region, but keeps them in the database. (The local unmanaged version of the object will not be shown on any maps.) This eliminates the duplicate polling, but still incurs the data storage overhead. If the collection station should fail, the management station can be made the primary collection station to quickly restore management to the affected objects. This will not happen automatically. Refer to "Changing the Primary Collection Station for an Object" on page 151 or to the *xnmtopoconf* reference page in NNM online help (or the UNIX system manpage) for information on configuring failover.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0668
3740
Doc:

3. "`Delete Secondary`" deletes the local version of overlapping objects from the topology database. This eliminates the overhead of both duplicate monitoring and duplicate objects in the database. You then rely on the collection station to provide all information about the objects in the overlap.

   When this is the mode, a local version of any overlapping networks is retained in an unmanaged state. The `netmon` on the management station will not discover nodes that belong to an unmanaged network. If a collection station fails, you will have to delete the collection station, then manage the networks and wait for `netmon` to discover the nodes that have been deleted unless you have failover configured.

The third option is the default behavior of an NNM management station. However, only non-connector nodes are deleted; NNM does not delete networks, segments or routers that overlap with the collection station's collection domain. This maintains visibility to the boundary of the collection domain of the collection station even in the event of collection station failure. The local versions of connector objects are put in the "unmanaged" state. If the normal primary collection station for these objects becomes unavailable, the local versions can become the primary version.

You can choose which behavior you prefer by using `xnmtopoconf`.[22]

Configuration Concepts

For a station to either be, or make use of, a collection station requires additional configuration steps.

This section provides only a brief summary of configuration to acquaint you with the general concepts, and gain a better understanding of what is required when deploying distributed IP discovery and monitoring. Detailed steps for configuring management and collection stations are provided in "Configuring Collection Stations" on page 133.

NOTE NNM does not provide remote configuration utilities. Therefore, the configuration steps used to set up a collection station have to be made from the collection station itself. You can, of course, use `telnet` to log in

22. See the *xnmtopoconf* reference page in NNM online help (or the UNIX system manpage).

and remotely configure the collection station. Similarly, you could redirect an X display from the collection station back to the management console to do the configuration, but the speed of the display will degrade noticeably when using a wide-area network connection. You may have security issues as well in taking either approach.

Overview of Collection Station Configuration

To set up an NNM station to be used as a collection station, you have to do the following:[23]

- Configure the local collection domain, including any discovery filters desired.
- Configure the exported collection domain, by setting up topology filters.
- Configure SNMP security (get and set community names) in a way that will match the SNMP security configuration on the management station.

Once the above configuration steps are done, you need to restart the platform, via `ovstart`.

About the Remote Managers List As noted earlier, a management station designates and begins to use the services of a collection station by using the `xnmtopoconf` command to begin managing the collection station.

This causes the collection station to add that management station to a list of remote managers that it maintains. The remote managers list keeps up with the changes as management stations come and go.

At various places in the NNM interface, such as the `Event Configuration` window (when you are configuring event forwarding), this list is called the "`%REMOTE_MANAGERS_LIST%`".[24] Forwarding events

23. See "Configuring Collection Stations" on page 133 for more details.
24. See "Configuring Event Forwarding and Correlation" on page 154 for more details.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0669
3740
Doc:

to this list makes system administration much easier, since you are not required to make individual updates whenever DIDM configuration changes.

For example, in Figure 2-1, suppose Station A has been using Station E as a collection station; the list of remote managers that Station E maintains includes Station A.

If Station B now starts using Station E as a collection station, it gets added to Station E's list of remote managers. That list now includes both Station A and Station B.

Overview of Management Station Configuration

To make use of collection stations, a management station needs to be configured as follows:[25]

- The `ovrepld` service must be running (it normally starts with `ovstart`).
- Any nodes on the network that are running NNM are potential collection stations; `xnmtopoconf -print` can help you identify the ones that have been discovered by the local `netmon` service. You have to select which ones you want to use, and manually add in any that have not been discovered locally. Versions of NNM that predate NNM 4.1 can not be collection stations.
- You need to configure SNMP security (get and set community names) using `xnmsnmpconf` in a way that will match the SNMP security configuration on the collection stations.

After this configuration is done, you can use the `xnmtopoconf` command to begin "managing" the collection station. In this context, "manage" means to use the IP discovery and monitoring services of the collection station.

25. See "Configuring for a Specific Collection Station" on page 138 for more details on this procedure.

Distributed Threshold Monitoring and Event Forwarding

The event subsystem for NNM allows forwarding of events (including topology changes, correlated events, and threshold events) from collection stations to management stations.

The services (background processes on UNIX systems) that NNM uses in basic event forwarding are:

- The trap service (`ovtrapd`).
- The postmaster service (`pmd`).

Figure 2-4 illustrates these services, and their relationship to other key NNM files and services.

The `ovtrapd` service is responsible for receiving SNMP traps and inform-requests on port 162 via UDP, the protocol of the SNMP standard. It buffers them, and passes them to the postmaster (pmd) service.

The `ovtrapd` service automatically provides an inform-reply to inbound SNMPv2C inform-requests.

The postmaster service routes the traps it receives from `ovtrapd` to the appropriate subsystem. Moreover, the postmaster service is the central dispatcher that all management applications (both NNM and third-party) use to communicate with each other. It uses the TCP protocol to route events between them so messages are not dropped, even over noisy or congested links.

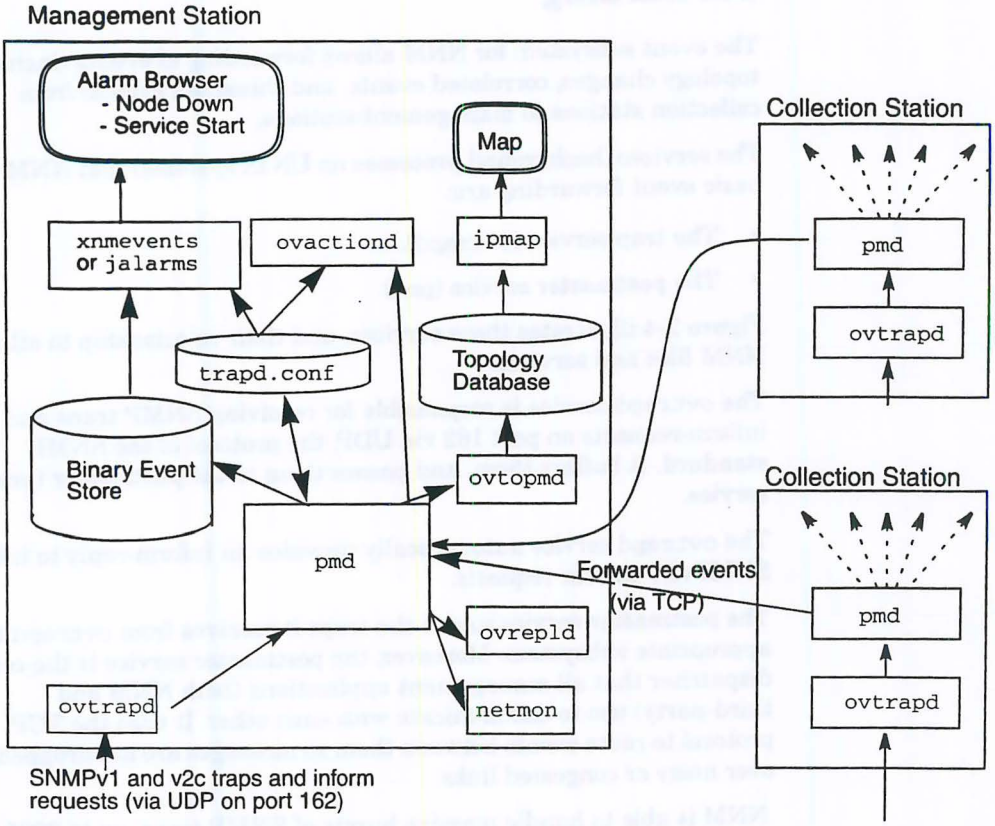
NNM is able to handle massive bursts of SNMP traps, up to 2000 per second. This is because the `ovtrapd` service can buffer traps while forwarding them to the postmaster for routing. This buffering reduces the likelihood that traps in a burst will be dropped.

The `Event Configuration` window supports event forwarding. It also supports an event-identifier naming convention, where SNMP version 1 traps, SNMP version 2C traps, and SNMP version 2C inform requests

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0670
Doc. 3740

use the same naming conventions for event IDs. See the online help and the *trapd.conf* reference page in NNM online help (or the UNIX system manpage) for details.

Figure 2-4 The Basic Event System in NNM



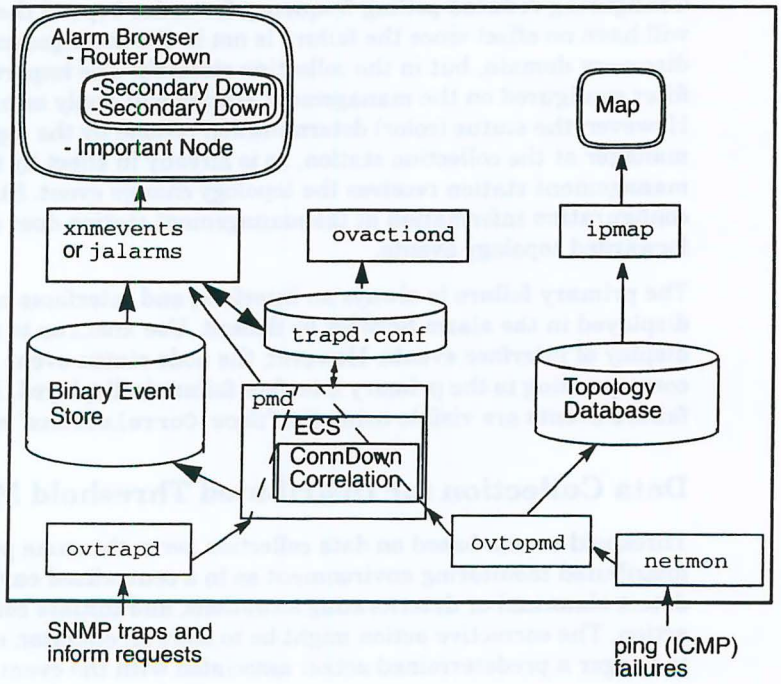
Event Correlation for "Connector Down"

One of NNM's key features is its ability to correlate incoming event information. See *Managing Your Network with HP OpenView Network Node Manager* for a complete description. The most useful correlation

rules for a distributed environment clarify information coming in when a connector (router, gateway, etc.) goes down and all the nodes beyond the connector become unreachable.

Since these events originate from netmon polling rather than from SNMP traps coming in through ovtrapd, the internal handling and forwarding is somewhat different from basic events. This is shown in Figure 2-5.

Figure 2-5 The Correlated Event System for "Connector Down"



When netmon recognizes a ping failure, which in the case of interest happens to be a connector failure, it notifies ovtopmd to update the topology database. ovtopmd notifies pmd that it has done so, and pmd runs the event through the Event Correlation System while ipmap updates the map. The correlated event then appears with a "children" indicator in the Alarm Browser.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0671
Doc: 3740

In a distributed environment, pmd forwards the topology change for the nodes to the management station. At the management station, the pmd informs ovrepld to update the topology database. When ovtopmd makes that change, it informs pmd of the topology change. pmd then handles that topology change notice just like a local topology change notice, and routes it through the ECS correlation for "Connector Down." Note that the "Connector Down" event itself was not forwarded. The management station automatically derives that event from the topology change notification.

Operation of the "Connector Down" correlation on the management station receiving the topology changes may be slightly unexpected. Configuring reduced polling frequency for nodes beyond the connector will have no effect since the failure is not in the management station's discovery domain, but in the collection station's. The important node filter configured on the management station will apply as expected. However, the status (color) determination is done by the topology manager at the collection station, so is already in effect by the time the management station receives the topology change event. Status (color) configuration information at the management station does not apply to forwarded topology events.

The primary failure is always an interface, and interfaces are not displayed in the alarm browser by default. Use xnmtrap to enable display of interface events. However, the node status event corresponding to the primary interface failure is displayed. All secondary failure events are visible using the "Show Correlations" menu.

Data Collection for Distributed Threshold Monitoring

Threshold events based on data collection serve the same purpose in a distributed monitoring environment as in a centralized environment: to detect abnormal or deteriorating situations, and initiate corrective action. The corrective action might be to alert an operator, or it might be to trigger a predetermined action associated with the event.

A collection station can independently collect data (from the objects that it monitors) for threshold monitoring. When a threshold event is triggered, it can be automatically forwarded to a management station.

At the management station, it doesn't matter whether a threshold event was triggered by local data collection (done at the management station), or forwarded from a collection station. Forwarded threshold events are

automatically consolidated with local threshold events. Whether forwarded or locally triggered, the threshold event looks the same to the management station, and receives the same treatment.

NOTE Topology filters do not affect the events that are passed from collection stations to management stations. This means that any events that you have configured to be forwarded are in fact forwarded from the collection station to the management stations, regardless of whether the objects to which the events refer pass the topology filter or not. Listing particular event sources in the event configuration at the management station can reduce the likelihood of operator confusion. Also, this note does not apply to events internal to NNM.

See "Configuring Event Forwarding and Correlation" on page 154 for details about configuring event forwarding, including threshold event forwarding.

Remote Thresholds with Remote Actions

For some threshold events on collections stations, you may want to consider creating actions at the collection station. Where this is a reasonable tactic, it has the advantage that the action will be invoked even if contact is lost with the central site.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0672
3740
Doc:

On-Demand Submaps

As described in "On-Demand Submaps" on page 26, the reason for enabling the on-demand submap feature is to improve NNM's performance and reduce it's use of memory and disk space. Rather than keep all the submaps in memory (which, for a large map, can require large amounts of memory), you can specify that many of the submaps only be created at the moment you need them.

A **persistent submap** is created and maintained for the life of the map. In contrast, a **transient submap** is created (and removed) only as necessary; that is, "on-demand." Transient submaps are created and maintained by the `ipmap` service, and removed by the `ovw` service.

Figure 2-6, A Typical Hierarchy of Persistent Submaps, and Figure 2-7, A Typical Hierarchy of Transient Submaps, show the difference between persistent submaps and transient submaps.

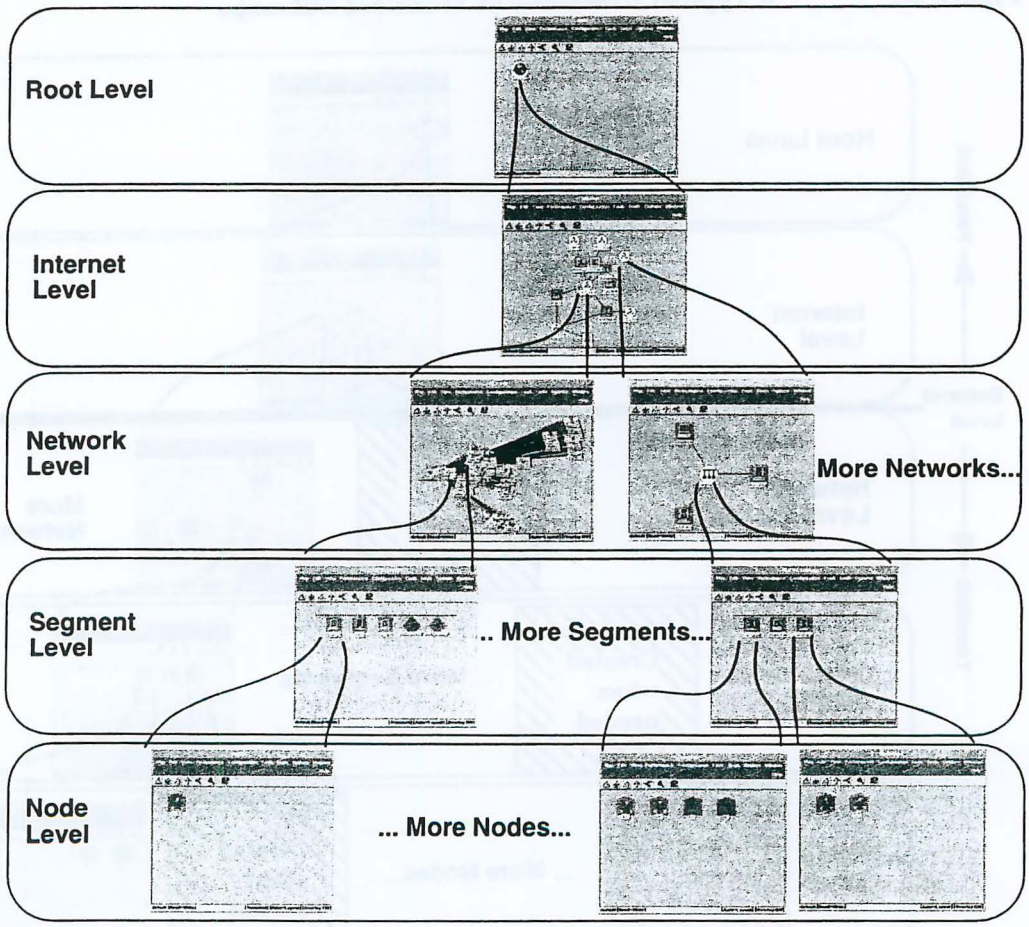
All the submaps in Figure 2-6 are persistent; this is the default when you first install NNM on UNIX systems. On Windows operating system management stations, the default is `Internet Level`. In contrast, in Figure 2-7 only the "Root" and "Internet" submap levels are persistent. Submaps from the "Network" level down are transient submaps. These are created only as they are needed. The `ipmap` service does not allocate memory for them, nor does it maintain topology changes in them. This saves both memory and execution time. Note that status from transient submaps is propagated up in the usual way.

The visible submaps (when on the same levels as the crossed-out ones) are also transient submaps, but the operator has navigated into that part of the submap hierarchy, and so these submaps are currently resident in memory.

You use the `IP Map Configuration` dialog box to set submaps to be persistent down to whatever level of the submap hierarchy you select. On Windows operating systems, the initial configuration for demand level is `Internet Level`.

For example, in Figure 2-7, the level of persistence is set to `Internet Level`, so submaps at and above that level are persistent.

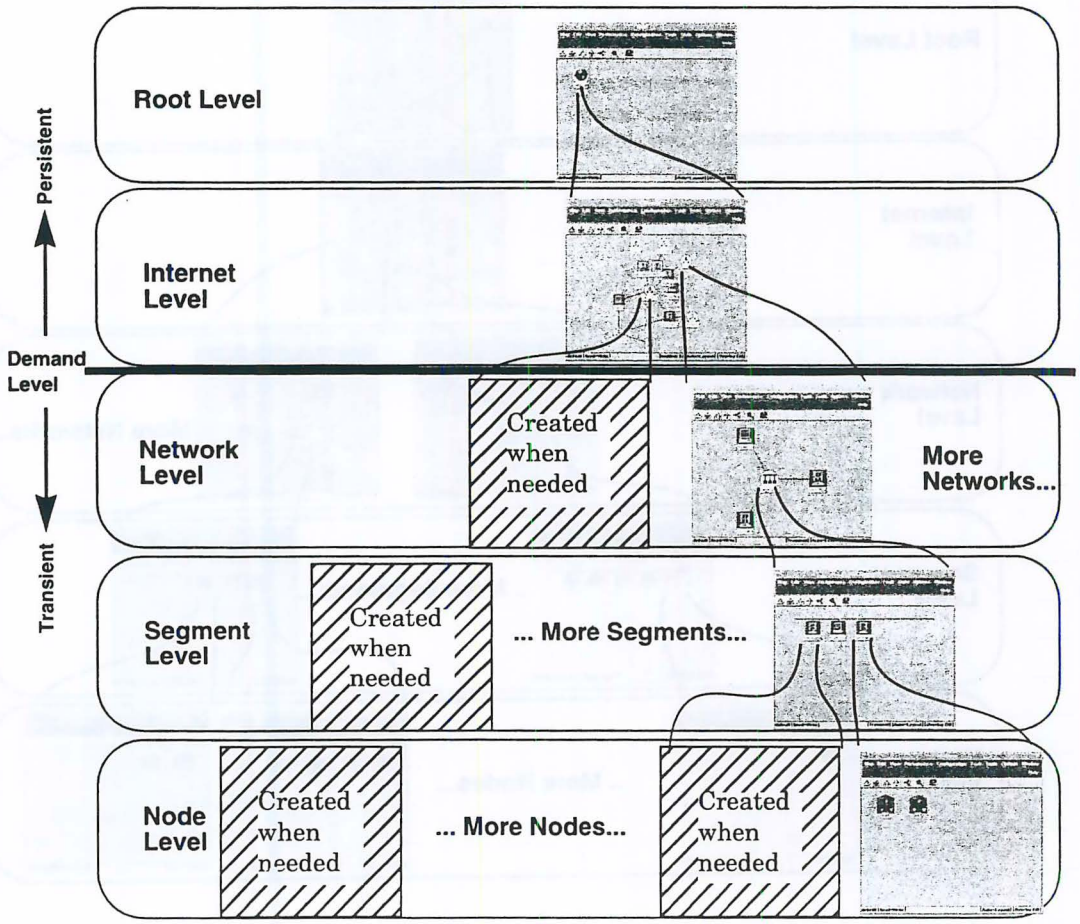
Figure 2-6 **A Typical Hierarchy of Persistent Submaps**



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0673
3740
Doc:

You can choose to make submaps persistent down to the `Internet Level` (as shown Figure 2-7), `Network Level`, `Segment Level`, or `All Levels` of the submap hierarchy. Submaps below the level you select will be transient. Of course, selecting `All Levels` means no submaps are transient.[26]

Figure 2-7 A Typical Hierarchy of Transient Submaps



26. Also see "Persistence Filtering" on page 68.

Most users of this feature will start with submaps set to be persistent at the `Internet Level` (as in Figure 2-7), and set it to lower levels only to improve submap-opening performance. This is typically necessary only when the higher-level submaps are densely populated.[27]

If you want to reset the on-demand submap feature to its default, use the `IP Map Configuration` dialog box in NNM to set submap persistence to `Unset`. On Windows operating systems, `Unset` sets the persistence level to `Internet Level`. On UNIX systems, `Unset` sets the persistence level to `All Levels`.

With on-demand submaps enabled at any level, most NNM features and operations work as they always have. Locate operations and IP status propagation, in particular, are not limited to what is currently in memory. Both functions work across all submaps, regardless of whether they are persistent or transient.

In cases where a located item is not yet in memory, the necessary submap is created, on-demand, if and when the user opens that submap from the locate dialog box.

Transient Submaps and the Submap List Dialog

The only feature that changes its behavior when the on-demand feature is enabled, is the `Submaps in Map` dialog box. Only submaps that are currently in memory (that is, either persistent, or transient but currently in memory) can appear in the `Submaps in Map` dialog box.[28]

In other words, when the on-demand submap feature is enabled, submaps that are not presently in memory are not present in the `Submaps in Map` list. This behavior may alter the usefulness of the `Submaps in Map` dialog box, depending on the expectations of the operator.

To reduce the possibility of operator confusion when the on-demand submap feature is enabled, you may wish to remove the following menu item (which opens the `Submaps in Map` dialog box):

```
Map:Submap->Open
```

27. See also the "Caution" block on "Configuring Management Consoles" on page 109.
28. See the online help for more information about this dialog box.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0674
3740
Doc:

See *Managing Your Network with HP OpenView Network Node Manager* for information about how to remove a menu item.

Persistence Filtering

Unlike the filters described earlier, the purpose of persistence filtering is not to reduce the amount of unnecessary management data in the data stream. Instead, the purpose of persistence filtering is to let some older applications that are not inherently compatible with the on-demand submap feature operate normally when the on-demand submap feature is enabled.

NOTE This is probably not an issue on Windows operating systems, since there are few "older" applications. However, some third-party developers may port their older UNIX system applications without changes.

Suppose an application has been created with the implicit assumption that the object or objects it is interested in are always available in memory. Such an application may fail or exhibit unstable behavior if the object it needs resides in a transient submap, and is thus not in memory at all times.

For example, a vendor you use may have developed an application that adds statistics component symbols under the router symbols created by the `ipmap` service. Such an application may assume that routers are part of the map (that is, present in memory) as soon as they are discovered. The on-demand feature, when enabled, invalidates that assumption.

A persistence filter can provide backwards compatibility for this type of application. The necessary persistence filter for the example application passes all routers. Then any submap that contains a router is made persistent, so that the expectation of the application is met.

A persistence filter tells the `ipmap` service that any submap containing an object that passes the filter should be made into a persistent submap. The object will then be in memory, as the application expects.

Persistence filters are set-defining type filters. A persistence filter is automatically applied to existing map and object data to determine which submaps must be persistent. When you change a persistence filter, all the objects currently in the topology database are reevaluated to see if

they pass the new filter. Submaps containing objects that pass the new filter are made persistent. Submaps that do not contain such objects are made transient if they are below the current persistence level. [29]

Comparing Map Filters and Persistence Filters

A persistence filter is different from a map filter. A map filter specifies a subset of the topology data that is allowed on the map. The persistence filter states which objects should be made persistent in memory; those objects are made persistent by making the submaps they reside on persistent.

You can think of this as a two step process. First, the map filter passes a set of objects that are allowed to be present on the map. Then the persistence filter tests these objects to see which, if any, must be persistent in memory.

No matter what the persistence filter specifies, the user still has access to all of the objects that passed through the map filter.

When an object is found to meet the criteria in the persistence filter, all submaps containing that object are made persistent. That is, a submap is made persistent if it contains even one persistent object; it might also contain objects that do not meet the persistence specification criteria. In addition, the child submap of the persistent object is also made persistent.

Because persistence and map filters are both set-defining filters, if you change either for a given map (via the `IP Map Configuration` dialog box; see the online help for details), the `ipmap` service recalculates which submaps should be persistent. This might take a long time for larger databases.[30]

29. See "On-Demand Submaps" on page 64 for more details on persistence filtering. See "Specifying a Persistence Filter" on page 124 for configuration information.
30. See also "Map Filtering" on page 42.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0675
3740
Doc:

Management Consoles

Distribution of management consoles is done via NFS (or Windows operating system file sharing) mounting of the map database and the appropriate configuration files, and by then using the distributed RPC capability of the object database service, ovwdb, the topology database, and the event system.

Figure 2-8 is a diagram of the resulting services, and where they are located. As shown, each management console actually runs the user-specific ovw-related services. The management station keeps the common databases, and runs the services (background processes on UNIX systems) common to all users.

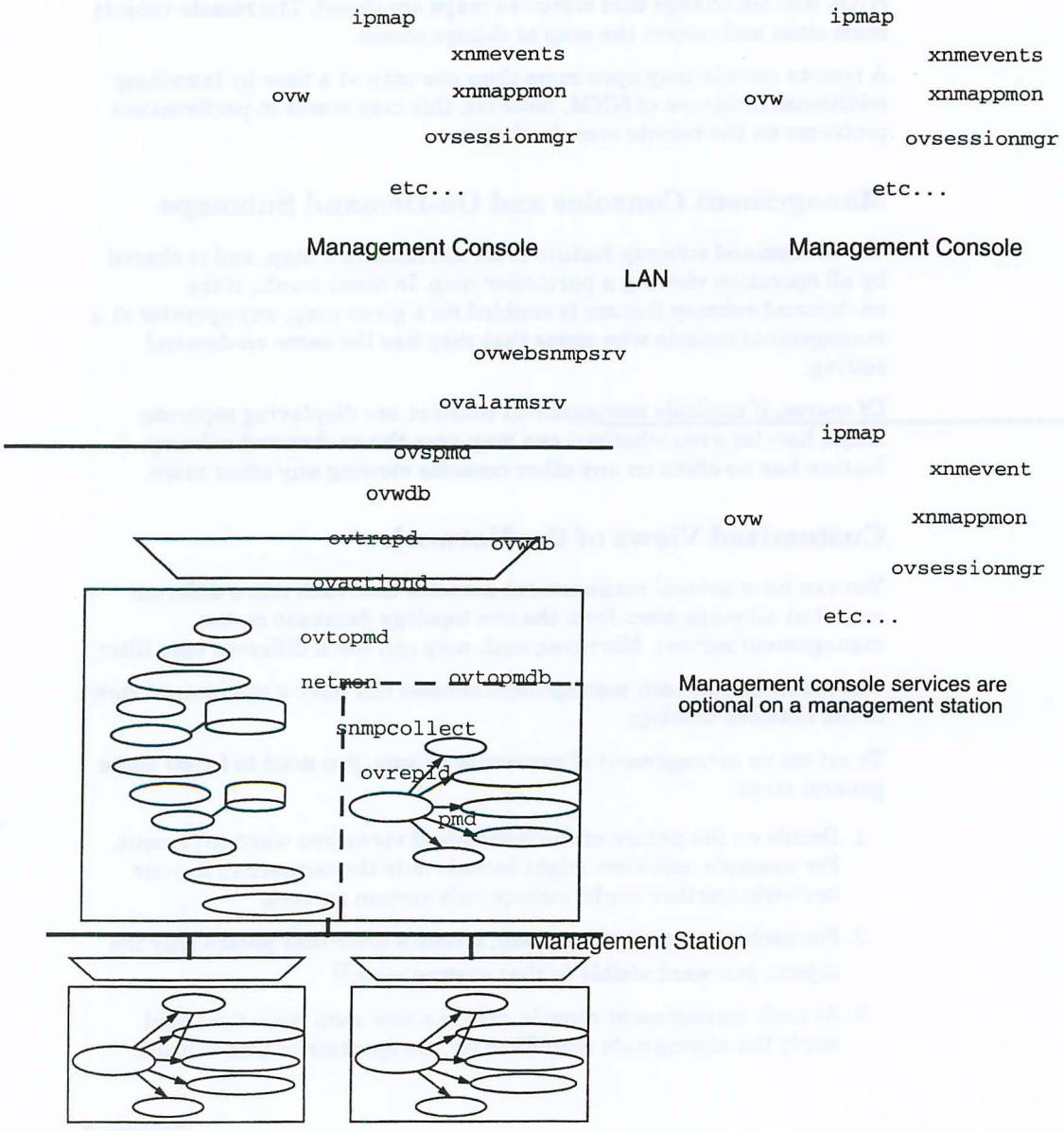
This relieves the management station of a significant demand for its resources (memory and CPU), since otherwise each operator would have independent copies of these services executing on the management station.

Relocating the ovw-related services allows the management station to apply more of its resources to network management and monitoring activities, and less to supporting the operators.

The object database remains centrally located on the management station, and is accessed by the management consoles over the network sockets. In addition to the various ovw-related services that communicate with the NNM services via socket connections, the map database and configuration files use NFS (or Windows operating system) file sharing.

NOTE Management consoles are *not* the same as NFS diskless clients. NFS diskless is an operating system concept. As described above, the distribution mechanism for management consoles uses NFS and sockets.

Figure 2-8 Management Consoles



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0676
3740
Doc:

Operators can each have their own maps. If, on the other hand, they share a map, only the first operator to open the map can edit it; others have read-only access. When using remote console into a management server that is being accessed by other remote or local console operators, maps currently open by other operators are available in read-only access. NNM will not change that status as maps are closed. The remote console must close and reopen the map to change access.

A remote console may open more than one map at a time by launching additional instances of NNM, however, this may result in performance problems on the remote console station.

Management Consoles and On-Demand Submaps

The on-demand submap feature is an attribute of a map, and is shared by all operators viewing a particular map. In other words, if the on-demand submap feature is enabled for a given map, any operator at a management console who opens that map has the same on-demand setting.

Of course, if multiple management consoles are displaying separate maps, how (or even whether) one map uses the on-demand submap feature has no effect on any other consoles viewing any other maps.

Customized Views of the Network

You can have several management consoles that each run a different map (but all maps stem from the one topology database on the management server). Moreover, each map can use a different map filter.

The result is that each management console can have a customized view of the network topology.

To set up an arrangement of customized views, you need to follow these general steps:

1. Decide on the nature of the customized views you want to present. For example, one view might include only the connectors in your network; another might include only certain servers.
2. For each custom view you want, create a filter that passes only the objects you want visible in that custom view.[31]
3. At each management console, create a new map (`Map:New`), and apply the appropriate map filter for the operator at that console.

Management Consoles and X-Terminals

In principle, it is possible to run several X-terminal sessions from a management console, or directly from the management station. You might speculate that this would allow NNM to support more operators.

However, due to internal constraints, this approach *does not* allow the management server to support more operators. You should limit the number of operators per management station to avoid degrading the performance of the interface.

Attaching X-terminals to a management console might nevertheless have cost savings, if the management console host has sufficient CPU, memory, and disk space to support the X-sessions, and low cost X-terminals are available and suitable for the operators. The key services described earlier are still off-loaded from the management station to the management console.

---

31. See "Filters" on page 37 and Appendix A, The Filter Definition Language, for more information on creating filters.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0677
3740
Doc:

Interface Managed-state Automation

As you probably know, NNM lets you "unmanage" interfaces. NNM does not do status polling on unmanged interfaces, so setting interfaces to the Unmanaged state significantly lightens the load on the management station.

NNM lets you automatically manage or unmanage interfaces based on filters. Interface managed-state automation makes it easier to manage large environments, where frequently many discovered interfaces do not require active status polling.

Interface managed-state automation relys on a command (`ovautoifmgr`) that periodically sweeps through the topology and sets the managed state of interface objects according to rules in the managed-state configuration file (`ovautoifmgr.conf`).

Based on the rules in the configuration file, interfaces that do not need to be managed are put into the Unmanaged state. Interfaces which do need to be managed (and are not already) are put into the Managed state with their status set to `UNKNOWN`. Then `netmon` begins to monitor the interface's operational status and generate events.

The the `ovautoifmgr` command is not a continuously-running process. Instead, it is designed to be run periodically by a scheduling mechanism. It requires that `ovtopmd` be running.

For further information and instructions on using interface managed-state automation, refer to the `ovautoifmgr(1m)` and `ovautoifmgr.conf(4)` reference (man) pages.

Microsoft Terminal Server Access

You can connect to Network Node Manager (on a Microsoft Terminal Server) from a remote workstation through a Terminal Server Client. You can do any of the following:

- Install or upgrade NNM on the remote server.
- Perform administrative NNM functions such as backup/restore of NNM database.
- Open NNM and display the network map onto the local workstation.
- Start multiple Terminal Server Client sessions to the same remote NNM management station, open NNM in each session and display the network maps onto the local workstation.
- Start multiple Terminal Server Client sessions to different remote NNM management stations, open NNM on each NNM management station and display the network maps onto the local workstation.

The following examples provide a few of the possible implementation strategies available to network managers when running the NNM application on servers with the Microsoft Terminal Server features enabled.

Accessing a Single NNM Station From Multiple Terminal Server Clients

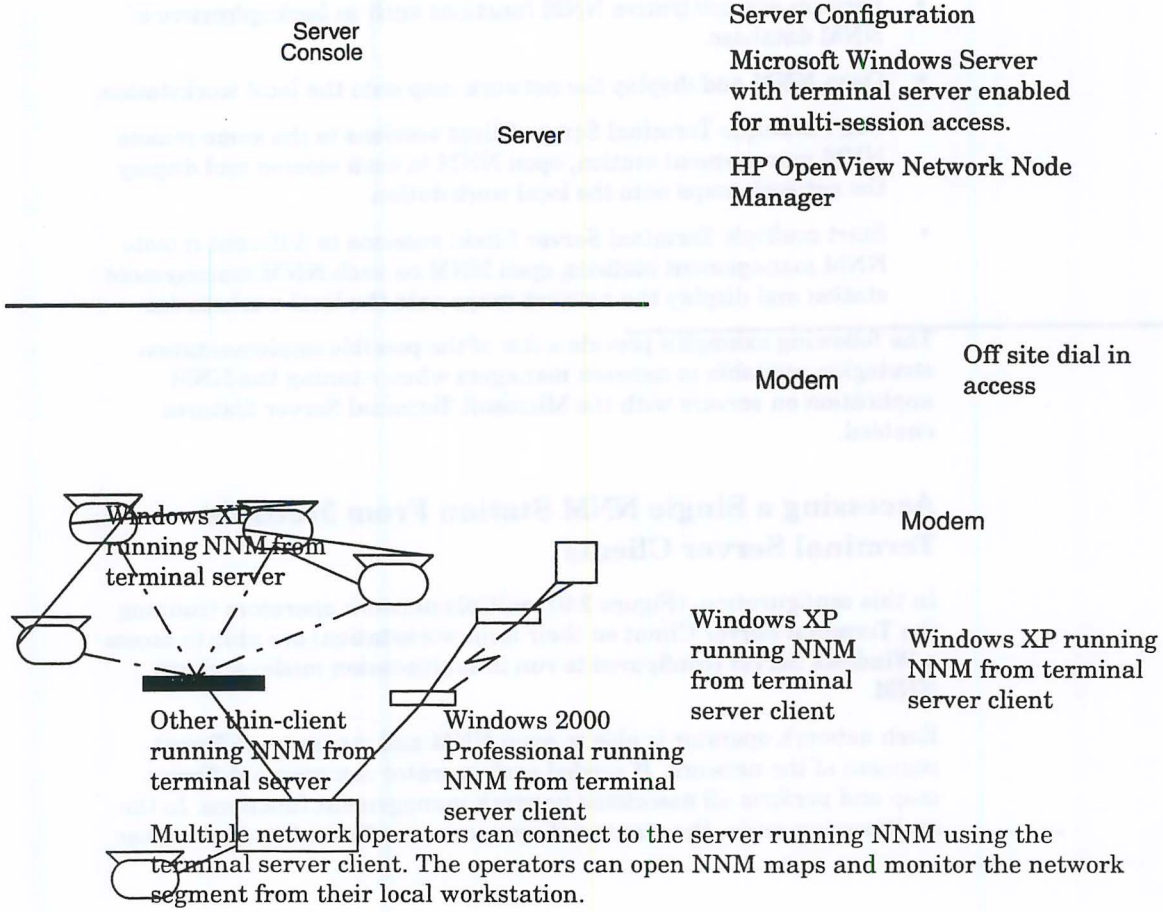
In this configuration, (Figure 2-9) multiple network operators (running the Terminal Server Client on their local workstation) are able to access a Windows Server (configured to run in multisession mode) and run NNM.

Each network operator is able to open NNM and monitor a different segment of the network. If needed each operator can open a different map and perform all associated network management functions. In the multisession mode, the number of connections is limited by the number

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0678
3740
Doc:

of client licenses available. Accounts with administrator privileges can be used to start and stop NNM processes, run NNM database backups, and install NNM patches.

Figure 2-9 Multiple Terminal Server Clients Accessing a Single NNM Station



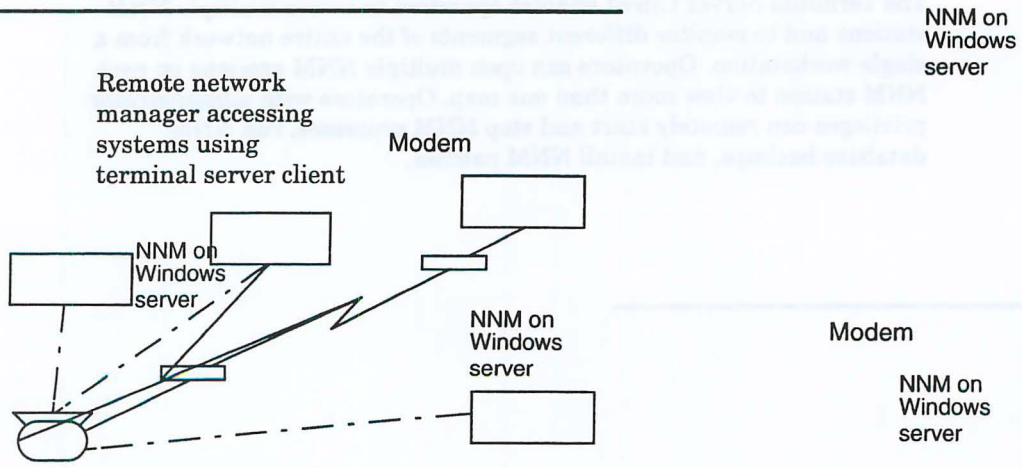
Multiple network operators can connect to the server running NNM using the terminal server client. The operators can open NNM maps and monitor the network segment from their local workstation.

Accessing Multiple NNM Stations From a Single Terminal Server Client

In this configuration, (Figure 2-10) a single network manager is able to access multiple Windows servers configured to run under Remote Administrator mode. The NNM application is installed on each Windows server. The remote network manager, using the Terminal Server Client, is able to connect to each remote system, monitor the network, and perform all network management functions. With this configuration a network manager has the ability to access and display multiple NNM sessions on their local workstation.

The remote administration mode limits the number of connections to the server (maximum of two) and only grants connections to accounts that have administrator privileges.

Figure 2-10 Accessing Multiple NNM Stations



Server Configuration

Microsoft Windows Server with terminal server enabled and installed as Remote Administrator mode.

HP OpenView Network Node Manager running on each server to manage the local network

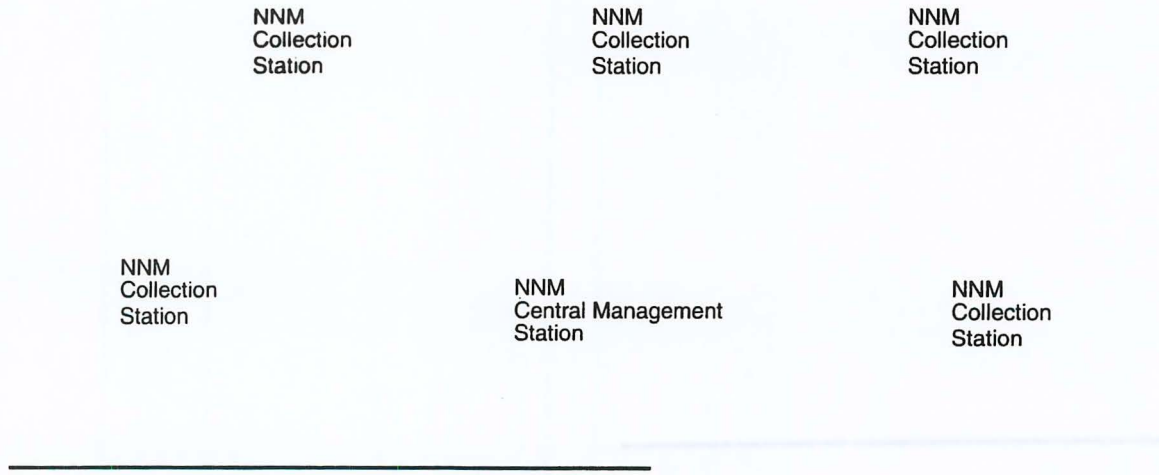
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0679
3740
Doc:

Accessing Multiple NNM Stations From Multiple Terminal Server Clients

In this configuration, (Figure 2-11) a central Network Operations Center (NOC) is responsible for monitoring the entire network. The network management architecture is constructed of multiple Windows servers running NNM configured as collection stations, each collection station forwards information to a central NNM management station. The NOC operators are responsible for monitoring the health of the network.

The Terminal Server Client enables operators to access multiple NNM stations and to monitor different segments of the entire network from a single workstation. Operators can open multiple NNM sessions on each NNM station to view more than one map. Operators with administrator privileges can remotely start and stop NNM processes, run NNM database backups, and install NNM patches.

Figure 2-11 **Multiple NNM Stations Accessed by Multiple Terminal Server Clients**



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0680
3740
Doc:

3 Strategies for Deploying Network Node Manager

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0681
Doc: 3740

This chapter contains guidelines and ideas for deploying an HP OpenView Network Node Manager (NNM) solution that meets your goals and fits well with your organization.

The purpose of this chapter is to help you understand some of the reasonable models you can use as you plan your network management solution, and some criteria you can use to select a model.

It includes general approaches and general tips to help you succeed. With this knowledge, you will be able to better plan and implement your distributed, scalable network management solution.

NOTE

The information in this chapter is not introductory; readers are assumed to have read the previous chapters. Readers are also assumed to be conversant with NNM's key features for network monitoring, data collection, event handling, and so on. This includes a functional understanding of some key elements in non-distributed NNM, including `ovw`, `ipmap`, `ovtopmd`, and `netmon`. See *Managing Your Network with HP OpenView Network Node Manager* for details about these key services (background processes on UNIX systems) in Network Node Manager.

The remaining chapters and appendices contain specific configuration procedures to use with the scaling and distribution features of NNM.

Planning the Right Approach

Now that you understand Network Node Manager's scalable and distributable features, your questions naturally turn to issues like:

- "What should I *do* with all this?"
- "Can I just ignore NNM's scalability features for now? Should I?"
- "How would I employ distribution and scalability on a massive scale?"
- "What makes sense in my organization?"

You have a wide range of choices in your deployment of NNM. The simplest choice, and one that will make sense to some, is to use none of the scalability features at all. Others, who manage large, dispersed networks, will elect to scale up their use of NNM to deal with that large environment. Still others will find that a mix of some scalability features meets their requirements.

You can combine several different models as you plan your strategy. Each fits well with a particular set of goals. Your choice of approach will be driven, in large measure, by the nature of your organization and the problems you are solving with your network management solution.

Remember as you plan that you are never "locked-in" to one strategy; as your organization changes, you can adapt your use of NNM to keep up with those changes.

Organizations differ in many ways. Organizational variables to consider as you begin planning your deployment of NNM include:

Size The needs of a small organization, with perhaps a few hundred nodes, are very different from the needs of a corporate campus where you may have thousands or tens of thousands of networked objects. The networks in larger organizations are inevitably larger and more complex than in small organizations. Consequently, the larger the organization, the stronger are the reasons to use more of the scalability features of NNM.

Structure Some organizations, like the military, have clear hierarchies of authority and reporting. Others, like universities, may consist of looser affiliations between

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0682
3740
Doc:

cooperating but largely autonomous groups. These structural differences will have a significant effect on how network management is conducted.

Geography Some organizations, like a hospital, are geographically compact but require reliable network management. Within the confines of the hospital, NNM may have few requirements for scaling. But suppose that hospital is part of a medical services company; the central site, located thousands of miles away, may want to perform network management functions in *all* their many hospitals. Then issues of distribution and scalability are very important.

Trends The network that supports an organization is in a constant state of change. Yet it is important to understand general trends in how a network is evolving: is it stable? is it becoming more geographically dispersed? bigger? more expensive to manage? You will want your network management plans to account, as best you can, for the trends in your network.

General Considerations about Scalability and Distribution

The following general points are useful when planning your deployment of NNM. Margin notes summarize key concepts from the adjoining text.

Limits to netmon affect the maximum number of nodes you can monitor.

Due to the nature of ICMP pings, the netmon service (background process on UNIX systems) has limits to the amount of polling it can perform in a given period of time. You can maximize the number of nodes the netmon service can handle (while maintaining a consistent five-minute status polling cycle) by increasing the polling interval, especially for less important nodes. See "Configuring SNMP" in *Managing Your Network with HP OpenView Network Node Manager* for details on how to set special polling intervals. For more current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide.*

You may also want to take advantage of interface managed-state automation, as described in "Interface Managed-state Automation" on page 74.

If the environment you want to manage has more nodes than you can monitor efficiently with a single netmon service, you will want to have another netmon service, in the form of another collection station, to off-load some of the polling work from the management station.

WAN performance also limits remote monitoring.

A WAN link introduces propagation delays that compound the above issue. That means that if your environment is split, with part of it accessible via LAN and the rest via WAN, the actual limit of managed nodes for a netmon service will be less than the limit stated above. How much less depends on the proportion of nodes on the LAN link vs. on the WAN link. In general, you will want to avoid monitoring nodes over a WAN link, unless you have only a few nodes at the remote site, or the node there are unimportant, and can receive infrequent polling.

In some circumstances, however, remote monitoring is necessary. As a rule-of-thumb, if a netmon service is monitoring remote sites, reduce the number of nodes it handles by one-tenth for each remote site. Thus, if a collection station is monitoring, say, 3 remote sites, you would expect it to handle up to 1400 nodes, rather than 2000.[1] The calculation for this estimate is as follows: 2000 - ((0.1 x 2000) x 3) = 1400.

In addition, remote monitoring via a WAN has very high operating costs in network traffic compared to the operating cost of monitoring via a remote collection station. Each status and configuration poll and response would have to cross the link, rather than simply any topology changes.

Take advantage of NNM wherever you can.

Given the low performance of WAN links, you can always achieve higher NNM performance by using a collection station for remote (WAN) nodes.

Since scalability is part of every NNM station (including NNM 250), it makes excellent sense to take advantage of NNM wherever it exists in your network. For example, you might have a "hidden" NNM station at a remote site, running NNM as the basis for another application like HP OpenView Operations. Consider using it as a collection station.

If your remote site has no NNM installation, you may want to install a collection station if you have perhaps fifty or more nodes to be monitored; NNM 250 might be a good choice for a small remote site. As an alternative, you could have a collection station located at one remote site, and monitoring multiple other remote sites.

1. Again, this estimate assumes that reliable 5-minute polling of all nodes is required.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0683
Doc 3740

The final layout of your solution will depend at least in part on an analysis of the costs involved with each alternative you consider.

Ensure that you can always contact your collection stations.

Relying on a remote station for network management carries certain risks, but that risk can be driven down or eliminated.

As an example, suppose some collection station is your sole source of information for a part of your network, and the main gateway between the management station and that collection station goes down. By default, it takes up to twenty minutes before a "Collection Station Critical" event is generated, and an event confirmation popup dialog is presented to the operator. The nodes affected by the failure are *not* marked "Unknown".[2]

You can diminish the likelihood and effect of such a situation in three ways.

- First, arrange to have overlapping management domains or failover coverage, particularly for key connection nodes between the management station and collection stations.
- Second, make contingency arrangements that allow alternative communication paths to the collection station. You can establish redundant routes to the collection station via multiple gateways, or by adding a direct link from the manager to the collection station if that is possible. Consider lower-cost approaches that may have lower (but still acceptable) performance in an emergency.

  Third, use HP Service Guard for your management and/or collection stations.

Use as many collection stations as you can efficiently manage.

The more collection stations you have, the smaller the impact of temporarily losing any one of them, and the easier it is to roll management of that region to a different collection station. Within the limits of your ability to configure and manage collection stations, use as many collection stations as possible to ensure redundancy and off-load polling. For more current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide.*

2. See the note about `ovrepld`'s periodic status checks in "How Distributed Internet Discovery and Monitoring Works" on page 49.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0684
3740
Doc:

Start small You don't have to implement every aspect of your final plan all at once. Begin by setting up just one piece of the final picture.

You might choose to implement on-demand submaps on a management console. Or, you might decide to set up one collection station to see how that goes. Choose something that makes sense in your final plan, implement it, and then test it thoroughly before you proceed.

Go slowly Add more small pieces of your final plan one at a time. As you go, keep testing and rechecking your implementation to ensure that you are obtaining the results you want.

Be particularly attentive to your filters. Carefully designed and implemented filtering can be central to the effectiveness of your solution, and the set of filters provided in the default filter file will be useful to many people. Those who need to design other filters should be aware that creating filters can be complicated, and requires considerable attention to detail.

Also, review your polling intervals (under the menu item `Options:SNMP Configuration`). Poll your most important nodes more often (for example, every 3 minutes) than your less important nodes (for example, every 15 or 30 minutes). This will help you maximize the benefits of scalability.

Keep records Maintaining a large network management solution is not trivial. Along with the planning documents, keep records of what steps have been taken and when. Note any issues that came up with a step, and, more importantly, the resolution of those issues. This "paper trail" can be useful in the event that you want to roll back to an earlier configuration for troubleshooting or re-engineering your distribution scheme.

Backup your system NNM pauses all services yet queues information coming in from collection stations, so you can backup your database without missing any information. Refer to *Managing Your Network with HP OpenView Network Node Manager* for more information.

Deployment Strategies for NNM

You have a number of choices about which of the scalability features of NNM you want to use, and to what degree you want to use them. This section describes several models of deployment to help you understand some alternatives to consider as you put scalable NNM into operation.

The following models are considered in this chapter:

- Fully centralized
- Centralized hierarchical
- Hierarchical
- Cooperative independent

NOTE This chapter uses the above models to show how different organizational structures can be reflected in the deployment of network management within the organization. The deployment models in this chapter are not, by any means, the only way to convey the ideas presented here. This can not be overemphasized. Few organizations, if any, will use one of these models in a pure form. As you read this section, you are encouraged to look for ideas and approaches that can be applied in some part of your own organization. It can be helpful to imagine that the strategies in this section apply to very small parts of your overall network management solution. For example, a management station that has a hierarchical relationship with another management station might simultaneously have a cooperative relationship with another management station.

Use of Scalability Features in NNM Deployment

All of these features are available to you in any way you choose to deploy NNM. The following table shows the most common scalable features used in each type of NNM scenario.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0685
Doc: 3740

Table 3-1 Scalability Features in Use Models

Scalability Feature	Centralized page 92	Centralized/ Hierarchical page 95	Hierarchical page 98	Cooperative page 103
Scalable Product Structure	X	X	X	X
Distributed Collection Stations, page 48		X	X	X
Management Consoles, page 70	X	X	X	X
Network Presenter web GUI, *Managing Your Network with HP OpenView Network Node Manager*,	X	X	X	X
On-Demand Submaps, page 64	X	X	X	X
Discovery Filtering, page 40	X	X	X	X
Topology Filtering from Collection Station to Management Station, page 41			X	X
Map Filtering for Operators, page 42	X	X	X	X
Event Forwarding, page 59		X	X	X
Threshold Event Forwarding, page 59		X	X	X
High Availability - Service Guard, page 50	X	X	X	X

Table 3-1 Scalability Features in Use Models (Continued)

Scalability Feature	Centralized page 92	Centralized/ Hierarchical page 95	Hierarchical page 98	Cooperative page 103
High Availability - Failover with Failover Filtering, page 52		X	X	X
High Availability - Overlapping Domains, page 55			X	X

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0686
Doc. 3740

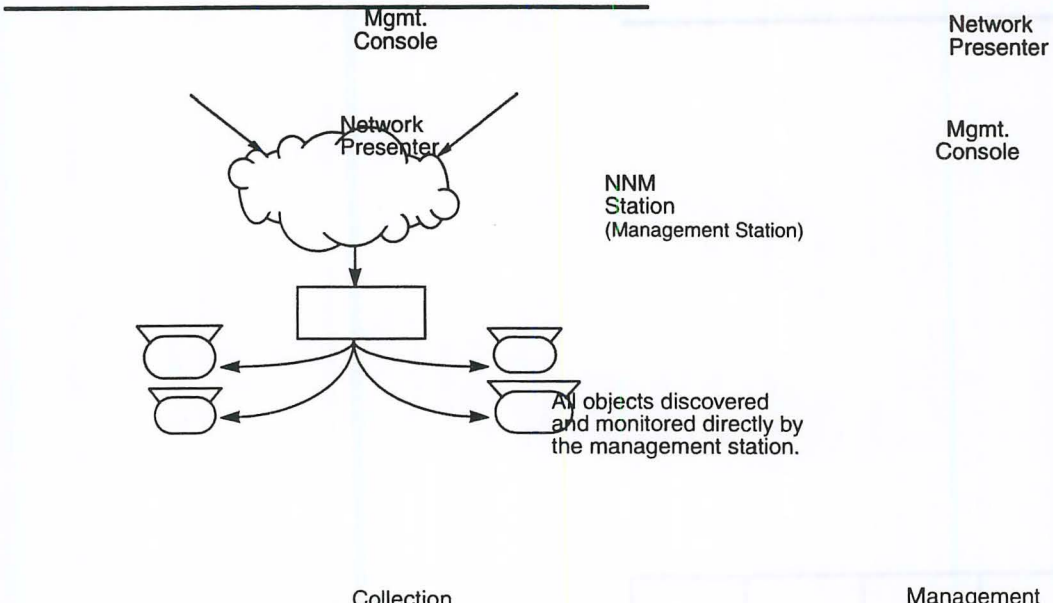
Fully Centralized Management

In a fully centralized network management scheme, one management station performs all monitoring and data collection functions for a whole management domain. There is little or no remote network management hardware or personnel. The primary focus is probably network management, with primary attention to the main connectors, like bridges, hubs, and routers.

Users of non-distributed network management products (including early versions of Network Node Manager) naturally use this model, since it is the only strongly supported model available. In fact, for many situations, a fully centralized usage of NNM is a highly functional and reasonable choice. Even in this model, scalability can be very useful.

Figure 3-1 illustrates a fully centralized network management scheme.

Figure 3-1 Fully Centralized Management Model



Notice that the collection domain and the management domain are identical. This is characteristic of this management model.

Remember that the management domain is an attribute of the management station, not the operators. You may have several operators, each of whom has a different view of the overall topology (via map filtering), and who therefore deal only with subsets of the management domain.

Implementation Tactics

Using a fully centralized model is probably the simplest (though not always the most efficient) way to use Network Node Manager. Depending on the nature of your situation, it might make sense to use one or more of the following scalability features in a fully centralized management situation:[3]

- Management consoles, for multiple operators and Network Presenter GUI for location independence.
- Map filtering, for specialized views of the topology.
- On-demand submaps, for better performance, especially on low-end management consoles.
- Discovery filtering, to eliminate unnecessary objects, enhancing performance.

  Consider an HP Service Guard cluster for the critical management station.

These features are especially useful if you have a large environment that you are managing centrally, and you have several specialized operators to monitor it. They are also useful features in a smaller management station, where you want to get the maximum performance from the available system.

3. See "Filters" on page 37, "On-Demand Submaps" on page 64, and "Management Consoles" on page 70.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0687
3740
Doc:

Implications of Using the Fully Centralized Management Model

A centralized management model is simple to understand and control. Using a centralized model puts the management responsibilities (and expertise) in one location, which works well in some organizations. However, if you do not use the scalability features of NNM, performance of the map may become problematic in a very large environment.

If you have to monitor remote nodes over a WAN, a centralized approach causes unnecessary traffic on those expensive links. Furthermore, in a very large network, the overall performance of your network management solution is probably slowest if you use a fully centralized approach, and will require that you tune polling intervals so that the `netmon` service doesn't fall behind in polling.[4]

You may also want to take advantage of interface managed-state automation, as described in "Interface Managed-state Automation" on page 74.

For the most current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide*.

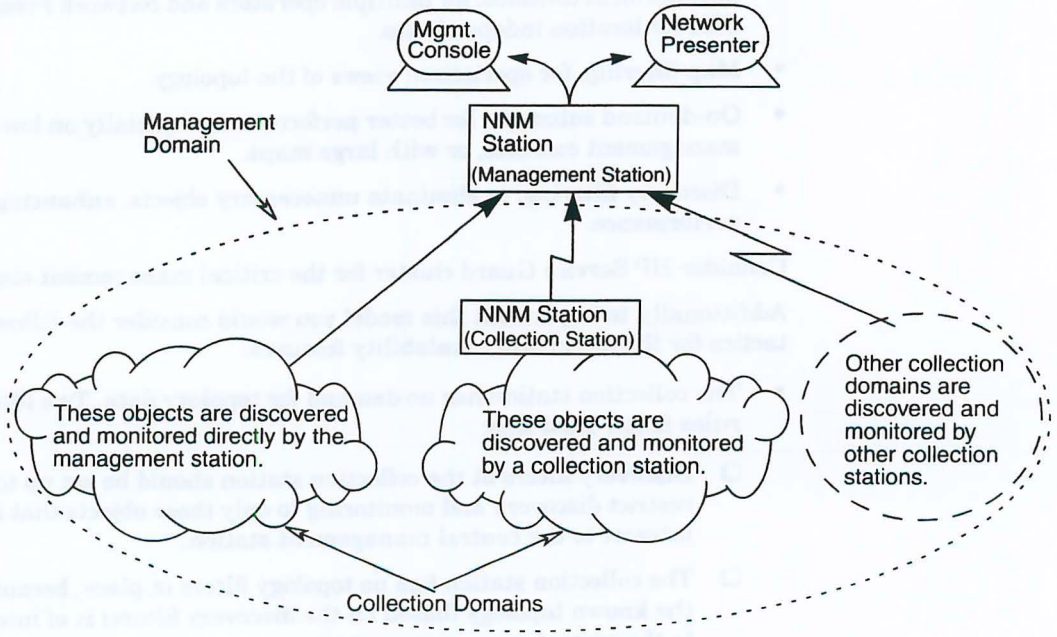
4. See the `Performance:Network Polling Statistics` menu item, and associated online help, for information on how to see if `netmon` is keeping up with polling.

Centralized-Hierarchical Management

Sometimes, one primary group has responsibility for a large network management environment. The centralized-hierarchical model involves a network that for some reason is not suitable for monitoring by a fully centralized model. The environment may be too large,[5] or you may have sizeable remote sites where network management support is minimal.

In Figure 3-2, all operators are located at the management station; this is the main characteristic of a centralized-hierarchical situation.

Figure 3-2 Centralized-Hierarchical Management Model



5. See "General Considerations about Scalability and Distribution" on page 84.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0688
3740
Doc:

While the management station in the diagram has its own collection domain, it keeps a hierarchy of several remote collection stations that provide distributed network management services. Human support for network management at the remote sites is minimal and probably does not extend to operating NNM from a console.

Implementation Tactics

Implementing a centralized-hierarchical management model is, like all distributed models, more complex than a simple centralized approach.

All of the scalability features mentioned for the fully centralized model are still applicable in exactly the same way, and for the same purposes, as for the centralized-hierarchical model:[6]

- Management consoles, for multiple operators and Network Presenter GUI for location independence.
- Map filtering, for specialized views of the topology.
- On-demand submaps, for better performance, especially on low-end management consoles, or with large maps.
- Discovery filtering, to eliminate unnecessary objects, enhancing performance.

Consider HP Service Guard cluster for the critical management station.

Additionally, to implement this model you would consider the following tactics for the use of other scalability features:

- The collection station has no demand for topology data. Two filtering rules follow from this:
  - ❑ Discovery filters at the collection station should be set up to restrict discovery and monitoring to only those objects that are of interest to the central management station.
  - ❑ The collection station has no topology filters in place, because all the known topology (based on the discovery filters) is of interest to the central management station.
- Configure collection station failover so that the management station can pick up for critical collection stations.

6. See "Filters" on page 37, "On-Demand Submaps" on page 64, and "Management Consoles" on page 70.

- You will probably want to forward all threshold events that you configure for the collection station. The most likely forwarding would be to the %REMOTE_MANAGERS_LIST%, so that any interested manager would receive the events.

  One potential exception to this rule would occur if you only want a local action performed for a particular threshold event, and no higher level attention to the matter.

- If you are dealing with a large environment and using the centralized-hierarchical model, you may want the collection stations (even though essentially unmanned) to perform remote trend data collection. You would then plan to pull that data to the central management station for merging, report generation, and analysis.[7]

Implications of Using Centralized-Hierarchical Management

The centralized-hierarchical model is somewhat more complex to deploy and maintain than the fully centralized model, because each collection station requires special configuration. However, it has many advantages for environments that are either geographically dispersed, or too large to monitor from a single station.

You can manage networks with up to about 25,000 devices (assuming one interface per device, on average), and roughly fifteen operators. Performance of the map in a large environment can be improved by using map filtering and on-demand submaps.

A centralized-hierarchical model (like a fully centralized approach) puts the management responsibilities (and expertise) in one location, which works well in some organizations.

If you have to monitor remote nodes over a WAN, and still want centralized network management, a centralized-hierarchical approach can reduce traffic on expensive WAN links. The risk is slightly higher, since you are relying on the remote collection stations for data.

Finally, in a large network, the overall performance of your network management solution is probably better, because you are not performing polling over the lower performance WAN links.

---

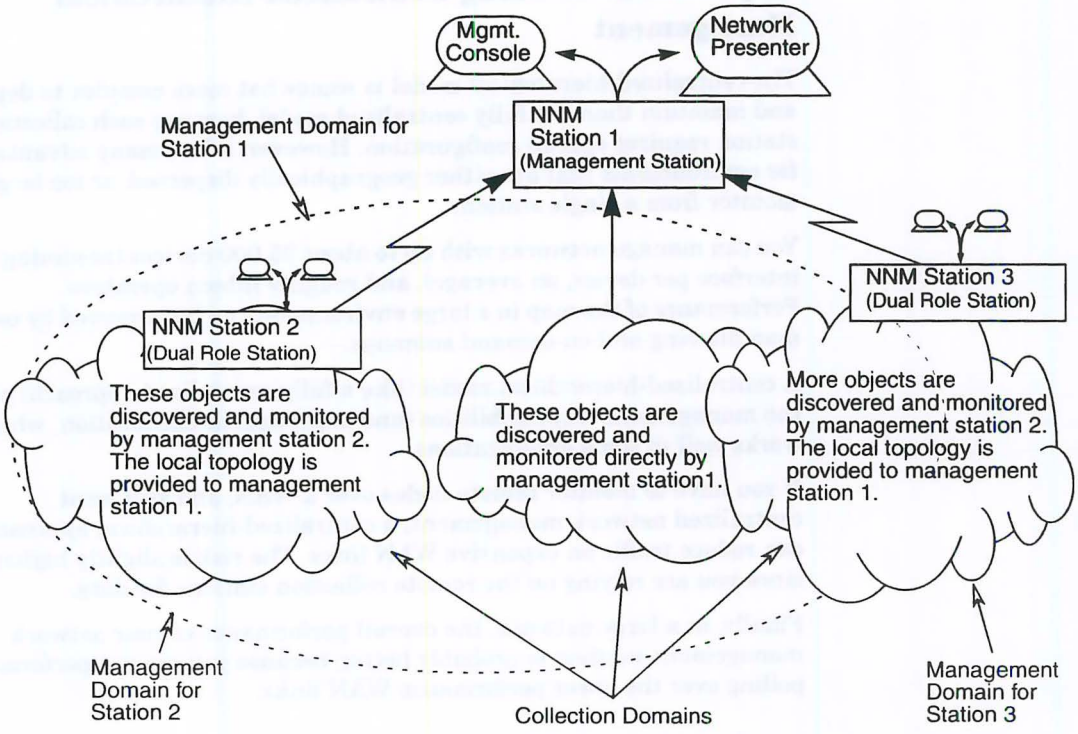
7. See the reference page in NNM online help (or the UNIX system manpage) for *ovcoltosql*.

PROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0689
3740
Doc:

Hierarchical Management

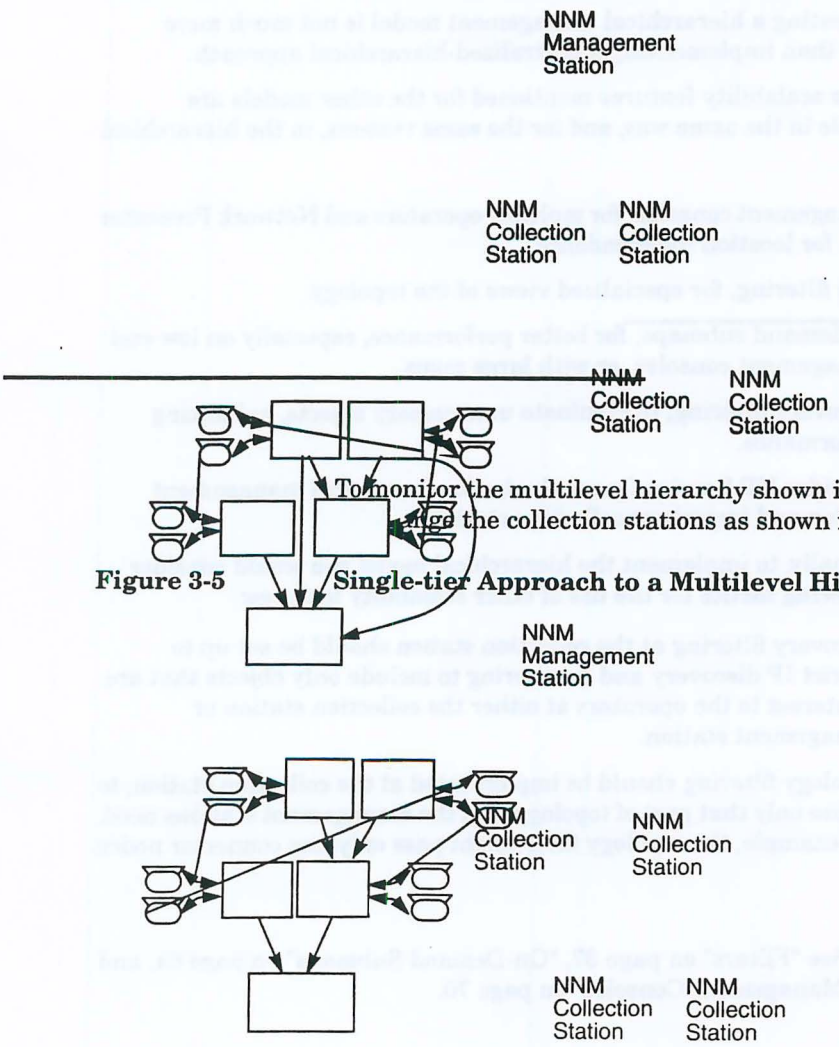
In many large organizations, a central group has broad responsibility for the network resources of the organization, usually for the major gateways and connecting infrastructure of the network (commonly called the network "backbone"). In the outlying sites, local network managers control the local configuration, usually including local connectivity, server availability, etc. This hierarchy of responsibility is reflected in the scheme illustrated in Figure 3-3, where NNM Stations are 2 and 3 are independent management stations, while also acting as collection stations for NNM Station 1.

Figure 3-3 Hierarchical Management Model



While multiple levels are possible in a hierarchical environment, Network Node Manager passes topology and status data only one level. That is, topology data received from a collection station can not be forwarded again. Only topology and status data that is derived from a local `netmon` service can be forwarded to remote managers.

Figure 3-4 Unsupported Multilevel Hierarchical Management



To monitor the multilevel hierarchy shown in Figure 3-4, you would have to configure the collection stations as shown in Figure 3-5.

Figure 3-5 Single-tier Approach to a Multilevel Hierarchy

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: Nº 0690
Doc: 3740

In Figure 3-5, the top-level management station uses both the first- *and* second-tier collection stations directly, to obtain all the information it needs.

Topology filters at the second-tier must pass all the objects needed by either first-tier or top-level management stations, but the same would be true even if multiple-level management were possible.

Implementation Tactics

Implementing a hierarchical management model is not much more complex than implementing a centralized-hierarchical approach.

All of the scalability features mentioned for the other models are applicable in the same way, and for the same reasons, in the hierarchical model:[8]

- Management consoles, for multiple operators and Network Presenter GUI for location independence.
- Map filtering, for specialized views of the topology.
- On-demand submaps, for better performance, especially on low-end management consoles, or with large maps.
- Discovery filtering, to eliminate unnecessary objects, enhancing performance.

  Consider HP Service Guard cluster for the critical management station and important collection stations.

Additionally, to implement the hierarchical model you would consider the following tactics for the use of other scalability features:

- Discovery filtering at the collection station should be set up to restrict IP discovery and monitoring to include only objects that are of interest to the operators at either the collection station or management station.
- Topology filtering should be implemented at the collection station, to expose only that part of topology that the management stations need. For example, the topology filter might pass only key connector nodes.

8. See "Filters" on page 37, "On-Demand Submaps" on page 64, and "Management Consoles" on page 70.

- The interests of operators at the management stations and the collection stations may overlap on some objects. Map filtering can be cooperatively designed and implemented between the management stations and the collection stations, so that any overlap is considered and deliberate.
- Configure collection station failover so that the management station can pick up for critical collection stations.
- You might want to forward some threshold events that you configure on the collection station, most probably to the `%REMOTE_MANAGERS_LIST%`, so that all interested managers receive those events.

  Or, you might want to duplicate a MIB variable via a MIB expression. This lets you set two different thresholds on the value, one that triggers local action and one that triggers attention at the management station.

  Of course, some thresholds might be of local interest only, and not be forwarded to the managers.
- If you are dealing with a large environment and using the hierarchical model, you may want collection stations to perform remote trend data collection.

  You would then plan to pull that data to the central management station for merging, report generation, and analysis. The administrators at the remote site may also have local use for the same trend data, or a subset of it.[9]

Implications of Using the Hierarchical Management Model

The hierarchical management model takes full advantage of the benefits that scalability offers. On the other hand, it can be complex to deploy and maintain in a large environment.

9. See "Trend Data Collection in a Distributed NNM Solution" on page 28 for more information.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0691
Doc 3740

Implementing a fully hierarchical management scheme makes it possible to manage larger environments than any other approach. Such environments are often geographically dispersed, too large to monitor effectively from a single site, and staffed, at least some of the time, with network management personnel at the remote sites.

Performance of the maps at any management station can always be improved through map filtering and using on-demand submaps. Your experiences will depend on the resources you have available, and the performance tuning you implement.[10] For the most current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide*.

A hierarchical model (unlike any centralized approach) disperses the management responsibilities and expertise across the organization. Failures at any point in the system are less likely to have wide ranging consequences.

A hierarchical approach can significantly cut traffic on costly WAN links.

Finally, in a large network, the overall performance of your network management solution is probably better this way than with any other approach, in part because situations that develop in the collection domain of the collection stations can be generally handled by the local operators.

10. See "General Considerations about Scalability and Distribution" on page 84 for ideas.

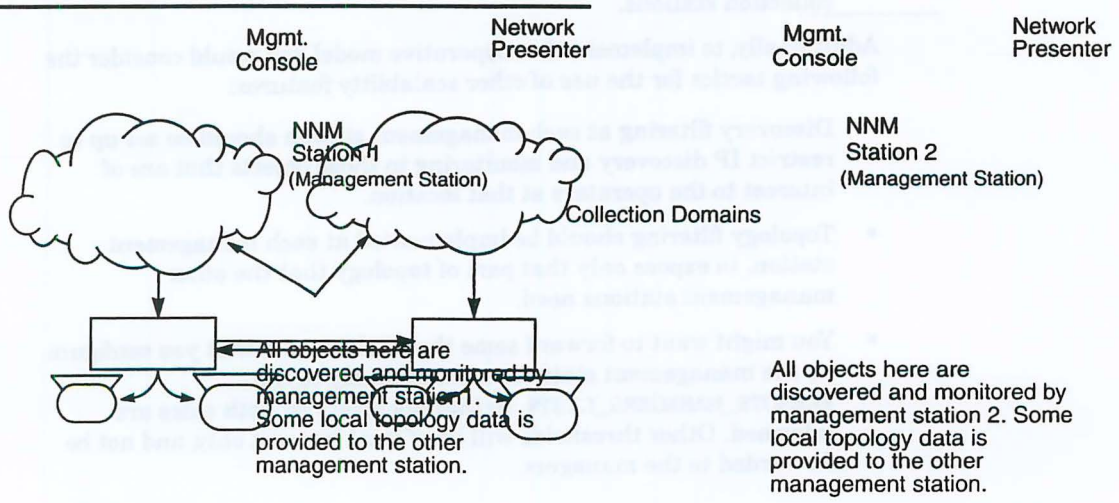
Cooperative Independent Management

In some situations, two largely independent sites need to share information at the boundaries of their management domains. Administrators at each site have primary responsibility for their part of the overall managed domain. This is shown in Figure 3-6.

In addition, these administrators are likely to have a strong interest in the major connecting nodes they share with other sites, in the primary servers at other sites, or in other key nodes or resources that reside in the domains of other sites.

This peer relationship may or may not reflect the organizational structure. You might choose this model because of the need for tight cooperation, even though one site is actually "higher" in the organizational hierarchy.

Figure 3-6 Cooperative Independent Management Model



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0692
3740
Doc:

Implementation Tactics

Implementing a cooperative management model is similar to implementing a hierarchical approach. In fact, cooperative management could be viewed as simply a variant of the hierarchical model, where each management station is, from the perspective of the other, just a subordinate collection station.

Again, all of the scalability features useful in the centralized model are still applicable in exactly the same way, and for exactly the same reasons, in the cooperative model:[11]

- Management consoles, for multiple operators and Network Presenter GUI for location independence.
- Map filtering, for specialized views of the topology.
- On-demand submaps, for better performance, especially on low-end management consoles, or with large maps.
- Discovery filtering at each management station can eliminate unnecessary objects, enhancing performance.

Consider HP Service Guard cluster for critical management or collection stations.

Additionally, to implement the cooperative model you would consider the following tactics for the use of other scalability features:

- Discovery filtering at each management station should be set up to restrict IP discovery and monitoring to those objects that are of interest to the operators at that location.
- Topology filtering should be implemented at each management station, to expose only that part of topology that the other management stations need.
- You might want to forward some threshold events that you configure on the management stations, most probably to the `%REMOTE_MANAGERS_LIST%`, so that operators on both sides are informed. Other thresholds will be of local interest only, and not be forwarded to the managers.

11. See "Filters" on page 37, "On-Demand Submaps" on page 64, and "Management Consoles" on page 70.

- When using the cooperative independent model, you may want to collect trend data on the shared resources. Depending on the actual configuration of the resources, you may want one or all management stations to perform trend data collection. If multiple stations are collecting trend data, you might want to choose one to act as the central location for merging the data, report generation, and analysis. The administrators at each management site may also have local use for the same trend data.

Implications of Using the Cooperative Independent Model

The cooperative independent management model is ver[illegible] technical complexity to a more purely hierarchical appr[illegible] likewise requires that the sites cooperate in nontechnic[illegible] For example, scheduled downtime of critical or shared r[illegible] site should not come as a surprise to the other sites.

In implementing a cooperative independent manageme[illegible] can assume that each site has complete responsibility f[illegible] management of non-shared resources and objects.

A management station with a cooperative relationship [illegible] management station can, at the same time, have a hier[illegible] relationship with one or more other collection stations.

The cooperative model acknowledges that management [illegible] and expertise are not centralized in the organization, a[illegible] skills and requirements exist at different sites. While a[illegible] point in the system is unlikely to have wide ranging con[illegible] local problem may get little attention from a remote site.

Finally, the overall performance of your network management solution is good, in part because situations that develop in the collection domains are generally handled locally.[12] Thus, a cooperative approach provides benefits without creating significant traffic on costly WAN links.

12. See "Filters" on page 37, "On-Demand Submaps" on page 64, and "Management Consoles" on page 70.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0693
3740
Doc.

4 Procedures for Scaling NNM

IRQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0694
Doc: 3740

This chapter is not an introduction to NNM procedures. Readers are assumed to be conversant with NNM's key features for network monitoring, data collection, event handling, and so on. Readers who are looking for that information should turn to *Managing Your Network with HP OpenView Network Node Manager* instead. That manual also covers basic configuration of NNM station options that are not exclusive to distributed management.

This chapter covers procedures for scaling NNM. These procedures are:

- Configuring management consoles.
- Configuring on-demand submaps.
- Configuring distributed internet monitoring.
  - Data collection
  - Collection station
  - Management station
  - Domain overlap and failover
- Configuring event forwarding.
- Using distributed data collection.

The accompanying diagram serves as your roadmap through this chapter. As new areas of configuration are introduced, they are circled on the diagram.

All of the documentation for HP OpenView Windows and Network Node Manager is written with the assumption that you have activated environment variables on UNIX systems. For information about environment variables, see the reference page in NNM online help (manpage on UNIX systems) for *ov.envvars*.

NOTE This chapter refers to operating systems in the form OS Version.X (for example, HP-UX 11.X). Refer to the Release Notes, Supported Configurations topic for the operating systems that are supported with this release.

Configuring Management Consoles

Distribution of the HP OpenView Windows Graphical User Interface (GUI) is done via NFS mounting (Windows operating system file sharing for Windows operating system servers) of the map database and the appropriate configuration files, and by using the distributed RPC capability of the object database service (or background process on UNIX systems), ovwdb.

Display

Mgmt. Station

Domain

Collection Station

This section has five components:

- Configuring an NNM server on a machine running the Windows operating system (Windows operating system file sharing).

Domain

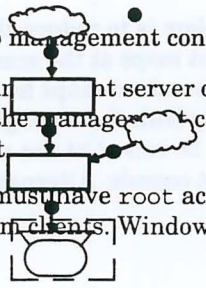
Filter

- Configuring a client on a Windows system for server on a Windows system (Windows operating system file sharing).
- Configuring a server on a UNIX operating system.
- Configuring a client on a Windows system to use a server on a UNIX
- Configuring a client on a UNIX system.

NOTE The management console (client) and the server must run the same revision of NNM. Refer to the Release Notes, Supported Configurations topic for the operating systems that are supported with this release.

To set up management consoles, the following must be true:

- A management server on UNIX must be configured as an NFS server and the management console (client) must be configured as an NFS client.
- You must have `root` access on UNIX system servers and UNIX system clients. Windows systems require `Administrator` rights.



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0695
3740
Doc:

- The client must have read-write access to a UNIX system server's file system via NFS.
- User and group IDs must be synchronized between the client and server.

The basic steps in installing management consoles are:

1. Install NNM on the server system, following the instructions in the *HP OpenView Network Node Manager Installation Quick Start*. (You do not need an additional license for the client.)
2. Mount the server's HP OpenView data directories on the client system.
3. Install NNM on the client system.
4. For UNIX system clients, run the `ovwsetupclient` configuration script on the client to have it use the mounted databases for maps and objects.
5. Run `ovstart` on the server system.
6. Run `ovw` on the client system.

CAUTION If a "lightweight" system (for example, a HP9000/715 with 64 Mbytes of RAM) is configured as a management console client for a server with a large database, it is possible that the resulting performance of the client system will be unacceptably slow, or that one or more of the background processes that run on the management console will run out of memory.

This is because `ipmap` and the `ovw` process sizes grow in proportion to the number of objects that are associated with persistent maps. For example, suppose that management station has 40,000 objects in its default map and the on-demand submap feature is disabled. If a lightweight management console tries to open this map, the synchronization process on the management console will cause `ovw` and `ipmap` to grow so large that either performance will be exceedingly slow, or one of the processes will run out of memory and fail.

The solution to this problem is to reduce the number of objects that are associated with persistent maps at the management console. This can be done by using the on-demand submaps feature, or map filters, or both. If the map is to be shared by both the management station and the console, the demand level should be raised at the *management* station *prior* to starting the management console. Alternatively, a copy of the map can be

created at the management station, and that copy can be configured with a higher demand level and/or filters. This new map can then be started up by the management console. For the best performance at the management console, set the demand level to Internet.

Configuring a Windows System Console Server

1. Share the *install_dir* directory from the NNM management server as *ShareName*. You may use Windows Explorer using a right mouse click. Give the users `Full Control` access.
2. Start the NNM services from the Control Panel at the NNM management server. These services must run during instal installation will fail.

Installing a Management Console on Windows NNM Server on Windows

First, install NNM on the Windows operating system machine be the management server, then follow these steps. You will ne know the name of the server to which the console will connect *ShareName* on the server.

NNM remote console, verify that yc connect to the *ShareName* share. You may use Windows Ex

NOTE During installation, the *install_dir*`\conf\*.auth` files are edited to give the remote console access to the manager's database and services. If you experience problems connecting to a management server, you may want to verify the rights granted in these files. You may also edit these files to customize rights for remote console operators.

2. On the NNM remote console system, insert the CD-ROM and run `setup.exe`. When installing, pick the `[Remote Console Installation]`. This removes any databases or local configuration files (these files might be in place if you had previously installed the full NNM management server). Supply the machine name of the NNM management server and share name *ShareName*.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0696
Doc: 3740

3. You can now run NNM from this remote console as if you were at a full management server. The remote console has no icons for `[ovstop]` and `[ovstart]`, since to use these from a remote console, you must explicitly name what to start-up or shutdown. However, you can run these services from the command line.

Remote console operator rights to view maps are controlled the same way as operators viewing maps directly on the management server. Use NTFS file system access assignments to the *`install_dir`*`\databases\openview\mapdb` directory and subdirectories. Refer to *Managing Your Network with HP OpenView Network Node Manager* for details.

UNIX System Server Configuration

The server system is the management station on which you installed NNM and whose map and object database you want to export to the client system. You must be `root` to perform these steps. In the following steps, replace *`client_name`* with the hostname of the client from which you want to use these databases.

The following steps allow all users, including `root`, to run `ovw` sessions

1. Install NNM on the server as described in the *HP OpenView Network Node Manager Installation Quick Start* for the system.
2. If management consoles are connecting to this server from a Windows system, verify that the `pcnfsd` process is running on the server. This process lets your Windows operating system consoles know the name of the management station and that the station is running the `pcnfsd` daemons.

NOTE This step explains how to configure the `pcnfsd` process to authenticate NFS access requests from Windows clients. Although the `pcnfsd` process is commonly used for authentication, third-party providers of Windows NFS client products offer alternative methods, such as NIS authentication. If you prefer to use the `pcnfsd` process, complete this step. If you skip this step and use a third-party authentication procedure, it must be configured to allow access to user IDs in the range of 0-60002.

a. Create the file `/etc/pcnfsd.conf`. It will contain one line that reads:

```
uidrange 0-60002
```

Save and close this file.

b. Start PCNFS.

- On HP-UX:

  Edit the `/etc/rc.config.d/nfsconf` file. In it, change the PCNFS_SERVER= line to look like this:

  ```
  PCNFS_SERVER=1
  ```

  Save and close this file. To start the service, run the command:

  `/sbin/init.d/nfs.server start`

- On Solaris:

  Verify that the PCNFS product is installed on the management station and that `pcnfsd` is running:

  `ps -ef | grep pcnfsd`

  If it is not running, start it with `/opt/SUNW/pcnfs/scripts/pcnfs start`.

3. Ensure that NFS is running on the server.

- **On HP-UX:**

  a. Run this command:

  `ps -ef | grep nfsd`

  b. If the `nfsd` process is not running, edit the file `/etc/rc.config.d/nfsconf` and change `NFS_SERVER=0` to `NFS_SERVER=1` and run the following command:

  `/sbin/init.d/nfs.server start`

- **On Solaris 2.X systems** (NFS must already be installed):

  a. Run this command:

  `ps -ef | grep nfsd`

  b. If the `nfsd` process is not running, execute:

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0697
3740
Doc:

```
/etc/init.d/nfs.server start
```

4. Configure the exportation of the HP OpenView file system to the client as follows:

   - For an HP-UX server, edit the `/etc/exports` file. You will either modify two existing lines or add new ones, depending on the contents of this file.

     -- If the line `/etc/opt/OV/share -root=` is present, add your console system's name after the equal sign. If there is already a system name after the equal sign, then add a colon (:) followed by your console system's name after the first system name.

     -- If the line `/etc/opt/OV/share -root=` is not present, add it and include your console system's name.

     -- Do the same for the line `/var/opt/OV/share -root=`.

     When you have finished editing, the file should look like this:

     ```
     /etc/opt/OV/share root=First_System:Console_System
     /var/opt/OV/share -root=First_System:Console_System
     ```

     or

     ```
     /etc/opt/OV/share -root=Console_System
     /var/opt/OV/share -root=Console_System
     ```

     Save and close the `/etc/exports` file.

   - For a Solaris server, edit the `/etc/dfs/dfstab` file by adding the following two lines to it:

     ```
     share -F nfs -o root=Console_System /etc/opt/OV/share
     share -F nfs -o root=Console_System /var/opt/OV/share
     ```

     Save and close the `/etc/dfs/dfstab` file.

5. Run the following two commands to unexport and re-export the directories from the server:

   On HP-UX:

   ```
   /usr/sbin/exportfs  -au
   /usr/sbin/exportfs  -av
   ```

   On Solaris 2.X:

   ```
   share -F nfs -o root=client_name /var/opt/OV/share
   share -F nfs -o root=client_name /etc/opt/OV/share
   ```

Use the fully qualified domain name when specifying the *client_name*.

6. Verify that NNM is running on the management station. Type

   /opt/OV/bin/ovstatus | more

   You should see a list of processes that are currently running. Check the list to verify that the ovwdb process is running. If ovwdb is not, type

   /opt/OV/bin/ovstart ovwdb

   Then, type **/opt/OV/bin/ovstatus | more** again to verify that ovwdb is now running.

Installing Management Consoles on Windows for UNIX System Management Servers

To set up a remote management console on a Windows operating system to use a UNIX management station server, first satisfy the following prerequisites:

- Make sure that the management station server is not already mapped as a network drive on your Windows operating system console. If it is, remove the network drive connection.
- Verify that you have a compatible NFS client product installed on your Windows operating system console. (See the NNM Release Notes for a list of NFS client products that have been tested with NNM.)
- You will need to know the name of the server to which the console will connect and the two directories exported in step 4 and 5 of "UNIX System Server Configuration" on page 112.

Once the prerequisites are satisfied, perform the following steps:

1. Verify or configure the following settings in the NFS client software on the system running Windows that will be a management console.
   - The name of the management station you are connecting your management console to. Indicate the station by name, not by IP address.
   - The root login name and password for connecting to the management station.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0698
Doc: 740

5. Once installation is completed, it is recommended that you change the configuration of your PCNFS server product so that the authentication is that of the user using NNM on the Windows operating system console, instead of `root`. For example, if a user called `ovuser` is running NNM on both the management station and the Windows operating system station, the configured PCNFS authentication should be `ovuser` instead of `root`. By changing the authentication, you ensure that any files generated during an NNM session will be accessible from both the station and the Windows operating system console.

UNIX System Console Configuration

Before you begin, you will need to know the name of the server to which the console will connect. Perform the following steps on each client machine:

1. Install NNM on the console as described in the *HP OpenView Network Node Manager Installation Quick Start* for the system.
2. Ensure that the console is running as an NFS client.

- **On HP-UX:**

  a. Run this command:

  ```
  ps -ef | grep biod
  ```

  b. If the `biod` process is not running, edit the file `/etc/rc.config.d/nfsconf` and change `NFS_CLIENT=0` to `NFS_CLIENT=1` and run the following command:

  ```
  /sbin/init.d/nfs.client start
  ```

- **On Solaris 2.X:**

  a. Run this command:

  ```
  ps -ef | grep -e "statd|lockd"
  ```

  b. If you do not see both the `/usr/lib/nfs/statd` and the `/usr/lib/nfs/lockd` processes running, execute:

  ```
  /etc/init.d/nfs.client start
  ```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
0699
Fls. Nº
Doc: 3740

3. Choose a mount point for the server's HP OpenView file systems. To make sure this file system is mounted at boot time, you must modify the appropriate file shown below. You must be root to modify these files. Replace *server_name* with the name of the server whose databases you want to use on this client.

NOTE As an alternative to these steps, NFS access may be provided via the NFS automounter. Consult your operating system's manual for details.

- On **HP-UX:**
  a. Run these commands:

     mkdir -p /opt/OV/nfs/*server***/var/opt/OV/share**

     mkdir -p /opt/OV/nfs/*server***/etc/opt/OV/share**

  b. Add these lines to the /etc/fstab file:

```
server:/var/opt/OV/share /opt/OV/nfs/server/var/opt/OV/share nfs rw 0 0
server:/etc/opt/OV/share /opt/OV/nfs/server/etc/opt/OV/share nfs rw 0 0
```

  c. Run these commands:

     /etc/mount *server***:/etc/opt/OV/share**

     /etc/mount *server***:/var/opt/OV/share**

- **On Solaris 2.X**:
  a. Run these commands:

     mkdir -p /opt/OV/nfs/*server***/var/opt/OV/share**

     mkdir -p /opt/OV/nfs/*server***/etc/opt/OV/share**

  b. Add these lines to the /etc/vfstab file:

```
server:/var/opt/OV/share - /opt/OV/nfs/server/var/opt/OV/share/ nfs - yes rw
server:/etc/opt/OV/share - /opt/OV/nfs/server/etc/opt/OV/share/ nfs - yes rw
```

  c. Run these commands:

     /etc/mount *server***:/etc/opt/OV/share**

     /etc/mount *server***:/var/opt/OV/share**

4. Set up the client by running the following script:

   $OV_BIN/ovwsetupclient /opt/OV/nfs/*server*

NOTE If you have used the NFS automounter, the path may be different.

5. To verify that the configuration is correct, run the following command:

   ovw -server

   Look at the return value from the `ovw -server` command on your display. It should look similar to:

   ```
   %ovw -server

   your server name shows up here
   ```

6. Run **ovw** on the management console.

   If you are running on an HP Service Guard cluster, you may run **ovwrs** rather than **ovw**, if NNM is configured as a package. Refer to the *ovwrs* man page for more information about restartable **ovw**.

Increasing Security for Management Consoles

Authorization files on the server allow you to limit which consoles may access the information on the server. If you have modified default authorizations, add the server hostname and each client hostname to the authorization file for `ovwdb` and `ovw`. Be sure to add the line *client_name* + for each client you are giving access to the server. The files `ovwdb.auth` and `ovw.auth` are located in `$OV_CONF`.

```
server_name +

client_name_1 +

client_name_2 +
```

where *server_name* is the name of the system where your map database resides. The addition of these lines enables any user from *client_name_1* or *client_name_2* to use the database on *server_name*.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0700
3740
Doc:

NOTE A third authorization file also exists, `ovspmd.auth`. This file limits which consoles have permission to run `ovstop` and `ovstart`. **You should be careful about giving too many users this permission.**

Undoing a Management Console

If you want to undo the management console setup and run NNM in a normal manner, you must follow these steps in the order listed.

CAUTION Failure to follow these steps could result in damage to your databases.

- On UNIX systems:
  1. Run the following command on the console:

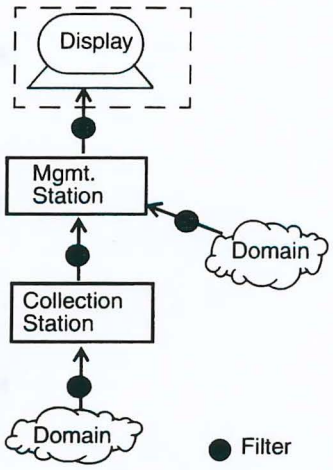
     ```
     $OV_BIN/ovwsetupclient -u
     ```

  2. Remove the lines that were added to the `/etc` files in the previous Server Configuration and Client Configuration sections.
- On Windows systems:
  1. Reinstall NNM from the installation CD.

Configuring On-Demand Submaps

This section discusses how to:

- Configure on-demand submaps.
- Specify a persistence filter.
- Integrate applications with on-demand submaps.



Configuring Demand Level

You can set the demand level of maps as you create them or after you have already created the map. You can set the submap demand level using the `-D` option on the `ipmap` command or using the `IP Map Configuration` dialog box. See the reference page in NNM online help (or manpage on UNIX systems) for *ipmap* for information setting the demand level using the command line.

To set the demand level as you are creating the map, use the following procedure:

1. Select `Map:New...` from the menu bar; the `New Map` wizard (dialog box on UNIX systems) appears.
2. Select `IP Map` from the `Configurable Applications` list. Figure 4-1 illustrates the list under the Windows operating system.
3. Click `[Configure For This Map...]`; the `IP Map Configuration` dialog box differs according to the operating system, as shown in Figure 4-2 and Figure 4-3.
4. On UNIX systems, in the `IP Map Configuration` dialog box, use the scroll bar in the top pane to scroll down to the `------ On-Demand Specification -----` section of the pane.
5. Use the option button under the question "`To what level should submaps be persistent?`" to specify the demand level. You can specify one of the following:

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0701
Doc: 3740

`Unset`

Resets the demand level to the platform default. On systems running the Windows operating system, this is `Internet Level`. On UNIX systems, it is `All Levels`.

`All Levels`

Specifies all submaps as persistent. This is the same as specifying level 1 when using the `ipmap -D` command.

`Segment Level and Higher`

Specifies that segment, network, and Internet level submaps are persistent. This is the same as specifying level 2 when using the `ipmap -D` command.

`Network Level and Higher`

Specifies that network and Internet level submaps are persistent. This is the same as specifying level 3 when using the `ipmap -D` command.

`Internet Level`

Specifies that Internet level submaps are persistent. This is the same as specifying level 4 when using the `ipmap -D` command.

6. Click `[Verify]` to verify that the values are valid.
7. Click `[OK]` to close the `IP Map Configuration` dialog box.
8. On systems running the Windows operating system, click `[Next]` to continue filling in the wizard windows. On UNIX systems, click `[OK]` from the `New Map` dialog box after you have completed the required fields.

You can use the `Map:Properties` menu from the menu bar to change the demand level after the map has already been created.

Click the `[Applications]` tab in the `Map:Properties` dialog box on systems running the Windows operating system. Using the `Map Properties` dialog box, follow the above procedure for setting the demand level of a new map. You must have read-write access to the map in order to change its demand level.

Refer to "On-Demand Submaps" on page 64 for more information about the on-demand submap feature.

Figure 4-1 Windows Map Properties Property Sheet, Applications Tab

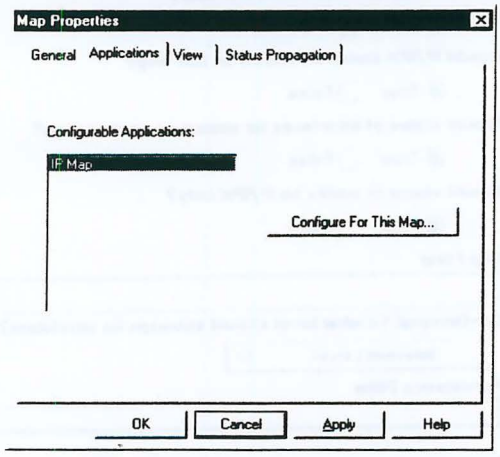
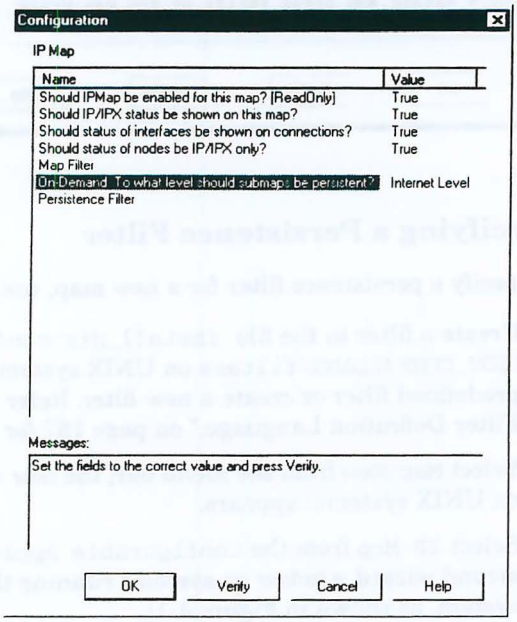
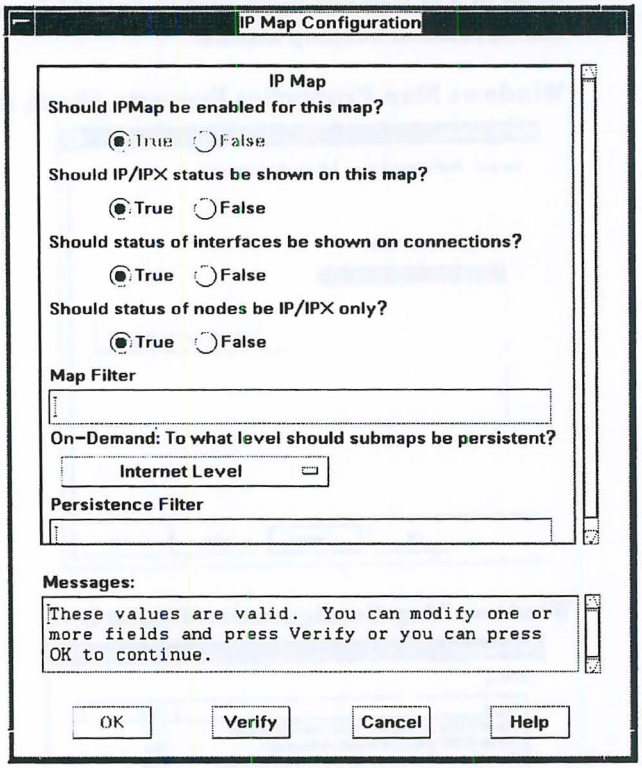


Figure 4-2 Windows Map Configuration Dialog Box



ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0702
3740
Doc:

Figure 4-3 IP Map Configuration Dialog Box on UNIX Systems



Specifying a Persistence Filter

To specify a persistence filter for a new map, use the following procedure:

1. Create a filter in the file *install_dir*\conf\C\filters (`$OV_CONF/$LANG/filters` on UNIX systems). You can either use a predefined filter or create a new filter. Refer to Appendix A, "The Filter Definition Language," on page 167 for information on filters.
2. Select `Map:New` from the menu bar; the `New Map` wizard (dialog box on UNIX systems) appears.
3. Select `IP Map` from the `Configurable Applications` list (in the second wizard window on systems running the Windows operating system, as shown in Figure 4-1).

4. Click [Configure For This Map...]; the IP Map Configuration dialog box appears, as shown in Figure 4-2 and Figure 4-3.
5. On Windows systems, select Persistence Filter. The Persistence Filter dialog box opens.

   On UNIX systems, in the IP Map Configuration dialog box, use the scroll bar in the top pane to scroll down to the
   ------ On-Demand Specification-----
   section of the pane.
6. In the Persistence Filter text field, enter a filter name or expression.
7. Click [Verify] to verify that the values are valid.
8. Click [OK] to close the IP Map Configuration dialog box.
9. On Windows systems, click [Next] to continue filling in the wizard windows.

   On UNIX systems, click [OK] from the New Map dialog box after you have completed the required fields.

You can use Map:Properties from the menu bar to change the persistence filter after the map has already been created.

Using [Applications] tab in the Map:Properties dialog box, as shown in Figure 4-1 on page 123, (or the Map Description dialog box on UNIX systems), follow the above procedure for setting the persistence filter of a new map. You must have read-write access to the map in order to specify a persistence filter.

Refer to "Persistence Filtering" on page 68 for more information about persistence filters.

Integrating Applications With On-Demand Submaps

Before integrating a new application with NNM, you should have a good understanding of how your application works so your application can produce the same results whether you are using the on-demand submap feature of NNM or not. This may require a persistence filter to use when on-demand submaps are enabled.

For example, if your application adds a hub symbol to a segment submap and needs the status of the hubs to propagate up the submap hierarchy, then you need to specify a persistence filter.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0703
Doc: 3740

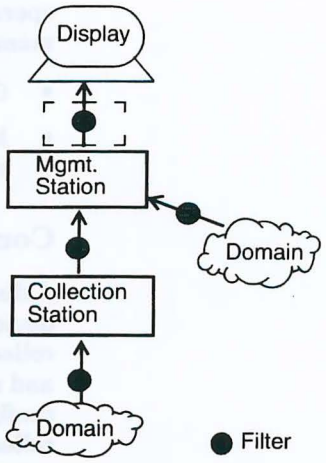
Another example of when a persistence filter is needed is if your application, at start-up, queries the map for all objects of a certain type and performs an operation for each of those objects found. Your application needs to ensure that the objects of this type are on the map by including a persistence filter that specifies this object type.

Use the following procedure to create and specify a persistence filter.

1. Determine what objects your application requires in the map.
2. Start your application running on NNM.
3. Select an object that your application has added and that you want to remain persistent in the submap.
4. Select `Edit:Object Properties` from the menu bar.
5. From the `Object Description` dialog box, view the object attributes for `Capabilities`.
6. Determine which capabilities are unique to that object type, for example, which are set to true.
7. With this information you can create a filter that will allow this object type to pass through.
8. Follow the steps for configuring the demand level and specifying a persistence filter.

Configuring a Map Filter

A map filter allows the operator to display only the objects of interest to that operator. Objects that are rejected by a map filter remain in the management station's topology database and are still subject to status polling. Use the following procedure to configure a map filter on a management station:



1. Create a filter in the file *install_dir*\conf\C\filters (`$OV_CONF/$LANG/filters` on UNIX systems). You can either use a predefined filter or create a new filter. Refer to Appendix A, "The Filter Definition Language," on page 167 for information on filters.
2. On systems running the Windows operating system, select the `Applications` tab in the `Map:Properties` dialog box.

   On UNIX systems, select `Map:Properties` from the menu bar. The `Map Description` dialog box appears.
3. Select `IP Map` from the `Configurable Applications` list and click `[Configure For This Map]`. The `IP Map Configuration` dialog box appears, as shown in Figure 4-2 on page 123 (Figure 4-3 for UNIX systems).
4. You must have read/write rights to the current map.

   On systems running the Windows operating system, select `Map Filter`, and enter the filter name.

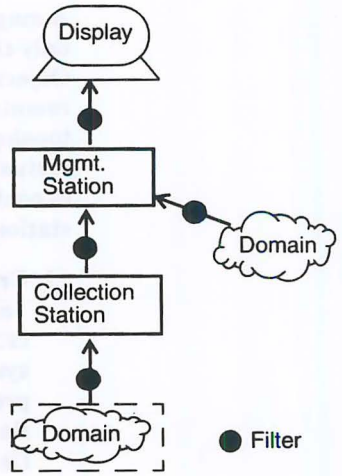
   On UNIX systems, enter the filter name that you created in the text box under `Map Filter`.
5. Click `[Verify]` to make sure the filter name or expression you specified is a valid filter.
6. Click `[OK]` to save the changes and close the dialog box.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0704
Doc: 3740

Configuring Data Collection for a Station

This section describes how to perform operations required on all collection and management stations:

- Configure a discovery filter.
- Manage and unmanage a locally monitored object.



Configuring a Discovery Filter

A discovery filter reduces the number of devices a management station or collection station is actively discovering and monitoring. A discovery filter can be configured on a management station or a collection station. Use the following procedure to configure a discovery filter:

1. Create a filter in the file *install_dir*\conf\C\filters (`$OV_CONF/$LANG/filters` on UNIX systems). You can either use a predefined filter or create a new filter. Refer to Appendix A, "The Filter Definition Language," on page 167 for information on filters.
2. Select `Options:Network Polling Configuration:IP/IPX` (`Options:Network Polling Configuration:IP` on UNIX systems) from the menu bar. The dialog box tabs under the Windows operating system are shown in Figure 4-4, Figure 4-5, and Figure 4-6. The `Network Polling Configuration` dialog box for UNIX systems appears as shown in Figure 4-7.
3. Make sure the `Discover New Nodes` option button is on in the IP and IPX tabs, as needed. (There is no IPX on UNIX systems.)
4. On Windows systems, click the `[Use Filter]` option button on the `[General]` tab and choose a filter from the list box.

   On UNIX systems, click the `Use Discovery Filter` option button to the on position. The corresponding text box will ungray.
5. Enter the filter name as defined in the filters file into this text box.

6. Click [OK] to save the changes and close the dialog box.

The discovery filter will be applied to all newly discovered objects. Polling is still done on all previously discovered objects whether or not they would have passed the filter.

To apply the filter to previously discovered objects you need to perform the following steps (from a command window on the Windows operating system):

1. Stop netmon by typing

   ovstop netmon

2. Once netmon is stopped, execute the following command:

   ovtopofix -f *filtername*

3. Then start netmon by typing:

   ovstart netmon

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0705
3740
Doc:

Figure 4-4 Windows Network Polling Configuration, General Tab

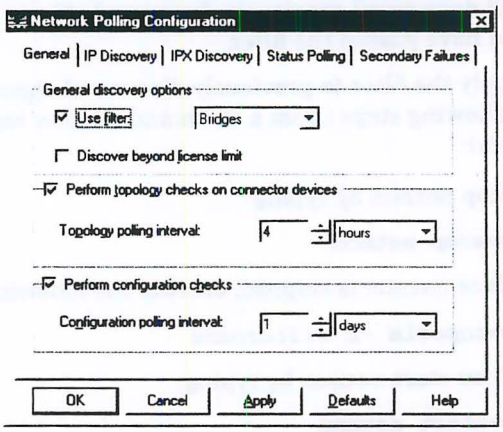


Figure 4-5 Windows Network Polling Configuration, IP Discovery Tab

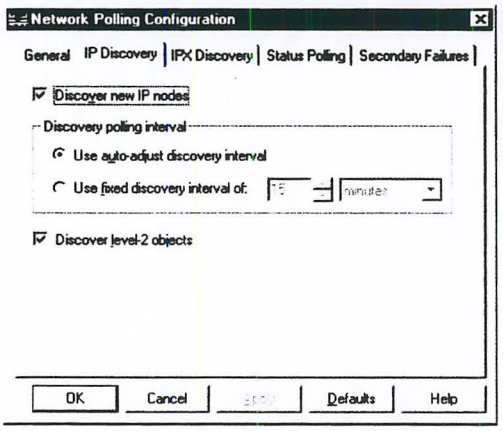


Figure 4-6 Windows Network Polling Configuration, IPX Discovery Tab

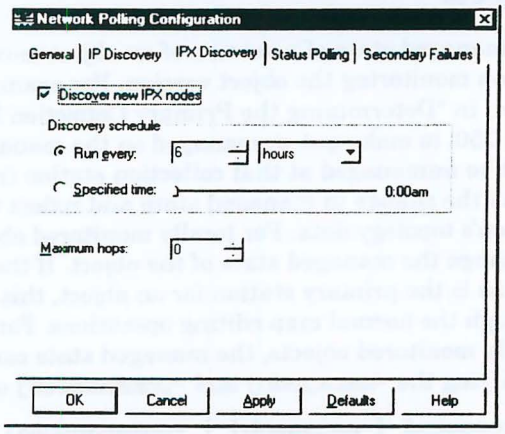
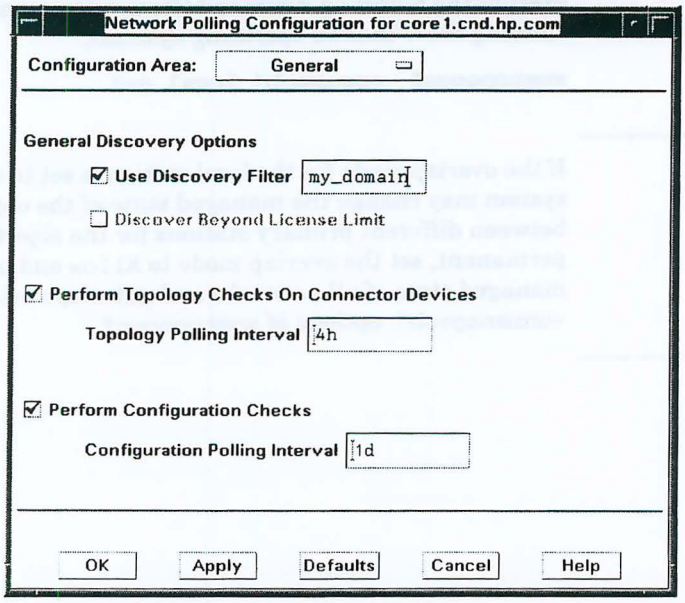


Figure 4-7 UNIX System Network Polling Configuration Dialog Box



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0706
Doc. 3740

Managing and Unmanaging Locally Monitored Objects

The managed state of a version of an object must be set on the collection station monitoring the object version. For example, in the examples shown in "Determining the Primary Collection Station for an Object" on page 150, to make `gw1` unmanaged on the management station, the node must be unmanaged at that collection station (`remstn1`). `remstn1` will detect the change in managed state and reflect that in the management station's topology data. For locally monitored objects, it may be desirable to change the managed state of the object. If the local management station is the primary station for an object, this can be accomplished through the normal map editing operations. For non-primary versions of locally monitored objects, the managed state can be changed by specifying the `-manageobj` and `-unmanageobj` options of `xnmtopoconf`:

`xnmtopoconf [-manageobj | -unmanageobj]` *`station object`*

For example, to manage the locally monitored version of node `gw1` execute the following command (from a command window on systems running the Windows operating system):

```
xnmtopoconf -manageobj local gw1
```

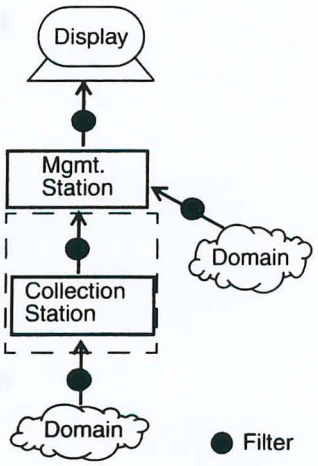
NOTE

If the overlap mode for the local station is set to `Unmanage` or `Delete`, the system may change the managed state of the object during a transition between different primary stations for the object. To make your changes permanent, set the overlap mode to `Allow` and manually set the managed state of all networks and gateways using the `-manageobj` and `-unmanageobj` options of `xnmtopoconf`.

Configuring Collection Stations

This section describes how to:

- Configure security for a collection station.
- Configure a topology filter for a collection station.
- Change the topology filter a collection station.
- Configure a Windowsoperating system IPX collection station.



Configuring Security for a Collection Station

On the collection station, you need to configure SNMP security to allow the exporting of topology information. Use the following procedure to do this (on UNIX systems, you must be `root` to execute this procedure).

1. Make sure NNM is not running. If NNM is running,

   Windows Stop all NNM services by clicking the `NNM Services - Stop` icon.

   UNIX Exit all sessions and issue the command **`ovstop`**

2. Make sure the SNMP master agent is not running by executing the following command:

   Windows Stop `SNMP EMANATE Adapter for Windows` and `SNMP EMANATE Master Agent` using the `Control Panel Services` applet.

   UNIX **`/usr/sbin/snmpd -k`**

3. Edit the set community name line in the *`install_dir`*`\conf\SnmpAgent\snmpd.conf` (`/etc/SnmpAgent.d/snmpd.conf` on UNIX systems) file to read as follows:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
FLS. Nº 0707
3740
Doc:

```
set-community-name: name #enter community name
```

where, *name* is the community name of your choice. By default, NNM does not install a default set community name. You must set this value before attempting to manage a station.

4. Restart the SNMP master agent by executing the following commands:

   Windows Restart `SNMP Emanate Adaptor` and `SNMP Emanate Master Agent` using the `Control Panel Services` applet.

   UNIX **`/usr/sbin/snmpd`**

5. Start NNM by executing the following command:

   Windows Click the `NNM Services - Start` icon.

   UNIX **`ovstart -v`**

6. Make sure the `ovtopmd` service (background process on UNIX systems) is running by executing the following command:

   Windows Click the `NNM Status` icon.

   UNIX **`ovstatus ovtopmd`**

Configuring a Topology Filter for a Collection Station

A topology filter at a collection station defines the subset of topology data that management stations can access. For more information, see "Topology Filtering" on page 41. Use the following procedure to configure a topology filter on a collection station:

1. Create a filter for the *install_dir*`\conf\C\filters` (`$OV_CONF/$LANG/filters` on UNIX systems) file. You can either use a predefined filter or create a new filter. Refer to Appendix A, "The Filter Definition Language," on page 167 for information on filters.

2. Make sure NNM is not running. If NNM is running, exit all sessions and issue the following command:

   Windows Click the `NNM Services - Stop` icon.

   UNIX **`ovstop`**

3. Edit the `vtopmd.lrf` file to include the `-f` option followed by the desired filter name or filter expression name. For example,

```
ovtopmd:ovtopmd:
OVs_YES_START:pmd,ovwdb:0 -f Routers: OVs_WELL_BEHAVED:15:
```

where, `Routers` is a predefined filter contained in the standard filter definition file.

4. Reconfigure `ovtopmd` by executing the following command (from a command window on systems running the Windows operating system):

   `ovaddobj ovtopmd.lrf`

5. Start the NNM services by executing the following command:

   Windows Click the `NNM Services - Start` icon.

   UNIX **`ovstart -v`**

   The start-up of NNM may take a little longer the first time, to adjust for `ovtopmd` to apply the filter to the existing topology database.

Only information that passes the topology filter is passed on to the management station. Existing information on the management station that does not pass the newly-configured filter will be removed from the management station's topology database.

Changing the Topology Filter for a Collection Station

You can change the topology filter for a collection without stopping NNM using the following procedure.

1. Create a filter for the *`install_dir`*`\conf\C\filters` (`$OV_CONF/$LANG/filters` on UNIX systems) file. You can either use a predefined filter or create a new filter. Refer to Appendix A, "The Filter Definition Language," on page 167 for information on filters.
2. Execute the following command (from a command window on systems running Windows):

   `ovtopmd -f` *`filtername`*

   where filtername is the new filter that you want to apply to the database. This command sends an event that tells `ovtopmd` to apply the new filter to the topology database.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0708
Doc 3740

To remove the topology filter, execute the following command (from a command window on systems running Windows):

```
ovtopmd -f ""
```

NOTE To make the filter application permanent, perform steps 3 and 4 from the "Configuring a Topology Filter for a Collection Station" on page 134.

Configuring IPX on a Collection Station under Windows

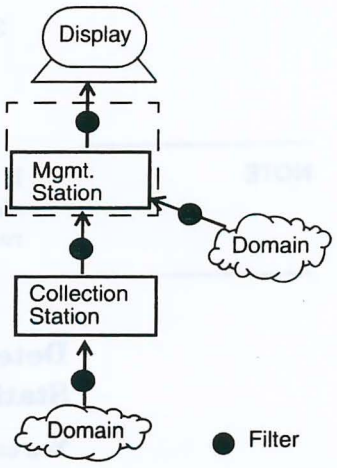
If you want to prevent IPX information from being passed to the NNM management station, do one of the following:

- During installation of the NNM collection station, disable IPX discovery. The following procedure prevents IPX discovery from occurring on the collection station.
  1. Choose the `Custom Installation` option, and disable the automatic starting of network discovery.
  2. Once installation is complete, start the NNM user interface.
  3. Select the `Options:Network Polling Configuration:IP/IPX` menu item.
  4. From the `[IPX Discovery]` tab, click on the `[Discover New Nodes]` button to disable IPX discovery.
  5. Start the IP discovery services using the `NNM Services - Start` icon in the `HP OpenView` program group.
- If you want IPX discovery enabled on the NNM collection station, proceed with a normal installation. After the system is installed, configure the `IPOnlyObjects` filter as a topology filter. Refer to "Configuring a Topology Filter for a Collection Station" on page 134 for this information. This prevents any IPX networks or IPX-only objects from being propagated to the management station. However, nodes that are discovered to support both IP and IPX will still contain IPX interfaces, with only a physical address and no IP address.

Configuring Management Stations

This section describes how to:

- Determine if a node is a collection station.
- Determine all objects monitored by a specific collection station.
- Configure a management station to use a specific collection station.
- Unmanage a collection station from a management station.
- Remove a collection station from a management station.
- Configure a remote communication timeout and retry count.
- Perform a full synchronization.



Determining if a Node is a Collection Station

There are several ways to determine what nodes are collection stations.

- The easiest is to use the Station view available from the `Tools:Views->Station` menu, or at this URL: `http://`*`nodename`*`:7510/topology/stationView`, where *nodename* is an NNM management station.
- Alternatively, you can execute the following command (from a command window on systems running a Windows operating system):

  `xnmtopoconf -print`

  This will give you a list of current collection stations and tell you if they are managed or unmanaged. The nodes with a managed status are currently acting as collection stations.
- Finally, you can also use ovw to determine which nodes are acting as collection stations. Use the following procedure:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0709
3740
Doc:

1. From the menu bar select `Edit:Find->Object By Attribute`. The `Find by Attribute` dialog box appears.
2. In the `Objects Attributes` list, select `isCollectionStationNode`.
3. Click `[Apply]`. The known collection stations will be in the `Located and Highlighted` list in the `Locate Attribute` dialog box.

NOTE It is possible for collection stations to exist without having a node object. For example, when a collection station is being used from a remote location and it is not part of the locally discovered topology.

Determining All Objects Monitored by a Collection Station

You can see all the objects monitored by a given collection station by specifying the `ovtopodump` command with the `-r` and `-C` options together. For example, (from a command window on systems running a Windows operating system)

```
ovtopodump -rRISC stn2
```

If there is both a node and a collection station with the same name, it may be necessary to use the object ID to distinguish the two objects with the `-r` option. Another option is to print all objects and use the `grep` command to find the objects from that collection station. For example,

```
ovtopodump -RISC | grep stn2
```

Configuring for a Specific Collection Station

You can configure a management station to connect to a collection station. Use the following procedure to do this (you must be `Administrator` on systems running a Windows operating system or `root` on UNIX systems to execute this procedure):

1. Make sure the NNM services (background processes on UNIX systems) are running:

- On Windows , use the `Control Panel Services` applet to check status. If the NNM services are not running, use the `Control Panel Services` applet to start the services.
- On UNIX, execute the following command:

  `ovstatus`

  If the NNM services are not running, execute the following command:

  `ovstart`

2. Determine what collection stations already exist as described in "Determining if a Node is a Collection Station" on page 137to get a list of current collection stations and see if they are managed or unmanaged. If the collection station you want does not appear, continue to the next step. If the collection station *does* appear, continue with step 4.
3. Add the collection station to the topology by executing the following command:

   `nnmtopoconf -add -unmanage` *`collectionstation`*

TIP When NNM is first started, all the collection stations attempt to report to the management station at the same time, slowing down the system. Unmanage them and bring them on one at a time.

This same command is used for the floating host name of a Service Guard cluster on UNIX systems. As part of your Service Guard configuration process, you updated the `ov.conf` configuration file `HOSTNAME= parameter`. Refer to the *ov.conf* reference page in NNM online help (or manpage on UNIX systems) for more information.

4. Configure the `set` community name to be used when communicating with the collection station by selecting `Options:SNMP Configuration` from the menu bar. This displays the `SNMP Configuration` dialog box.
5. In the "`Specific Nodes`" tab (`SNMP Parameters` pane of the dialog box on UNIX systems), specify in the `Set Community` text field the same set community name that you configured on the collection station.

RQS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 0710
3740
Doc:

6. Click [OK] to close the SNMP Configuration dialog box.
7. To make sure the collection station is configured correctly, execute the following command (from a command window on systems running a Windows operating system):

   xnmtopoconf -test *collectionstation*

   If you see SNMP errors or timeouts reported, refer to "Troubleshooting Collection Station Communication" on page 147 for more information.
8. Manage the collection station by executing the following command:

   xnmtopoconf -manage *collectionstation*

   This causes the management station to start monitoring and synchronizing with the remote collection station. As part of this, the management station will be added to the collection station's internal list of interested managers. This internal list is referred to as %REMOTE_MANAGERS_LIST% in various places in the interface, such as the event configuration system, when forwarding is being configured.

Unmanaging a Collection Station

To unmanage a collection station from a management station, execute the following command (as Administrator on systems running a Windows operating system or root on UNIX systems) from the management station (from a command window on systems running a Windows operating system):

xnmtopoconf -unmanage *collectionstation*

This removes the management station from the list of active management stations (%REMOTE_MANAGERS_LIST%) for this collection station. The collection station however remains in the management station's database. This command may take a few minutes to complete. All objects for which the collection station is the primary collection station are either assigned a new primary collection station or have their status set to unknown.

Since new primary collection stations are being assigned, this command may take some time to complete.

Removing a Collection Station from a Management Station

Determine what collection stations already exist as described in "Determining if a Node is a Collection Station" on page 137to get a list of current collection stations and see if they are managed or unmanaged.

To remove a collection station from the management station's database, execute the following command (as `Administrator` on systems running a Windows operating system or `root` on UNIX systems) from the management station (from a command window on systems running a Windows operating system):

`xnmtopoconf -delete` *`collectionstation`*

This will remove all the symbols representing the collection station objects from the maps on the management station. When a collection station is deleted, a new primary is picked automatically. If none exists, the node is deleted from the management station.

This command may take some time to complete since all data reported from that collection station is removed. If you will be using this data in the future, you may want to unmanage the collection station instead of removing it.

Configuring a Remote Communication Timeout and Retry Count

A WAN link connecting a management station and a collection station will likely have a slow response time and a larger packet loss rate due to congestion. The following procedure will determine the appropriate set of timeouts to use for remote communication.

1. Ping the remote collection station by executing the following command (from a command window on systems running a Windows operating system):

   `ping` *`collectionstation`*

   For Solaris, use **`ping -s`** *`collectionstation`*.

   After a period of time, stop the ping and note the average round trip time and the packet loss rate.

2. Configure the timeouts and retry count for the remote collection station, based on the behavior received from the ping.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0711
3740
Doc:

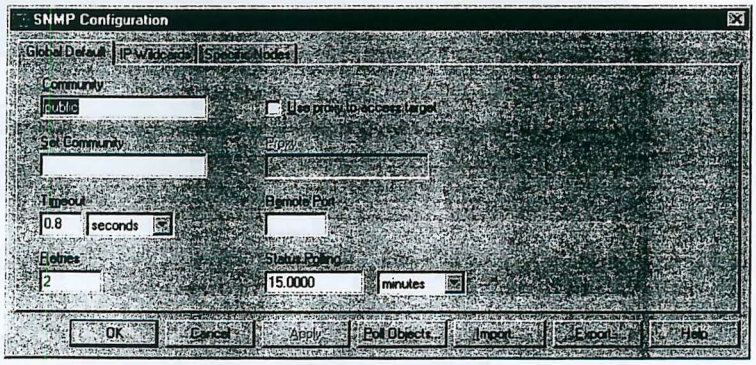
For example, for a reasonable timeout configuration, take the average ping round-trip time, double it, and add a little. For a retry count, the higher the packet loss rate, the more retransmissions you should specify to occur before a failed SNMP request. You should keep a retry count of at least 3.

3. Select `Options:SNMP Configuration` from the menu bar; the `SNMP Configuration` dialog box appears, as shown in Figure 4-8 (Figure 4-9 for UNIX systems).
4. In the `SNMP Parameters` section of the dialog box, specify the timeout configuration in the `Timeout` text box and the retry count in the `Retry Count` text box.
5. Click `[OK]` to save the changes and close the dialog box.
6. Verify communication with the remote collection station by executing the following command (from a command window on systems running a Windows operating system):

```
xnmtopoconf -test collectionstation
```

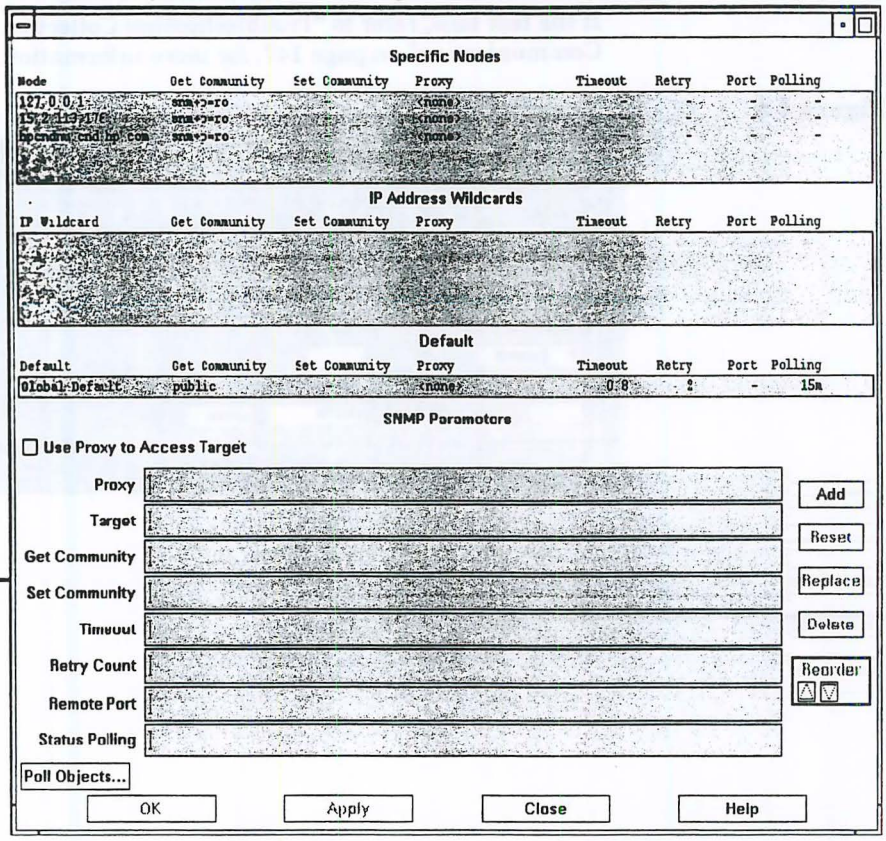
If the test fails, refer to "Troubleshooting Collection Station Communication" on page 147, for more information.

Figure 4-8 Windows SNMP Configuration Dialog Box



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0712
Doc: 3740

Figure 4-9 UNIX System SNMP Configuration Dialog Box



Performing a Full Topology Synchronization

A full topology synchronization causes a complete check of every attribute of every object reported by the remote collection station. This includes adding objects that are unknown and deleting objects that are not known at the remote collection station.

Perform a full synchronization by executing the command (from a command window on aWindows operating system):

nmdemandpoll -s *collectionstation*

All results and actions taken are reported to the command line. The output consists of the following:

- General processing status. There will be output noting the general flow of the synchronization process as well as general information related to the remote collection station (for example, hostname, port, version).
- Detailed output concerning the processing of all objects, regardless of whether any changes were detected.
- Warnings about objects that have conflicts or other errors in updating the objects in the database.
- Information about objects that no longer exist in the remote site's database and that are being removed from the local topology database.

TIP When resynchronizing peer-to-peer management stations, the simultaneous resynchronization can cause NNM to slow down and fail. Unmanage one until the other has resynchronized, then remanage it to synchronize it.

Identifying Collection Station Communication Problems

You can check the status of a collection station or management station using the NNM Station view.

One way to open an NNM Station view is by using the NNM `Tools:Views->Station` command. For other ways of opening an NNM Station view, see the *Interacting with Views* section of the HP OpenView web online help.

The status color of the local management station indicates whether or not it is responding to NNM status polls. The status color of a collection station indicates whether or not the local management station is receiving data from that remote collection station:

- Tan color: The collection station is unmanaged.
- Green color (management station): The management station operational status is normal.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0713
3740
Doc:

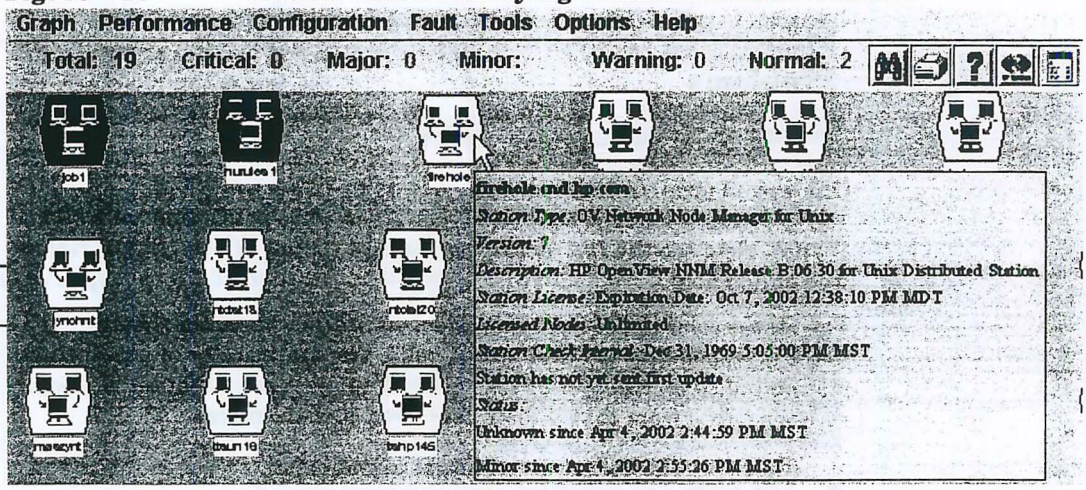
- Other color (management station): The management station operational status is abnormal.
- Green color (collection station): The collection station to management station communication status is normal.
- Other color (collection station): The collection station to management station communication status is abnormal.

In Figure 4-10 on page 146, the NNM Station view shows you that management station `job1` is managing `nurules1`. The status of both collection station `nurules1` and management station `job1` is normal.

However, the communication status of collection station `firehole` recently changed, as shown by the exclamation point, and is now showing an abnormal status color. You need to troubleshoot the communication from collection station `firehole` to management station `nurules1`. See "Troubleshooting Collection Station Communication" on page 147for troubleshooting techniques.

NOTE By resting your mouse pointer over collection station `firehole`, NNM displays some additional information.

Figure 4-10 Station View: Identifying Communication Problems



Troubleshooting Collection Station Communication

To troubleshoot the communication between a management station and a collection station use `xnmtopoconf`, as shown in the following procedure.

1. To determine the status of the managed collection stations, execute the command (from a command window on systems running a Windows operating system):

   `xnmtopoconf -print`

   This will produce a list of managed collection stations and their status as follows:

```
STATION              STATUS     INTERVAL OVERLAP MODE     FAILOVER   FAILOVER FILTER
ab.cnd.hp.com        Unmanaged  5m       AllowOverlap     off        <none>
be.cnd.hp.com        Critical   2m       AllowOverlap     ON         Routers
cat.cnd.hp.com       Unmanaged  5m       AllowOverlap     off        <none>
dog.cnd.hp.com       Normal     5m       AllowOverlap     configured <none>
emu.cnd.hp.com       Critical   5m       AllowOverlap     off        <none>
local                Normal     5m       DeleteSecondary  off        <none>
yak.cnd.hp.com       Unmanaged  5m       AllowOverlap     off        <none>
```

   The `STATUS` is determined by the status checks, which are performed, by default, at 5 minute intervals. The `STATUS` can be one of the following values:

`Unmanaged`	The collection station is currently not being monitored.
`Unknown`	The collection station has not yet had a status check. The initial synchronization may be in progress.
`Normal`	The collection station has responded to the most recent status check.
`Warning`	The collection station has not responded to the most recent status check, but it did respond to the status check before that.
`Minor`	The collection station has not responded to two consecutive status checks.
`Major`	The collection station has not responded to three consecutive status checks.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3714
Doc:

`Critical`	The collection station has not responded to four consecutive status checks.

2. If the results of this command produce any collection stations with a status other than unmanaged, unknown, or normal, execute the following command to help determine the problem with this Windows operating system):

   `xnmtopoconf -test` *`collectionstation`*

   For example, executing this command on `hobbes.msr.hp.com` produces output similar to the following:

```
Testing station hobbes.msr.hp.com.
ICMP round trip time = 120 ms.
  Ping test to hobbes.msr.hp.com (15.31.16.141) succeeded.
  Get sysObjectID test failed:
    Error in SNMP reply: No response arrived before timeout
Test for station hobbes.msr.hp.com failed
```

   In this example, the get `sysObjectID` test failed. (Refer to the information below for potential causes.)

   Executing `xnmtopoconf -test` on a collection station with a status other than unmanaged, unknown, or normal can produce one of the following results:

   - `Ping test to the` *`collection station`* `failed:`

     This could be because the node is down or that the SNMP timeout or retry count needs to be increased.

   - `Get sysObjectID test to the` *`collection station`* `failed:`

     This could be because

     — the SNMP agent on the collection station is down.

     — the SNMP timeout or retry count needs to be increased.

     — the get community name is incorrectly configured.

   - `Get topology info test to the` *`collection station`* `failed:`

This could be because

— one or more of the services (background processes on UNIX systems) are not running on the collection station. Run `ovstatus` on the collection station to determine which services are not running. If necessary, run `ovstart` to start the services.

— the get community name is incorrectly configured.

- `Set event forwarding test to the` *`collection station`* `failed:`

  This could be because the set community name is incorrectly configured on either the collection station or the management station.

IRQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 715
3740
Doc:

2956

39

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0716
3740
Doc:

Configuring Domain Overlaps and Failover

This section describes how to:

- Determine the primary station for an object.
- Change the primary station for an object.
- Change the overlap mode.
- Configure collection station failover.

Determining the Primary Collection Station for an Object

To determine the primary collection station for a given object, execute the following command (from a command window on systems running a Windows operating system):

ovtopodump -C *object*

This will print the primary version of the object with the name of the collection station reporting that version. For example, executing

ovtopodump -C gw1

produces the following output:

```
OBJECT ID(S)    OBJECT      STATUS       IP ADDRESS       STATION
146/145          gw1        Normal       10.2.112.1       remstn1
146/145          gw1        Normal       10.2.112.1       remstn1
146/595          gw1        Normal       10.2.104.1       remstn1
146/1158         gw1        Unmanaged    10.2.120.1       remstn1
```

In this example, the object gw1 is a gateway being monitored by the collection station remstn1.

You can see which collections stations are monitoring an object by using the -RISC option of ovtopodump. For example, executing

ovtopodump -RISC gw1

produces the following output:

```
OBJECT ID(S)    OBJECT      STATUS       IP ADDRESS       STATION
146               gw1       Normal       10.2.104.1       remstn1
146/145           gw1       Normal       10.2.112.1       remstn1
146/595           gw1       Normal       10.2.104.1       remstn1
146/1158          gw1       Normal       10.2.120.1       remstn1
146              &gw1       Unmanaged    10.2.104.1       local
146/145          &gw1       Unmanaged    10.2.112.1       local
146/595          &gw1       Unmanaged    10.2.104.1       local
146/1158         &gw1       Unmanaged    10.2.120.1       local
146              &gw1       Unknown      10.2.104.1       stn2
146/145          &gw1       Unknown      10.2.112.1       stn2
146/595          &gw1       Unknown      10.2.104.1       stn2
146/1158         &gw1       Unknown      10.2.120.1       stn2
```

In the second example, the node `gw1` has the collection station `remstn1` as its primary station, but is also known to be monitored by `stn2` and by the local management station. (The special station name `local` is used to represent locally monitored objects.) The "&" symbol designates the secondary versions of the objects. (Meanings of other symbols in this location are documented in the *ovtopodump* reference page in NNM online help (or manpage on UNIX systems)).

Changing the Primary Collection Station for an Object

The system will choose a primary collection station for an object, based on the rules as described in "The Selection of Primary and Secondary Collection Stations" on page 53. This choice should be adequate for most purposes. However, you can explicitly override the choice of primary by specifying the `-primary` option to the `xnmtopoconf` command. For example, executing the following command makes the designated collection station the primary for the listed objects. This requires `root` access on UNIX systems or `Administrator` privileges on systems running a Windows operating system.

`xnmtopoconf -primary` *`collectionstation object`*

For example, if it was desired that `stn2` be the primary for `gw1`, the following command could be executed (from a command window on systems running a Windows operating system):

```
xnmtopoconf -primary stn2 gw1
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0717
3740
Doc:

This temporarily overrides the system's choice of primary. If something changes to affect the choice of primary according to the described rules, the system will change to a new primary. The choice can be made stronger by specifying the `-preferred` option of `xnmtopoconf`. For example, execute the following command (from a command window on systems running a Windows operating system):

```
xnmtopoconf -preferred -primary stn2 gw1
```

to mark the version from `stn2` as the preferred choice for the primary collection station for this object. So long as `stn2` is managed and in a noncritical state it will be the primary collection station for `gw1`. You can clear the preference by specifying the `-clearPreferred` option (from a command window on systems running a Windows operating system):

```
xnmtopoconf -clearPreferred stn2 gw1
```

Changing the Overlap Mode

The overlap mode determines how the system behaves when an overlap is detected between the local management station and a remote collection station. The overlap mode applies to the collection station from the management station's perspective. The overlap mode is applied when an object is made a secondary to another remotely monitored version of the object. (See "Overlaps with the Collection Domain of the Management Station" on page 55 for a complete description.) To change the overlap mode use the `-overlap` option of `xnmtopoconf` (from a command window on systems running a Windows operating system):

```
xnmtopoconf -overlap mode local
```

where *mode* can be one of the following:

- `Allow Secondary Local Objects`
- `Unmanage Secondary Local Objects`
- `Delete Secondary Local Objects` (default)

The mode applies to all monitored objects for the local management station that are made secondaries for other remotely monitored objects. The mode cannot be changed on an individual object basis.

Collection Station Failover

Collection station failover allows a management station to pick up status polling responsibility for a collection station that fails. To enable failover (from a command window on systems running a Windows operating system):

xnmtopoconf -failover *stationlist*

The station or stations in the *stationlist* will have status polling automatically taken over when the collection station is downgraded to critical. See the *xnmtopoconf* reference page in NNM online help (or manpage on UNIX systems) for details. If the collection station is currently critical, `-failover` causes the management station to take over status polling immediately.

To disable failover, use `xnmtopoconf -nofailover`.

Failover Filters

To specify which objects from the collection station's topology to include in status polling, specify a failover filter to `xnmtopoconf` (from a command window on systems running the Windows operating system):

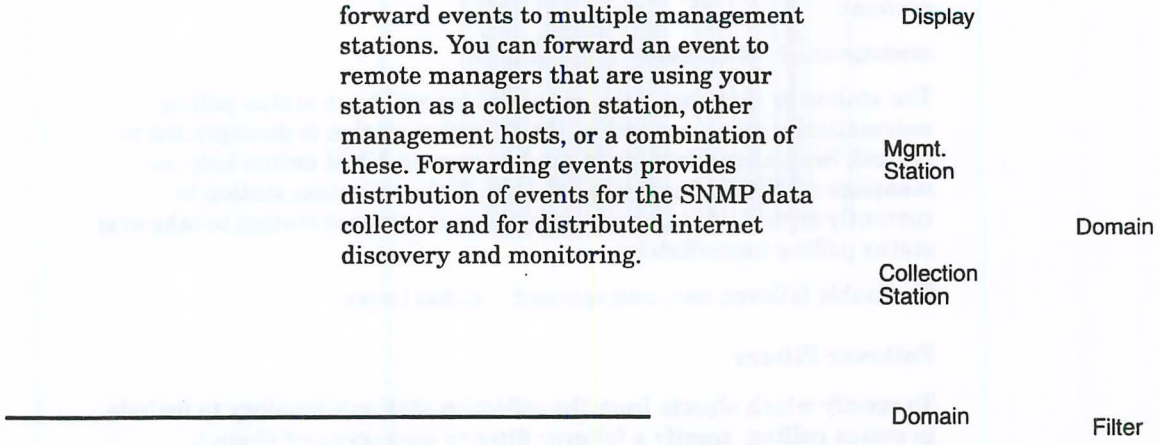
xnmtopoconf -failoverFilter *filter stationlist*

A new or changed filter is applied to the objects associated with the collection stations in the *stationlist*. If the collection station is not failed over, the filter will be applied the next time it fails. However if the objects from a station are already failed over, `netmon` on the management station releases the objects associated with the collection station(s) and then reloads the collection station topology and applies the new filter as it loads the topology.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0718
3740
Doc:

Configuring Event Forwarding and Correlation

You can configure the event system to forward events to multiple management stations. You can forward an event to remote managers that are using your station as a collection station, other management hosts, or a combination of these. Forwarding events provides distribution of events for the SNMP data collector and for distributed internet discovery and monitoring.



NOTE When forwarding threshold events, be sure that you forward the corresponding rearm event. See the *Managing Your Network with HP OpenView Network Node Manager* manual for information on configuring threshold and rearm events.

Forwarding an Event

You can modify events to have them forwarded to multiple management stations. When you create a new event, you can specify to have that event forwarded. HP recommends that you use multiple varbinds with individual pieces of data rather than using a full string. This allows the receiving application to specify the formatting. This procedure explains how to modify an event.

1. Select Options:Event Configuration from the menu bar; the Event Configuration window appears. From the command line, you may run xnmtrap.

2. Select an enterprise from the Enterprise list (the Enterprise Identification pane on UNIX systems).
3. Select an event that you want to forward from the Event Identification pane.
4. On Windows systems, select Edit:Events->Modify Event from the menu bar in the Event Configuration window; the Modify Events dialog box appears. See Figure 4-11.

   On UNIX systems, select Edit:Modify Event from the menu bar in the Event Configuration window; the Event Configurator/Modify Event dialog box appears. Figure 4-12 shows the Event Configurator/Modify Event dialog box.
5. On Windows systems, click the [Forwarding] tab.

   On UNIX systems, click on the Forward Event check box to expand the dialog box to display the Forwarded Event Destinations pane.
6. Complete the Forwarded Event Destinations pane ([Forwarding] tab) by specifying the destinations to forward the events to.

   You can add destinations in the following ways:

   - Clicking [Remote Mgrs] to add all remote management stations to the Forwarded Event Destinations list. The remote ons are specified in a list indicated by the special string %REMOTE_MANAGERS_LIST%. This list is created automatically as systems are defined to be collection stations.
   - Clicking [Add From Map] to add the destinations that are p.

NOTE Even though the %REMOTE_MANAGERS_LIST% string exists, the actual file (*install_dir*\bin\databases\remoteMgrs on stations running a Windows operating system, $OV_DB/remoteMgrs on UNIX systems) may not exist, or may not contain the remote management stations you expect. You can verify the contents of the remoteMgrs file using a text editor.

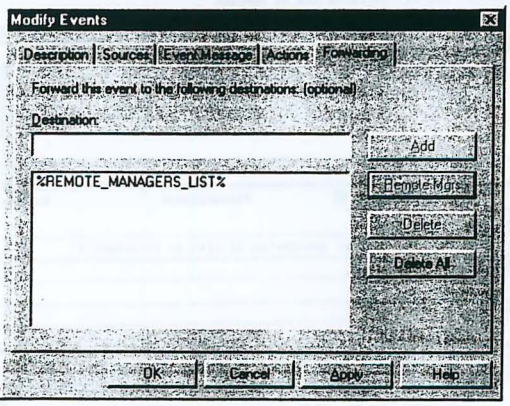
   - Typing the destination in the Destination text box and clicking [Add]. The destination you specify can be a file containing a list of destinations, a hostname, or an Internet address.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0719
3740
Doc:

7. Click `[OK]` from the `Modify Events` dialog box.
8. Click `File:Save` from the `Event Configuration` window to save the changes.

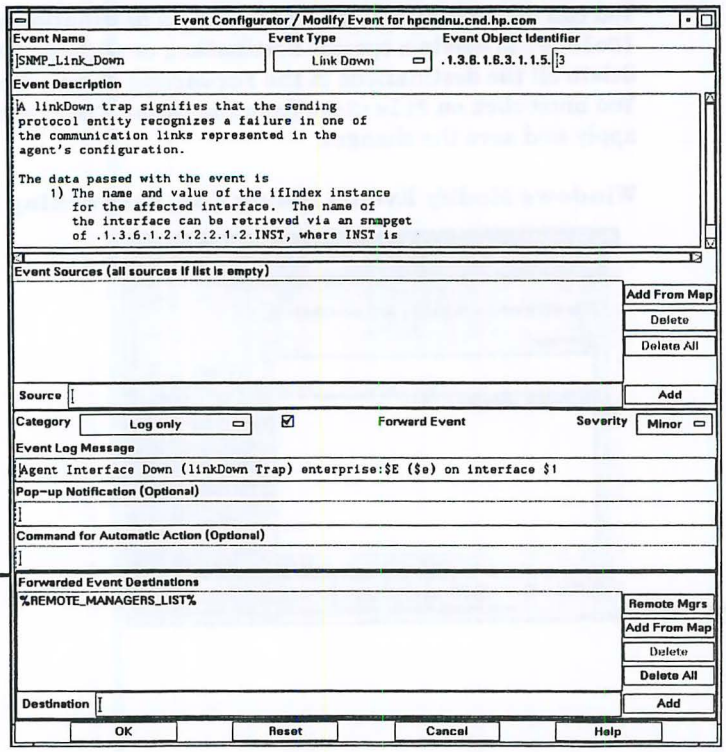
You can delete destinations by selecting a destination and clicking `[Delete]` to delete a specific destination, or clicking `[Delete All]` to delete all the destinations in the `Forwarded Event Destinations` list. You must click on `File:Save` from the `Event Configuration` window to apply and save the changes.

Figure 4-11 Windows Modify Events Dialog Box, Forwarding Tab



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0720
3740
Doc:

Figure 4-12 UNIX System Event Configuration/Modify Event Dialog Box



Using Distributed Data Collection

This section discusses how to export data from collection stations into a single Relational Database Management System (RDBMS) for report generation. For each collection station, use the following procedure:

1. Use the Network Node Manager data collector tool to collect MIB data. Refer to the *Managing Your Network with HP OpenView Network Node Manager* manual for information on data collection.
2. Determine which data collector files you want to merge into the RDBMS. These files are located in *install_dir*\databases\snmpCollect (`$OV_DB/snmpCollect` on UNIX systems).
3. Use `ftp` or `rcp` to copy the files from the collection station to a temporary data directory on the management station. You should also copy each data file's corresponding description file. The description file is named identically to the data file, except that an exclamation mark (!) is appended to the end of the filename. For example,

   ```
   rcp $OV_DB/snmpCollect/ifInOctets.1 clifford:/tmp/collsta5
   rcp $OV_DB/snmpCollect/ifInOctets.1! clifford:/tmp/collsta5
   ```

   copies the data and description files for instance 1 of MIB variable `ifInOctets` to the management station `clifford`.

   Alternately, if the network link between the management station and collection station is of sufficient capacity, you may make the files accessible via NFS.
4. If the file *install_dir*\conf\collectProxyMap (`$OV_CONF/collectProxyMap` on UNIX systems) exists on the collection station, copy it to the management station as well, either in the temporary data directory or another directory.
5. Make sure the temporary directory on the management station has `drwxrwxrwx` permission and that each data file has `-rw-rw-rw` permission.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0721
3740
Doc:

6. On the management station, run the `ovcoltosql` command as `root`, to export the data into the RDBMS. Specify the temporary data directory as the data source by using the `-s` option. For example, (from a command window on systems running a Windows operating system):

   ```
   ovcoltosql -Ro -s /tmp/collsta5
   ```

   This example exports data from the directory `/tmp/collsta5` into an Oracle database.

   If there is a `collectProxyMap` file for the collection station, use the `-p` option of `ovcoltosql` to specify the proxy map file location.

   Refer to the *ovcoltosql* reference page in NNM online help (or manpage on UNIX systems), and to the *Reporting and Data Analysis with HP OpenView Network Node Manager* manual for options that you can specify with this command.

If two or more collection stations collect on the same instance of the same MIB variable on the same node, they are said to have an overlapping collection. If data from an overlapping collection is merged into a single RDBMS, some of the data will not be entered into the RDBMS. `ovcoltosql` exports the data that is more recent than that already in the RDBMS. The collection station from which data is exported first will have data from its overlapping collection entered into the RDBMS, while most, if not all of the overlapping data from the second collection station

NOTE

You can execute `ovcoltosql` on the collection stations themselves to a common RDBMS server, but it is not recommended. This can cause potential performance problems when slow network links are traversed. Also, this approach results in the `topo_id` column of the `snmp_trend_dataset` table, which consists of topology IDs, to be assigned by different collection stations. Hence, the column will be useless for performing SQL joins across topology and trend tables.

Refer to the *Reporting and Data Analysis with HP OpenView Network Node Manager* online manual for information on RDBMS querying and administering operations.

5 Dynamic Views and Distributed Management

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0722
3740
Doc:

This chapter discusses how several NNM dynamic views function when you use them with DIDM. Readers are assumed to have read previous chapters and understand how to configure collection station to management station communication.

Dynamic Views and Distributed Management

Dynamic Views and Distributed Management

Numerous dynamic views are available from NNM. These views present a graphical (or tabular) representation of your network infrastructure.

Management station views of the Neighbor view and Path view will display links to views from collection stations or provide additional information in the following situation:

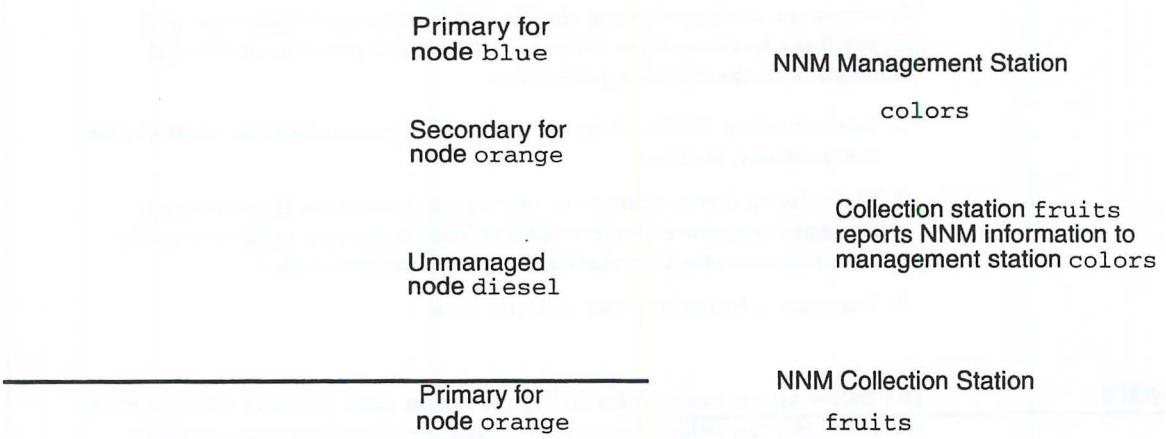
1. You are using NNM 6.3 or newer for both your collection station and management station.
2. You select a device from your management station that is being managed by your collection station.Your collection station must be the primary collection station for the device you select.
3. You open a Neighbor view or Path view.

NOTE The following examples refer to Figure 5-1 on page 164 and assume that you managed the collection station named `fruits` from management station named `colors`.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0723
3740
Doc:

Figure 5-1 shows node `colors` acting as a management station that manages node `blue` and collection station `fruits` within an NNM distributed environment. In this example, collection station `fruits` forwards NNM information to management station `colors`.

Figure 5-1 NNM Dynamic Views: Collection Station to Management Station Communication



NNM Neighbor View

The Neighbor view shows you a graphical representation of the selected device and the connector devices related to it, within a specified number of hops of the selected device.

To open a Neighbor view from NNM, use the `Tools:Views->Neighbor` me[illegible]wser to htt[illegible]0/topology/neighborView.

NOTE Replace *hostname* in the examples with the actual hostname or the IP address of the system NNM is installed on.

A N[illegible]es the following information in the environment shown in Figure 5-1:

- The management station `colors` is primary for `blue`. If you open a Neighbor view from `colors` with `blue` selected, it does not show nodes that are managed remotely. In this example, `orange` is not in the view, even if it is within the hop distance, because it is remotely managed by `fruits`. The Neighbor view includes a graphical representation of `blue` and other locally managed nodes of `colors`.
- Assume `colors` has a secondary copy of `orange` in its topology database, but that `fruits` is primary for `orange`. If you open a Neighbor view from `colors` with `orange` selected, it does not show nodes that are managed locally. In this example, `blue` is not in the view, even if it is within the hop distance, because it is locally managed by `colors`. The Neighbor view includes a graphical representation of `orange` and other locally managed nodes of `fruits`. This view also provides a link to a Neighbor view from `fruits`.
- If you try to open a Neighbor view of `diesel`, the Neighbor view tells you that `diesel` does not exist in the topology.

NNM Path View

The Path view presents a graphical representation of the path between two nodes and a table of interface information about the devices contained in the path.

To open a Path view from NNM with Extended Topology, use the `Tools:Views->Path` menu or point your browser to `http://`*`hostname`*`:7510/topology/pathView`.

Refer to Figure 5-1 on page 164. If you open a Path view from `colors` with `blue` as the source node and `orange` as the destination node, NNM displays the Path view, a table of interface information about the devices contained in the path, and tells you that `orange` is managed by `fruits`.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0724
3748

Dynamic Views and Distributed Management

A The Filter Definition Language

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0725
3740
Doc:

This appendix discusses in detail the language used to define filters in the filter definition file, giving you the information you need to modify existing filters, or define new ones.

This appendix is a reference to the contents of the filter definition file, and to the grammar of the filter definition language.

NOTE

This appendix assumes that you are familiar with two topics normally covered in the study of computer science: Boolean expressions and Backus-Naur Form (BNF) grammars. This appendix makes no attempt to teach the fundamentals of either Boolean expressions or BNF grammars. If you are unfamiliar with these topics, you may find it helpful to review these ideas in a computer science text book before you feel entirely comfortable defining new filters.

The Filter Definition File

Filters are defined in an editable file of ASCII characters; this is called the filter definition file. The format and contents of this file make up the subject of this appendix.

The filter definition file for all the filters you use with HP OpenView Network Node Manager (discovery, topology, map, and persistence) is *install_dir*\conf\C\filters on Windows operating systems and $OV_CONF/$LANG/filters on UNIX systems.

After you install NNM, the filter definition file contains a selection of useful definitions that you may be able to use as is, or with some modifications.

The filter definition file has several key components, and they appear in the file in the following order:

- Set definitions.
- Filter definitions, which each include one or more Attribute Value Assertions.
- Filter-Expression definitions, which each refer to one or more filters.

Each of these components is described in considerable detail in later sections of this appendix.

The filter definition file contains many instances of the above elements, always in order. That is, all set definitions are together at the top of the file, all filter definitions follow next, and all filter-expression definitions are at the end of the file.

As you examine the filter and filter-expression definitions in the sample filter definition file ("Default Filter File" on page 197), you will notice that some are intended for use as map filters, others are for discovery filtering. This distinction helps clarify the purpose of each filter and its components, and simplifies your troubleshooting of new or modified filters. Also, remember which types of filters are intended to *exclude* items and which are to *include*. Refer to Table 2-1 on page 38 for more information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0726
3740
Doc:

Filters and Filter-Expressions

The whole purpose of the filter definition file is to define the filters that are used with the scalability features of NNM. You have two basic types of filters: "simple" filters (which are simple only in that they do not refer to other filters), and filter-expressions.

Filters and filter-expressions are closely related and used identically. Everywhere else, they are referred to broadly as "filters." Within the filter definition file, however, there is a distinction between them:

- A **filter** is a combination (or "expression") of one or more Attribute Value Assertions.[1]
- A **filter-expression** is a combination (or "expression") of one or more previously defined filters. In other words, a filter-expression is a "high- level filter," created by combining lower-level filters that are already defined.

In every other respect, a filter-expression is exactly like a filter. You use filters and filter-expressions in exactly the same way. That is, anywhere a filter can be used, a filter-expression can also be used. Although most of the examples in this section uses filters, filter-expressions would be equally valid in those same examples.

You use logical, also called Boolean, operators (that is, And (`&&`), Or (`||`), and Not (`!`)), and normal precedence grouping via parentheses, to combine multiple filters in a filter-expression, or to combine multiple Attribute Value Assertions (AVAs) in a filter.

Defining filters and filter-expressions has two important rules:

1. A filter definition can include *only* AVAs. A filter definition can *not* include filters or filter-expressions.
2. A filter-expression definition can include *only* filters or filter-expressions that are defined earlier in the filter file. A filter-expression definition can *not* include AVAs.

1. See "Attribute Value Assertions" on page 172 for more details.

Sets

String-valued attributes can be tested for membership in a set. A **set** is simply a list of strings. The only operation available on sets is the test for membership.

You can enumerate the members of a set in two ways:

- Within the filter file itself, according the filter file grammar.[1]
- In a separate file, where set members are listed, one per line. You cannot use wildcards or ranges. If the set member begins with a slash ("/"), it is used as the absolute pathname of such a file. Relative pathnames and environment variables are invalid. In the Windows operating system, filter files must use the forward slash and should include a drive specification.

Files and member strings can be mixed in the same set definition. Set definitions can not be nested.

1. See "Filter File Grammar" on page 187 for details

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0727
Doc: 3740

Attribute Value Assertions

An **attribute value assertion** (**AVA**) is a statement about the value of an attribute. For example, here is an AVA about the `"IP Hostname"` attribute:

```
"IP Hostname" == "server7"
```

An object can be compared against an AVA to determine whether that assertion is true or false for the object. In other words, an AVA is a condition that an object either does or does not meet. When an AVA is tested against a particular object, one of three results can occur:

- The object does not have that attribute.
- The object has the attribute, but the value of the attribute does not match the value in the filter.
- The object has the attribute, and the value of the attribute matches the value in the filter.

The above AVA will be false when the object has an IP hostname attribute, but the IP hostname of the object is *not* "server7". It will *also* be false when the IP hostname attribute is not present in an object.

The above AVA will only be true when the object has an IP hostname attribute, and the IP hostname of the object is "server7". Similarly the AVA `isRouter==TRUE` is only true for routers.

AVAs are defined in terms the of fields of an object and possible values of those fields. The fields used in creating AVAs for filters are a subset of the fields contained in the object database (`ovwdb`).[1]

NOTE Many field names in the object database have embedded white space. Any field name or field value containing white space must be enclosed in double quotes (for example `"Selection Name"`).

In the object database, attributes can have four types:

1. See "Filterable Objects and Attributes" on page 181 for the specific fields you can use in filters.

- Boolean
- Integer
- String
- Enumerated

Attribute value assertions fall into one of these four categories, depending on the attribute type.

After a short section that discusses the operators that are valid in AVAs, AVAs for each of the above types of attributes are covered in more detail.

NOTE Attribute Value Assertions can only be tested against literal constant values. The attributes of two different objects cannot be tested against each other.

Valid Operators for AVAs

These are the operators that you can use to express AVAs:

Operator	Meaning
==	Equal to
!=	Not equal to
>	Greater than
>=	Greater than or equal to
<	Less than
<=	Less than or equal to
~	Like, which used for pattern matching.[1]
!~	Not like, also used for pattern matching.
IN	Is a member of the set

1. See "String AVAs" on page 175 for more information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0728
3740
Doc:

TIP Filters are "short-circuit" evaluated. This means NNM only reads far enough to get an answer, then doesn't read the rest of the filter definition. For best performance, put likely TRUE clauses first when OR-in, and put likely FALSE clauses first when AND-ing.

Table A-1, Operators Allowed in AVAs for Each Field Type, shows which of these operators are valid in particular AVAs, depending on the field type of the attribute.

Table A-1 Operators Allowed in AVAs for Each Field Type

Operator	ovwStringValue	ovwEnumValue	ovwIntValue	ovwBooleanValue
==	Yes	Yes	Yes	Yes
!=	Yes	Yes	Yes	Yes
>	Yes	No	Yes	No
>=	Yes	No	Yes	No
<	Yes	No	Yes	No
<=	Yes	No	Yes	No
~	Yes	No	No	No
!~	Yes	No	No	No
IN	Yes[1]	No	No	No

1. Valid only if the value of the expression is the name of a defined set. See "Sets" on page 171 for details.

Boolean AVAs

Boolean AVAs can be expressed with just an attribute name (with an optional, leading `NOT` operator), or can be explicitly tested against the keyword values `TRUE` and `FALSE`. For example, testing for a object being a router can be expressed in either of the two following ways:

```
(isRouter)
(isRouter == TRUE)
```

The inverse expression, testing for a non-router, could be expressed in either of following ways:

```
(! isRouter)
```

```
(isRouter == FALSE)
```

Integer AVAs

Integer AVAs can be tested for equality, inequality, greater than, greater than or equal to, less than, and less than and equal to (==, !=, >, >=, <, <=). For example, to test for a multi-homed node, an expression using an integer AVA might look like this:

```
(numInterfaces > 1)
```

Enumerated (Enum) AVAs

In the object database, enum valued attributes have their enumerated values expressed explicitly. In enumerated AVAs these same enumerated values are used. For example, to test whether an object is from a particular vendor, the following AVA might be used:

```
(vendor == "HP")
```

Enum AVAs can only test for equality or inequality. Because the integer value of a given enum value can change, you must use enum strings in enum AVAs, and not their integer equivalents.

All enumerated values must be delimited (enclosed) in double quotes ("), as in the above example.

String AVAs

String AVAs can be tested using any lexical operator (==, !=, >, >=, <, <=). For example, if you were testing for a particular host, you might use the following AVA:

```
("IP Hostname" == "gomez")
```

Strings are tested using the `strcoll` function, and thus take advantage of any natural language semantics provided by that function.[1]

1. See the manpage on UNIX systems for *strcoll*(3).

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0729
3740
Doc:

In addition to standard lexical comparison, extended regular-expression matching (as defined in *regcomp*(3))[1] is also available via the "like" (~) operator. When you use this operator, the string is treated as a regcomp-style regular expression, in which certain characters have special meaning.

The AVA below matches *any* hostname with the sub-string "morticia" in it:

```
("IP Hostname" ~ "morticia")
```

while the next AVA (because it tests for "equality" rather than "like", and thus does not use regular-expression matching) matches only and exactly the hostname composed of the string "morticia":

```
("IP Hostname" == "morticia")
```

All regular expressions must be delimited (enclosed) in double quotes (" "), as in the above example.

CAUTION

When negating the "is like" operator (~), place the negation *outside* of the expression. This is necessary due to NNM discovering all level 2 interfaces, including objects like serial cards which have no IP address. When no IP address is present, the object is assigned 0.0.0.0. If you negate the operator, as in `"IP Address" !~ 1.2.3.4`, you will inadvertently *include* all non-IP level 2 interfaces. By negating the `idress" ~ 1.2.3.4)`, you get the set of all objects that *have* an IP address, and it is not like the one in the expression.

NOTE

See the "Caution" block in "Set Specifications in SNMP OIDs" on page 179 before using regular-expression matching with SNMP object identifiers or with IP addresses.

1. See the manpage on UNIX systems for *regcomp*(3).

Specialized Pattern Matching in NNM Filters

There are two special types of string-valued AVAs for which NNM provides specialized pattern matching on the associated attributes:

SNMP Object IDs (SNMP OIDs)	In a filter, an SNMP OID is identified as a leading period followed by decimal octets separated by periods. For example: `.1.3.6.34.2.209`
IP addresses	An IP address is identified as a string of exactly four (4) decimal octets separated by periods, but *without* a leading period: `23.26.11.14`

Three types of specialized pattern matching are available—wildcards, ranges, and sets. Set patterns are available only for SNMP OIDs. You can replace any decimal octet in an IP address or SNMP OID with a special pattern matching string.

NOTE Do not overlook the "Caution" block in "Set Specifications in SNMP OIDs" on page 179.

Wildcard Characters in SNMP OIDs and IP Addresses For IP address and SNMP OID pattern matching, the wildcard operator is the asterisk (*). An asterisk in an IP address indicates that any value is acceptable in the given decimal octet.

For example, to pass any address in the Class A IP network "23", you would use the following in your AVA:

```
"IP Address" ~ 2 3.*.*.*
```

The wildcard character acts slightly differently for SNMP OIDs. In this case, a wildcard indicates that any value *for zero or more* decimal octets is acceptable. For example, the following pattern:

```
.1.4.5.1.*.13.2.*
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0730
Doc: 3740

matches any OID with ".1.4.5.1" followed by any number of decimal octets of any value (including no octets at all), followed by "13.2" followed by zero or more trailing decimal octets. Therefore, the above pattern would match the following OIDs:

- .1.4.5.1.13.2
- .1.4.5.1.22.33.13.2
- .1.4.5.1.13.2.14.55.232
- .1.4.5.1.22.44.33.13.2.23.32.1

but not:

- .1.4.5.1.13 (no 2 after the 13)
- .1.4.5.2.2.13.2 (no 1 after the 5)
- .1.4.5.1.33.22.2 (missing the 13)

Range Specifications in SNMP OIDs and IP Addresses A range is expressed by a decimal integer, a hyphen (-), and another decimal integer that is greater than the first. Decimal octet values between 2 and 68 would be specified as follows:

```
2-68
```

A range indicates that any value in the range (inclusive) is acceptable in the given decimal octet. Ranges are significant for the given decimal octet only, in both SNMP OIDs and IP addresses. The values specified in a range must be in their natural order, from smallest to largest; a reversed range (like, for example, 68-2) is not permitted.

The following are more examples of valid SNMP OIDs and IP address AVAs, using sets, wildcards, and ranges in combinations:

```
("IP Address" ~ 23.2.*.*)
("IP Address" ~ 23.2.3-9.*)
("IP Address" ~ 23.2.16-22.0-1)
("SNMP sysObjectID" ~ .1.3.6.*.9.5)
("SNMP sysObjectID" ~ .1.3.6.8-9.*)
("SNMP sysObjectID" ~ .1.3.6.7-8.12-13)
```

Set Specifications in SNMP OIDs In SNMP OIDs (but not IP addresses), you can specify a set of decimal octets in any position by separating the members by a comma. For example, in the following AVA:

```
("SNMP sysObjectID" ~ .1.3.6.34.8,9,11,23)
```

would match the following SNMP OIDs:

```
("SNMP sysObjectID" ~ .1.3.6.34.8)
("SNMP sysObjectID" ~ .1.3.6.34.9)
("SNMP sysObjectID" ~ .1.3.6.34.11)
("SNMP sysObjectID" ~ .1.3.6.34.23)
```

CAUTION To invoke special pattern matching on IP address and SNMP OID strings, either the "like" operator (`~`) or "not like (`!~`) *must* be used.

Furthermore, to use NNM's specialized pattern matching facility, the IP address or SNMP OID string *must not* be enclosed in quotation marks. The presence of enclosing quotation marks means that the string will be treated as a regular expression, and *not* given specialized pattern matching; the absence of such quotation marks means the comparison *will* use NNM's specialized pattern matching facility.

The difference is important. Consider this AVA, where the value is quoted:

```
"IP Address" ~ "23.18.3.*"
```

With the quotation marks around the value (`"23.18.3.*"`), it is treated as a regular expression. The result is that *many* IP addresses beginning with "`23.18.3`" would cause the AVA to evaluate to `TRUE`, including, for example, `23.18.34.7`, which was probably not intended. In fact, even some strange and improbable IP address strings (like, for example, `23518.3711.1011.23033`) would pass this AVA. The reason is that, for regular expressions, the period character (`.`) matches *any* character in that location of the comparison string (including, confusingly, the period character itself).

However, if we use the same AVA, but *without* the quotation marks around the value (`"IP Address" ~ 23.18.3.*`), NNM's special pattern matching facility guarantees that only IP addresses in the apparently intended range would cause the AVA to evaluate to `TRUE`.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0731
3740
Doc:

Excluding a Node

For the purposes of building and using filters, a node can be thought of as a "super-object", which comprises the node and all its interfaces.

Thus, if a node object passes a filter, the filter will also pass all interfaces of the node regardless of whether they would, considered in isolation, pass the filter.

Similarly, if an interface passes a filter, the node object it belongs to, and all other interfaces of that node, also pass the filter.

Consequently, if you want a filter to exclude a node, the filter must block the node object itself and all of its interfaces.

NOTE Keep in mind that the `ovfiltertest` command does not follow this pattern. Instead of treating a node and its interfaces as a "super-object,", the `ovfiltertest` command treats nodes and interfaces as separate objects. See the *ovfiltertest* reference page in NNM online help (or the UNIX system manpage) for more information.

Relationships Between Nodes and Interfaces

You can create a filter that combines nodes and interfaces, as shown in the following example.

```
nodeNinterface "" {(vendor = "SUN") && (IP Address ~ 15.2.112.*)}
```

Valid Operators for Logical Combinations of AVAs or Filters

AVAs, filter names, and filter-expression names are combined to create filter and filter-expression definitions (as noted before, *only* AVAs are allowed in a filter definition, and AVAs are *never* allowed in a filter-expression definition).

You use the following operators to create logical combinations (or "expressions") of these components. Likewise, you combine filters or filter-expressions in a filter-expression definition with these operators:

Operator	Meaning
&&	Logical "and", used to combine multiple AVAs and filter names into logical expressions.
||	Logical "or", used to combine multiple AVAs and filter names into logical expressions.
!	Logical negation, used to negate stand-alone field names and other logical expressions. Fields that are already part of an expression cannot be negated; rather the entire expression should be negated.

Use parentheses—"(" and ")"—to specify explicit precedence in a group of operations. For example, a filter definition might look like this:

```
Filtr1 "" { isRouter && (numInterfaces > 1) }
```

Or a filter-expression definition might look like this:

```
FiltrExpr1 "" { (Filtr1 || Filtr2) && Filtr3 }
```

Filterable Objects and Attributes

The following four tables specify, for each type of object, the attributes (fields) for which filters can be defined. This is a subset of the objects and attributes in the ovwdb database.

Table A-2 Filterable Fields in Node Object

Field	Field Type
IP Hostname	String
IP Status	Enumerated
isATM *	Boolean
isBGP4 *	Boolean
isBridge	Boolean
isCDP *	Boolean
isCollectionStationNode	Boolean
isConnector	Boolean
isDS1 *	Boolean

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0732
3740
Doc:

Table A-2 Filterable Fields in Node Object (Continued)

Field	Field Type
isDS3 *	Boolean
isFrameRelay *	Boolean
isHSRP *	Boolean
isHub	Boolean
isIP	Boolean
isIPRouter	Boolean
isIPV6 *	Boolean
isIPX	Boolean
isIPXRouter	Boolean
isMcClusterMember	Boolean
isMPLS *	Boolean
isNetWareServer	Boolean
isNode	Boolean
isOSPF *	Boolean
isRMON *	Boolean
isRMON2 *	Boolean
isRouter	Boolean
isSONET *	Boolean
isSNMPSupported	Boolean
isSTP *	Boolean
isVRRP *	Boolean
isWireless *	Boolean
NetWare Server Name	String

Table A-2 Filterable Fields in Node Object (Continued)

Field	Field Type
Selection Name	String
SNMPAgent	Enumerated
SNMP sysContact	String
SNMP sysDescr	String
SNMP sysLocation	String
SNMP sysName	String
SNMP sysObjectID	String
TopM Interface Count	Integer
vendor	Enumerated

IMPORTANT * Fields marked with an asterisk have no effect on discovery filters.

Table A-3 Filterable Fields in Interface Object

Field	Field Type
isInterface	Boolean
isIP	Boolean
isIPX	Boolean
IPX Address	String
IP Address	String
IP Status	Enumerated
IP Subnet Mask	String
Selection Name	String

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0733
3740
Doc:

Table A-3 Filterable Fields in Interface Object

Field	Field Type
SNMP ifDescr	String
SNMP ifName	String
SNMP ifPhysAddr	String
SNMP ifType	Enumerated
TopM Network ID	Integer
TopM Node ID	Integer
TopM Segment ID	Integer

Table A-4 Filterable Fields in Segment Object

Field	Field Type
IP Segment Name	String
IP Status	Enumerated
isBusSegment	Boolean
isFDDIRingSegment	Boolean
isSegment	Boolean
isSerialSegment	Boolean
isStarSegment	Boolean
isTokenRingSegment	Boolean
Selection Name	String
TopM Interface Count	Integer
TopM Network ID	Integer

Table A-5 Filterable Fields in Network Object

Field	Field Type
IP Address	String
IP Network Name	String
IP Status	Enumerated
IP Subnet Mask	String
IPX Address	String
IPX Network Hop Count	Integer
isIP	Boolean
isIPX	Boolean
isNetwork	Boolean
Selection Name	String
TopM Default Seg ID	Integer
TopM Interface Count	Integer
TopM Segment Count	Integer

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 0734
3740
Doc:

Valid values for the enumerated fields can be found in the files listed in Table A-6, Value Definitions for Enumerated Fields,

Table A-6 Value Definitions for Enumerated Fields

For the field named:	The enumerated values are defined in:
`IP Status`	On Windows operating systems: *install_dir*`\fields\C\ip_fields` On UNIX systems: `$OV_FIELDS/$LANG/ip_fields`
`SNMP ifType`	On Windows operating systems: *install_dir*`\fields\C\snmp_fields` On UNIX systems: `$OV_FIELDS/$LANG/snmp_fields`
`SNMPAgent`	On Windows operating systems: *install_dir*`\fields\C\snmp_fields` On UNIX systems: `$OV_FIELDS/$LANG/snmp_fields`
`vendor`	On Windows operating systems: *install_dir*`\fields\C\ovw_fields` On UNIX systems: `$OV_FIELDS/$LANG/ovw_fields`

Filter File Grammar

The following is the formal Backus-Naur Form (BNF) grammar for a filter file. See "Filters" on page 37 for details about where such a file is used.

```
Filter_File          ::=   Filters
                           | Filters FilterExprs
                           | Sets Filters
                           | Sets FiltersFilterExprs

Sets                 ::=   "Sets" "{" Set_Stmts"}
                           | "Sets" "{" "}"

Set_Stmts            ::=   Set_Stmt
                           | Set_Stmts Set_Stmt

Set_Stmt             ::=   SetName Description "{" Memberlist"}"

Memberlist           ::=   Member_Stmt
                           | Memberlist "," Member_Stmt

Member_Stmt          ::=   StringOrIdentifier
                           | <absolute_file_pathname>

Filters              ::=   Filters" "{" Filter_Stmts"}"
                           | "Filters" "{" "}"

Filter_Stmts         ::=   Filter_Stmt
                           | Filter_Stmts Filter_Stmt

Filter_Stmt          ::=   FilterName Description "{" Expression"}"

Expression           ::=   Expression "&&" Expression
                           | Expression"||" Expression
                           | "!" Expression
                           | "(" Expression ")""
                           | BoolExpr
                           | SetExpr

BoolExpr             ::=   FieldName
                           | FieldName ExprOperator <string>
                           | FieldName ExprOperator <integer>
                           | FieldName PatternOperator <string>
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0735
3740

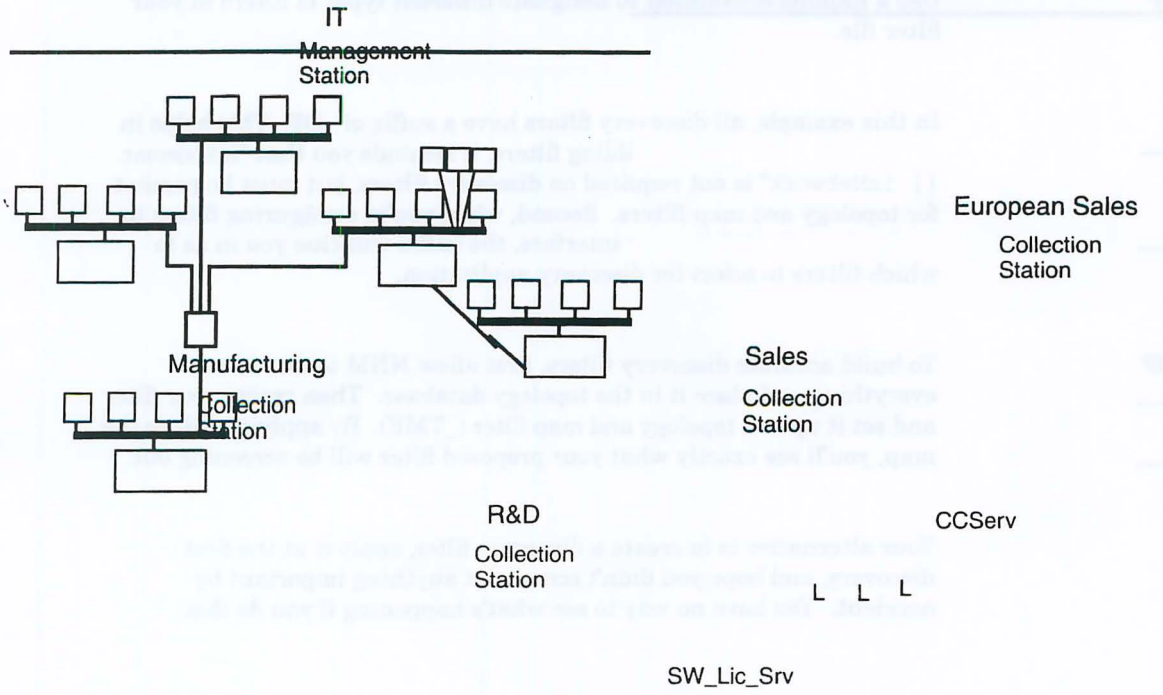
```
SetExpr              ::=    FieldName "IN" SetName

FilterExprs          ::=    "FilterExpressions" "{" FilterExpr_Stmts "}"
                            | "FilterExpressions" "{" "}"

FilterExpr_Stmts     ::=    FilterExpr_Stmt
                            | FilterExpr_Stmts FilterExpr_Stmt

FilterExpr_Stmt      ::=    FilterExprName Description "{" FiltExpr "}"

FiltExpr             ::=  FiltExpr "&&" FiltExpr
                          | FiltExpr "||" FiltExpr
                          | "!" FiltExpr
                          | "(" FiltExpr ")"
                          | FilterName

FieldName            ::=  StringOrIdentifier

ExprOperator         ::=  "==" | "!=" | "<" | "<=" | ">" | ">="

PatternOperator      ::=  "~" | "!~"

FilterExprName       ::= <unquoted_string>

FilterName           ::= <unquoted_string>

SetName              ::= <unquoted_string>

StringOrIdentifier   ::= <quoted_string> | <unquoted_string>

Description            ::=  <quoted_string>
```

Filter File Example

This example describes how these rules translate into usable filters for a sample network management solution. Hemispheres-Petroleum Company has decided to implement HP OpenView Network Node Manager's distribution capabilities to gain control over their overall network. They have a typical network organization that parallels their personnel organization -- local area networks for the Research and Development, Manufacturing, and Sales departments, with an additional network in place in Paris for European Sales. The network architecture is diagrammed in Figure A-1.

The IT department will be responsible for managing these networks, along with their own. They have decided to have a collection station for each department report to the management station in IT.

Figure A-1 Hemispheres-Petroleum Company Network Layout



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0736
3740
Doc:

The default filter file shipped with NNM has several useful building blocks already in place. (The default filter file appears on page 197.) Simple filters appear in the second section of the files, in the format `FilterName "Description" { AVA }`. For example, look at the line that says `Hubs "Any multi-port repeater" { isHub }`. The name of the filter, as it would later be used from the ovw user interface or in building filter expressions, is Hubs. `netmon` compares every node's SNMP response, looking for the `isHub` property. Any object possessing this property fits the filter `Hubs`. Similarly useful simple filters are in place for Networks, Segments, Nodes, IPRouters, Bridges, SNMPNode, HPNodes, and NonHPNodes.

Setting Up Collection Domains

Collection domains are specified through discovery filters. Setting these up demonstrates several tips that will help you manage filters for your network.

TIP Use a naming convention to designate different types of filters in your filter file.

In this example, all discovery filters have a suffix of _DF. This helps in ilding filters, it reminds you that "`isSegment || isNetwork`" is not required on discovery filters, but must be present for topology and map filters. Second, when you're configuring filters to interface, the suffix will clue you in as to which filters to select for discovery application.

TIP To build accurate discovery filters, first allow NNM to discover everything and place it in the topology database. Then create your filter and set it up as a topology and map filter (_TMF). By applying this to the map, you'll see exactly what your proposed filter will be screening out.

Your alternative is to create a discovery filter, apply it at the first discovery, and hope you didn't screen out anything important by accident. You have no way to see what's happening if you do this.

First set up the collection domain for the IT department's own management station. Using the pattern filter named EngrLan in the default filter file, add a filter named ITLan_DF, which includes the IP address range for IT nodes (15.2.107-117):

```
ITLan_DF "IT's IP subnet" { ("IP Address" ~ 15.2.107-117.*) }
```

Reading that back, the name of the filter is ITLan_DF and can be referred to by filter expressions and user interface fields that ask for a filter name. It passes objects whose IP Address field in their SNMP data is between (is like) 15.2.107.* and 15.2.117.*.

Now build a filter expression (combination of filters) to turn that into a topology and map filter:

```
ITLan_TMF "IT's IP subnet" {("IP Address" ~ 15.2.107-117.*)|| NetsNSegs}
```

The addition of NetsNSegs, a standard NNM filter, passes all objects with SNMP data matching isSegment or isNetwork. A discovery filter includes these by default, but topology and map filters must add them explicitly. Networks and segments are required so that node objects will have containers in which to reside. Without them, your map database becomes corrupted.

Now is the time to use the tip above. First allow NNM to discover everything and place it in the topology database. Then apply the TMF filter to the map using ovtopodump -f, showing exactly what will be screened out.

The IT network management administrator sets up similar filters for SalesLan, MfgLan, RDLan, and ESalesLan. Here is the filter file so far (without all the comment lines):

```
Filters {
Networks "Any network" { isNetwork }
Segments "Any segment" { isSegment }
NetsNSegs "All networks & segments" { isNetwork || isSegment }
Nodes "Any node" { isNode }
IPRouters "Any IP Router" { isIPRouter }
Bridges "Any bridge" { isBridge }
Hubs "Any multi-port repeater" { isHub }
SNMPNode "Any node supporting SNMP" { isNode && isSNMPSupported }
HPNodes "Hewlett-Packard nodes" { isNode && ( vendor == "Hewlett-Packard" ) }
UBNodes "Ungermann-Bass Nodes"  { isNode && vendor == "Ungermann-Bass" }
NonHPNodes "Non-HP nodes" { isNode && ( vendor != "Hewlett-Packard" ) }
ITLan_DF "IT's IP subnet" { ("IP Address" ~ 15.2.107-117."*) }
SalesLan_DF "Sales's IP subnet" { ("IP Address" ~ 15.2.125-140.*) }
MfgLan_DF "Manufacturing's IP subnet" { ("IP Address" ~ 15.2.145-160.*) }
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0737
Doc. 3740

```
RDLan_DF "R&D's IP subnet" { ("IP Address" ~ 15.2.175-250.*) }
ESalesLan_DF "European Sales's IP subnet" { ("IP Address" ~ 192.5.32-50.*) }
}

FilterExpressions {
ITLan_TMF "IT's IP subnet map filter" { ITLan_DF || NetsNSegs }
SalesLan_TMF "Sales's IP subnet map filter" { SalesLan_DF || NetsNSegs }
MfgLan_TMF "Manufacturing's IP subnet map filter" { MfgLan_DF || NetsNSegs }
RDLan_TMF "R&D's IP subnet map filter" { RDLan_DF || NetsNSegs }
ESalesLan_TMF "European Sale's IP subnet map filter" { ESalesLan_DF || NetsNSegs
}
}
```

With these filters, each collection station can specify its own domain of interest with no overlap.

TIP Build your overall filter file once and propagate it from your management station to all the collection stations. Use RCS for version control on the file and `rcp` to copy it to the collection stations. This way you know exactly what each collection station operator is looking at. You retain control over the file contents. And you can see a collection station's view of the network from the management station by applying the collection station's topology filter as a map filter on the management station.

Excluding Nodes

Take another look at the Sales LAN. It includes three laptop computers for sales people who are often on the road. The network operator really doesn't need to track whether those nodes are up or down, so write a DHCP filter that can exclude them:

```
SalesLaptops "Laptop units often offline in Sales
department" {"IP Address" ~ 15.2.135-140.*}
```

Now in a filter expression you can refer to `{SalesLan && !(SalesLaptops)}`. This is rather long, but it allows you to identify those laptops separately sometimes. Certainly, you could use this in a topology filter on the Sales collection station that would disable the status of these nodes being sent to the management station continuously.

You could also have specified `&& !("IP Address" ~ 15.2.135-140.*)` on the overall `SalesLan` filter if you know you would never want the laptops included.

CAUTION When negating the "is like" operator (~), place the negation *outside* of the expression. This is necessary due to NNM discovering all level 2 interfaces, including objects like serial cards which have no IP address. When no IP address is present, the object is assigned 0.0.0.0. If you negate the operator, as in `"IP Address" !~ 1.2.3.4`, you will inadvertently *include* all non-IP level 2 interfaces. By negating the expression, as in `!("IP Address" ~ 1.2.3.4)`, you get the set of all objects that *have* an IP address, and it is not like the one in the expression.

Failover Filters

What would happen if the Sales collection station failed? Assuming you have the management station configured for failover, all the nodes that the Sales collection station has in its topology database are polled by the management station. A failover filter would specify only the most critical nodes for which the management station would actually pick up status polling.

Sales is currently a fairly small department, so no filter is needed yet. When the Sales department grows, IT will probably want to limit which ones qualify for management failover.

Important Node Filters

Suppose the hub between the management station and the Sales collection station (actually, all the collection stations in this example) goes down. The management station will log an event that the hub is down, with secondary information that each of the nodes behind the hub is also unreachable. Getting that hub back online is a top priority, and most of the other stations are indeed secondary -- except that credit card authorization server. Access to that server is critical to business and the network operator needs to know about that immediately. By setting up an important node filter, you can assure that this node always qualifies as a primary event in the alarm browser.

RQS nº 03/2005 - CPMI - CORREIOS
FLS Nº 0738
3740
Doc.

```
SalesImptNodes "Critical nodes to have primary alarms if
Sales becomes unreachable" { "IP Hostname" == "ccserv" }
```

Similarly, the network management administrator creates important node filters for the other departments and adds them to the file.

Topology Filters

Looking at performance on the management station, IT realizes that they still see every node in the network -- it's as if they had never bothered with collection stations at all. Every bit of information is getting passed right on up to the management station.

Reviewing the Manufacturing LAN, they realize that it contains over 100 actual nodes, mostly PCs automating fabrication processes. At this point, PCs are not critical to your success, but the production servers from which they run their inventory and instruction data are vital. The collection station operator can monitor the availability of the PCs. All you need to monitor at the management station are the servers.

Use the set construct in the filter file to build your topology filter that only forwards information about the servers to the management station.

```
Sets{
MfgServersSet = { "parts", "prefab", "finalfinish",
"inventory" }
}
```

The previous filter expression for Manufacturing was `MfgLan_TMF "Manufacturing's IP subnet map filter" { MfgLan_DF || NetsNSegs }`. You still only want the Manufacturing domain, and you do want all the networks and segments. Use the set of servers to limit what gets forwarded:

```
MfgLan_TMF "Manufacturing's IP subnet map filter"
      { (MfgLan_DF && MfgServersSet) || NetsNSegs }
```

The collection station in Manufacturing uses `MfgLan_DF` to discover all nodes in its domain. The topology database on the collection station contains all these nodes. When the collection station starts to forward information to the management station, it applies `MfgLan_TMF` to the data stream. Only the servers in the `MfgServersSet` and the networks and segments pass the filter and get sent to the management station. The management station's topology database contains only this information and not the rest of the nodes on the Manufacturing LAN.

The network administrator in IT creates similar topology filters to reduce clutter coming in to the management station from the other collection stations.

Map Filters

The management station serves various operators in the IT department. Connie has received extensive training in troubleshooting connector devices, and specializes in them throughout the network. Sergai only cares about the servers for the various departments. Look at each of their map filters.

The filter expression from which Connie works looks like this:

```
Connectors "All connector devices"
      { Bridges || IPRouters || Hubs }
```

But there is a problem. IT's topology filter from Manufacturing, for example, only passes servers, networks, and segments. They'll have to modify the topology filter to give you the connector information first:

```
MfgLan_TMF "Manufacturing's IP subnet map filter"
      { (MfgLan_DF && MfgServersSet)
        || Connectors || NetsNSegs }
```

Now Connie needs a map filter which includes `NetsNSegs` for her map database to work:

```
Connectors_MF "All connector devices"
      { Bridges || IPRouters || Hubs || NetsNSegs }
```

With this map, Connie will see all the connecting devices from all the LANs.

Using the Network Presenter

With so many PCs on the site, IT hires Paul to keep them all up and running. But Paul's map on the management station has a problem. It says there are no PCs for him to manage. You have specifically filtered out the PCs before they reach the management station.

You could add all the PCs back in for all the topology filters. Paul would have one view with all the PCs and could do combined trend analysis. However, the management station topology database would get bogged down and everyone would have to filter them back out with their map filters.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0739
3740
Doc:

You might think to purchase a separate management station for Paul and set up the collection station topology filters to only send PC information. However, topology filters are defined only once per collection station; a collection station cannot pass different data to different management stations.

As an alternative, Paul can use the Network Presenter through his web browser to act as a console on each of the collection stations. He would have more windows to watch, but network traffic would be minimized. Paul would be able to see the maps, but he would not be able to do any NNM administration through the Network Presenter since it is read-only.

This is an example of the trade-offs your organization will consider during your network management planning phase.

Default Filter File

The following is the default filter file, based on the above grammar:

```
//
// @(#)$OV_CONF/$LANG/filters
// @(#)HP OpenView NNM Pre-Release X.06.20 (Pre-Preview)  Jan 17 2001
// @(#)Copyright (c) 1990-2001 Hewlett-Packard Company
// $Revision: /main/PULSAR/PULSAR_REP/NEPTUNE/4 $  $Date: 2001/01/11 23:58 UTC $
//
// This is the default filter file.  These filters are examples
// which may be useful in your environment.  Feel free to modify this
// file and/or add your own.
// See OVfilterIntro(5) for more information on this file.
//

// Sets are a simple way to list string values to test
// against in a filter.  The "IN" operator tests a field value
// for membership in a set defined here.
//

Sets {

        // These are simple examples of sets.
        //
        // servers "Set of Servers" { "sv1", "sv2", "sv3" }
        // gateways "Backbone gateways " { "gw1", "gw2", "gw3" }
        //
        // sets can include a filename which contains the entries.
        // On Windows, the set file must be on the partition where NNM
        // is installed.

        // routers "Set of Routers" { /openview/conf/routers.set }
}

//
// Filters and FilterExpressions are used as Topology, Discovery,
// Map or Persistence filters.  Applications which use filters
// (like ipmap(1), ovtopmd(1m), ovtopodump(1), and ovtopofix(1m))
// can take the name of a Filter or a FilterExpression.
//

Filters {

        // The following filters are potentially useful as either Discovery
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0740
3740
Doc:

```
// or Topology filters, or components for building Map filters.
//
// NOTES CONCERNING DISCOVERY FILTERS:
// Networks and Segments are not directly testing with Discovery
// filters (and so there is no need to include
// "isNetwork || isSegment" in these filters).
// However, it does not hurt to include networks or segments in
// a discovery filter, so long as you realize that they will not
// be acted on.
//
// Since nodes are only discovered in managed networks, the network
// must already exist and be managed before the filtering test
// will be applied.  New networks connected to discovered nodes will
// be discovered unmanaged.   For discovery filters,
// a node and all its interfaces can be thought of
// as a single object. If any interface or the node itself passes the
// filter, the node and all of its interfaces will pass the filter.
//
// ovtopofix -f follows the discovery filter semantics and only
// applies to locally monitored objects.  However, if a network or
// segment is empty after the processing of the nodes with the -f
// option, that segment or network will also be removed.
//
// ovtopodump(1) also follows the discovery filter semantic, and
// the filter only applies to nodes/interfaces.
//
// NOTES CONCERNING MAP AND TOPOLOGY FILTERS:
// For these filters, all objects are subject to filtering.
// One must specify the networks and segments to be passed.
// Furthermore, objects are displayed/included only if all their
// parent objects (submaps) pass the map/topology filter.  For example,
// if no networks would pass the filter ("isNetwork" is not included),
// then all segments and non-gateways nodes would be filtered out.
// Like Discovery filters, if any interface or
// node passes a Map filter, the node and all of its interfaces
// also pass the filter.
//
// See the FilterExpressions section for map and topology
// filter examples.
//

Networks "Any network" { isNetwork }
Segments "Any segment" { isSegment }
Nodes "Any node" { isNode }
```

```
// The following filters are primarily for example purposes, though
// they might be useful as discovery filters.  They do not generally
// make sense as map or topology filters because they do not specify
// the inclusion of networks and segments.  They also make sense as
// parts of a filter expression.

Routers "Any Router" { isRouter }
IPRouters "Any IP Router" { isIPRouter }
Bridges "Any bridge" { isBridge }
Hubs "Any multi-port repeater" { isHub }
SNMPNode "Any node supporting SNMP" { isNode && isSNMPSupported }

// The next filter is useful for defining map and topology filters
// (see the FilterExpresssions section).  It is not
// particularly useful as a discovery filter
// since all networks and segments automatically pass Discovery
// filters.  Nor is it useful as a standalone
// map filter, since it doesn't pass any nodes.

NetsNSegs "All networks & segments" { isNetwork || isSegment }

// This filter specifies that only objects that support IP should
// be included.  This filter should be used as a topology filter on
// any collection station discovering non-IP information (Level 2
// or IPX only nodes or networks) that is forwarding to a
// NNM 4.X management station.  This will not completely remove
// all non-IP information (e.g. IPX interfaces on a node that also
// supports IP will come through), but will limit the impact on the
// management station, and make migration to NNM 5.X easier.

IPOnlyObjects "Only objects that support IP"
        { isIP || isSegment }

// The following filters are examples that you can customize to
// match your environment.

// LocalLAN "Nodes with interfaces on the 15.2.112-119 subnet"
//      { "IP Address" ~ 15.2.112-119.* }
// NeighborLANs "Node with interfaces on the neighboring LANs on site"
//      { "IP Address" ~ 192.1.2-10.* }
// HPNodes "Hewlett-Packard nodes"
//      { isNode && ( vendor == "Hewlett-Packard" ) }
// NonHPNodes "Non-HP nodes"
//      { isNode && ( vendor != "Hewlett-Packard" ) }

// These are example filters using the sets defined above.
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. 0741
3740
Doc:

```
// GatewaysSet "Any designated Gateway node"
//      { "IP Hostname" in gateways }
// ServersSet "Any designated Server node"
//      { "IP Hostname" in servers }

// The next filter is useful for defining map and topology filters
// (see the FilterExpresssions section).  It is not
// particularly useful as a discovery filter
// since all networks and segments automatically pass Discovery
// filters.  Nor is it useful as a standalone
// map filter, since it doesn't pass any nodes.
//
// The network name below assumes an entry in /etc/networks.
// If no such entry exists, the actual network name will be
// something like "15.2.112".
// MyNet "The network in which I'm interested"
//      { isNetwork && "IP Network Name" == "yellow-lan" }

// This filter would be an example of a way to pass all objects
// contained in the subnet 15.2.112.0 with a subnet mask
// of 255.255.248.0 (so the subnet range is 15.2.112.0 to
// 15.2.119.255).  Note that the inclusion of "isSegment" is
// not a concern, because all segments outside of this network
// would be filtered out because the networks containing them
// were filtered out.  We must have some specification of segments
// if we want the segment contents to be included.

// EngrLan "The 15.2.112 subnet used by engineering"
//      { ("IP Address" ~ 15.2.112-119.* ) || isSegment }

// This filter accomplishes the same thing, but is more restrictive
// in the specification of segments to only include segments in that
// engineering network.  This assumes there is an entry in /etc/networks
// such that the subnet gets the name "engr-LAN", and hence the segments
// in that network all have a name of form "engr-LAN.<something>"
// Generally, the above will accomplish what you want, but this
// may be necessary in some situations if you want specific segments.
// In particular, it works well if you want to use this to EXCLUDE
// the objects in this network.  See the example in the Filter
// expressions below.

// EngrLan2 "The 15.2.112 subnet used by engineering"
//      { ( "IP Address" ~ 15.2.112-119.* ) ||
//        ( "IP Segment Name" ~ "engr-LAN.*" ) }
```

```
        // The following are some sample DHCPFilters.
        // They can be specified by using the Network Polling Configuration
        // dialog application, xnmpolling, on the Status Polling page.

        // DHCPSubnet "Addresses in subnet 15.70.177 are DHCP allocated"
        //      { "IP Address" ~ 15.70.177.* }

        // DHCPNode  "A particular address is DHCP allocated"
        //      { "IP Address" ~ 15.70.177.9 }

        // DHCPRange "IP Addresses from 15.70.177.5 through 15.70.177.10"
        //      { "IP Address" ~ 15.70.177.5-10 }

        //
        // Access to various nodes based on SNMP MIBs that have
        // been discovered as supporting a particular MIB
        //

        CDPnodes "Nodes supporting Cisco Discovery Protocol" { isCDP }
        ATMnodes "Nodes supporting ATM" { ("SNMP ifType" == "ATM")  ||
            ("SNMP ifType" == "atmLogical") ||
            ("SNMP ifType" == "atmDxi") ||
            ("SNMP ifType" == "atmFuni") || ("SNMP ifType" == "atmIma") }
        DS1nodes "Nodes supporting DS1" { "SNMP ifType" == "T-1 Carrier (ds1)" }
        DS3nodes "Nodes supporting DS3" { "SNMP ifType" == "T-3 Carrier (ds3)" }
        SONETnodes "Nodes supporting SONET" { "SNMP ifType" == "SONET" }
        FrameRelayNodes "Nodes supporting Frame-Relay" {
            ("SNMP ifType" == "Frame Relay") ||
            ("SNMP ifType" == "Frame Relay Service") ||
            ("SNMP ifType" == "frameRelayInterconnect") }
        RMON1nodes "Nodes supporting RMON-1" { isRMON }
        RMON2nodes "Nodes supporting RMON-2" { isRMON2 }
        // Short-hand for any RMON device
        RMONnodes "Nodes supporting RMON-1 or RMON-2" { isRMON || isRMON2 }
}

// FilterExpressions are simply combinations of filters defined in the
// same filter file (above).  FilterExpressions make it simple to
// combine filters without reproducing the expressions of each
// filter again

FilterExpressions {

        // One can turn the filters defined above into viable map or
        // topology filters by simply adding "|| NetsNSegs".  (Doing so
        // does not invalidate the filters as discovery
        // filters.  It just adds a superfluous test.)
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0742
3740
Doc:

```
NetInfrastructure "Any network connecting device and what they connect"
        { Routers || Bridges || Hubs || NetsNSegs }
NetBackbone "Networks and gateways/routers"
        { Routers || Networks }

// The following combines the two set filters
// defined above into one FilterExpression.
// It works unmodified as a discovery filter.
// To work as a map filter, network and segment filtering
// must be added (see below).

// VitalNodes "All Gateways and Servers"
//      { GatewaysSet || ServersSet }
// One can turn the filters defined above into viable map or
// topology filters by simply adding "|| NetsNSegs".  (Doing so
// does not invalidate the filters as discovery
// filters.  It just adds a superfluous test.)

// VitalNodesMap "All nets & segs, but only gateway and server nodes"
//      { GatewaysSet || ServersSet || NetsNSegs}
// LocalLANView "All nets & segs, but only local nodes"
//      { LocalLAN || NetsNSegs }

// Using the filters defined above that include only a specific
// network, we can also exclude the specific network like this
// Note the use of the more specific form to exclude only the segments
// in the engineering lan.  This could have been specified directly
// as a negation in the filter part, but this form works well if you
// have several networks to manipulate in this manner.
// EverythingButEngr "Everything but the engineering LAN"
//      { !EngrLan2 }

// Of course the above filter expressions, when used as
// map filters, pass all networks and segments.  You
// may wish to see only a particular network.  The following map
// filters accomplish this.  Note that though segments
// and nodes from other networks will pass the filters, IP Map
// will ignore them because their parent networks will not pass.
// NOTE:  These filters will not work as Discovery
// filters because all network and segments automatically pass
// Discovery and Topology filters.

// MyNetMap "Only the network of interest and all its constituent parts"
//      { MyNet || Segments || Nodes}
// MyVitalNodesMap "Gateways, servers and segments in net of interest"
//      { MyNet || Segments ||  GatewaysSet || ServersSet }
```

```
        // This is a map persistence filter which ensures that
        // all Ungermann-Bass are kept in memory and up to date.
        // Note that this will also keep any containing submaps in memory.

        // PersFilter "Objects to keep in map memory"
        //      { HPNodes }
}
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0743
3740
Doc:

2901

B Using NNM Under a Mixed Codeset Environment

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0744
3740
Doc:

This chapter covers requirements for using NNM's alarm browser, `xnmevents`, in a mixed-codeset environment. These steps are not required if you are using the web interface to alarms, `jalarms`.

Event forwarding in NNM's distribution and scalability model expects that the management station and the collection station share a codeset. That is, if a management station is operating under the ISO8859-1 codeset, then the collection station must share its data using the ISO8859-1 codeset.

This restriction is minimal for English and European language users since ISO8859-1 contains both English (ASCII) characters and most of the European accented characters. Furthermore, NNM is not localized to any of the European languages.

However, this restriction becomes a problem for the Japanese language users that may need to use both Japanese EUC and Shift-JIS codesets. For instance, if a management station is running under Japanese EUC, but one of its collection station is running under Japanese Shift-JIS, the management station's GUI will fail to display the Shift-JIS data obtained from a Shift-JIS collection station. This is because a management station assumes that the data from the collection stations are using the same codeset as itself, and parses and displays all data (including the Shift-JIS data) as Japanese EUC data. This results in a data corruption of all Shift-JIS characters.

Therefore, in this mixed codeset environment, the collection stations must be configured to forward event data to the management station using ASCII only, and furthermore, "user events" must not contain non-ASCII characters. Since ASCII is a subset of all other codesets, data from the collection station will not be corrupted by the management stations' GUI.

SNMP traps do not support non-ASCII characters, but NNM does not prevent you from forwarding events that contain non-ASCII characters. Do not generate user-sendable events containing non-ASCII characters, if these events are forwarded from a collection station to a management station. For example, do not send events, such as the "`OV_Popup_Message`" or "`OV_Message`," with non-ASCII characters, using the `snmptrap` command from a collection station to a management station.

When configuring a collection station to operate under a mixed-codeset environment (Japanese system users should see Table B-1, Mixed Codeset Environment for Japanese Systems,), the following steps should be taken:

1. Create a new file called `$OV_CONF/ovlang.conf` (for example, `C:install_dir\conf\ovlang.conf`) that contains the following two entries, each on a separate line:

   ```
   ovtopmd
   netmon
   ```

   If you need to forward threshold events, add `snmpCollect` to `ovlang.conf`.

2. Restart the `ovw` processes by executing the following commands:

   ```
   ovstop
   ovstart
   ```

NOTE There is no need to remove or clear the `ovtrapd.log` file of a management station, but if it contains data from this collection station prior to this step, that data may be corrupted.

The first two steps will force the collection station to generate data forwarded to the management station with English/ASCII characters only. However, data that is not forwarded to a management station will continue to operate using the codeset specified by you or by the environment.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0745
3740
Doc:

Table B-1 Mixed Codeset Environment for Japanese Systems

Collection Station's System/Codeset	Management Station's System / Codeset			
	Windows / SJIS	HP-UX/SJIS	HP-UX/EUC	Solaris/EUC
Windows/SJIS	(1)	(1)	(2)	(2)
HP-UX/SJIS	(1)	(1)	(2)	(2)
HP-UX/EUC	(2)	(2)	(1)	(1)
Solaris/EUC	(2)	(2)	(1)	(1)

(1) -- this is not a mixed codeset environment; no configuration necessary.

(2) -- this a mixed codeset environment; configure the collection station to forward ASCII data to the management station.

Glossary

A

agent In the network management model, the agent is the component that "instruments" or provides management information about a particular network device, such as a file server, to a network management system. *See also: proxy agent.*

C

client A computer system, on a network, that accesses a service from another computer (server). A client may run any arbitrary operating system.

client/server A concept that functionally divides the execution of a unit of work between activities initiated by an end user or program (client) and resource responses (server) to the activity request.

collection domain The set of nodes and other objects for which trend data collection and threshold checking is occurring on a collection station. Frequently the discovery domain and the collection domain include the same set of nodes and objects. Discussions in this document assume that is the case, and use this term to refer to both. *See also: management domain, discovery domain.*

collection station A management station that acts as a collection point for information being gathered on managed elements. *See also: management stotion.*

correlated events Multiple events analyzed by NNM and presented under a single event in the browser.

D

discovery domain The set of nodes and other objects actively being discovered and monitored by an NNM station.

discovery filter Specifies which devices an NNM station is actively discovering and monitoring. *See also: filtering.*

F

failover Configuring a management station to pick up status polling duties for a collection station that goes into critical status.

failover filter List of specific nodes the management station should poll, leaving the status of the rest as they were when the collection station went critical.

filtering Refers to the process of limiting the object the user is interested in having discovered, monitored, displayed, etc., by determining certain attributes that are of interest to the user. Filtering generally is used to limit processing to a subset of information already available, to reduce the cognitive load on the user, align presentation with the users needs, and generally reduce system load by filtering the amount of data handled as soon as possible. *See also: discovery filter, failover filter, map filter, persistence filter, and topology filter.*

I

IP address The Internet Protocol address is a network level address assigned to each system is a TCP/IP network. It is 4 bytes long. An example IP address is 192.215.15.46.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0746
3740
Doc:

M

management application Software that obtains and presents information from agents, or proxy agents. The information is usually presented in a graphical user interface.

management console An instance of the user interface from which you can control applications that do network and system management. The console may be on the system that contains the management software or it may be on another system in the management domain.

management domain The set of all nodes and other objects in the network that are of interest to the user.

management station The computer system used in the management of other objects in the network, system, and software environment. Management stations run network or system management services, daemons, processes, and/or management user interfaces. Management clients, management servers, management consoles, and stand-alone management systems are all examples of management stations. *See also: collection station.*

map A set of related objects, symbols, and submaps that provides a graphical and hierarchical presentation of your network and its systems. Because a map is defined by the collections of submaps it comprises, you never view a map directly, but rather one or more of its submaps. Maps are derived from the HP OpenView Windows object database, and multiple maps can be created from the same object database. *See also: submap.*

map filter Defines what objects in the HP OpenView Windows object database will be permitted on the map. Objects that are rejected by a map filter remain in the management station's topology database, and are still subject to status polling. Map filtering occurs on a per-map basis, not a per-display basis. *See also: filtering.*

N

node A termination point for two or more communication links - or more simply, a device on a network. The node can serve as the control location for forwarding data among the elements of a network, as well as perform other networking, and in some cases local processing functions.

O

object A computer system, interface card, printer, or any other device or object that appears in the network.

P

persistence filter Specifies one or more objects which are required to be in memory at all times, and therefore are not permitted to be on a transient submap. *See also: filtering, persistent submap, persistent object.*

persistent object An object which has passed a persistence filter, and is therefore in memory whenever the map on which it resides is open. Any submap that contains a persistent object is automatically a persistent submap. *See also: persistent submap, persistence filter.*

persistent submap A submap that is always in memory, either because it is above the configured persistence level, because it

contains a persistent object, or because it is the child of a persistent object. *See also: transient submap.*

primary collection station When applied to a particular object, this refers to the collection station which has been chosen as having primary responsibility for monitoring the object. In particular, it is used to determine the status and other attributes of the object. A given object may be reported and monitored by multiple collection stations, but only one station will be the primary station. *See also: secondary collection station.*

proxy agent A proxy agent performs information preparation and exchange on behalf of a device it is representing. For example, an agent is a proxy if it is located on the file server but is representing a client. *See also: agent.*

R

root submap A standard, top-level submap for every map.

router A router uses a packet's destination address to determine which network or network segment is its destination.

S

server A computer system that provides services to other computer systems on the network. A server could be a file server and provide data storage, application, routing, and print services.

secondary collection station When applied to a particular object, refers to a collection station that is known to be monitoring the object, but which has not been chosen as the primary collection station.

site A group of nodes connected completely by a Local Area Network (LAN), i.e. all at the same geographic location.

SNMP Simple Network Management Protocol. A protocol running above TCP/IP used to exchange network management information. SNMPv2C has extended functionality over the original protocol.

station *See: workstation, collection station, or management station.*

submap A particular view of the network environment, consisting of related symbols that are displayed in a single window. Multiple submaps can be displayed simultaneously. Submaps are typically (though not necessarily) organized in a hierarchy, with the root submap at the top of the hierarchy. *See also: map.*

T

TCP/IP Transmission Control Protocol/Internet Protocol. A set of protocols for Layers 3 and 4 of the seven-layered Open Systems Interconnect network model

topology filter A topology filter at a collection station defines the subset of local topology data that management stations can see. *See also: filtering.*

transient submap A submap that is not necessarily in memory at all times, but which is available "on-demand" when the operator opens it. Any submap that can be recreated at any time based wholly on topological information is potentially a

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0747
3740
Doc:

transient submap, depending on how and whether the on- demand submap feature is enabled. *See also: persistent submap.*

W

workstation A computer or terminal that is connected to the network.

Index

Symbols

%REMOTE_MANAGERS_LIST%, 57, 97, 140, 155

A

applications
  backward compatibility, 68
  integrating, 26, 68, 125
attribute value assertion
  See AVAs
automated managed-state, 18, 74
AVAs, 172
  boolean, 174
  enumerated, 175
  enumerated field values, 186
  evaluating, 172, 174
  filterable fields, 181
  integer, 175
  operators, 173
  regular expressions, 176
  special pattern matching, 177
  string, 175
  whitespace in field name, 172

B

backup, 18, 88
backward compatibility
  applications, 68
benefits of scalability, 15

C

capacity, 21
  centralized-hierarchical model, 97
  collection stations, 86
  devices, 34, 84
  management console, 34
  remote monitoring, 85
centralized model, 92
  discovery filters, 93
  management consoles, 93
  map filters, 93
  on-demand submaps, 93
  web GUI, 93
centralized-hierarchical model, 95
  capacity, 97
  discovery filters, 96
  failover, 96
  management consoles, 96
  map filters, 96
  on-demand submaps, 96
  web GUI, 96
codeset,mixed, 206
collection domain, 46
  overlapping, 52
collection station, 33
  changing primary station for an object, 151
  checking status, 145, 146
  configuration overview, 57
  configuring, 133
  configuring remote communication, 141
  connections, 36
  determining if a node is, 137
  determining primary, 150
  failover, 51
  how many to have, 86
  identifying with Station view, 23
  in DIDM, 21
  introduction, 22
  listing monitored objects, 138
  managing, 138
  new primary, 55
  preferred, 54
  primary vs. secondary, 53
  removing from management station, 141
  security configuration, 133
  serving multiple management stations, 36
  synchronization, 144
  topology filter, 41
  troubleshooting, 147
  unmanaging, 140
configuration
  remote, 56
configuration files
  filter, 169
  nfsconf, 113
  ov.conf, 50, 139
  ovwdb.auth, 119
  pcnfsd.conf, 113
  snmpd.conf, 133
  trapd.conf, 27, 60
configurationfiles
  ovtopmd.lrf, 135
configuring
  collection station, 133
  collection station security, 133
  demand level, 121
  discovery filter, 128

RQS nº 03/2005 - CN
CPMI - CORREIOS
0748
Fls. Nº
3740
Doc:

Index

event forwarding, 154
failover, 150, 153
failover filter, 153
filters, 127
management console, 109
management stations, 137
on-demand submaps, 121
overlapping domains, 150
persistence filter, 124
topology filter, 134
UNIX console client, 117
UNIX console server, 112
Windows NT console for UNIX server, 115
Windows NT console server, 111
connections between components, 36
connector down, 60
forwarding, 62
important node filter, 193
console
See management console
cooperative independent model, 103
discovery filters, 104
management consoles, 104
map filters, 104
on-demand submaps, 104
threshold events, 104
topology filters, 104
web GUI, 104
correlated events, 60
forwarding, 60
custom views, 72

D

data collection
threshold, 28
trend data, 28, 159
databases, 159
SQL, 28
data-stream filters, 37
demand level
changing, 122
configuring, 121
devices
limit per station, 34
DHCP, 39, 192, 197
discovery filtering, 40
applying to previously discovered objects, 129
centralized-hierarchical model, 96
configuration, 128
cooperative independent model, 104
example, 190
fully centralized model, 93
hierarchical model, 100
distributed internet discovery and monitoring
architecture, 48
configuring, 133, 137, 150
internals, 46
introduction, 20
distribution, 19, 20, 33
architecture, 49
benefits, 15
DIDM configuration overview, 56
distributed internet discovery and monitoring, 16, 20
models, 89
network connections, 36
overview, 15
processes, 48
risks of, 86
the GUI, 109
threshold monitoring, 18

E

ECS, 60
EMANATE, 134
events, 27, 57, 59
configuring forwarding, 154
correlated, 60
forwarding, 18, 42, 62, 63
map filtering, 43

F

failover, 18, 51, 86
centralized-hierarchical model, 96
configuring, 153
disabling, 153
filter,configuration, 52, 153
hierarchical model, 101
failover filter
configuration, 153
failover filter configuration, 52
fault tolerance, 18
fields,filterable, 181
filter expression, 170
filtering, 48, 72
and scalability, 17
configuration, 127, 128

discovery, 40, 128
example, 189
filter definition file, 43, 44, 197
important nodes, 193
introduction to, 19
map, 42, 48, 127
overview, 37
performance, 17, 19
persistence, 26, 68
topology, 41, 50, 134
utilities, 45
filters, 169
attribute value assertion See AVAs
boolean expressions, 174
default file, 197
enumerated expressions, 175
enumerated field values, 186
example, 189
excluding a node, 180, 192
failover,configuring, 153
filterable fields, 181
formal grammar, 187
integer expressions, 175
language definition, 169
pattern matching, 177
regular expressions, 176
relationship between nodes and interfaces, 180
sets, 171
string expressions, 175
testing, 45
types of, 37, 38
find, 67
forwarding, 18
events, 59, 154
threshold events, 62

H

hierarchical model, 98
discovery filters, 100
failover, 101
management consoles, 100
map filters, 100
multiple levels, 99
on-demand submaps, 100
performance, 102
threshold events, 101
topology filters, 100
web GUI, 100
high availability, 18

I

inform request, 59
integrating applications
on-demand submaps, 125
interface
automatic managed-state, 18, 74
Internet level, 122
IP discovery and monitoring, 16
ipmap, 48, 61, 64, 68

L

LAN, 36
languages,international, 206
large maps, viewing, 17, 29, 87
list
of remote managers, 57
localization, 206

M

managed interfaces
automated, 18, 74
management console, 17, 20, 24, 33, 70, 73
capacity, 110
centralized-hierarchical model, 96
choosing mount point, 118
configuration overview, 110
cooperative independent model, 104
fully centralized model, 93
hierarchical model, 100
introduction, 24
modifying ovwdb.auth file, 119
platform, 110
prerequisites for, 109
read-only vs. read-write maps, 72
security, 119
supported configurations, 109
undoing, 120
UNIX client, 117
UNIX server, 112
Windows NT console for UNIX, 115
Windows NT server, 111
management domain, 46
management station, 22, 33
changing overlap mode, 152
changing primary collection station, 151
configuring, 137
remote communication, 141

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0749
3740
Doc:

configuring collection stations to manage, 138
connections, 36
identifying with Station view, 23
overlapping domains, 55
removing collection station, 141
synchronization, 144
troubleshooting, 147
unmanaging a collection station, 140
managing
locally monitored objects, 132
map filtering, 42
centralized-hierarchical model, 96
configuration, 127
cooperative independent model, 104
events, 43
example, 191, 195
fully centralized model, 93
hierarchical model, 100
recalculating for a map, 43, 68
maps, 72
Microsoft Terminal Server, 75
mixed codeset, 206
model, 33
centralized-heirarchical, 95
cooperative independent, 103
fully centralized, 92
hierarchical, 98
multi-level hierarchical, 99
monitoring domain, 46

N

Neighbor view, 163, 164
netmon, 40, 48, 49, 50, 51, 56, 58, 61, 99
limits, 84
network level, 122
Network Presenter, 25
See also web GUI, 17
NFS, 70, 109
diskless, and management consoles, 70
nmdemandpoll, 144
NNM 250
limitations, 34
multiple licenses to increase node limit, 87
nodes, excluding via filtering, 180

O

on-demand submaps, 26, 64
and find, 67
and submap list dialog, 67
centralized-hierarchical model, 96
changing demand level, 122
changing persistence filter, 125
configuring, 121
cooperative independent model, 104
disabling, 67, 122
fully centralized model, 93
hierarchical model, 100
inital configuration, 64
integrating applications, 125
ipmap and ovw, 64
performance, 17
persistence filters in, 26, 68
recalculating persistence of submaps, 69
sharing, 72
terms, 64
operators, 42
ovaddobj, 135
ovcoltosql, 28, 160
overlap mode, 152
overlapping collection domains, 52, 53, 55, 86
configuring, 152
ovfilter utilities, 45
ovrepld, 48, 50, 58, 62
ovstart, 49
ovtopmd, 48, 49, 50, 61, 135
ovtopmd.lrf, 135
ovtopodump, 138, 150
ovtopofix, 40, 129
ovtrapd, 59, 61
ovwdb, 70
ovwdb.auth file, 119
ovwrs, 51
ovwsetupclient command, 120

P

packet loss rate, 141
panner, 17, 29
partitioned internet submap, 87
Path view, 163, 165
performance, 16, 21, 97
hierarchical model, 102
memory, 26
persistence filtering, 26, 68, 69
changing, 125
configuring, 124
persistent submaps, 64
pmd, 59, 61
primary collection station, 53, 150
changing, 151

preferred, 54, 152
with failover, 55
processes, distribution for IP discovery and monitoring, 48

Q

quick navigator, 17, 30

R

remote communication
configuring, 141
remote configuration, 56
remote managers list, 57, 97, 155
replication of topology, 50
resident submaps, 64
retry count, 141

S

scalability, 15
benefits, 15
general considerations, 84
strategies for deployment, 87, 89
secondary collection station, 53
security
collection station configuration, 133
management console, 119
segment level, 122
Service Guard, 18, 50, 86, 93, 96, 100, 104, 119, 139
set-defining filters, 37
sets, 171
snmpd.conf, 133
SNMPv2C
inform request, 59
SQL databases, 28
Station view, 145, 146
collection station
checking status, 146
submap list dialog, effect of on-demand, 67
submaps
partitioned, 87
synchronization, 144

T

Terminal Server, 75
threshold events
cooperative independent model, 104
forwarding, 62, 154
hierarchical model, 101
monitoring, 27
remote, and remote actions, 63
threshold monitoring, 18, 28
timeout value, 141
topology filtering, 41, 50
changing, 135
configuration, 134
cooperative independent model, 104
events, 42, 63
example, 191, 194
hierarchical model, 100
removing, 136
topology replicator, 50
transient submaps, 64
trapd.conf, 59
traps, 59
troubleshooting
communication between management station and collection station, 147

U

UDP, 59
undoing
management console, 120
on-demand submaps, 122
UNIX, 117
unmanage
automated, 18, 74
unmanaging
collection station, 140
objects, 132
use models, 89
centralized-hierarchical, 95
cooperative independent, 103
fully centralized, 92
hierarchical, 98

V

view
Neighbor, 163, 164
Path, 163, 165
Station, 145, 146
views
custom, 42, 72

W

WAN, 15, 36
and remote monitoring, 85, 94, 97
configuring, 141
web GUI, 17, 25

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: Nº 0750
3740
Doc:

Index

centralized-hierarchical model, 96
cooperative independent model, 104
fully centralized model, 93
hierarchical model, 100
web server, 25
wide area network
See WAN

X

xnmsnmpconf, 58
xnmtopoconf, 49, 52, 53, 54, 56, 57, 58, 132, 137, 140, 141, 147, 152
xnmtrap, 60
X-terminals, 33, 34
and management consoles, 73

E-TAILOR ENTERPRISE

2086

CORREIOS

Anexos – Caderno 2

Pregão nº 118/2003 – CPL/AC

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls.: Nº 0751
3740 Doc.

HP OpenView Network Node Manager

Managing Your Network with HP OpenView Network Node Manager

Version: 6.4



Manufacturing Part Number : J5323-90000

January, 2003

© Copyright 2003 Hewlett-Packard Company.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0752
3740
Doc:

Legal Notices

Warranty.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices.

No part of this document may be copied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

©Copyright 1983-2003 Hewlett-Packard Company, all rights reserved.

Contains software from AirMedia, Inc.

© Copyright 1996 AirMedia, Inc.

Trademark Notices.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

Windows NT® is a U.S. registered trademark of Microsoft Corporation.

Windows® 2000 is a U.S. registered trademark of Microsoft Corporation.

Windows® and MS Windows® are U.S. registered trademarks of Microsoft Corporation.

Netscape™ and Netscape Navigator™ are U.S. trademarks of Netscape Communications Corporation.

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

Oracle7™ is a trademark of Oracle Corporation, Redwood City, California.

OSF/Motif® and Open Software Foundation® are trademarks of Open Software Foundation in the U.S. and other countries.

Pentium® is a U.S. registered trademark of Intel Corporation.

UNIX® is a registered trademark of The Open Group.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0753
Doc: 3740

1. Network Management with NNM

The Network Management Challenge 39
How Network Node Manager Can Help 39
Moving to Proactive Network Management 40
Poll for Network Information 40
Watch for Events 41
Network Management Functions 42
Fault/Problem Management 43
Performance Management 45
Configuration and Change Management 46
Additional HP OpenView Product Information 47

2. How Does NNM Work?

Collecting Critical Information 51
SNMP's Network Management Model 51
Desktop Management Interface (DMI) 54
Automatic Discovery and Layout 56
How IP Discovery and Layout Work 56
How IPX Discovery and Layout Work 57
Interactions Between IPX Discovery and IP Discovery 58
Level 2 Discovery 59
Event Reduction Capabilities 61
NNM's Databases 62
Operational Databases 62
Data Warehouse 63

3. Resources Available While Learning NNM

Resources Included with NNM 67
NNM Online Help System 67
Tip of the Day 69
Manuals: Printed and Online 69
Release Notes 71
Reference Pages (Manpages) 71
The contrib Directory 74
The support Directory 74
White Papers 75

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0754
3740
Doc:

Resources and Services Available Through HP 76
HP Web Sites 76
HP Consulting Service 76
HP Education 77
HP Product Support 77
OpenView Forum 77
Summary of HP OpenView Web Sites 78

4. Planning Your NNM Configuration

Budgeting Time for Planning and Configuration 81
Time for Planning 81
Time for Configuration 81
Taking Over NNM from Someone Else 82
Understanding the Network Information Needs of Your Organization 83
Who Needs What Information? 83
Work Sheet for Planning 85
Knowing Your Network 87
Deciding to Manage or Not to Manage Devices 87
Starting with a Well-Configured Network 90
Consistent IP Addressing Scheme 90
Consistent Name Resolution Scheme 91
SNMP Agents and Their MIBs Configured 93
DMI Service Providers and Their MIFs Configured 94

5. Initial Network Discovery: Options and Troubleshooting

Install Network Node Manager (if you have not already done so) 100
Installing IPX Transport Software (Windows only) 100
Establishing Universal Pathnames (UNIX only) 100
Discover the Network... Let NNM Do It 103
Overview 103
Start the NNM Services (background processes) 105
Make Sure NNM's Services Are Successfully Running 106
Open NNM 106
Configure an Inventory Report 107
Let NNM Run Over Night to Populate the Maps 107
Verify the Accuracy of the Initial Discovery 109

Printing the Inventory Report 110
Viewing the Properties of Your Network Configuration 111
Finding Specific Devices on the Map 113
Interactively Expand/Limit Your Management Domain 117
Adding Networks to Your Management Domain 117
Managing an Unmanaged Network Device 118
Unmanaging a Managed Network Device 118
Automatically Expand Your Management Domain 119
Create a Seed File Specifying Multiple IP Networks to Manage 120
Use loadhosts 122
Expand the IPX Hop Count (Windows only) 123
Automatically Limit Your Management Domain 124
Create a netmon.noDiscover File to Exclude Devices 125
Use loadhosts 127
Create a Discovery Filter Identifying Which Devices to Include 128
Modify the oid_to_type File to Unmanage Devices by Type 129
Limit the IPX Hop Count (Windows only) 130
Troubleshooting Discovery 131
IP Discovery and Layout 131
General IP Suggestions 144
IPX Discovery and Layout (Windows only) 153
Stop Everything and Start Discovery Over Again 161

6. Preserve Your Sanity: Backup and Polling Configuration

Backup/Restore to Protect Your Investment of Time 165
How Does the Backup Work? 166
Backing Up and Archiving All Critical Files 167
Restoring All of NNM (procedures/options) 171
Restoring Part of NNM (procedures/options) 173
Troubleshooting Information 174
Custom Scripts 176
Controlling the Amount of Traffic Generated by NNM 178
Status Polling 181
Configuration-Check Polling 183
Connector Topology Polling 184
New Node Discovery Polling (IP, Level-2, and IPX) 184

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0755
3740
Doc:

Controlling Level-2 Device Discovery and Layout 185
Secondary Failure Polling 192
Fine-Tuning the Polling Services 193
Watching NNM's Polling Queue 194
Running NNM Without Network Polling 195

7. Map Making Fundamentals

Maps versus Submaps 199
Maps 199
Submaps 200
Understanding Objects versus Symbols 203
Objects 204
Symbols 207

8. Map Customization

Putting It All Together 212
Which Maps for Which Users 212
Copying the Default Map 215
Your Map Strategy 215
Controlling the Display of Devices Attached to Switches or Bridges 217
Turning On Star Configuration for Attached Devices 218
Turning Off Star Configuration for Attached Devices 219
Giving Your Network Symbols Meaningful Names 221
Turning Connection Labels on or off 223
Configuring Trunking and Meshing 225
Establishing Submap Persistence Settings 229
By Logical-level of Your Network's Structure 230
By Presence of Specific Devices 230
Controlling Which Devices Appear on the Map 232
Creating a Map Filter 232
Using the Hide Feature 233
Changing/Adding Object Attribute Fields 235
Changing the Value in an Attribute Field 236
Changing Symbol Type to Switch Attribute Sets 237
Adding Attribute Fields in the Object Database 238
Making the Maps Look Like Your World 240

Controlling the Placement of the Symbols on Your Map 241
Adding Your Own Submaps 244
Customizing the Internet Level of Your Network Map 247
Customizing Network-, Segment-, or Node-Level Submaps 256
Background Graphics 260
Creating Your Own Map Symbols 263
What Is a Symbol 263
Specifying the Placement and Size of the Submap Windows 266
Window Geometry 266
Submap Overlay 266
Miscellaneous Configuration Changes 268
Windows Operating System 268
UNIX Operating Systems 269
Controlling Symbol Status 270
Object Status Colors 270
Compound Status 274
Creating New NNM Features to Meet Your Team's Needs 278
Adding to NNM's Menu Structure 278
Creating Executable Symbols with Custom Behaviors 279

9. Controlling Map Access

Establishing and Communicating a Process for Requesting Changes to the Map . . 286
Not Allowing Team Members to Make Changes 286
Allowing Team Members to Make Changes 286
Setting User Preferences Within NNM 287
Using Command Line Startup Options 289
Options 289
Examples 290
Using Operating-System Level File Permissions for the Map 292
Windows: Setting Permissions 293
UNIX: Setting Permissions 294
Using the Context Feature to Control Menu Choices 296
Using NNM's Predefined Contexts 296
Creating Your Own Contexts 297
Using ARF Files to Control Menu Choices 299
ARF File Modifications Example 305

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0756
Doc:

Allowing Others to View NNM from Many Computers 317
Remote Consoles 317
NNM's Web Interface 318
Microsoft Terminal Services 318
Closing All Current Sessions 319

10. Keeping Up with Events on Your Network: Beyond the Maps

How NNM's Event System Works 323
SNMPv1 Traps / SNMPv2c Traps and Informs 325
DMI Events (Indications) 327
Alarm Browser Overview 329
Displaying Alarms 330
Alarm Categories/Alarm Browser Windows 331
Acknowledging Alarms 334
Filtering Alarms 335
Deleting Alarms 337
NNM's Map and the Alarm Browser 338
Specifying Additional Actions on Alarms 339
Launching Specific Views or URLs from Alarms 340
Configuring the Alarm Browser 342
Controlling the Size of the Event Database 343
Controlling the Size of the Alarm Browser's State File 344
Controlling How Many Alarms to Delete Automatically 345
Copy or Restore the Alarm Browser's State File 347
Controlling How the Alarm Browser Looks 347
Assigning Alarm Categories 348

11. Event Reduction Capabilities: Getting to the Root Cause

NNM's Event Reduction Capabilities 352
Correlation Concepts 354
De-Duplication of Alarms 358
ECS Correlations 360
NNM's Built-In Correlations 360
Command Line Control 380
Correlation File Structure 381
Troubleshooting 381

Obtaining Additional Event Correlations 382
Correlation Composer Correlators 386
NNM's Built-In Correlators 386
Correlator Fact Store File 397
Troubleshooting 397
Creating Additional Correlators 398
What is an SNMP Variable-Binding and How Do I Identify One? 404
Look within the MIB File 404
Check the Alarm Message Text in the Alarm Browser 405
Special SNMP Variable-Bindings within NNM Interface and Node Status Alarms 405

12. Customizing Events: Doing It Your Way

SNMP MIB Browser 412
Loading MIBs in the MIB Database 413
Prerequisites 414
Procedure Tips 415
DMI Browser 417
Creating DMI Queries 417
Loading DMI-to-SNMP Event Mappings 419
If a MIB Translation of the MIF File Is Available 420
If No MIB Translation of the MIF File Is Available 420
Event Configuration Overview 422
Prerequisites 422
Event Configuration Window 423
Controlling Alarm Message Posting and Text 431
Defining Automatic Actions for Events 433
Variables and Special Characters Allowed 436
Defining Additional Actions 441
Using the MIB Application Builder 443
Prerequisites 444
Procedure Tips 445
Data Collection & Thresholds 447
Prerequisites 447
Procedure Tips 449
Defining Thresholds for Monitored MIB Objects 453
Collecting and Storing Textual Data 460

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0757
3740
Doc:

Creating and Using MIB Expressions 460
Unique Properties of the SNMP MIB Object sysObjectID 465

13. Using Event Data

Graphing SNMP Data 471
. 471
Graphing Historical and Real-Time Data in the Same Graph 473
Grapher Operations 474
Printing a Graph 475
Data Warehouse 476
Data in the Data Warehouse 478
Reporting 478

14. NNM on the Web

Overview 484
Setting Up the HP OpenView Web 485
Role Configuration Files for the HP OpenView Web 486
The HP OpenView Launcher 492
Launcher User Interface 492
Configuring the Launcher 494
HP OpenView Network Presenter 501
Starting the Network Presenter 501
The Network Presenter Window 502
Network Presenter versus NNM on a Management Station 503
Configuring the Network Presenter 505
Using Symbol Registration Files and Bitmaps 506
Listing Multiple Maps in the Launcher 508
SNMP Data Presenter 509
Configuring the SNMP Data Presenter 511
Alarm Browser 512
Using and Configuring the Alarm Browser 513
Event Reduction 515
Reporting Interface 516
Additional Views 518
Neighbor View 518
Path View 519

Node View 520
CDP View 521
Station View 522
Internet View 522
Port-Address Mapping 522

15. Maintaining NNM
Daily Tasks 527
Check Running Services 527
Check Disk Space 527
Trim Files 528
Weekly Tasks 531
Back Up NNM 531
Check Polling Performance 531
Check Web Launcher Log Files 532
Monthly Maintenance Tasks 533
Check Patch Releases 533
Check License Requirements 533
Yearly Maintenance Tasks 534
Evaluate Latest Release 534
Other Maintenance Tasks 535
Enabling/Disabling Automatic Startup 535
Customizing the Startup Configuration 535

A. NNM Services and Files
Services and Files 541
Background Services 541
Foreground Services 543
Web CGI Programs 545
Behavior of the Services and Files 547

B. Network Troubleshooting Tools
Tools in NNM on a Management Station 555
Map Snapshots 555
Performance Tools 556
Configuration 562

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0758
3740
Doc:

Fault Resolution Tools 566
Miscellaneous Tools 569
Tools in NNM's Web Applications 575
HP OpenView Launcher 575

C. Troubleshooting NNM Itself

General Troubleshooting Considerations 579
When You Need More Information 579
Preventive Practices 579
Characterizing the Problem 582
Distinguish Local versus Remote Problems 582
Remote Nodes' Level of Manageability 582
Context: What Changed? 583
Duration: How Long or How Often? 583
Context: What Action Was Performed? 583
Troubleshooting Background Services 584
The httpd Background Service 586
The netmon Background Service 587
The ovactiond Background Service 590
The ovalarmsrv Background Service 590
The ovcapsd Background Service 591
The ovspmd Background Service 592
The ovrepld Background Service 594
The ovtopmd Background Service 594
The ovtrapd Background Service 599
The ovuispmd Background Service 600
The ovwdb Background Service 602
The pmd Background Service 604
The ovrequestd Background Service 607
Troubleshooting Data Collector Problems 608
Set-community Name and Trap-dest Loss Upon Re-Installation 612
Troubleshooting Web Components 613
Language Selection Problems 614
HP OpenView Launcher 615
Network Presenter 618
Alarm Browser 619

SNMP Data Presenter 620
Troubleshooting NNM Operations 623
Runtime Components 623
Network Management Operations 626
Browsing an Internet MIB 628
Building and Executing MIB Applications 628
Configuring Events 631
Event Reduction Capabilities 632
Loading Internet MIBs 633
X Windows Components (UNIX operating systems only) 635
Online Help 636
Troubleshooting Windows Applications 637
Problems Launching Applications 637
Windows Operating System Tools 637
Recommended Logging and Tracing Practices 639
Logging and Tracing 639
Web Launcher Error Log 653
Improving Traffic Management and Performance 654
Traffic Management 654
Performance 656

D. Changing All the Symbols for a Particular Device

Procedure 662
Example 663
Create a Symbol Registration File 664
Copy and Modify the Symbol Graphics 664
Map a sysObjectID to the New Symbol 666
Define the Capabilities for Computer_workstation_700 667
Inform NNM about the New Fields 668
Provide Additional Information in the oid_to_type File 669
Update the Database 670
Verify Symbol Changes 671
Back Up Your Efforts 673

E. Changing an Object's Vendor and SNMP Agent

How NNM Discovers Vendor and SNMP Agent Values 676

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0759
3740
Doc:

When the Vendor and SNMP Agent Would Not Be Set 677
Procedure 678
Example 679

Index 685

Support

Please visit the HP OpenView web site at:

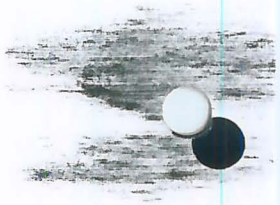
`http://openview.hp.com/`

There you will find contact information and details about the products, services, and support that HP OpenView offers.

The support area of the HP OpenView web site includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0760
3740
Doc:



What Do I Need to Know?

This chapter presents an overview of network management concepts, platforms, and technologies, and discusses how they work together. This information is intended to provide a reminder of the kind of information you need to know in order to be successful with Network Node Manager.

This chapter does not attempt to provide full details about these topics. If you need more information, check the references provided at the end of the chapter.

The following topics are covered in this chapter:

- Networking concepts, including an overview of the OSI model and network management protocols (page 20).
- Network hardware, the management protocols it uses, and how it fits into the OSI model (page 25).
- How management information is exchanged between devices, including a discussion of MIBs and MIFs (page 27).
- General operating system knowledge that you should have, including a discussion of cross-platform issues (page 31).
- References to other sources of information (page 33).

The use of the term Windows or Windows operating system in this manual refers to NNM supported Microsoft® Windows® operating systems. For a list of supported Windows operating systems, see the *Release Notes for HP OpenView Network Node Manager*.

The use of the term UNIX or UNIX operating system in this manual refers to NNM supported UNIX® operating systems. For a list of supported UNIX operating systems, see the *Release Notes for HP OpenView Network Node Manager*.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0761
Doc 3740

Understanding Networking Concepts

To use HP OpenView Network Node Manager (NNM) successfully, you need to have a good understanding of networking concepts, hardware, protocols, and architecture.

In addition to general networking knowledge, you also need to be familiar with your specific network — the operating system platforms on your network, how the network is currently configured, what protocols are being used, and what kind of devices are on your network.

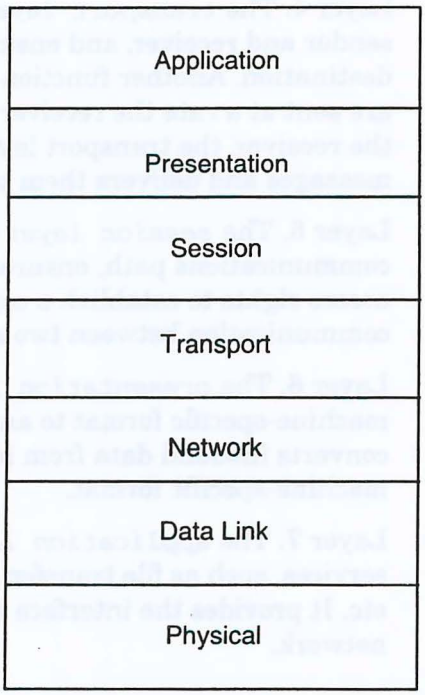
The OSI Reference Model

The need to provide communications among the devices supplied by different vendors gave rise to the Open Systems Interconnect (OSI) reference model. Because the unique network architectures and proprietary protocols developed by numerous vendors are frequently incompatible, the OSI model was developed by the International Standards Organization to resolve the compatibility issues and allow hardware from different vendors to communicate. The layer concept on which the OSI model is based establishes a set of rules for data transmission on a variety of levels.

The OSI model is important to review, because the various protocols operate at different layers, as do various hardware devices.

Figure 1 shows the layers of the OSI model.

Figure 1 **Layers in the OSI Model**



In a layered scheme, messages originate from the top layer (Layer 7) of a transmitting computer, move down to the lowest layer (Layer 1) and travel across the network media to the receiving computer. The message arrives at the lowest layer (Layer 1) of the receiving computer and moves up through its various layers to Layer 7.

Each of the layers is described below.

- Layer 1. The *physical layer* establishes the actual physical connection between the computer equipment and the network, and provides the transmission of bits from one system to another.
- Layer 2. The *data link layer* provides the transmission of packets, and performs error detection and correction functions to ensure that a packet contains the same information received as sent.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0762
3740
Doc:

- Layer 3. The *network layer* determines the path that will be taken through the network. The network layer also controls the rate at which the network accepts packets, to avoid and recover from congestion.
- Layer 4. The *transport layer* provides for the flow of data between sender and receiver, and ensures that the data arrives at the correct destination. Another function of this layer is to ensure that packets are sent at a rate the receiver and the application can cope with. At the receiver, the transport layer reassembles the packets into messages and delivers them to the next highest layer.
- Layer 5. The *session layer* allows the setup and termination of a communications path, ensures that the sender is authentic and has access rights to establish a connection, and synchronizes the communication between two systems.
- Layer 6. The *presentation layer* converts outbound data from a machine-specific format to an international standard format. It converts inbound data from international format to a machine-specific format.
- Layer 7. The *application layer* provides the software for network services, such as file transfer, remote login, remote execution, e-mail, etc. It provides the interface between user programs and the network.

Network Management Protocols

You should be familiar with the terminology and concepts of network management protocols, specifically the following.

SNMPv1 (Simple Network Management Protocol version 1)

SNMP is the most common management protocol in use in data networks. It provides a means of obtaining information from, and sending information to, network devices. SNMP is based on the manager-agent model, and uses Management Information Bases (MIBs) to exchange information between them (see "Exchanging Management Information" on page 27). Using the SNMP protocol, a manager can query and modify the status and configuration information on each managed device by making requests to the agent running on the managed device. All commands use the UDP/IP protocol, which means that communication between the manager and the agent is connectionless. SNMP operates at Layer 7, the application layer.

SNMPv2C (version 2) SNMPv2C includes the basic functions of SNMPv1, and adds new message types, standardized multiprotocol support, enhanced security, new MIB objects, and a way to co-exist with SNMPv1. SNMPv2C is useful for the retrieval of large amounts of management information using fewer network resources.

UDP (User Datagram Protocol) UDP is a protocol that allows an application program on one machine to exchange datagrams with an application program on another machine, without acknowledgments or guaranteed delivery. UDP operates at Layer 4, the transport layer.

TCP/IP (Transmission Control Protocol/Internet Protocol) TCP and IP are the two most widely-used Internet protocols, with TCP providing transmission of data on IP networks, and IP containing addressing and control information for packets to be routed. TCP operates at Layer 4 of the OSI model, while IP operates at Layer 3.

TCP/IP plays a significant role as a common denominator in interconnecting devices and networks, and is widely used to connect computers with dissimilar technologies. Most management solutions require TCP/IP as an information source and information carrier.

ICMP (Internet Control Message Protocol) ICMP is the part of IP that handles error and control messages. It operates at Layer 3, the network layer. ICMP supports an `echo` function, which sends a packet on a round-trip between two hosts. `ping`, which sends a signal to see if an interface is up and running, is based on this feature. ICMP can also send an address mask request that returns the address of the subnet mask on the remote system. This feature is important for non-SNMP devices.

IPX (Internet Packet Exchange) IPX is a network protocol that allows personal computers to communicate on local area networks and wide area networks. Operating at Layer 3 of the OSI model, IPX establishes a connection between the sender and the receiver. When a message is sent and the receiver does not issue a response, the message is simply retransmitted. IPX uses a broadcast technique to track all the computers and services on the network.

ARP/RARP (Address Resolution Protocol) ARP is used at Layer 2, the link layer, to map an IP address to a MAC (or link level, or hardware) address. RARP (Reverse Address Resolution Protocol) is used to map a MAC address to an IP address.

ECT 03/2005 - CN -
ROS II 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0763
3740
Doc:

DHCP (Dynamic Host Configuration Protocol)DHCP allows IP addresses to be allocated on a temporary basis (a lease). When the lease for an IP address expires, the address can be reused by a different node. This is useful in environments supporting mobile users who connect to the network with a laptop from many different places. This helps alleviate the problem of limited IP addresses and simplifies TCP/IP client configurations.

Protocols and the OSI Model

Figure 2 illustrates which protocols operate at the various layers of the OSI model. This illustration shows the major protocols used in network management; there are other protocols that are not shown in this illustration.

Figure 2 Protocols Operating at the OSI Layers

	Layers in the OSI Model	Protocols Operating at the OSI Layers
7	Application	SNMP Berkeley Services ARPA Services
6	Presentation	
5	Session	
4	Transport	TCP UDP
3	Network	IP/IPX ICMP
2	Data Link	ARP/RARP IEEE 802.x DHCP MAC address
1	Physical	10BASE2 10BASE5

Network Hardware Devices

The basic kinds of network communication devices include repeaters, hubs, bridges, routers, and switches. Figure 3 shows the layers at which these devices operate. These hardware devices operate at different layers of the OSI model, use different protocols, and perform different functions, thus requiring different levels of monitoring for network management. NNM will assist you with this task.

Figure 3 Hardware Devices Operating at the OSI Layers

Layers in the OSI Model		Protocols Operating at the OSI Layers	Hardware Devices at the OSI Layers
7	Application	SNMP Berkeley Services ARPA Services	Gateways
6	Presentation		
5	Session		
4	Transport	TCP UDP	
3	Network	IP/IPX ICMP	Routers Switches
2	Data Link	ARP/RARP IEEE 802.x DHCP MAC addresses	Switches Bridges
1	Physical	10BASE2 10BASE5	Simple Repeaters Hubs

- Simple Repeaters

  Simple repeaters operate at Layer 1, the physical layer, and are generally used to connect two network segments into one large segment, or to expand an existing segment. There is no filtering of messages transmitted between the two segments. A simple repeater

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0764
3740
Doc:

enhances data signals and thus can be used to extend maximum cabling distances. There is no network intelligence built into a simple repeater; it is used strictly for signal propagation.

- Hubs

  Hubs operate at Layer 1, the physical layer. A hub is simply a multiport repeater, and can be used to increase overall network size and number of nodes on a single segment. A hub allows you to isolate faults within the subnet and add stations to a segment without disrupting the entire network.

- Bridges

  Bridges operate at Layer 2, the data link layer. A bridge is used to allow networks with different physical signaling, but with compatible data link addressing schemes, to communicate. Bridges help reduce traffic on a backbone LAN by filtering any information coming from one segment to another that does not need to be forwarded through the backbone. A common use for a bridge is to allow users on an Ethernet LAN and a Token Ring LAN to communicate with each other.

- Switches

  Switches operate at Layer 2, the data link layer. The function of a switch is to dispatch data to its destination, which it determines from the packet's lower-layer media access control (MAC) address. A switch, like a bridge, limits traffic, and does not understand network protocols. A fairly new device is the multi-layer switch, or routing switch, which operates at Layer 3, and combines the intelligence of a router with the efficiency of a switch, thus routing data at higher speeds.

- Routers

  Routers operate at Layer 3, the network layer. A router is used to connect two networks with different technologies, and provides an intelligent means of transferring packets from one network to the other. A router also forwards traffic among multiple hubs and bridges.

- Gateways

Gateways operate at Layer 7, the application layer, and can encompass all seven of the OSI model layers. A gateway is a computing system that can be programmed to do any number of intricate protocol conversions and negotiations, such as between IP and IPX.

Exchanging Management Information

There are two standard logical information exchange bases used to communicate about the configuration and status values of managed objects — MIBs for SNMP-based objects and MIFs for DMI-based objects.

MIBsThe data exchanged between managers and agents on an SNMP-based system uses the **Management Information Base** (MIB). A MIB is a standard set of definitions for exchanging information about hardware and software components. Each MIB contains a group of objects, which specify a structure and format for defining manageable elements.

Types of MIBs There are several MIBs with which you should be familiar.

- MIB-I

  MIB-I is the original standard for explaining and defining the exact information base needed for monitoring and controlling devices on TCP/IP networks. The objects included in MIB-I are essential for configuration control and fault monitoring. All other MIBs are built upon and include the definitions of MIB-I.

- MIB-II

  MIB-II extends the information defined in MIB-I by expanding the set of objects defined in the MIB. The types of objects added to MIB-II include those for dealing with various transmission media types, and those for using SNMP to control and monitor the network management itself.

- RMON MIB

  The Remote Monitoring (RMON) MIB defines information that can be collected by remote monitoring devices. The main functions of the RMON MIB are to provide offline operation of remote devices, pre-emptive monitoring, problem detection and reporting, data analysis, and support for multiple managers.

RQS nº 03/2003 - CN
CPMI - CORREIOS
Fls. Nº 0765
3740
Doc:

- Bridge MIB

  There are two modes of bridging — transparent mode and source route. The Bridge MIB defines objects needed to manage a bridge operating in transparent mode, as well as some objects applicable to all types of bridges. NNM includes a Source Route Bridge MIB that, although not used by NNM for discovery, can be used for your own needs.

- Repeater MIB

  The Repeater MIB defines objects used to manage repeater devices, including multiple repeaters and non-standard repeaters.

- MAU MIB

  The MAU MIB defines objects used to manage Medium Attachment Units (MAUs). These MAUs may be connected to IEEE 802.3 repeaters or to 802.3 (Ethernet-like) interfaces.

- Private MIBs

  Private MIBs are extensions to a MIB, usually developed by a vendor or a workgroup, to manage specific devices. The most common objects in these MIBs relate to information about the physical configuration and software configuration of a device.

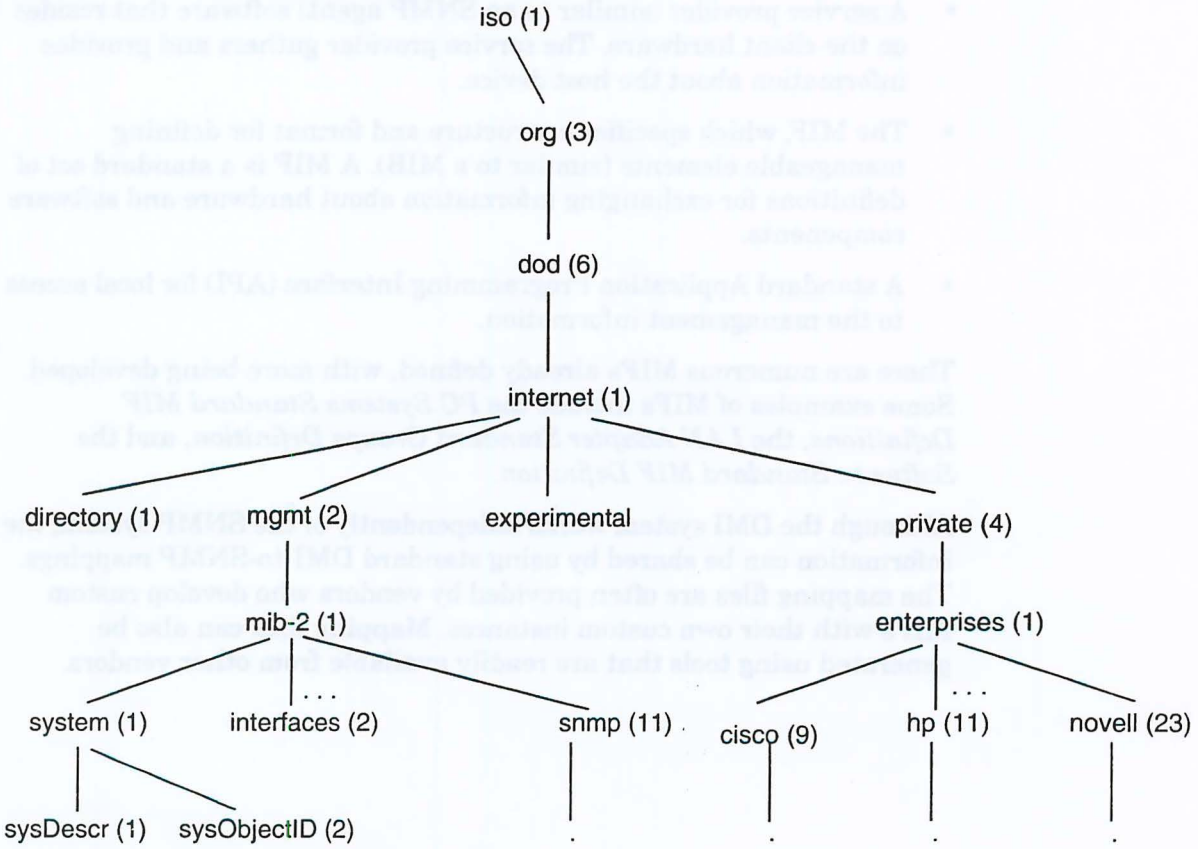
How MIBs Are OrganizedMIB objects are conceptually organized in a hierarchical tree structure. Each branch in the tree has a unique name and numeric identifier. Intermediate branches of the tree serve as a way to group related MIB objects together. The "leaves" of the tree represent the actual MIB objects. Figure 4 illustrates the tree structure, with special attention to the Internet MIB tree.

A MIB object is uniquely identified (named) by its place in the tree. A full object identifier consists of the identifier of each branch along the path through the tree hierarchy, from the top of the tree. For example:

2859

.iso.org.dod.internet.mgmt.mib-2.system.sysObjectID
(.1.3.6.1.2.1.1.2)

Figure 4 MIB Organization



MIB Objects and InstancesA specific type or class of management information is called a **MIB object** (for example, a system description or an interface status). The existence of a particular returned value for a MIB object in the agent database is called an **instance**. Some MIB objects have only a single instance for a given agent system (for example, system description). Other MIB objects have multiple instances for a given agent system (for example, interface status for each interface on the system).

MIFs A **MIF** is a **Management Information Framework** for objects conforming to the Desktop Management Interface specification.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0766
3740
Doc:

The **Desktop Management Interface** (**DMI**) facilitates the management of PCs in a networked environment by providing a common interface and information access method. DMI provides a management framework that consists of three elements:

- A service provider (similar to an SNMP agent) software that resides on the client hardware. The service provider gathers and provides information about the host device.
- The MIF, which specifies a structure and format for defining manageable elements (similar to a MIB). A MIF is a standard set of definitions for exchanging information about hardware and software components.
- A standard Application Programming Interface (API) for local access to the management information.

There are numerous MIFs already defined, with more being developed. Some examples of MIFs include the *PC Systems Standard MIF Definitions*, the *LAN Adapter Standard Groups Definition*, and the *Software Standard MIF Definition*.

Although the DMI system works independently of the SNMP system, the information can be shared by using standard DMI-to-SNMP mappings. The mapping files are often provided by vendors who develop custom MIFs with their own custom instances. Mapping files can also be generated using tools that are readily available from other vendors.

General Operating System Knowledge

In addition to understanding networking concepts, it is critical that you have a good working knowledge of the operating system, or systems, that are present on your network. This book does not attempt to explain any concepts of the UNIX®[1] or the Windows®[2] operating systems. It frequently refers to commands and functions of these operating systems, without further explanation. Refer to the documentation that came with your operating system for more information.

Cross-Platform Issues

Since it is likely that your network environment contains a combination of systems, you need to be aware of the differences between their operating systems. Some of the differences are listed below.

- Reference pages in NNM's online help on a Windows operating system are called manpages on a UNIX operating system.
- Directories and paths are different on each system. Consult the *ov.envvars* reference page in NNM's online help (or the UNIX manpage) for a mapping of paths across systems.
- Watch your use of the forward slash (/) and the backslash (\) when entering pathnames. When switching from a UNIX operating system to a Windows operating system, it is easy to misuse one for the other.
- Do not use spaces in directory names or file names.
- Watch the use of upper and lower case of file names. Even though the Windows operating system preserves file name case, not all applications on the Windows operating system distinguish between upper and lower case. In addition, case is significant on UNIX operating systems.
- On Solaris systems, `pc nfs` must be installed, and the `pcnfsd` process running, before a Solaris management station will interoperate with a Windows operating system.

---

1. The term *UNIX* in this manual refers to HP-UX and Solaris operating systems only.
2. See the *Release Notes* for supported versions of *Windows* operating systems.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. 0767
Doc: 3740



- If you are using remote consoles running a Windows operating system with a management server running a UNIX operating system, be sure your NFS client product on the Windows operating system supports file locking. Not all do.

For More Information

If you need more information about networking or operating system concepts, the following documentation may be helpful.

Internet Request for Comments (RFC) Documents

Copies of RFCs are shipped on Network Node Manager's installation CD. RFC file names other than those mentioned in Table 1 may be included in the *Windows* and *UNIX* directories mentioned below.

Windows: installed on your hard drive through a custom installation in the *install_dir*\doc\RFC directory.

UNIX: in the $OV_DOC/RFCs directory.

Table 1 Where to Find RFC Documents about MIBs

To find out about...	See...	Filename
How MIB objects are defined	*RFC1155: Structure and Identification of Management Information for TCP/IP-based Internets*	rfc1155.txt
The protocol used to manage the MIB objects	*RFC1157: A Simple Network Management Protocol (SNMP)*	rfc1157.txt
The format for creating MIB object files	*RFC1212: Concise MIB Definitions*	rfc1212.txt
The objects contained in the Internet-standard MIB	*RFC1213: Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*	rfc1213.txt
Defining objects for managing MAC bridges	*RFC1493: Definition of Managed Objects for Bridges*	rfc1493.txt
Defining objects for managing IEEE 802.3 Medium Attachment Units (MAUs)	*RFC1515: Definition of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)*	rfc1515.txt
Definitions of Community-based SNMPv2C	*RFC 1901:Introduction to Community- based SNMPv2*	rfc1901.txt

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0768
3740

Table 1 Where to Find RFC Documents about MIBs (Continued)

To find out about...	See...	Filename
MIB definition language for managed objects	*RFC1902:Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)*	`rfc1902.txt`
MIB definition language for conformance and capability definitions	*RFC 1904: Conformance Statements for version 2 of the Simple Network Management Protocol (SNMPv2)*	`rfc1904.txt`
Definitions of SNMPv2C protocol	*RFC 1905: Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*	`rfc1905.txt`
Definitions of SNMPv2 transport mappings for IP, IPX, and DDP	*RFC 1906: Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)*	`rfc1906.txt`
Definitions of SNMPv2 MIBs for IP, IPX, and DDP	*RFC 1907: Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)*	`rfc1907.txt`
MIB definition language for refined data types	*RFC 1903: Textual Conventions for version 2 of the Simple Network Management Protocol (SNMPv2)*	`rfc1903.txt`
Co-existence guidelines for SNMPv1 and SNMPv2	*RFC 1908: Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework*	`rfc1908.txt`
Defining objects for managing IEEE 802.3 baseband repeaters	*RFC2108:Definition of Managed Objects for IEEE802.3 Repeater Devices*	`rfc2108.txt`

Table 2 Where to Find RFC Documents about DMI and MIFs

To find out about...	See...	Filename
Desktop Management Interface 2.0 Standard	*DMTF: Desktop Management Interface Specification, version 2.0*	`dmi-v20.doc`

Table 2 Where to Find RFC Documents about DMI and MIFs (Continued)

To find out about...	See...	Filename
Access to DMI instrumentation and events using SNMP	*DMTF: DMI to SMP Mapping Standard, Version 1.0*	`dmi-snmp.doc`
General information about the DMTF and DMI	Desktop Management Task Force web site	`www.dmtf.org`
Defining objects for managing MAC bridges	*RFC1493: Definition of Managed Objects for Bridges*	`rfc1493.txt`

Web Sites

There are numerous sites on the World Wide Web that contain lists of reference materials and links to other useful networking sites. Hewlett-Packard does not endorse these sites, but has found them to contain informative references. Note that the URLs for these sites are subject to change without notice, but were valid as of the date of printing of this document.

Table 3 Web Sites Related to Network Management

Web Site URL	Description
`www.ovforum.org`	The web site of HP OpenView Forum, an association of users and developers of HP OpenView network and system management solutions
`www.iol.unh.edu/training/index.html`	Tutorial documents on network technologies and network management
`www.ietf.org`	The web site of the Internet Engineering Task Force
`netman.cit.buffalo.edu`	Archives for `comp.dcom.net-management`
`www2.tmforum.org`	The web site of the TeleManagement Forum

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0769
Doc: 3740

Table 3 Web Sites Related to Network Management (Continued)

Web Site URL	Description
www.dmtf.org	The web site for the Distributed Management Task Force, Inc.
www.opengroup.org	The web site for The OpenGroup (X/Open and OSF®)
www.ieee.org	The web site for the Institute of Electrical and Electronic Engineers
www.simple-times.org	The *Simple Times* newsletter

1 Network Management with NNM

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0770
3740
Doc:



This chapter describes the basic challenges of network management, and how Network Node Manager and other HP OpenView products address those challenges.

Topics covered include:

- How NNM can help you move toward proactive network management (page 40).
- An overview of each function of network management, and how NNM and other HP OpenView products address several of those functions (page 42).

The Network Management Challenge

As a network administrator, you are under increasing pressure to perform the necessary tasks to meet the business demands of your organization. Some of the challenges you often face include:

- Dealing with user dissatisfaction in the face of increasing user expectations. Users want to be able to have the tools they want, when they want them to maintain their productivity.
- Deploying network services so that end users maintain productivity from their desktop systems.
- Keeping the systems operating 24 hours a day, 7 days a week.
- Producing faster, more predictable response times.
- Integrating and managing diverse and complex technologies — networks, servers, databases, applications, legacy systems, web-based systems—all from different vendors.
- Managing multiple sites and global distribution.
- Moving to proactive management techniques to keep it all running smoothly.

Clearly, the demands on a network administrator are great. Network management is now a high-pressure situation where more services are requested on tight schedules with fewer resources.

How Network Node Manager Can Help

Network Node Manager is the foundation from which most of the HP OpenView products operate. When installed, the other HP OpenView products appear as added functionality within NNM. NNM not only functions as a solution on its own, but can collect data for, and forward data to, other HP OpenView products. It is the starting point for implementing a network management solution.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0771
3740



Moving to Proactive Network Management

By using proactive, rather than reactive, network management, you can reap the true benefits of NNM. Several things must be present in order for proactive network management to be a reality.

- First, you must find out the current state of your network—what devices are present, how they are configured, how they are behaving, their performance levels, what is currently going wrong. NNM does this for you by polling for network information and screening problems through event correlation.
- Second, you must identify trends and determine how to optimize the network by changing configurations, replacing network devices, etc. NNM assists you by collecting historical information. You can easily access the historical data that NNM gathers and use it in your favorite statistical analysis programs.
- Third, you must learn how to predict what might go wrong, determine how to prevent it from happening, and learn to avoid future problems. NNM allows you to monitor thresholds of your choosing for critical network devices.

Poll for Network Information

The first step to proactive network management is to gather all the information that you can about the current state of your network.

NNM continually polls for:

- Status of objects (for example, up, down, or marginal).
- Network topology changes, including the discovery of new nodes.
- Configuration changes.

You can configure thresholds for NNM to monitor on critical network devices and configure NNM to notify you or your team members when anything goes wrong. For example, you can set thresholds on CPU loads, disk space used, interface and link errors, and collected MIB data. You can configure NNM to dial a pager when any of these situations become critical.

Watch for Events

NNM actively notifies you when an important event occurs. The event is reflected by a change in the color of the device's symbol on the map, and is reported through NNM's Alarm Browser.

Each category of alarms has a corresponding button that changes color to show the highest severity alarm in the category. Thus, you are immediately notified of potential or current problems.

You can browse through alarms to help you diagnose problems. You can view alarms by specific node or other sort criteria to help you solve problems quickly. The event reduction features in NNM monitor incoming alarms, identify patterns of common network problems, and for an identified problem, post one meaningful alarm with all related alarms nested beneath.

You can define the format of alarm messages so that they are most useful to your team. Your team can use the Alarm Browser to notify everyone else about which issues are being covered.

You can use event customization to automate some of the common fault management tasks for your team by using NNM to configure automatic actions upon the receipt of specific alarms. You can also filter out less important events, or simply send them to a log file.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0772
3740
Doc:

Network Management Functions

Network management can be defined in general terms as the ability to have a single point of control to accomplish the activities required to manage a network. Network Node Manager provides an integrated tool for the network manager to control and manage multiple networked systems and applications from a single graphical representation of the network.

When properly implemented, a network management station can result in:

- Reduced downtime of network systems and devices.
- Quick detection and correction of network problems without disrupting the network.
- The ability to monitor data to anticipate problems (predictive).
- The ability to log information for historical analysis.
- The ability to perform an action when some pre-defined event or situation has occurred.

To understand how Network Node Manager and other HP OpenView products address these problems, it is helpful to break network management down into functional categories, listed below. Following this list is an explanation of how NNM and other HP OpenView products help you manage these areas.

- Fault and Problem Management

  This function detects, isolates, and controls problems, or faults, on the network. This is carried out by network status monitoring, alarms, alerts, reporting, and predictive tools.

- Performance Management

  This function measures the performance of network hardware, software, and media, such as throughput rate, percentage utilization, error rates, and response time, through the collection and analysis of data about the network.

- Configuration and Change Management

This function is responsible for finding and setting up the network devices that control the behavior of the network. This function also includes central control of configurations.

- Accounting Management

  This function obtains statistical information on network use. You can collect and process data related to resource consumption on the network, track each individual and group's utilization of resources, and control access to the network for individuals and groups.

- Security Management

  This function protects the network and its interconnections, systems, and network management information from unauthorized access, unauthorized use, and other harm.

Fault/Problem Management

NNM's Capabilities

Often times the most difficult management task is identifying the source of a problem when it occurs. NNM helps you identify problems and errors, recognize trends, and proactively avoid problems. NMM lets you:

- Automatically discover the IP and IPX nodes in your network.
- Automatically monitor your network's status through the map interface and the event browser interface.
- Manage any vendor device that supports the Simple Network Management Protocol (SNMP). NNM manages both standard and enterprise-specific Management Information Base (MIB) objects.
- Manage non-SNMP nodes that use IP or IPX protocols.
- Manage any vendor device that supports the Desktop Management Interface (DMI). NNM monitors both standard and enterprise-specific Management Information Format (MIF) objects.
- Include new enterprise-specific Internet MIBs in NNM's MIB. Once you have loaded the new MIB module on the management station, you can access any of the MIB objects defined in that MIB module.
- Build new MIB applications (without programming) for Internet-standard and enterprise-specific MIBs. Once you have built a MIB application, you can monitor objects through the menu bar.

RGS
CPMI - CORREIOS
Fls 0773
3740
Doc

- Define event thresholds for MIB objects; for example, an event can be generated when the disk usage on a particular device exceeds a limit.
- Define actions to be taken upon receipt of an SNMP trap.
- Manage event storms and improve the information content of events by suppressing unwanted, redundant events and adding new, more informative events, using NNM's event reduction strategies: de-duplication, ECS correlations and Correlation Composer correlators.
- Integrate your own fault detection applications into the menu bar to yield an integrated management solution.
- Diagnose network faults and performance problems from one location, and diagnose problems by looking at trends over time. This includes customizing and automating the monitoring of your network and the response of management stations to events.
- Launch Systems Management Server (SMS) Administrator, or view the SMS properties of a node. From SMS Administrator, you can select a node and open the submap containing that node.
- Launch Windowsoperating system applets such as the Event Viewer, Performance Monitor, and Registry Editor from within NNM on remote systems with the Windowsoperating system.

Other HP OpenView Products' Capabilities

HP OpenView NNM Extended Topology Extended Topology augments NNM by discovering and displaying additional device connectivity information that you can use to diagnose network problems. It includes:

- Management of heterogeneous switched layer 2 environments and routed layer 3 environments.
- An enhanced web user interface with dynamic views.
- Views from protocols and technology running on top of your network, such as OSPF and VLAN.
- Launching targeted views from events for rapid problem resolution.

HP OpenView Operations IHP OpenView Operations is an event and problem management solution that allows you to identify, locate, correlate, and resolve system and network faults. It includes:

- A central management console for monitoring events.
- Intelligent agents that can be preconfigured to solve problems immediately without interacting with the management console.
- Management of workstations running UNIX operating systems, the Windows operating systems, Novell Netware, and legacy systems.
- Integration with other OpenView products.

Performance Management

NNM's Capabilities

Figuring out how to fine-tune your network's performance can be a real challenge. To assist in this task, NNM gathers and reports information on network performance, availability, inventory, and exceptions. NNM can forward information to other HP OpenView products that provide statistical analysis on the data.

The following is a brief summary of NNM information gathering features:

- Automatically monitor your network's status.
- Collect historical MIB information about MIB objects and MIF events, store the data for trend analysis, and graph collected data. This helps you determine performance trends.
- Automatically set thresholds based upon standard deviations of historically collected data.
- Automatically collect data and generate General Availability and General Inventory reports.
- Manage and modify reports using the NNM Report Configuration Interface.
- Manage information being collected and stored in the data warehouse.
- Integrate your own performance monitoring applications with the menu bar to yield an integrated management solution.
- Diagnose network faults and performance problems from one location, and diagnose problems by looking at trends over time. This includes customizing and automating the monitoring of your network and the response of management stations to events.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0774
3740
Doc:

Configuration and Change Management

NNM's Capabilities

Keeping track of the devices on your network, their configurations, and their interrelationships can be time consuming. NNM helps you keep a record of this information, by allowing you to:

- Store critical configuration information from devices such as routers and switches.
- Track inventory of the devices on the network.
- Generate snapshots of your network before any departmental moves to speed reconstruction after the move.

PREGÃO
118/2003

PASTA 03

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: Nº 0775
3740
Doc:

Additional HP OpenView Product Information

You can find additional information about other HP OpenView products and solutions at `http://openview.hp.com`.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0776
3740



2 How Does NNM Work?

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0777
3740
Doc:



When you set up NNM to run on a management station, your team can access NNM from the management station, from remote consoles, or from the worldwide web. All three forms of access tie into the same databases running on the management station. Therefore, all members of your team continuously see the most current information. NNM works for you in the following ways, as explained in this chapter:

- Maps out your network for you. The map symbols change color to indicate if something is wrong (page 56).
- Collects critical information about your network and maintains a current log of alarms that you need to know about (page 51).
- Correlates collected information to help you quickly determine the probable cause of problems (page 61).
- Maintains a relational database from which data can be exported for historical analysis using your choice of statistical programs (page 62).
- Provides easy access to report generation, see the NNM online help for more information. See also the *Reporting and Data Analysis* online manual. You can create reports using a set of predefined templates that are populated from the data warehouse.

The remainder of this book then leads you through the process of understanding, configuring, customizing, and troubleshooting NNM.

Collecting Critical Information

NNM uses several protocols to maintain communication channels with each managed device on your network. These include:

- SNMPv1; SNMPv2
- TCP/IP
- IPX/DMI
- UDP
- ICMP
- ARP/RARP

Since SNMP is the primary protocol used for NNM's communications, an understanding of the SNMP management model will help you better understand how NNM works.

NNM also uses other, lower-level families of protocols (sometimes referred to as services), such as the ARPA family, the Berkeley family, and the NFS family. These protocols are used for functions such as file transfer, e-mail, or remote login.

SNMP's Network Management Model

The network management model consists of a network management station, managed nodes with agents, and a network management protocol. NNM uses SNMP as its standard protocol, and uses this protocol to communicate over other protocols, such as TCP/IP, IPX, and UDP.

The Role of Manager and Agents

A manageable network consists of one or more network management stations (manager), a collection of SNMP agents, and network objects.

- A **manager** is an application that executes network management operations to monitor and control agent systems. The implementation of these network management operations is called the manager.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0778
3740
Doc:



- An **SNMP agent**, which resides on a managed node, is an application that acts on behalf of an **object** to perform network management operations requested by the manager.
- An **object** is anything that will be managed, such as a host, gateway, terminal server, hub, bridge, application, or database.

A manager and an agent may exist on the same system. The manager and agent communicate using the Simple Network Management Protocol (**SNMP**). Network Node Manager supports both SNMP version 1 (SNMPv1) and Community-based SNMP version 2 (SNMPv2C). SNMP permits the following activities:

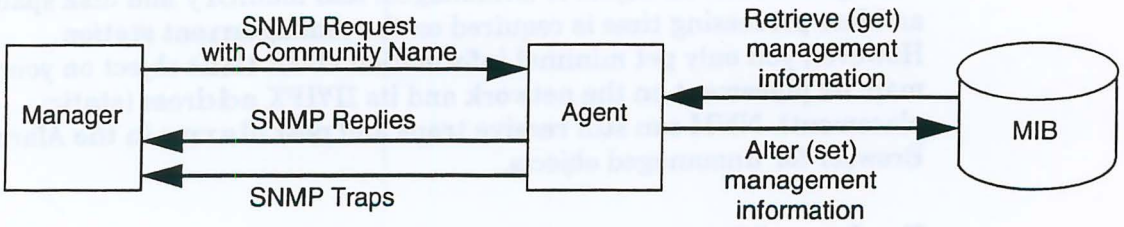
- A manager can retrieve management information from an agent. (The actual mechanism to retrieve management information depends upon the SNMP versions supported by the agent, and can include `get`, `getNext`, and `getBulk`.)
- A manager can alter, or `set`, management information on the agent's system.
- An agent can send information to the manager without an explicit request from the manager. This operation is called a **trap** in SNMPv1, or a **notification** in SNMPv2C.

Traps and notifications alert the manager to changes that occur on the agent system, such as a reboot. The agent must usually be preconfigured to know where to send traps or notifications (see page 325).

SNMP requests for information from an agent are accompanied by a **community name**. A community name is much like a password; it must be correctly received from the manager before information can be accessed from the agent. You must inform NNM about the community names that are in use on your network (see page 145). The manager accesses the agent's MIB object instances using SNMP's `get`, `getNext`, `getBulk`, and `set` operations.

Figure 2-1 shows a simplified diagram of the manager-agent interactions just described.

Figure 2-1 Manager-Agent Communication through SNMP



Basic SNMP Services

There are six basic operations associated with SNMP. They are:

- `get` request. Reads a value from a specific variable.
- `getNext` request. Traverse information from a table of specific variables.
- `getBulk` request.
- `get` response. Replies to a `get` or a `set` request.
- `set` request. Writes a value into a specific variable.
- `trap` or `notification`. A message initiated by the agent without requiring the management station to send a request.

Managed versus Unmanaged Objects

A **managed object** is one that is actively being polled by NNM to determine its status and configuration. An **unmanaged object** is one that exists in the databases and within maps, but is not being polled by NNM.

NNM gives you the choice of managing or not managing objects, depending on your information needs and network resources.

When an object is managed, NNM can obtain any information that you specify about that object (as long as that object's protocol is supported). The more objects you manage, the more memory and disk space is required on the management station. In addition to the information that you specify, the management station will need processing power for the

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0779
3740
Doc:

routine status and configuration polling and the event monitoring of each managed object. If an object is critical to the network function, then you should manage it.

If the object is not critical to the functioning of your network, you might choose to *unmanage* it; which means that NNM will not actively monitor the object. When an object is unmanaged, less memory and disk space and less processing time is required on the management station. However, you only get minimal information about that object on your map: its placement on the network and its IP/IPX address (static placement). NNM can still receive traps and post alarms in the Alarm Browser for unmanaged objects.

Desktop Management Interface (DMI)

The Desktop Management Interface (DMI) is a parallel management strategy to SNMP. DMI standards were developed by the Desktop Management Task Force (DMTF). Although DMI is entirely independent from the SNMP protocol, there are many similarities:

- The DMI **client** is similar to the SNMP management station.
- The DMI **service provider** is similar to the SNMP agent and must be running on each remote DMI device.
- The DMI **MIF** (Management Information Format) file is similar to the SNMP MIB file and defines the management information that can be provided by the service provider (event) or requested by the client (get/set).
- The **DMI event** is similar to the SNMP trap.

If your management station is running NNM on the Windows operating system, during discovery polling, NNM **subscribes** to receive DMI events from all managed systems running DMI version 2.0. All DMI events are received by NNM's ovcapsd service (background process) and converted to SNMP traps as specified in the Desktop Management Task Force's DMI to SNMP Mapping Standard. The SNMP-equivalent message is posted to NNM's Alarm Browser.

NOTE If your management station is running NNM for a UNIX operating system, you must communicate with the DMI service provider indirectly through an SNMP agent installed on the remote DMI-enabled device itself along with a DMI-to-SNMP mapping agent. The SNMP agent then

handles all communications. Therefore, NNM doesn't need to subscribe to the DMI service provider in order to receive DMI events from this node.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0780
3740
Doc:



Automatic Discovery and Layout

When you start the NNM background processes, all IP and Level 2 devices (devices that support bridge, repeater, and MAU MIBs) on your network are automatically discovered and mapped out. If you are running NNM on a management station running the Windows operating system, IPX devices are also discovered and mapped out. This map is a visual representation of the communications channels established between NNM and the devices in your network. Be aware that this map is not a physical representation; rather, it is a logical representation. The accuracy of these communications channels between NNM and your network devices determine whether or not NNM can provide the information you need in order to manage your network.

The initial polling process may take several hours, or even over night, to discover all the devices on your network. However, it is worth the wait! You start benefiting from NNM immediately. You will use NNM's default map, and Alarm Browser to pin-point any gaps in your well-configured network scheme.

How IP Discovery and Layout Work

The `netmon` service (background process) uses a combination of SNMP requests and ICMP `pings` transmitted over UDP and IPX to find out about the nodes on your network.

To discover the nodes on the network, `netmon` needs access to the following information:

- The subnet mask from the agent on the management station.
- The address of the default router in the management station's routing table.
- SNMP information from, at a minimum, the default router, and from other routers and nodes on the network.

For `netmon` to work, it requires the following:

- The management station must be correctly configured for networking.
- The management station must be running an SNMP agent.

- Nodes must be up and responding to ping requests to be discovered.
- All gateways/routers and the management station must have correctly configured subnet masks for all interfaces.

During IP discovery, netmon works best in these situations:

- The more routers in the network the better; and those routers should be running configured SNMP agents.
- The more nodes running configured SNMP agents the better.
- The more SNMP information netmon gets the better; for example, valid ARP caches and, from serial connections to routers, routing tables.

Information about the discovered nodes is stored in NNM's databases and is used to automatically generate the network map.

Over time, NNM will discover new nodes on the network. However, if a new node never talks with a gateway or other nodes on the network that support SNMP, NNM may not find it. In this instance you can use menu items within NNM to send a low-level ICMP ping that forces NNM to discover the node; or you can add the node manually.

How IPX Discovery and Layout Work

If you are running NNM on a management station running the Windows operating system, in addition to discovering IP nodes on your network, netmon performs IPX discovery of your network. However, the methods used are very different from those used for IP discovery. The IP discovery process relies primarily on SNMP queries to gain hints of new IP nodes. For IPX discovery, netmon relies on using broadcast versions of various IPX protocols to discover the nodes, then uses SNMP once the node is discovered to fill in additional information about the node. In particular, netmon will be able to determine that an IPX node supports IP only if that node supports SNMP over IPX.

While the discovery model is different, the layout results in the submap are very similar. IPX network symbols are created in the Internet submap, connected by IPX gateways. IPX network symbols can be exploded to display segment and node submaps. However, IPX nodes always are connected to a single segment in the IPX network.

To discover IPX nodes on the network, netmon requires the following:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0781
3740
Doc:

- The management station must be correctly configured for IPX networking.
- At least one IPX server or router must be connected to the same network as the management station.
- Nodes must be up and responding to IPX diagnostic requests to be discovered.

During IPX discovery, `netmon` works best in the following conditions:

- The management station is not also an IPX/NetWare gateway.
- Servers, routers, and nodes in the environment respond to IPX diagnostic, Routing Information Protocol (RIP), and Service Advertising Protocol (SAP) requests.
- IPX nodes in the environment support SNMP over IPX.

As with IP discovery, the information about the discovered nodes is stored in the NNM's databases and is used to automatically generate the network map.

Because `netmon` uses broadcasts, most IPX nodes should be recognized after the first few IPX polling cycles. After the default IPX discovery interval of six hours, most IPX nodes will be discovered, with the majority coming soon after the initial discovery cycle at system installation or startup. However, this discovery rate will vary depending on the number and type of nodes in the network. So before you start to troubleshoot `netmon`, allow the process sufficient time to discover your network. This may require allowing IPX discovery to run over night.

Interactions Between IPX Discovery and IP Discovery

If an IPX node supports SNMP over IPX, `netmon` will attempt to use the MIB-II `ipAddrTable` to also include IP addresses and interfaces on the IPX node, as well as using the other MIB-II variables to provide additional information. When a node is discovered to support both IP and IPX, the following rules apply:

- Preference is generally given to the IP values as the name and labels for the node.
- After a node is determined to support IP, IP will be the preferred SNMP transport protocol.

- If a node is first discovered as an IP node, and a later IPX node is discovered to have the same set of IP addresses via SNMP, the IP node may be deleted in favor of the IPX node. For this reason, we recommend that you delay extensive map customization until IPX discovery is complete.

Level 2 Discovery

NNM takes advantage of information provided in three standard MIBs to discover bridges (switches) and hubs. These MIBs are the bridge MIB (RFC 1493), the repeater MIB (RFC 2108), and the 802.3 MAU MIB (RFC 1515). If a network device supports any of these MIBs, `netmon` will use the information reported to develop a model of the topology which better represents how and to what the device is interconnected.

In the case of switches and bridges, additional information is gathered from the bridge MIB. In the case of hubs, addition information is gathered either from the repeater MIB or the 802.3MAU MIB.

The status of non-IP or non-IPX interfaces on switches, bridges, and hubs is determined via SNMP based on the administrative and operating status of the port.

If the MAC address of a node, which does not support IP or IPX, is reported by any of these MIBs, the node is added to the topology relative to the device which hears it. A label for this device is determined by the MAC address reported by the network interface card. Because no MAC layer control message protocol is available, the status of the devices is determined indirectly via information provided by the surrounding network elements.

Trunking and Meshing

Configuring two or more ports between two network devices into a single group is referred to as port trunking. This is done to increase the available bandwidth between the two devices. For example, you can increase the available bandwidth between two devices, such as two ethernet switches, by configuring a group of two or more connections between the two devices.

Meshing involves connecting devices on the network via multiple paths. Meshing is used when devices are used in a critical function and redundant network connectivity is required.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 0782
Doc: 3740

You can configure NNM to label port trunking and meshing connections with information you add to the `netmon.equivPorts` file. See "Configuring Trunking and Meshing" on page 225 for more information.

Event Reduction Capabilities

NNM includes several event reduction capabilities that identify relationships between different events to quickly determine the root cause of problems, such as event storms. This improves the information content of alarms by suppressing unwanted, redundant alarms and adding new, more meaningful alarms.

You see fewer, but more informative alarms that show the relationships and dependencies between network events. It then becomes easier to identify trends, to isolate important events, and to react more quickly to problems. You view these events through the NNM Alarm Browser.

Event reduction involves processing events based upon relationships between individual events. Event reduction:

- Analyzes events based upon previous, current, or subsequent events.
- Can create new events.

  By analyzing the relationships between events in the stream, single events can replace groups of events. These events may have increased information content, and can be of a different protocol, compared to the original events.
- Dramatically reduces the number of alarms displayed by the NNM Alarm Browser.
- Correlates alarms between different event protocols.

NNM contains pre-defined event reduction configurations that you can modify, if desired. You can also create your own new ones to address specific needs within your environment. Refer to "Event Reduction Capabilities: Getting to the Root Cause" on page 351 for more information about these features.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0783
3740
Doc:

NNM's Databases

NNM provides several operational databases, each designed to store specific kinds of data and used for a variety of purposes. In addition, NNM includes a data warehouse: a relational database used to store historical information about your network.

For more information about the NNM databases and the data warehouse, consult the online manual *Reporting and Data Analysis with HP OpenView Network Node Manager*.

Operational Databases

NNM's operational databases—object, map, topology, trend, and event—can be thought of as a single logical database. These databases store the operational data used by NNM, putting critical information at your fingertips.

The Object Database

The object database contains semantic information about symbols on the map. The information is generic; that is, it is not customized to any specific application. The object database contains field definitions such as `sysObjectID`, vendor, and SNMP Agent. You can see the field values in the object database for a particular object through the `Properties` dialog box for that object.

Map Database

The map database contains presentation information specific to each map. Examples of presentation information that is stored in the map database include the exact symbol placement on the map, the symbol associated with each object, and symbol labels. NNM updates the map database based on requests from the user, or from various NNM services.

Topology Database

The topology database manages information critical to the management of IP nodes. It includes state information, such as time stamps indicating when the object last changed and when it should be polled next. This

information helps NNM detect changes and communicate them to various NNM services. The topology database is stored in a proprietary HP OpenView format.

Event Database

The event database is the repository for SNMP traps and OVW events that are received by NNM. It also stores events that are output from the Event Correlation Service (ECS). In addition, the event database stores information for the event browser tools about the state of the events displayed in the web browser applications. The information in the event database is displayed in the Alarm Browser.

Trend Database

The trend database (sometimes called the `snmpCollect` database) stores MIB data and threshold information that is gathered through the `snmpCollect` service (process). Information from the trend database is used in the Reporting and the Data Collection features, and can be viewed with the Grapher feature of NNM on a management station.

Data Warehouse

The NNM data warehouse stores data exported from the NNM databases into a relational database. You export this data to the data warehouse using the `Tools:Data Warehouse` menu choices (`Export Topology`, `Export Events`, and `Export Trend Data`).

You can use the information in the data warehouse to define your own reports. You can also use the NNM web Reporting interface to configure and view reports. When you create a report using the web Reporting interface, NNM automatically starts exporting the appropriate data to the data warehouse.

An embedded relational database is provided with NNM, and Oracle® and SQLServer are also supported.

ROS nº 03/2005 - C
CPMI - CORREIOS
Fls. Nº 0784
3740
Doc:



3 Resources Available While Learning NNM

ROS nº 03/2005 - C
CPMI - CORREIO
Fls. Nº 0785
3740
Doc:

There are many resources included with NNM that will help you use the product more effectively. In addition, there are also multiple additional services available through HP.

Resources included with NNM:

- Online help system (page 67)
- Tip of the Day (page 69)
- NNM's manuals, both printed and online (page 69)
- Release notes (page 71)
- Online reference pages/manpages (page 71)
- `contrib` programs (page 74)
- `support` directory (page 74)
- White papers (page 75)

Resources and services available through HP:

- HP web sites (page 76)
- HP Consulting Service (page 76)
- HP Education (page 77).
- HP Product Support (page 77)
- OpenView Forum (page 77)

Resources Included with NNM

NNM Online Help System

NNM includes an online help system that contains all the specific procedural information you will need while you are working with NNM. The help system has extensive search capabilities and a comprehensive index so you can easily find information. You can print or copy pages or sections of help information that are appropriate for the most common tasks for your organization.

TIP The help system includes hyperlinks that make it more convenient and informative. By clicking on designated link words, you gain instant access to more topics and information related to your currently selected topic.

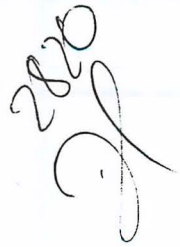
The online help system enables you to display information on the features of NNM, explains how to perform tasks with NNM, and includes conceptual information about how NNM works. Help entries are available from three general locations:

- `Help` menu
- `[Help]` button on dialog boxes
- Help from some symbol pop-up menus

Using the Help Menu

The contents of the `Help` menu varies from one submap to another, depending on additional installed applications. The `Help` menu also differs between NNM on a workstation running the UNIX operating system, NNM on a workstation running the Windows operating system, and the NNM web interface.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0786
3740
Doc:



Printing Information from Online Help

NNM for the Windows operating system uses a standard Microsoft® Windows help system. Each help window has a `Print` button or menu item that you can use to print the current topic. You can also select multiple topics in the help table of contents, then print those topics.

On UNIX operating systems, you can select a topic in the `Contents` window of help, then select the `Print` menu item. In the `Print` dialog box, select `Print Topic` to print only that topic. If you want to print all the subtopics under that topic, select `Print Topic and All Subtopics`.

You can then combine these help printouts into a binder for future reference. This is especially useful for frequently-accessed information, so that you do not have to access the help system every time you need to look up a common task or function. You can also use these printouts to create your own operating manuals.

Searching for Information

The most efficient way to find a particular help topic is index search. You access index search via the `Index` tab in the help system on a Windows operating system or by the `Index` button on a UNIX operating system. Every topic in the help system is indexed by the keywords that are used in the topic. When using index search, enter the word that best describes what you are looking for and that is most likely to narrow down your search. For example, if you want to find help on automatic map generation, enter the word "automatic" or "auto-generate" rather than the word "map." Those words are more likely to find the entry that you want.

In a Windows operating system only: another way to find information is by using the `Find` function in the online help. The `Find` function searches every word in every topic for the word or phrase of your choice, and returns a list of the titles of topics where those words or phrases appear.

Customizing Information for Your Organization

You can create custom information for your team or for a specific site within your organization. Simply copy and paste the contents of a help window to a word processor. Then add your own site-specific information or specific procedural information for your tasks to the help text. This can save you time when writing your own training or procedural manuals.

Using Online Help Independently from the Software (Windows only)

The NNM help system on the Windows operating system is designed so that you can copy the help volume onto a diskette, take it with you, and run it independently of the software—whether on your home computer or traveling with you on your laptop.

Copy the following files to a floppy disk. These files are found in the *install_dir*\help\%LANG% directory:

- *help_file_name*.hlp
- *help_file_name*.cnt

Double-click on the *help_file_name*.hlp file to start the help system.

Using Dialog Box Help

The [Help] button in a dialog box explains the purpose of the dialog box.

Using Symbol Pop-up Menu Help

The right mouse button pop-up menu on a selected symbol may contain a help item for that symbol. You can customize this menu through the application registration file (ARF) to add a help topic if it does not already contain one.

Tip of the Day

When you start NNM on the Windows operating system, the Tip of the Day appears. Add new tips by editing the *install_dir*\help\%LANG%\tipOfTheDay.txt file. Turn off Tip of the Day by removing the check from the Show tips at startup check box located in the Help:Tip of the Day menu.

Manuals: Printed and Online

NNM includes a library of detailed reference materials for your use. Some are provided in printed form, some are provided online as PDF files. Get additional information from the online help or the release notes. The following manuals are provided with NNM.

- *Installation Guide for HP OpenView Network Node Manager*

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0787
3740
Doc:



This manual contains instructions about installing and configuring NNM.

- *Welcome to Network Node Manager*

  An overview of NNM, its features, and its capabilities.

- *Managing Your Network with HP OpenView Network Node Manager*

  This manual (that you are currently reading) contains detailed information to help network administrators configure, maintain, and troubleshoot NNM for their team.

- *Correlation Composer's Guide*

  This manual provides information about the HP OpenView Correlation Composer. You can use the Correlation Composer to create new event correlation logic. Be sure to read the information in Chapter 11, "Event Reduction Capabilities: Getting to the Root Cause," on page 351 before you start.

- *Guide to Scalability and Distribution for HP OpenView Network Node Manager*

  This advanced manual outlines the steps you need to take to deploy NNM across multiple management stations within your organization. It contains specific configuration procedures for using the scaling and distribution features of NNM. These features are important when the size of your organization's network exceeds the resources of one NNM management station. They allow you to divide the work load among multiple management stations, yet share the network management information as needed.

- *Reporting and Data Analysis with HP OpenView Network Node Manager*

  This manual is available only online and contains information about configuring and using NNM's reporting and data warehouse features. This book also contains information about how to export the historical data collected by NNM for your use with other statistical analysis programs of your choice.

- *Creating and Using Registration Files*

  This advanced manual is available only online and contains information about how to create and modify NNM's registration files, customizing the appearance and behavior of NNM.

- *Integrating HP OpenView Reporter*

  NNM and HP OpenView Reporter can be integrated, so that Reporter can query the NNM data warehouse to generate reports that help you to solve real network problems. This manual shows you how to configure the integration, as well as how to run and view reports. It also describes the preconfigured reports that are provided.

To access the online manuals shipped with NNM, use the `Help` menu. When you choose `Online Manuals`, a list of manuals appears. Choose the manual you want to view, and follow the instructions in the viewer.

Numerous additional HP OpenView online manuals are available at the following web site: `http://www.docs.hp.com`

Release Notes

For information about NNM that becomes available after this book is published, refer to the `ReleaseNotes` directory or the `README.html` file on the CD-ROM.

Release notes are available on your hard drive after installing NNM. You can access the release notes from NNM's menu `Help:NNM:Release Notes` (or on the Windows operating system under `Start:Programs:HP OpenView:HP OpenView Online Documentation:NNM Release Notes`).

You can also launch the release notes in your web browser:

Windows:

install_dir\www\htdocs\%LANG%\ReleaseNotes\README.html

UNIX: `/opt/OV/www/htdocs/$LANG/ReleaseNotes/README.html`

NOTE In this manual, `C` and `$LANG` in directory listings are variables for the language currently in use. `C` contains the English version.

Reference Pages (Manpages)

Reference pages (Windows operating system) or manpages (UNIX operating system) document NNM configuration possibilities in much greater detail than you will find any place else. These pages include information about every possible parameter and available command line

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0788
3740
Doc:

option, as well as useful background information that may be helpful when troubleshooting issues. These pages are named according to the function or feature that they are documenting.

Throughout this book, you will be referred to specific reference pages (manpages) for more information about the topic being discussed. You may want to browse through this resource collection yourself. You will find many more reference pages than are mentioned in this book.

Accessing Reference Pages

On Windows operating systems, reference pages are provided through the help system. You can access them from these locations:

- `Start:Programs->HP OpenView->HP OpenView Online Documentation->NNM Reference Pages`.
- Any submap within NNM, through the `Help` menu.

TIP

If you are not sure which reference page to access for a specific issue, use the `Find` feature of the help system. `Find` searches every word in every reference page and provides a list of all places where the word appears. For example, if you want to learn about the `netmon` service's parameter choices and relationship to other services, type `netmon` in the `Find` dialog box.

Accessing Manpages

On HP-UX systems, the following procedure is just one suggestion for displaying or printing manpages. This procedure requires that you have manpages installed locally on your system. (If your network provides manpages remotely instead (for example, from a central server), then check with your system administrator about how to access them.)

1. Determine where on your system the manpage files are kept. Type

   `echo $MANPATH`

   You should see a list with one or more directories. Multiple directories will be separated by colons (for example, `/usr/local/man:/usr/man`). It is recommended that you check the contents of each directory to make sure it actually has manpage files in it.

If you do not see a list of directories or you get no response to the `echo $MANPATH` command, refer to the section "Establishing Universal Pathnames" in Chapter 5.

2. Determine what syntax and options the `man` command is using. At a command-line prompt, type:

   `strings /usr/bin/man | grep col`

   You should receive a message similar to the following:

   ```
   tbl -TX %s |neqn|nroff -h -man|col -x > %s
   tbl -TX %s |neqn|nroff -man|col -x|%s
   ```

3. Use the command syntax shown in Step 2 in one of two ways:

   - Specify the qualified path of the directory containing manpage files as the `%s` value in the command.

     Example: you know that the *bggen*(1) manpage is stored in the `/usr/man/man1` directory on your system, but you are not currently in that directory. To display this manpage online, type the following command:

     `tbl -TX /usr/man/man1/bggen.1 |neqn|nroff -man|col|more`

     Example: to send the *bggen*(1) command's manpage to a file for printing instead, type the following:

     `tbl -TX /usr/man/man1/bggen.1 |neqn|nroff -man|col > /filename`

   - `cd` to the directory on your system that contains manpage files. Then specify just the command name and number as the `%s` value.

     Example: you are in the `/usr/man/man1` directory. Display the *bggen*(1) command's manpage online by typing:

     `tbl -TX bggen.1 |neqn|nroff -man|col| more`

     Example: to send this manpage to a file for printing instead, type the following:

     `tbl -TX bggen.1 |neqn|nroff -man|col > /filename`

On Solaris systems, consult your system documentation for information on accessing manpages online or printing them.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0789
3740
Doc:

The contrib Directory

The NNM `contrib` directory is a collection of programs and extensions to existing NNM programs that HP programmers have developed and want to share with NNM users.

The `contrib` directory contains a README file explaining the files in the directory. Many of the individual programs have README files as well, which contain information specific to the program.

When you install NNM on a UNIX operating system, the `contrib` directory is installed by default.

To install the `contrib` directory on a Windows operating system, you must use the "Custom Installation" feature.

The files are installed in:

Windows: *`install_dir`*`\contrib\NNM`

UNIX: `$OV_CONTRIB/NNM`

These programs are not supported by Hewlett-Packard and, as such, you use them at your own risk.

The support Directory

The NNM `support` directory is a collection of programs and Perl scripts that HP support engineers have developed and want to share with NNM users.

The `support` directory contains a README file explaining the files in the directory.

When you install NNM on a UNIX operating system, the `support` directory is installed by default.

To install the `support` directory on the Windows operating system, you must copy and paste the `support` directory from the NNM Installation CD to the management station's hard drive. Place the `support` directory in the following location:

The files are installed in:

Windows: *`install_dir`*`\support\*.*`

UNIX: `opt/OV/support/*`

These programs are not supported by Hewlett-Packard and, as such, you use them at your own risk.

White Papers

White papers are documents that explain various technical aspects of NNM and network management in general. Often these topics are not documented elsewhere.

When you install NNM on a UNIX operating system, the current white papers are installed by default.

To install the white papers on a Windows operating system, you must use the "Custom Installation" feature.

The white papers are installed in:

Windows: `install_dir\Doc\WhitePapers`

UNIX: `$OV_DOC/WhitePapers`

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0790
Doc: 3740

Resources and Services Available Through HP

You can find more information from the following sources:

- HP web sites
- HP Consulting Services
- HP Education
- HP Product Support
- OpenView Forum

HP Web Sites

General Information

Using a web browser, you can learn more about HP OpenView by visiting the main HP OpenView web page at: `http://openview.hp.com`.

This web site contains information on current products, as well as literature that you can print or download for viewing. There are links to HP technical support and sales offices.

Product Manuals

There is also a web site for accessing current HP OpenView product technical manuals that you can download and print. These manuals are available in PDF format. Its URL is:

`http://openview.hp.com`

Click on the `Support` icon, then select `Manuals`.

Another web site presents HP OpenView product manuals in searchable web-based format: `http://www.docs.hp.com`.

HP Consulting Service

The HP Consulting Service provides a wide range of consulting services, including initial installation and configuration, and network planning and organization. They can also help you plan and implement advanced strategies to help you take the best advantage of NNM's capabilities to

meet the specific needs of your organization. For more information about their services, visit the main HP Conculting web site, `http://www.hp.com/go/consulting`.

HP Education

HP Education presents numerous classes on Network Node Manager and HP OpenView, geared toward different levels of training. For more information about course descriptions and class schedules, visit the main HP OpenView web site, `http://openview.hp.com`.

HP Product Support

HP has more than 40 Response Centers worldwide offering telephone support in native languages and time zones. To register for telephone support, contact your local HP sales representative, or browse the HP OpenView web site at `http://openview.hp.com`.

In addition, HP offers software and materials support contracts so that you can automatically receive the newest versions of applications as they are available.

OpenView Forum

OpenView Forum is an association of users and developers of HP OpenView network and system management solutions. An independent corporation, the OpenView Forum represents a vast body of practical knowledge and experience provided through conferences, a web server, an email reflector, and personal contacts.

The OpenView Forum online discussion center provides members with a place where they can gain information and knowledge, and provide feedback to software developers about HP OpenView products.

OpenView Forum sponsors a conference each year, which is attended by vendors and more than 1000 Forum members. You can find out more about OpenView Forum at their web site: `http://www.ovforum.org`.

REQ Nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 0791
3740
Doc:

Summary of HP OpenView Web Sites

Table 3-1 presents a summary of the HP OpenView Web sites.

Table 3-1 Summary of HP OpenView Web Sites

HP Web Site	Contents
openview.hp.com	The primary web site for HP OpenView. Contains links to: HP OpenView training information Product literature Product manuals
www.hp.com/go/consulting	HP Consulting Services
www.docs.hp.com	Product manuals in searchable web-based format.
openview.hp.com-click on support panel	Access to HP support.
www.ovforum.org	OpenView Forum's web site where you can exchange information with other OpenView users.

4 Planning Your NNM Configuration

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0792
3740
Doc:



In order to get NNM the most benefit from NNM, you will probably want to configure NNM for your particular environment. NNM is a powerful program that can be configured in many ways. You need to budget time for planning how you wish to configure NNM and time for actually doing the configuration.

In order to make the whole process run as smoothly as possible, this chapter explains the issues to consider as you begin:

- "Budgeting Time for Planning and Configuration" on page 81
- "Taking Over NNM from Someone Else" on page 82
- "Understanding the Network Information Needs of Your Organization" on page 83
- "Knowing Your Network" on page 87
- "Starting with a Well-Configured Network" on page 90

Budgeting Time for Planning and Configuration

NNM is an extremely flexible program that can be configured to meet a large number of business needs. Read through this entire chapter before you begin configuring NNM. Clearly identify the specific ways in which you will use NNM to assist you in managing your management domain, to minimize the time you spend configuring NNM.

Time for Planning

If your management domain is small, this planning process could be quick. If your management domain is large and complex, it may take multiple meetings to gather the information that you need.

Time for Configuration

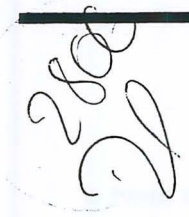
A quick sketch of the configuration process outlined in this book is:

- Install NNM--initial discovery, customization, and troubleshooting.
- Establish backup procedures for NNM's critical files.
- Configure NNM's active polling configuration.
- Configure the maps.
- Configure the event monitoring system.
- Decide what historical information is most useful, and establish data collection toward that objective.
- Establish the maintenance procedures and schedule.

Network management is complex and specific to each organization's needs. NNM can best assist you to meet your network management goals if it is optimally configured. Allow sufficient of time for the configuration process.

You need to have a clear idea about what devices you want to monitor, what kind of information you need from these devices, and how often you need the information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0793
3740
Doc:



Taking Over NNM from Someone Else

If you are responsible for taking over after someone else installed and configured NNM, browse through the chapters in this book in the order in which they are presented. As you read along, rather than configuring NNM, simply access all the configuration points as they are described to determine how NNM is currently configured. Once you understand the current configuration, you can go back through the process and implement your own ideas.

Understanding the Network Information Needs of Your Organization

To use NNM to its full potential, start with a clear idea of the business needs that NNM must address. You need to understand the groups within your organization and their information needs. You also need to start with a good understanding of your network itself.

Who Needs What Information?

First identify the groups within your organization who need access to information about the network. For example, upper management, facilities, technical support, and the printers group.

Then, identify what information each group needs, why they need it, and how they will use the information. For example, do they need real-time monitoring of specific devices around the clock or only during specific shifts for network troubleshooting? Do they need to know monthly trends of the volume of network traffic generated by each department for planning purposes?

Use the work sheet provided (page 85) as a starting point and detail the information needs of each group. Then decide which groups could share a map. Have a clear idea about what information everyone needs and how they want to receive that information before you start.

Ideal Uses for Maps

- At-a-glance notification that something has gone wrong.

  NNM's color-coded status notification alerts your team members immediately when a network or device is in trouble.

- Connectivity at-a-glance.

  A visual untangling of your network, the definitive authority of how everything is connected. The map is kept up-to-date automatically.

- Simultaneous monitoring of multiple sites.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0794
3740
Doc:



NNM can span multiple sites. In addition to NNM's map and alarm list, NNM's pull-down menus provide troubleshooting tools that allow your team to gather information and troubleshoot problems at the remote site.

- Quick response time.

  NNM's maps can be configured with floor plans of your site to speed your team's efforts in investigating hardware failures. If your team has a high turn-over rate, well designed maps can reduce training time.

- Establishing sphere of influence or management regions.

  You can have different maps for different areas of responsibility on your network. A map can manage a specific physical portion of your network or partition information about your network. Maps can have specific constraints and characteristics, run different applications, cover different geographic areas, and/or set compound status differently. You can customize maps so that they become a projection of your team member's responsibilities, showing what your team member wants to see about your network without requiring him/her to sifting through unneeded data.

Ideal Uses for the Alarm Browser

- Instant awareness of failures.

  NNM's Alarm Browser guarantees the speediest possible response, since your team members know instantly when trouble arises.

- Watching trends.

  Configure NNM to post threshold alarms from your mission-critical devices. Your team members detect developing trouble and start resolving it before users encounter network failures.

- Identify the device that is most likely causing the problem.

  NNM's event correlation system identifies the source device of certain issues and consolidates all alarms that were generated as a result of the root cause issue under the main alarm message.

- Automate responses.

You can configure NNM to automatically page or email a specific person whenever an alarm is received about a specific device. You can also configure a pop-up window to appear over the NNM map if a certain event occurs or launch any customized action that you wish.

- Facilitate team communication to eliminate duplicate efforts.

  Your support team can use NNM's Alarm Browser as a prioritized to-do list. Each team member can select issues to work on and change the alarm's status to *Acknowledged.* Everyone on the team will see immediately that the alarm is being addressed.

- Distribute responsibility.

  You can set up custom categories for incoming alarms and configure specific devices to post their alarms to your custom categories. For example, configure the alarms generated by devices in each department to post their alarms to a category identifying the department. Your team members can access the alarm list that applies to them, without needing to sort through alarms for all departments.

Work Sheet for Planning

Group/user: _____

Role/purpose: _____

Organization/Location: _____

Hours/shift: _____

Email address: _____

Phone number: _____

What do they need to know?

How often do they need this information?

Why do they need to know?

Which devices do they need to monitor?

RQS nº 03/2005 - CN
CPMI 85 CORREIO
Fls. Nº 0795
3740
Doc:

What type of system will they use to access NNM?

Which MIB value or MIB expression would provide access to this information?

What would be the most beneficial form in which to receive the information?

___ Map displayed on a monitor (map configuration)

___ Alarm list (event configuration)

___ Email (automatic action programmed through Event configuration)

___ Pager message (automatic action programmed through Event configuration)

___ Web site access

___ Reports

Knowing Your Network

You probably maintain lists of the devices that are currently installed on your network. Use your current lists when first installing NNM in order to verify that everything has been successfully discovered. Your lists will also be useful while deciding how often NNM should monitor each device for you.

Deciding to Manage or Not to Manage Devices

Because NNM is actively polling your network devices over standard network protocols (ICMP, SNMP, and IPX), a certain amount of network traffic is generated for each managed device. You need to determine the appropriate polling frequency in your business environment. Identify the mission-critical devices on your network, typically your routers, switches, hubs, and key servers. You will want to configure NNM to monitor these devices most frequently. NNM allows you to configure groups of devices by using wildcards or a number of other identifiers. Therefore, if you have a clear idea of where you are heading, the configuration process will be much easier and quicker.

For planning purposes, consider grouping your network devices into three network management categories:

- Mission-critical devices.

  You will monitor these devices aggressively, perhaps configuring NNM to poll them two or three times per minute to verify that continuous service is available. You may want to use NNM's event configuration to maximize the use of information available through these devices' SNMP agents and MIB files. Also consider collecting performance data for later trend analysis. Balance your desire for data and polling against the overhead you are imposing on devices.

- Important, but not critical.

  You will configure NNM to monitor these devices less frequently: perhaps your printers, certain application servers, firewalls, http proxies, etc. Depending on the situation at your site:

  — Every few minutes?

  — Every few hours?

ECT Nº 03/2005 - CN
CPMI - CORREIOS
FLS. Nº 0796
3740
Doc:

— Every few days?

- Devices that do not require active monitoring.

  Not important enough to warrant generating network traffic (for example individual PCs). Therefore, you can disable NNM's polling of these devices by setting them to *unmanaged* or you can configure polling to run very infrequently.

  Although you configure certain devices or groups of devices to be *unmanaged* by NNM, the device's SNMP agent can be configured to forward traps to the management station if anything goes wrong. These traps will appear as alarms in NNM's Alarm Browser once you configure them to do so by using NNM's event configuration feature.

  NNM can be configured either to include the unimportant devices on your maps or to exclude them from the map.

Work Sheet for Devices

Identify which devices on your network fit into the following groups. Your list will come in handy when you are troubleshooting NNM's initial discovery, when you are customizing NNM's polling configuration, and when you are creating customized maps for your team.

- Mission-critical devices.

  Must be frequently monitored on a proactive basis to ensure continuous service.

- Important (but not critical) devices.

  These devices can be monitored less frequently than mission-critical devices. For example: you may want NNM to monitor some devices every 30 minutes, or every 12 hours, or every 7 days. Decide upon meaningful monitoring frequencies for different groups of your network devices

- Devices that do not require network management.

  These devices do not require active monitoring (their SNMP agents can be configured to forward traps to the management station if anything goes wrong).

TIP

Network devices that did not show up on anyone's worksheet from the previous section in this chapter probably do not need to be actively managed by NNM.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0797
3740
Doc:

Starting with a Well-Configured Network

As explained in Chapter 2, "How Does NNM Work?," on page 49, NNM communicates with the devices on your network through standard network protocols. For NNM to gather accurate information, your network needs to be in a well-configured state so that each device can be successfully accessed.

The following aspects of a well-configured network do not need to be in perfect shape on your network before you install NNM. However, the closer you are to having a well-configured network, the quicker and easier it will be to configure NNM. Relevant issues include:

- Consistent IP addressing scheme
- Consistent subnet masks configured
- DHCP address ranges identified
- Consistent name resolution scheme (such as DNS or NIS)
- SNMP agents configured on each device:
  - — Know the agent's GET- and SET-community names
  - — Update the trap-forwarding (trap destination) list to include the NNM management station
  - — Know which MIB is being used and obtain a copy of it to load into the NNM management station's MIB database later on

Consistent IP Addressing Scheme

A list of your *network-level* IP addresses would be handy to have during the initial discovery process so that you can quickly verify that NNM has successfully discovered everything you need. This list could also be used to create a seed file to speed the discovery process.

Remember that all devices that you wish to manage must have a valid IP address. For hubs and other network devices that normally do not have IP addresses and enabled SNMP agents, it is often possible to manually establish them. Determine if the device can support SNMP, then physically visit each device or access it through a terminal and take the necessary steps to assign an IP address and enable the SNMP agent. Contact the device's vendor if you need more information.

Subnet Masks Consistently Configured

If the subnet masks on the management station or configured on your network devices are incorrect, discovery may be different from what you expected. If the subnet mask is too restrictive, you won't discover your whole management domain. If the subnet mask is not restrictive enough, you discover more than you bargained for.

Non-contiguous subnet masks (for example, 255.255.0.255) are not supported by NNM. Also, in hierarchical subnets, two subnets having the same IP subnet address but different subnet masks are not supported. See the white paper about subnet masks ("White Papers" on page 75) for more information.

TIP NNM does not detect proxy ARP (an alternative to defining extensive routing tables). If NNM is running in an environment using proxy ARP, alarms about misconfigured subnet masks are generated. In this case, these alarms can be ignored.

DHCP Address Ranges Identified

HP strongly suggests that you assign a range of IP addresses to be randomly assigned to mobile computers when they access your network. NNM can handle this range of addresses in a way that does not cause problems as users hook up to and disconnect from the network.

Consistent Name Resolution Scheme

NNM depends upon your network name resolution scheme being in good working order (DNS, NIS, NIS+, NetBios, local hosts files). NNM cannot conduct successful discovery if it is receiving inaccurate information. NNM will exhibit performance problems and erratic behavior when your name resolution scheme is not working. If you have name resolution in place prior to NNM's initial discovery process, hostnames are used for map symbol labels, rather than IP addresses. Hostnames generally make the NNM maps and alarm messages more meaningful to your team.

If you are using DNS, it is recommended that the management station be a caching or secondary name server. Ensure that the management station secondary name server is not serving any other clients.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0798
3740
Doc:

NOTE Point your web browser to `http://www.docs.hp.com` and search for a document titled *Installing and Administering Internet Services* (part number B2355-90147). This document contains information about configuring a caching-only name server.

Quick Check of Your Name Resolution Scheme

To test the health of the name resolution implementation before installing NNM, try the following procedure.

1. Find the `gethost.exe` tool (provided on the NNM installation CD) and copy it to the hard drive of the machine where you will install NNM.

   Windows: *`CD-ROM drive`*`:\support\gethost.exe`

   UNIX: Mount the CD drive,
   `/cdrom/OVDEPOT/OVNNMgr/OVNNM-RUN/opt/OV/support/gethost`

2. Choose an IP address that is not in use on your network.

3. Navigate to the directory where you copied `gethost`. At the command prompt type either:

`gethost -a -i bogusIPaddress`

`gethost -i realHostName`

4. If you receive an immediate answer, your name resolution scheme is in good shape. If your system hangs while trying to formulate an answer, clean up your network name resolution before installing NNM.

NOTE To test the health of the name resolution implementation after installing NNM, see "Opening NNM takes a long time" on page 133.

SNMP Agents and Their MIBs Configured

The SNMP agent on each network device responds to GET and SET requests from NNM and continuously monitors the device upon which it resides. The agent generates and sends SNMP traps to NNM whenever an error condition arises that is defined in the agent's MIB file.

Configure each SNMP agent's community names and trap destination list specifically for your particular network. Obtain a copy of the agent's MIB file so that you can configure NNM to take full advantage of all the management capabilities provided by the agent.

If an SNMP agent is not currently installed on a network device that you need to monitor, contact the vendor of the device.

GET- and SET-Community Naming Scheme

Community names are a lightweight security technique employed by SNMP agent software. If the network management software wants to communicate with the SNMP agent software, both must use the same community name during GET and SET requests and talk over the same port. By default, community names are often set to PUBLIC and the port is set to 161. NNM assumes that these defaults are in use unless you inform it otherwise. Many network administrators change the GET-community name so that hackers cannot obtain sensitive information about their devices. It is even more common for network administrators to change the SET-community name, since knowing this community name enables others to make system configuration changes to the device itself, either inadvertently or maliciously.

In order to work, NNM depends upon successful communication with the SNMP agents installed on your network devices. If the community names have been changed from PUBLIC or the port changed from 161, you need to inform NNM of the new ones. (NNM cannot obtain these automatically because that would defeat the security feature.) NNM tests community names in the file `netmon.cmstr`. See "GET- and SET-Community Name and SNMP Port Issues" on page 145.

Trap Destination List Updated to Include the NNM Management Station

The SNMP agent software continuously monitors its device for error conditions defined in the installed MIB. When an error condition is detected, a trap message is automatically forwarded to all devices listed in the agent's trap-forwarding list. When configuring the SNMP agent on

POS em 08/2005 CN
CPMI - CORREIOS
Fls. Nº 0799
3740
Doc:

each network device, configure the agent's trap forwarding list (or trap destination list) to include the NNM management station's host name or IP address. NNM will then receive traps from the device and keep you informed. Refer to the agent's documentation for information about how to do this. See "Ensuring that NNM Receives Traps from Your Network Devices" on page 325.

TIP

HP-UX systems only: For hosts with HP OpenView SNMP agents, NNM automatically updates the trap forwarding list when the device is discovered, provided that the correct SNMP SET-community name is configured within NNM. See "GET- and SET-Community Name and SNMP Port Issues" on page 145.

Obtain a Copy of the SNMP Agent's MIB File

Often vendors provide custom MIB files that define specific objects for monitoring the particular device. Be sure to request a copy of the custom MIB so that you can install it into NNM's MIB database later on.

NOTE

List of all of the MIBs in use on your network devices. These same MIBs will need to be installed on the NNM management station. See "Loading MIBs in the MIB Database" on page 413. After you install the MIB you can configure NNM to handle each trap as you wish. See "Event Configuration Overview" on page 422.

To obtain the most recent version of a MIB file, check NNM's installation CD, contact the vendor who wrote the MIB file, or search the website `ftp://ftp.isi.edu/mib/` for quick access to the MIB file. Make sure the MIB file that you load onto the management station's MIB database is the same version being used by the SNMP agent on your network device.

DMI Service Providers and Their MIFs Configured

If your management station uses a Windows operating system, NNM **automatically subscribes** to receive DMI events from all managed systems running DMI version 2.0.

Keep track of any vendor-specific MIF files being used on these devices. Your list will come in handy later in NNM's configuration process. If your DMI service provider software is using a vendor-specific MIF instead of or in addition to the DMTF's standard MIF, during NNM's configuration process you must configure NNM to understand the custom MIF events.

For information about configuring DMI MIFs, see "DMI Events (Indications)" on page 327, "DMI Browser" on page 417, and "Loading DMI-to-SNMP Event Mappings" on page 419.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0800
3740
Doc:

5 Initial Network Discovery: Options and Troubleshooting

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 0801
3740
Doc:

The first step toward configuring Network Node Manager (NNM) is to install the software and allow initial discovery to run.

NNM automatically discovers each device on your network and its connective relationship to other devices. NNM's object and topology databases store the discovered information and NNM uses this information to draw the default map and set up the event tracking system. After initial discovery has run to completion, you use the map to identify and fix problems on your network.

Often, network administrators with routed environments simply start NNM and allow it to run initial discovery with the default settings. By default, your management domain consists of the network indicated by your *management station's IP address and subnet mask*. NNM discovers everything to the edges of that network and **manages** (monitors) the devices discovered up to the number in your license agreement limit.

If you need to manage multiple networks, you can *add* them to the management domain by:

- Manually selecting symbols on the map and setting them to *managed* (see "Interactively Expand/Limit Your Management Domain" on page 117).
- Automatically setting devices on multiple networks to *managed* by creating and using a seed file, using the `loadhosts` program, and/or increasing the IPX-Hop Count (see "Automatically Expand Your Management Domain" on page 119).

In very large enterprises and bridged environments, the initial discovery process may detect such a large number of devices that managing them all would exceed your organization's and your management station's resources. In this case, you may want to *limit* the number of devices included in the initial discovery process. You can limit initial discovery so that it only includes your organization's mission-critical devices by:

- Manually selecting unimportant symbols on the map and setting them to *unmanaged* (see "Interactively Expand/Limit Your Management Domain" on page 117).
- Creating and using a `netmon.noDiscover` file that specifies which devices to *exclude* from the discovery process, using the `loadhost` program to discover only the devices on your list, creating and using a *discovery filter* that controls which devices or types of devices to

include in the discovery process, using the `oid_to_type` file to unmanage groups of devices, and/or decreasing the IPX Hop Count (see "Automatically Limit Your Management Domain" on page 124).

If your network is quite large, but you don't want to eliminate devices from the management domain, you can visually break the map into smaller units or create multiple maps that draw information from the same databases. You can use the hide feature or map filter to show different aspects of your network on each map. See Chapter 8, "Map Customization," on page 211.

It is also possible to use multiple management stations in a hierarchical arrangement that divides up the management responsibility yet shares critical information. See *A Guide to Scalability and Distribution* for more information.

You start benefiting from NNM immediately. This initial map discovery process may reveal configuration problems on your network, such as SNMP agents that are not communicating properly, incorrect subnet masks or DNS settings, mismatched community names, and unexpected connections to network segments that you do not own. The map is a visual representation of the communications channels established between NNM and the devices in your network. The accuracy of these links determines whether or not NNM can provide valuable information to help you manage your network. Be sure to follow the directions for verifying the accuracy of your maps (see page 109) and to fix any problems before continuing with further customizations to NNM (page 131).

TIP

Your company may have purchased multiple HP OpenView products. If you are using other HP OpenView applications in addition to NNM, you may notice that the menu choices and options provided within the software vary from what is presented in this book. This is because the other HP OpenView applications integrate closely with NNM to take advantage of the features that NNM already provides. Other HP OpenView programs build upon the foundation provided by NNM.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0802
3740
Doc:

Install Network Node Manager (if you have not already done so)

See the *Quick Start Installation Guide* included with the NNM Installation CD for instructions about how to install Network Node Manager. Make sure that your management station meets the minimum requirements before you start.

NOTE In this manual, `C` and `$LANG` in directory listings are variables for the language currently in use. `C` contains the English version.

Installing IPX Transport Software (Windows only)

For management stations running a Windows operating system:

IPX discovery is an optional component of Windows operating systems. If you want to discover and monitor IPX nodes, be sure to install the NWLink IPX/SPX Compatible Transport network software stack before or during the NNM installation process. These drivers are included with the Windows operating system installation software, but are not installed by default. See the *Quick Start Installation Guide* included with NNM's installation CD for more information.

Establishing Universal Pathnames (UNIX only)

For management stations running a UNIX operating system:

This book uses directory pathnames that are independent of the underlying file structure of the operating system you are using (see your data sheet to learn specifically which operating systems and versions this release supports). For each Network Node Manager directory, a single pathname is used rather than multiple pathnames that vary by system. For example, the pathname for the NNM log file is stated as `$OV_LOG` rather than `/var/opt/OV/share/log` for HP-UX 10.X, 11.X and Solaris 2.X systems.

Take the following steps to set up each user's environment. Setting the universal pathnames and paths as shown is temporary; you will need to do this every time you start a terminal window. Or you can permanently set each user's path by modifying the path in the appropriate files shown below:

If running sh or ksh: Modify the path in the `.profile` file.

If running csh: Modify the path in the `.login` file.

If running VUE: Modify the path in the `.vueprofile` file.

1. If you want to use the universal pathnames that have been incorporated into NNM, you need to *source* the file into your current environment. Use one of the following commands, depending on which shell you are running. If you are not sure which shell you are running, execute:

   ```
   echo $SHELL
   ```

NOTE Be sure to include a space between the `.` and the `/` in the `sh` or `ksh` commands.

If running sh or ksh:

HP-UX 10.X, HP-UX 11.X,
Solaris 2.X `. /opt/OV/bin/ov.envvars.sh`

If running csh:

HP-UX 10.X, HP-UX 11.X,
Solaris 2.X `source /opt/OV/bin/ov.envvars.csh`

See the *ov.envvars* manpage for additional information about this script and information about the universal pathname equivalents.

2. Set the path to include `$OV_BIN` and `$OV_MAN`. Execute the following commands:

   If running sh or ksh:

   ```
   PATH=$PATH:$OV_BIN
   MANPATH=${MANPATH:-/usr/man:/usr/share/man}:$OV_MAN
   export PATH
   export MANPATH
   ```

   If running csh:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0803
Doc: 3740

```
set path=($path $OV_BIN)
if (${?MANPATH} == 0)setenv MANPATH "/usr/man:/usr
/share/man"
setenv MANPATH "${MANPATH}:${OV_MAN}"
```

NOTE All NNM documentation referring specifically to a UNIX operating system assumes that you have activated the universal-pathname environment variables.

For example, a written procedure might include the following step:

```
cd $OV_BACKGROUNDS
```

This command takes you to the local directory containing submap backgrounds, and it works regardless of which version of the UNIX file system is involved. Note that if you need to know the actual pathname, you can always enter a command like the following:

```
echo $APP_DEFS
```

The response to this command will be the actual local pathname:

- *HP-UX*: `/usr/lib/X11/app-defaults`
- *Solaris 2. X:* `/usr/openwin/lib/app-defaults`

Discover the Network... Let NNM Do It

Let NNM do the work discovering your network for you. NNM sets up several databases, creates the default map, and establishes communication links for tracking events on your network.

Overview

First NNM's services (background processes) are started. Expect intense polling traffic at first as the network monitoring service, `netmon`, works as quickly as possible to discover each device on your network. An `ICMP ping` is issued for each device identified in any found ARP table and an `snmpwalk` command is issued to gather information about each discovered device. If a serial WAN link is discovered, NNM checks the router's routing table for clues about how to continue with discovery. The frequency of polling for new nodes automatically decreases as fewer new objects are discovered per polling cycle.

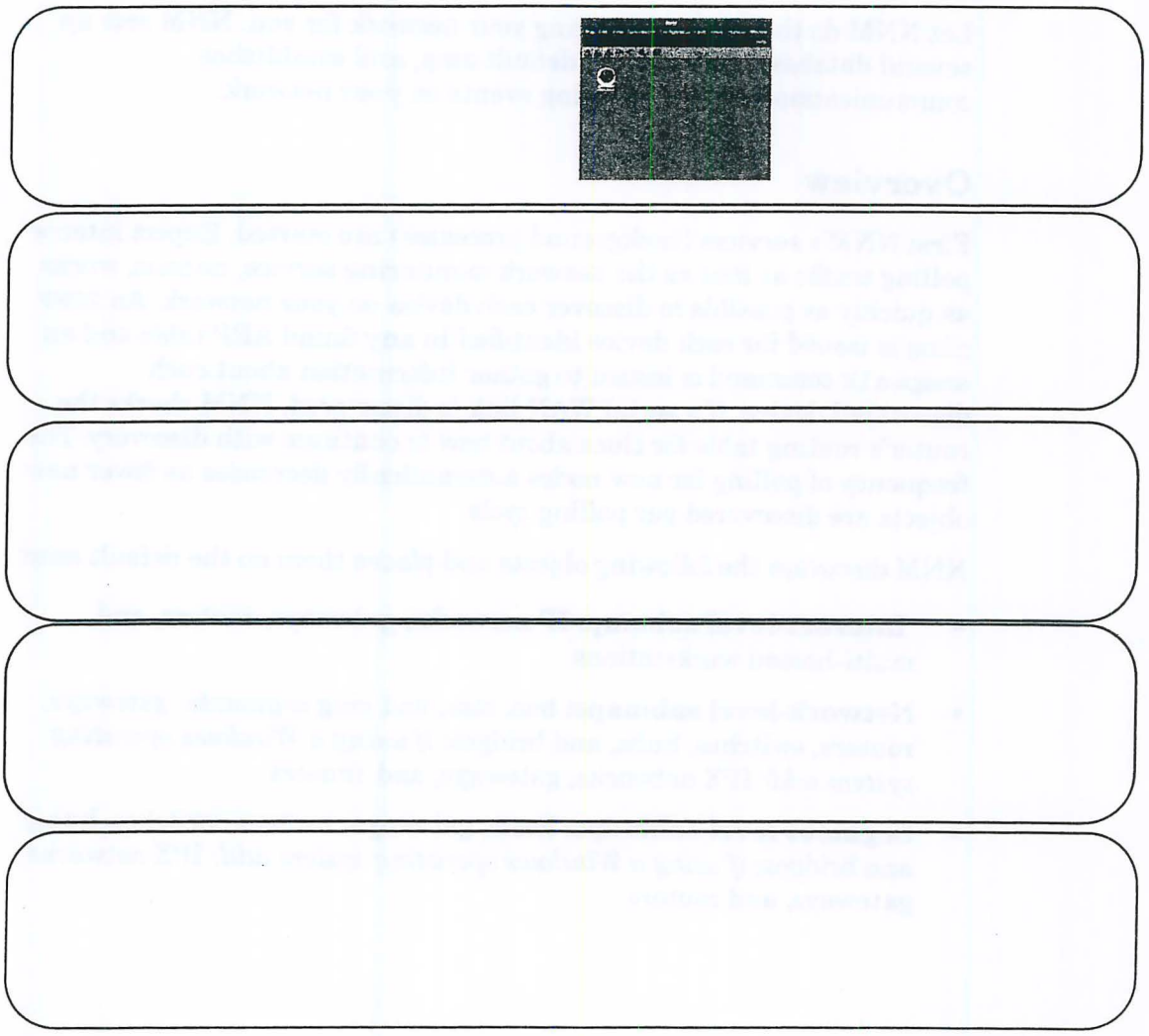
NNM discovers the following objects and places them on the default map:

- **Internet-level submap:** IP networks, gateways, routers, and multi-homed workstations
- **Network-level submaps:** bus, star, and ring segments; gateways, routers, switches, hubs, and bridges; *if using a Windows operating system add:* IPX networks, gateways, and routers
- **Segment-level submaps:** hosts, gateways, routers, switches, hubs, and bridges; *if using a Windows operating system add:* IPX networks, gateways, and routers

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0804
Doc: 3740

- **Node-level submaps:** network interface cards

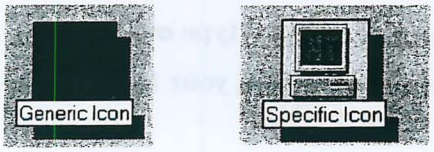
Figure 5-1 A Typical Hierarchy of Persistent Submaps



NNM uses the information about each device gathered by `netmon` to determine the most accurate and descriptive symbol to use on the map. If NNM cannot match the `sysObjectID` to a specific symbol type, the node will be represented as a generic symbol on the map (a shape without a specific descriptive icon inside of the shape). For example, some IP nodes

that are not computers (connectors such as bridges and repeaters) may initially appear on the map as hosts. See "Troubleshooting Discovery" on page 131 for more information.

Figure 5-2 **Generic Computer Icon versus Specific Descriptive Icon**



NOTE

NNM determines which symbol to use for each device by referencing the information contained in two configuration files:

- *Windows:*

  ```
  install_dir\conf\oid_to_sym
  install_dir\conf\oid_to_type
  ```

- *UNIX:*

  ```
  $OV_CONF/oid_to_sym
  $OV_CONF/oid_to_type
  ```

Although the entries in these files are already extensive, you may encounter a situation where you want to make additions or changes to these files. For example, if you see a generic icon on the map and wish to assign a specific icon or if you want to create your own new icons. See the instructions at the beginning of each of these ASCII files. See also the *oid_to_type* and *oid_to_sym* reference pages in NNM's online help (or the UNIX manpages) and Appendix D, "Changing All the Symbols for a Particular Device," on page 661 and Appendix E, "Changing an Object's Vendor and SNMP Agent," on page 675 for more information.

Start the NNM Services (background processes)

NNM starts collecting the information needed to draw the default map as soon as you start the NNM services. The services continually monitor the network and track activity. You need to start them the first time you use NNM; thereafter, they run continually whether or not you have the NNM user interface open. To learn more about these services, see Appendix A, "NNM Services and Files," on page 539.

RQS nº 03/2005 - CN - CPMI CORREIOS
Fls. Nº 0805
3740
Doc:

To start the services (background processes):

- *Windows:*
  Select `Start:Programs:HP OpenView: Network Node Manager Admin->NNM Services - Start`.
- *UNIX:*
  As root, at the command prompt, type **ovstart**

  The `$OV_BIN` directory must be in your `PATH`. If not, you must type **$OV_BIN/ovstart** to start NNM.

  See the *ov.envvar* manpage for a complete list of the universal pathnames and their equivalents, and information about a script for setting up environmental variables that will create the pathnames on your system.

Make Sure NNM's Services Are Successfully Running

To generate a status list of the services that make NNM work:

- *Windows:*

  Select `Start:Programs:HP OpenView:Network Node Manager Admin->NNM Services - Status`
- *UNIX:* At the command line prompt, type **ovstatus -c**.

TIP Type **ovstatus -c** for concise, one-line-per-process information.

If any of the services are not successfully running, see Appendix A, "NNM Services and Files," on page 539 for information about troubleshooting services before continuing.

Open NNM

Opening NNM takes a few minutes as the maps are synchronized with the databases. To start NNM's user interface (foreground processes):

- *Windows:*
  Select `Start:Programs:HP OpenView:Network Node Manager`.
  NNM automatically starts all installed and registered applications.

- *UNIX:* At the command prompt, type **ovw**. NNM automatically starts all installed and registered applications.

Configure an Inventory Report

Use the web Reporting interface to configure an inventory report. An inventory report lists the network nodes that are contained in the topology database, organized by subnet. You can use this report to help verify the accuracy of the initial discovery of your network. Refer to the online help for more information on configuring an inventory report.

Let NNM Run Over Night to Populate the Maps

The initial discovery process takes time. We recommend that you let NNM run over night to gather the majority of network information available. As NNM maps your network, it constantly rearranges icons. Therefore, it is best to wait until initial discovery has finished before exploring the default map.

NNM gathers information to the limits of the network indicated by the management station's IP address and subnet mask. NNM then checks the ARP table on each discovered device and expands the map by adding devices listed in each ARP table to the map. NNM also detects serial WAN links (for which ARP caches have no entries) and then checks the resident routing table instead. Devices listed in the routing table are then discovered and the process continues. NNM follows this process each time communication is established with a device, so your maps will continue to grow over time. (See Chapter 2, "How Does NNM Work?," on page 49 for a more detailed explanation about how NNM discovers network information.)

NOTE

While NNM discovers and maps your network information, explore the *Get Acquainted with HP OpenView Network Node Manager: Training for NNM Operators* CD provided with NNM so that you will understand what you are seeing after the discovery process is complete.

After NNM completes initial discovery, verify the accuracy of the map (see page 109), making sure that any devices that you have identified as mission-critical in Chapter 4, "Planning Your NNM Configuration," on page 79 appear on the map. Then fix any problems by:

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0806
Doc: 40

- Interactively expanding or limiting your management domain (see page 117).
- Automatically expanding your management domain (see page 119).
- Automatically limiting your management domain (see page 124).
- Troubleshooting the initial map to ensure your network is configured properly (see page 131).
- Delete NNM's object and topology databases and restart discovery, if necessary (see page 161).

When you are satisfied with the accuracy and completeness of the initial map, go to Chapter 6, "Preserve Your Sanity: Backup and Polling Configuration," on page 163 to learn how to back up your work and to customize the polling configurations.

Verify the Accuracy of the Initial Discovery

Now that NNM has had time to map all the network connections discovered, take the time to make sure you recognize what was found. Refer to the checklists that you developed in Chapter 4, "Planning Your NNM Configuration," on page 79 to verify that all mission-critical devices are present.

Usually there are a few surprises on your map. NNM allows you to easily identify such things as connectivity problems and security risks. Take the time to fix any problems that you discover (see "Troubleshooting Discovery" on page 131).

This section includes information about NNM's tools that make verifying the information on your maps easier:

- Inventory report

  View or print the inventory report.

- Object properties information

  View a detailed description of the underlying object properties for the selected internet, network, segment, node, or interface symbol.

- Find object feature

  Locate map elements quickly using the `Edit:Find` menu item.

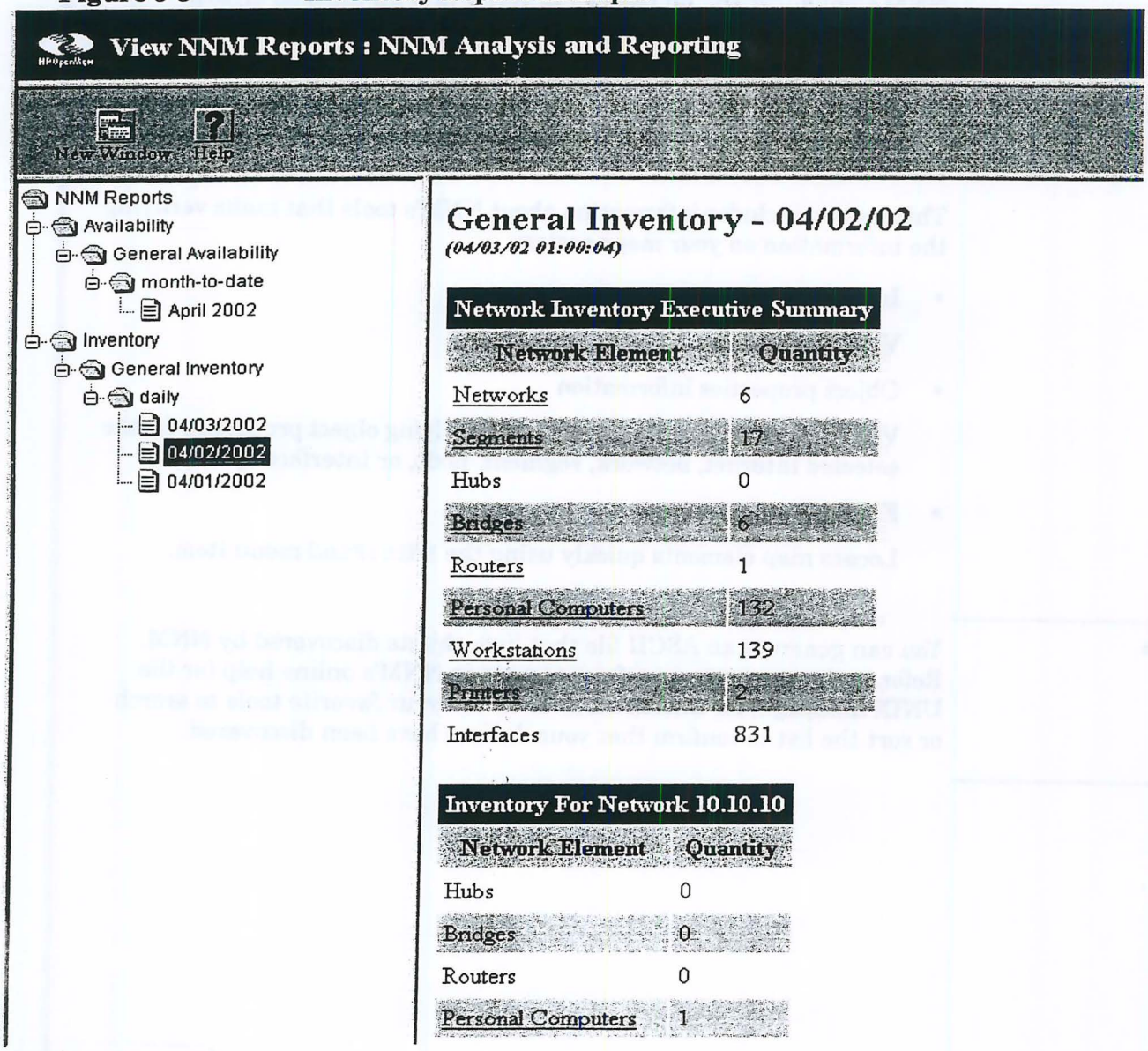
TIP You can generate an ASCII file that lists objects discovered by NNM. Refer to the *ovtopodump* reference page in NNM's online help (or the UNIX manpage) for information. Then use your favorite tools to search or sort the list to confirm that your devices have been discovered.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0807
Doc: 3740

Printing the Inventory Report

Use the inventory report to see a detailed list of what was discovered on your network. The inventory report lists the network nodes that are contained in the topology database, organized by subnet. An example of an inventory report follows.

Figure 5-3 Inventory Report Example



From the Network Inventory Executive Summary, you can click on entries in the Network Element column to see more details.

See the NNM online help for more information on the web Reporting interface.

Viewing the Properties of Your Network Configuration

You can gain quick access to the `IP Map` service's information that describes your network and system configurations. The information in the dialog boxes for object properties can help you determine if everything is present and accounted for on the initial map.

Viewing Object Descriptions

You can view the object properties for any network element that NNM manages, such as an internet, network, segment, node, or interface. The object database maintains this information. Object properties are always as current as NNM's last polling cycle.

Description of an Internet Object Simply select the Internet symbol on the root submap and right-click with the mouse. Select `Object Properties` and select `IP Map`. See NNM's online help for more information and specific directions. NNM provides the following information:

- number of networks on the internet
- number of segments on the internet
- number of nodes contained within the internet
- number of interfaces contained within the internet
- number of gateways/routers on the internet
- any status or error messages may appear in the `Messages` field

Description of a Network Object Simply select any network symbol on the map and right-click with the mouse. Select `Object Properties` and select `IP Map`. See NNM's online help for more information and specific directions. NNM provides the following information:

- the network name as it appears on the map
- network address

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0808
3740
Doc:

- subnet mask associated with the network number
- status of the network
- number of segments on the network
- number of nodes contained within the network
- any status or error messages may appear in the `Messages` field

Description of a Segment Object Simply select any segment symbol on the map and right-click with the mouse. Select `Object Properties` and select `IP Map`. See NNM's online help for more information and specific directions. NNM provides the following information:

- status of the segment
- number of nodes on the segment
- any status or error messages may appear in the `Messages` field

Description of a Node Object Simply select any node symbol on the map and right-click with the mouse. Select `Object Properties` and select `IP Map`. See NNM's online help for more information and specific directions. NNM provides the following information:

- hostname that was assigned when the node was initially discovered
- status of the node
- information about and status of each interface installed on the node
- system description as returned by the SNMP agent (*)
- system location and system contact as returned by the SNMP agent (*)
- system object ID of the node (*)
- any status or error messages may appear in the `Messages` field

* The node must support SNMP to return this information.

Description of an Interface Object Simply select any interface symbol on the map and right-click with the mouse. Select `Object Properties` and select `IP Map`. See NNM's online help for more information and specific directions. NNM provides the following information:

- address of the interface

- subnet mask (IP only)
- link-level address (physical address)
- interface type
- status
- any status or error messages may appear in the `Messages` field

Finding Specific Devices on the Map

The `Edit:Find` menu item enables you to search for objects that contain a common characteristic. You can:

- Find objects in either the open map or an open snapshot based on the value of a specific attribute.
- Create a selection list of objects with particular characteristics, such as all routers.
- Open the submap of each found object.

You can find objects based upon these object and symbol characteristics (see page 205 for more information):

- Selection Name

  You can find objects based on a selection name or part of a selection name.

- Attribute

  You can search for objects based on the values of chosen attributes, such as `isRouter`.

- Comments

  You can search for all objects that have a specific comment or portion of a comment. You may establish conventions for embedded keywords and use these in the `Find By Comment` operation. In this manner, you can find objects based on a key that is not a supported attribute.

- Symbol Status

  You can find objects that are represented by a symbol with the given status. Each found symbol is listed separately.

- Symbol Type

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0809
Doc. 3740

You can find all objects that have a symbol of a given type (class and subclass).

- Label

  You can search on the label string (comments added by you).

Entering Strings in Find Operations

When you select `Edit:Find`, input in the form of a string value is sometimes required. For several operations, you have a choice between two types of searches: exact match and pattern matching.

Exact Match — Exact match finds only those objects whose attribute value exactly matches the string entered. To switch to the exact match search, click on the `Exact Match` radio button. You must enter the complete string in this mode.

Pattern Matching — When pattern matching is used, you may enter a simple substring or a regular expression. The following section, "Regular Expressions," discusses some of the special characters you can use in regular expressions.

A valid regular expression may consist completely of printable characters. However, in a regular expression, certain symbols have special meaning; see the following table. (*HP-UX only:* more regular expressions are available, see the *regexp* manpage.)

Table 5-1 Regular Expressions for Pattern Matching

Special Character	Meaning	Examples

. (period)	Matches any single printable or nonprintable character except <newline> (unless it is used inside brackets).	`node.in` matches:
		`node3interface`
		`nodeXinterface`

Table 5-1 Regular Expressions for Pattern Matching (Continued)

Special Character	Meaning	Examples

* (asterisk)	Means zero or more occurrences of the preceding character.	`node*` matches:
		`nod`
		`node`
		`nodeTwo`
		`nodee`

^ (Caret)	If the caret is the first symbol, then the following string must be the first part of any matching string.	`^Box` matches the string:
		`Box elder`
		but does not match the string:
		`Big Box`

$(dollar)	If dollar is the last symbol, then the preceding string must be the last part of any matching string.	`long$` matches the string:
		`belong`
		but does not match the string:
		`longer`

Results of the Find Operation

NNM reports all found objects to you in the dialog box. The `Message` area reports the results of the search. It will display:

- the number of objects found
- errors
- further instructions

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0810
3740
Doc:

Symbols of found objects are listed by selection name in the `Located and Highlighted` area. If a found object is represented by multiple symbols, each symbol is displayed on a separate line.

Table 5-2 Results of the Find Operation

Parameter	Meaning
`Selection Name`	The selection name of the object.
`Submap Name`	The name of the submap that displays a symbol of a found object.
`Symbol Label`	The symbol label as it appears on the submap.

The following three example entries display one found object and three symbols that represent the object in three different submaps:

```
NodeBob:lanCard:IP address [connection to segment]
NodeBob [connection to segment]
NodeBob [hostname]
```

The symbols of found objects are highlighted on submaps.

Interactively Expand/Limit Your Management Domain

The NNM default map includes any devices that have already been discovered. You control which of these devices are **managed** (monitored by NNM's services) and which of these devices are **unmanaged** (placed on the map as a light-tan icon, but not monitored by NNM services). NNM does not actively monitor unmanaged devices through polling. However, you can still configure each unmanaged device's SNMP agent or DMI service provider to forward traps to the NNM management station's event tracking system (see "Ensuring that NNM Receives Traps from Your Network Devices" on page 325).

Normally, you customize the size of your management domain by interactively *managing* devices from other networks to expand it and/or *unmanaging* non-critical devices to limit network management traffic and the size of your map.

TIP If this approach seems too time consuming based upon the size of your management domain, see page 119 and page 124.

Adding Networks to Your Management Domain

To add a network to your management domain, find the IP address and hostname of at least one high-traffic device within the network that you wish to add. Gateways, routers, or multi-homed servers make the best choice. Then:

- On the Internet-level submap, select the `Edit:Add Objects` menu item.
- Select the *Connector* Symbol Class icon, then drag the *Gateway* Symbol Subclass icon onto your Internet-level submap. Choose this gateway connector regardless of the type of device you are using to start the discovery. The `Add Object Palette` appears.
- Double-click on `IP Map` to open the `Set Attributes` dialog box.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0811
3740
Doc:

- Type in the IP address and hostname of an SNMP enabled device within the network that you wish to add to your management domain, then click on the Verify button.

  Once NNM runs the configuration check, NNM will correct the symbol choice and (if necessary) placement for you. The device is configured to be managed by NNM.

Managing an Unmanaged Network Device

To change the status of a network device from unmanaged to managed (see NNM's online help for more information):

1. From any submap, use NNM's `Edit:Find` menu item to locate the device's symbol on the map.
2. Select the device's symbol and select `Edit:Manage Objects`.
3. Select a router that is connected to the new network symbol and use the `Fault:Network Connectivity->Poll Node` menu item.

   NNM conducts discovery on that device's assigned network or networks and the nodes within any neighboring networks. NNM updates the map, databases, and event monitoring to include these devices.

Unmanaging a Managed Network Device

If you *unmanage* a network symbol or segment symbol during active discovery, a few node symbols on that network or segment may not be reset to unmanaged. To avoid this problem while *unmanaging* the network symbol or segment symbol, do one of the following:

- Wait until NNM finishes active discovery before unmanaging an object.
- Turn *new-node discovery* polling off. From any submap, select the `Options:Network Polling Configuration`. Disable the `New Node Discovery` option. Don't forget to turn polling back on again when you are finished modifying the map.

Automatically Expand Your Management Domain

Normally, netmon generates the discovery process outward from the management station and includes only the management station's IP network in the management domain. If your NNM maps are too limited and do not show *all* the networks for which you are responsible, and adding the missing networks one by one (page 117) would be too time-consuming, you have several choices to consider for customizing the discovery process:

- Seed File(page 120)

  If your management domain contains multiple networks (especially networks that are not adjacent to each other), consider using a seed file. A **seed file** instructs netmon to generate the map starting from multiple IP addresses instead of or in addition to the management station's IP address. This saves you time by eliminating the manual process of expanding the management domain.

- loadhosts Program (page 122)

  If your management domain contains few SNMP devices, you can speed up netmon's discovery process by creating an ASCII file listing devices that need to be added to the topology database and map. The loadhosts program reads this file and adds the devices listed in this file directly to your topology database, bypassing the netmon discovery process. Upon being added to the topology database, netmon begins polling the devices as newly discovered devices and expands your management domain from these new nodes.

TIP If you already keep a local hosts file that lists important SNMP-enabled nodes on your network, you can use that file.

- IPX Hop Count (Windows only, page 123)

  If you installed the Windows drivers for the IPX stack, during discovery gateways and servers acting as routers return a **hop count** (how many hops are allowed through gateways and routers to

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 0812
3740
Doc:

get to the network) for each network of which the router is aware. You can expand the extent of discovery by setting the maximum hop count to a higher number.

TIP Remember that each additional managed network device increases the network management traffic being generated. Refer to the critical-device list that you established in Chapter 4, "Planning Your NNM Configuration," on page 79 for guidance about keeping the management polling traffic to a reasonable minimum. Unmanage devices that are not mission-critical.

Create a Seed File Specifying Multiple IP Networks to Manage

A seed file is an ASCII file containing a list of network-level IP addresses or host names (not IPX addresses). The contents of the seed file define your map's initial management region. Gateways make the best seeds because they maintain the largest ARP tables. If you add the major gateways, `netmon` will discover the rest of the nodes on the network, so you do not have to include all nodes in the seed file. All networks attached to the devices listed in your seed file will be discovered and set to *managed*. Networks implied by each node's IP address are discovered and added automatically to the map.

1. Create an ASCII file. The name and location of this ASCII seed file is up to you. In this file, list any hostnames or IP addresses that NNM should use to begin discovery. Each hostname or IP address must be on its own line, and each listed device must support SNMP. Specifically, `netmon` must be able to determine the subnet mask for each interface in a specified node. Otherwise, the seed file entry will be ignored.

   You can include notes to yourself in the seed file by using *comments* (preceded by a # sign) after the hostname or IP address on a line.

   Example seed file:

```
node1.division.company.com
router4.division.company.com  #Gateways are best
192.0.2.44
192.0.2.45
```

276

TIP Bridges and hubs may or may not maintain ARP tables. The ARP tables are the key to expanding NNM's discovery.

2. Make a backup copy of the netmon's local registration file:
   - *Windows:* `install_dir\lrf\netmon.lrf`
   - *UNIX:* `$OV_LRF/netmon.lrf`
3. Load the `netmon.lrf` file into your text editor. The `netmon.lrf` file consists of the following.

```
netmon:netmon:
OVs_YES_START:ovtopmd,pmd,ovwdb:-P:OVs_WELL_BEHAVED: 15:
```

4. Insert the seed file option (`-s filepath`) after the `-P`.

   For example, adding the seed file, `nodelist`, to use as input to `netmon` on a management station running the Windows operating system would change the file to look like:

   Windows (Note the required \ character after the drive letter and the \ character in the path statement.):

```
netmon:netmon:
OVs_YES_START:ovtopmd,pmd,ovwdb:-P -s
"C\:\install_dir\conf\nodelist":OVs_WELL_BEHAVED:15:
```

   UNIX:

```
netmon:netmon:
OVs_YES_START:ovtopmd,pmd,ovwdb:-P -s
/etc/opt/OV/share/conf/nodelist:OVs_WELL_BEHAVED:15:
```

5. Save the edited `netmon.lrf` file in the following location:
   - *Windows:* `install_dir\lrf\netmon.lrf`
   - *UNIX:* `$OV_LRF/netmon.lrf`
6. Stop the netmon service. At the command prompt, type:
   `ovstop netmon`
7. To update NNM's configuration file, `ovsuf`, at a command prompt, type:

   Windows: **`ovaddobj install_dir\lrf\netmon.lrf`**

   UNIX: **`ovaddobj $OV_LRF/netmon.lrf`**

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0813
3740
Doc:

`ovaddobj` updates `netmon`'s information in the `ovsuf` configuration file (which instructs the start-up process what to start).

8. Restart the `netmon` service. At the command prompt, type:

   `ovstart netmon`

NNM starts discovering from all locations identified in your seed file. Give NNM time to complete the process. Then you can manually make additions/changes to the map after the effects of the seed file are in place (see page 117).

Use loadhosts

`loadhosts` is a program provided with NNM that allows you to place a list of IP addresses directly into the topology database. This is useful when:

- There are few SNMP nodes on your network. Using `loadhosts` speeds up the discovery process.
- You already maintain a list of the important SNMP nodes on your network.

  Windows:
  `\WinNT\system32\drivers\etc\hosts` file or
  `\WinNT\system32\drivers\etc\Lmhosts` file

  UNIX: `/etc/hosts` file

  Using `loadhosts` ensures that your critical devices are immediately included in NNM's databases and on the map.
- If it is critical to keep network management traffic to an absolute minimum (see page 127).

See the *loadhosts* reference page in NNM's online help (or the UNIX manpage) for more information.

1. Create an ASCII file listing each IP address or hostname on a separate line.
2. At the command prompt, type:

`loadhosts -m` ***`subnet-mask filename`***

The following example loads the `\etc\hosts` file on a management station running a Windows operating system, with the subnet mask set:

```
loadhosts -m 255.255.248.0 \WinNT\system32\drivers\etc\hosts
```

The netmon service receives events about the new additions to the topology database and runs the discovery and configuration poll on those newly added nodes.

Expand the IPX Hop Count (Windows only)

If you installed the Windows drivers for the IPX stack, gateways and servers acting as routers return a hop count during discovery (how many hops through gateways and routers to get to the network) for each network of which the router is aware. You can control the extent of IPX discovery allowed by NNM.

To increase the maximum hop count for discovery, open any submap and select the `Options:Network Polling Configuration IP/IPX` menu item. On the `IPX Discovery` tab, specify the hop count of your choice. This change takes effect the next time IPX discovery runs.

To discover *all* IPX networks, set the value up to 16—the maximum allowed by IPX. However, see note below.

NOTE Setting the maximum hops to 16 can cause a large number of nodes to be discovered rapidly, causing both short-term and long-term system performance problems due to polling traffic. Unless you are sure your system is appropriately configured to handle the number of IPX nodes in your environment, Hewlett-Packard recommends that you expand your management domain slowly.

RQS nº 03/2005 - CN - CPMI 123 CORREIOS
Fls. Nº 0814
3740
Doc:

Automatically Limit Your Management Domain

If your network maps are too complex to be useful, you have several choices to consider for customizing the discovery process.

If all the devices that are shown on your map must remain in your management domain, you can use **container** icons (see page 248) and create custom submaps to break up the visual information into smaller chunks and customize your map in a number of ways. (See Chapter 8, "Map Customization," on page 211 for information about customizing the map itself rather than customizing the discovery process.)

If you do not need to retain all the devices that are shown on your map, NNM has options that you can use individually or in combination:

- `netmon.noDiscover` File (page 125)

  You create this file listing IP addresses or ranges of IP addresses for NNM to *exclude* from the discovery process; therefore, excluding them from NNM's databases and maps. During initial discovery when NNM discovers a device, the device's IP address is checked against the `netmon.noDiscover` file. If the IP address is matched in the `netmon.noDiscover` file, the device is dropped and not polled for any more information. The device may be discovered again during subsequent new-node-discovery polls; however, it will once again be discarded. This is the easiest method for limiting discovery and also reduces network management traffic more than using a discovery filter (explained below).

- `loadhosts` Program (page 127)

  If you need to keep network management traffic to an absolute minimum, you can turn off `netmon`'s discovery polling cycle and then use the `loadhosts` program to add your network's critical devices directly to your topology database. Only the devices that you specify in the ASCII file of IP addresses/hostnames are included in your management domain.

TIP If you already keep a local hosts file that lists important SNMP-enabled nodes on your network, you can use that file.

- Discovery Filter (page 128)

  You can write Boolean logic into the NNM filter file to specify which devices will or will not pass initial discovery and be added into NNM's object and topology databases. A discovery filter is much more work for the `netmon` service than the `netmon.noDiscover` file because *each device is polled for all MIB attributes* before it is checked against the discovery filter (this is because a discovery filter can be applied to many attributes of a device). If the device does not pass the discovery filter, all information is discarded. The device may be discovered and polled again during subsequent new node discovery polls; however, the information gathered will once again be discarded.

- `oid_to_type` File (page 129)

  You can open and modify the `oid_to_type` file so that specific *types* of devices are automatically configured as *unmanaged* during initial discovery. The devices show up on your map and are included in the NNM databases, but won't be included in the network management polling traffic generated by NNM.

- IPX Hop Count (Windows only, page 130)

  If you installed the Windows drivers for the IPX stack, during discovery gateways and servers acting as routers return a hop count (how many hops are allowed through gateways and routers to get to the network) for each network of which the router is aware. You can restrict the extent of discovery by lowering the maximum hop count.

Create a netmon.noDiscover File to Exclude Devices

The `netmon.noDiscover` file works at the very beginning of the discovery process. Entries in the `netmon.noDiscover` file are the "don't discover" list. No polling (SNMP or ICMP) is done on devices listed in the `netmon.noDiscover` file. Devices listed in your `netmon.noDiscover` file are not included in NNM's databases or displayed on NNM's maps.

IRQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0815
Doc. 3740

If you are using HSRP, you can add the virtual IP address of your HSRP-configured routers to the `$OV_CONF/netmon.noDiscover` file. This stops NNM from deleting and rediscovering the virtual IP address in a regular pattern, which can cause participating routers to be deleted from and re-added to your map. Use the following procedure:

1. Add the virtual IP address of your HSRP-configured routers to the `$OV_CONF/netmon.noDiscover` file.
2. If NNM has already discovered the virtual IP address of your HSRP-configured routers, execute `ovtopofix -r a.b.c.d` where *`a.b.c.d`* is the virtual IP address of your HSRP-configured routers.
3. Run `ovtopodump -lR` to make sure the virtual IP address is gone. See the `ovtopodump`, `ovtopofix`, and `netmon.noDiscover` reference page (or the UNIX manpage) for more information.

For more detailed information, see the *netmon.noDiscover* reference page in NNM's online help (or the UNIX manpage).

Use the following procedure to create entries in the `netmon.noDiscover` file.

1. Create an ASCII file. Name and place it as follows:
   - *Windows:* *`install_dir`*`\conf\netmon.noDiscover`
   - *UNIX:* `$OV_CONF/netmon.noDiscover`
2. List specific IP addresses or IP wildcards, one per line. Example `netmon.noDiscover` file entries are:

   `10.2.112.86` # one node

   `10.2.*.*` # all nodes from 10.2.0.0 to 10.2.255.255

   `10.2.1-255.0-49` # first 50 nodes in 10.2.1-255 range

   `*.*.*.*` # all nodes - nothing will be discovered

   `10.2.4-5.*` # all nodes in either 10.2.4.* or 10.2.5.*
3. After you have created or modified the `netmon.noDiscover` file, force `netmon` to acknowledge the change by doing one of the following:
   - To only affect future discovery, stop and restart the `netmon` service.
   - To force changes on the map as well as future discovery:

— Stop and restart the `netmon` service.

Use the `Edit:Find` feature with the same criteria that you used in your `netmon.noDiscover` file to select all the map objects to be excluded from the future discovery. Then delete them from your map. They will not be rediscovered.

-OR-

— Wipe out the databases and start again by following the directions in "Stop Everything and Start Discovery Over Again" on page 161.

TIP If you change your mind later and *remove* IP addresses from the `netmon.noDiscover` file, simply stop and restart the `netmon` service to force NNM to acknowledge the change. The nodes will be rediscovered at the next polling cycle.

Use loadhosts

`loadhosts` is a program provided with NNM that allows you to place a list of IP addresses directly into the topology database. This is useful when:

- There are few SNMP nodes on your network. Using `loadhosts` speeds up the discovery process (see page 122).
- You already maintain a list of the important SNMP nodes on your network:

  Windows:
  `\WinNT\system32\drivers\etc\hosts` file or
  `\WinNT\system32\drivers\etc\Lmhosts` file

  UNIX: `/etc/hosts` file

  Using loadhosts ensures that your critical devices are immediately included in NNM's databases and on the map.
- It is critical to keep network management traffic to an absolute minimum. Turn off the new-node discovery polling process, then use the `loadhosts` program to accomplish discovery of the critical devices you wish to monitor. As long as new-node discovery is turned off, these are the only devices that will appear on your maps.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0816
Doc. 3740



See "Controlling the Amount of Traffic Generated by NNM" on page 178 for more information about NNM's polling cycle choices.

See the *loadhosts* reference page in NNM's online help (or the UNIX manpage) for more information.

1. Create an ASCII file listing each IP address or hostname on a separate line.
2. Turn off NNM's new-node discovery polling feature.

   From any submap, select the `Options:Network Polling Configuration` menu item and disable the New-Node Discovery feature.

   See NNM's online help from this dialog box for more information.
3. If you want to start initial discovery over again, see "Stop Everything and Start Discovery Over Again" on page 161.
4. At the command prompt, type:

`loadhosts -M` ***`subnet-mask filename`***

The following example loads the `\etc\hosts` file on a management station running the Windows operating system, with the subnet mask set:

```
loadhosts -m 255.255.248.0 \WinNT\system32\drivers\etc\hosts
```

The `netmon` service receives events about the new additions to the topology database and runs the discovery and configuration poll on those newly added nodes.

Create a Discovery Filter Identifying Which Devices to Include

All filters consist of sets of Boolean logic that you enter into the NNM filters file:

- *Windows:* *`install_dir`*`\conf\c\filters`
- *UNIX:* `$OV_CONF/$LANG/filters`

After creating and testing your *discovery* filter, open the `Options:Network Polling Configuration` dialog box and enter the name of your filter in the `Use filter` field. Your filter will be used during all future discovery processes.

To update the object database and enforce the filter rules upon past discoveries, you must use the `ovtopofix` command to force `netmon` to acknowledge your new filter and clean out the existing information in NNM's databases so that your discovery filter changes are reflected on your maps.

See *A Guide to Scalability and Distribution* for information about writing, testing, and implementing the discovery filter. See also the *OVfilterIntro*, *netmon*, *ovfiltercheck*, and *ovfiltertest* reference pages in NNM's online help (or the UNIX manpages) for more information.

TIP

While learning how to use the Boolean language, you may wish to explore the information about *map* filters first (rather than discovery filters). NNM interactively reflects changes to the map filter on the existing maps (rather than requiring that you run the `ovtopofix` command first). Therefore, you can try different Boolean strategies and see their effect on the map right away. See *A Guide to Scalability and Distribution* for more information.

Modify the oid_to_type File to Unmanage Devices by Type

You can instruct NNM to automatically set specific types of devices to *unmanaged* during discovery, such as all end-user PCs or all printers. If you want to use this feature *after* you have already finished initial discovery, make the changes to the `oid_to_type` file and see "Stop Everything and Start Discovery Over Again" on page 161.

The `oid_to_type` file (included with NNM) lists a large number of known `sysObjectIDs`. You can use the `U` parameter to automatically set specific types of devices to unmanaged during initial discovery. This flag only affects initial discovery status. You can change any device from unmanaged to managed at a future time.

You do not need to stop NNM when editing this file. To notify `netmon` of the changes when you are done:

- To only affect devices discovered in the future, at the command line type **`xnmpolling -event`**

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0817
Doc. 3740

- To go back and start initial discovery again so that this change affects all devices on your network, see "Stop Everything and Start Discovery Over Again" on page 161.

See the directions at the beginning of the editable ASCII `oid_to_type` file. See also the *oid_to_type* references pages in NNM's online help (or the UNIX manpages) for more information.

The following example entries would set devices containing either of two specific Windows versions to unmanaged, would set to unmanaged any IPX device that is not specifically identified elsewhere in the `oid_to_type` file, and would set to unmanaged any non-SNMP/IPX/IP device not specifically identified elsewhere in the `oid_to_type` file:

```
1.3.6.1.4.1.311.1.1.3.1::Windows NT:U # Windows NT
1.3.6.1.4.1.311.1.1.3.1.1::Windows NT:U # Windows NT
DEFAULT:::U
DEFAULT_IP:::
DEFAULT_IPX:::U
DEFAULT_SNMP:::
```

The `oid_to_type` file acknowledges specific `sysObjectIDs`, then wildcard `sysObjectIDs`, and then the `DEFAULT` settings.

Limit the IPX Hop Count (Windows only)

If you installed the Windows drivers for the IPX stack, gateways and servers acting as routers return a hop count during discovery (how many hops through gateways and routers to get to the network) for each network of which the router is aware. You can control the extent of IPX discovery allowed by NNM.

To reduce the maximum hop count for discovery, open any submap and select the `Options:Network Polling Configuration IP/IPX` menu item. On the `IPX Discovery` tab, specify the hop count of your choice.

The extra devices that were discovered based upon the old hop-count number must be manually deleted from your map. Once deleted, the discovery process will not add them again.

Troubleshooting Discovery

This section contains information about resolving common challenges encountered during NNM's discovery of your network:

- IP discovery problems and solutions (page 131)
- IPX discovery problems and solutions (page 153)

Often times, the trouble is caused because of breakdowns in your well-configured network plan (see "Starting with a Well-Configured Network" on page 90): GET and SET community names other than *public*, DNS name resolution inconsistencies, duplicate IP addresses, incorrect subnet masks, or incorrectly configured SNMP agents or DMI service providers on specific devices. NNM's map and event tracking system can make it much easier for you to identify offending devices and isolate what exactly is wrong, so you can fix the problem.

Remember to take advantage of the online discussion group, OV Forum, provided for NNM customers to communicate with each other (see "OpenView Forum" on page 77). You will find a wealth of information there.

IP Discovery and Layout

The IP troubleshooting information is broken into several groups:

- "Network Issues" on page 133
  - "Opening NNM takes a long time" on page 133
  - "NNM's initial discovery found zero nodes" on page 133
  - "All or most of the map is wrong" on page 135
  - "Whole IP networks are missing from my map" on page 135
  - "Strange networks appeared on my map" on page 136
- "Router Issues" on page 136
  - "My default router shows up on the map as a host" on page 136
  - "Some of my routers are missing" on page 136

RQS nº 03/2005 - CN - CPMI CORREIOS
Fls. Nº 0818
3740
Doc:

— "One router shows up twice on my map as if it were two devices" on page 137
— "Logical interfaces (secondary IP addresses) are missing from my router's interface card submap" on page 137
— "NNM's discovery process negatively impacts my router's performance" on page 138
— "My routers are set to managed but the map doesn't expand" on page 138

- "Problems With Specific Devices" on page 138
  — "IP addresses are used to identify devices, rather than their hostnames" on page 138.
  — "The map includes devices and routing links that I have never heard of before" on page 139
  — "A few devices are depicted inaccurately on the map" on page 139
  — "An SNMP device shows up on the map as a non-SNMP node" on page 139
  — "A host shows up on the map as a router" on page 140
  — "Some of my devices are missing from the map" on page 140
  — "Devices are labeled with the IP address, when I have a name resolution system in place. What happened to the hostname" on page 141
  — "Multi-homed hosts show up as separate devices" on page 141
  — "How does NNM decide which one of multiple hostnames to use for a device" on page 142
  — "Devices have generic icons rather than manufacturer-specific icons" on page 142
  — "The name of a system running Windows is incorrect on the map" on page 143
  — "Addresses from two distinct nodes within a system running Windows are merged into a single node" on page 143
  — "DNS hostname is incorrect on map symbols for a system running Windows" on page 143
- "General IP Suggestions" on page 144

— "Check NNM's Alarm Browser: Configuration Alarms" on page 144

— "Duplicate IP Address Errors" on page 144

— "Routing Table Configuration" on page 144

— "GET- and SET-Community Name and SNMP Port Issues" on page 145

— "Subnet Mask Issues" on page 149

— "Running netmon with the Jumpstart (-J) option" on page 152

Network Issues

Opening NNM takes a long time

This is probably caused by an incorrectly configured name resolution scheme. To verify that this is the problem, do the following:

1. Find the `checkDNS.ovpl` tool.

   Windows: (located on the NNM installation CD) `\support\checkDNS.ovpl`

   You must copy `checkDNS.ovpl` and `gethost` into the following directory on the NNM management station:

   install_dir`\support\*`

   UNIX: `/opt/OV/support/checkDNS.ovpl`

2. Navigate to the directory containing `checkDNS.ovpl` on the NNM management station. At the command prompt type:

   `checkDNS.ovpl -v`

3. Every device listed in the NNM topology database is issued an appropriate `gethostbyaddr` or `gethostbyname` system call. Addresses or hostnames that are too slow in responding are identified in the output on the screen. Clean up the name resolution for addresses or hostnames identified as being too slow.

NNM's initial discovery found zero nodes

- First, verify that NNM's `netmon` service is running:

  — *Windows:* Select `Start:Programs:HP OpenView: Network Node Manager Admin->NNM Services - Status.`

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0819
3740

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0820
3740
Doc:

— *UNIX:* At the command line prompt, type **ovstatus -c**.

If any of the services are not successfully running, see "Troubleshooting NNM Itself" on page 577 for information about troubleshooting services before continuing.

- Make sure that your network devices are running and responding to pings and SNMP requests. From the command line, issue the `ping` commands and the SNMP requests (`snmpget` and `snmpwalk`), or from any submap use the `Fault:Network Connectivity` menu choices.

  Make sure that SNMP agents are installed and running on each agent system, particularly on gateways. The problem may be that there are no SNMP agents installed.

  Your SNMP GET- and SET-Community names may not be matching up with the settings on the management station. See "GET- and SET-Community Name and SNMP Port Issues" on page 145 for more information.

- If you have very few SNMP nodes on your network, run `loadhosts` to force `netmon` to find them. See "Use loadhosts" on page 122.

  Or run `netmon` with the jumpstart (`-J`) option. See "Running netmon with the Jumpstart (-J) option" on page 152 for more information.

- Make sure that the appropriate SNMP agent is installed and running on the management station:

  — *Windows:* `SNMP EMANATE Master Agent Service`. The service must be running on the management station for discovery to function correctly. You can verify status in the `Windows NT Services` applet in the Control Panel.

  — *UNIX:* `snmpdm`. An `snmpdm` agent must be running on the management station for discovery to function correctly.

- If you specified a seed file, verify that the seed file exists and that you are using the seed file's correct name in `netmon`'s LRF file. Also, verify that you included all the nodes that you want to use as seeds in the seed file and that all the nodes listed in the seed file support SNMP. Do not use bridges and hubs as seeds, since they do not maintain ARP tables.

- From any submap, select the `Fault:Network Connectivity:Ping` menu item to contact your default router and the closest SNMP-supporting router to start gathering ARP table information.

- Make sure your default route is configured correctly. This information determines how IP packets are routed on nodes. To find the default route, do one of the following:
  - Select your management station's symbol on the NNM map and select the `Configuration:Network Configuration:IP Routing Table` menu item.

TIP You may want to establish a policy for using a standard default route so that only one router needs to maintain the routing table.

  - From the command prompt, issue the following command:
    - *Windows:* `ipconfig /all`
    - *UNIX:* `netstat -r`

All or most of the map is wrong

If all or most of the map database is inaccurate, do the following.

On your NNM map, select the questionable router symbols on the map, then use the `Edit:Object Properties` and select `IP Map` to see the current subnet mask configuration.

If a router's subnet masks are incorrectly configured, correct the configuration (see "Subnet Mask Issues" on page 149) and restart discovery (see "Stop Everything and Start Discovery Over Again" on page 161).

Whole IP networks are missing from my map

NNM isn't yet managing any devices within the missing IP network:

- Routers with addresses in the missing IP networks may not be accessible via SNMP. See "GET- and SET-Community Name and SNMP Port Issues" on page 145.
- See "Interactively Expand/Limit Your Management Domain" on page 117.
- If you have several additional networks that you need to add, consider creating a seed file to set devices within those networks to *managed* all at once. See "Create a Seed File Specifying Multiple IP Networks to Manage" on page 120 for more information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0821
3740
Doc:

Strange networks appeared on my map

The most common cause of this problem is incorrect subnet masks. See "Subnet Mask Issues" on page 149 for more information.

To check the network device's current subnet mask configuration, select the device's symbol on the map and use the map's `Edit:Object Properties` and select `IP Map`.

Router Issues

My default router shows up on the map as a host

If the default router shows up as a host on the map, verify the following:

- The most common reason that `netmon` incorrectly identifies a router as a host is that your SNMP GET- and SET-Community names may not be matching up with the settings on the management station. See "GET- and SET-Community Name and SNMP Port Issues" on page 145 for more information.
- Make sure that IP Forwarding on the router is set to "forwarding" *and* that the router has more than one interface card. From any submap, select the router's symbol and select the `Tools:SNMP MIB Browser` menu item and browse the following information:
  - IP Forwarding configuration (`.1.3.6.1.2.1.4.1`)

    `.iso.org.dod.internet.mgmt.mib-2.ip.ipForwarding`
  - Number of interfaces (`.1.3.6.1.2.1.2.1`)

    `.iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber`

  IP Forwarding is a vendor/device-specific configuration. See your device's documentation for more information.

Some of my routers are missing

If routers are not showing up on your network, check to see if the routers are "backup" routers; that is, routers used in an emergency when another router goes down. `netmon` may not discover backup routers, because `netmon` looks only for nodes on the network that are actually used. Therefore, a backup router will be discovered either as a host or it may not be discovered at all. To solve this problem, follow these steps:

1. Manually add the router to the map. See "Interactively Expand/Limit Your Management Domain" on page 117 for information about manually adding the router.
2. Use the `Fault:Network Connectivity:Ping` to determine the initial status condition of the router and turn its map symbol green (managed).
3. Use the `Fault:Network Connectivity:Poll Node` to get the information that `netmon` needs to connect the router in the proper place on the map.

One router shows up twice on my map as if it were two devices

See "Multi-homed hosts show up as separate devices" on page 141.

Logical interfaces (secondary IP addresses) are missing from my router's interface card submap

Secondary addresses are logical interfaces that are configured in addition to the physical interfaces on a router. Unfortunately, for some agents, these additional interfaces are not included in the IP address table returned through SNMP. Therefore, NNM is unaware that these interfaces exist.

When an IP address is found in an ARP Cache and it resolves to the same official name as a router, the IP address is added as an additional interface. When the router's node submap is displayed, the primary interfaces (the ones returned through SNMP) have labels that contain the first word of the interface description. The secondary addresses (the ones discovered in an ARP Cache) have only their IP addresses as their labels.

NNM can discover secondary addresses only if:

- The secondary address resolves to the same official name as the router.
- The secondary address is connected to an existing subnet.

If NNM fails to discover all the configured secondary addresses, they can be manually added as interface symbols to the router's node submap. If the interface is connected to a new subnet, that subnet must also be manually added. NNM will not automatically add the subnet symbol. See the *netmon* reference page in NNM's online help (or the UNIX manpage) for information about the `-S` parameter.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0822
3740
Doc:

The secondary addresses can be placed in a seed file that will be used by the netmon service for discovery (see "Create a Seed File Specifying Multiple IP Networks to Manage" on page 120). In this case, the secondary address interface symbols and the corresponding networks will be added to the map automatically.

NNM's discovery process negatively impacts my router's performance

This can happen when NNM is requesting ARP cache tables or routing tables from the router. You can use the `netmon -R` parameter to stop NNM from polling any routing tables. This cuts down on polling traffic since routing tables can be quite extensive. However, using this option means that NNM cannot discover remote routers over serial WAN links without the help of either a seed file (page 120) or loadhosts (page 122). See the *netmon* reference page in NNM's online help (or the UNIX manpage) for more information about `netmon -R`.

My routers are set to managed but the map doesn't expand

One of the following may be the problem:

- Open the Interface submap for each router by double-clicking on the router symbol and verify that all interface cards are discovered. If any are missing add them manually.
- The missing network may simply be a quiet network; without network traffic, the ARP tables won't be populated to aid NNM in the discovery process. See "Running netmon with the Jumpstart (-J) option" on page 152.
- Your router may have static routes over serial interfaces. NNM can't discover the information it needs to expand discovery because static routes may not have an entry in the routing table with a next hop address. To bypass this issue:
  - — *Windows:* Manually add the corresponding interface card.
  - — *UNIX:* Ping the corresponding interface card.

Problems With Specific Devices

IP addresses are used to identify devices, rather than their hostnames

See "Opening NNM takes a long time" on page 133. See "Consistent Name Resolution Scheme" on page 91 for more information.

The map includes devices and routing links that I have never heard of before

This is probably caused by incorrectly configured subnet masks. See "Subnet Mask Issues" on page 149 for information about fixing problems with subnet masks.

A few devices are depicted inaccurately on the map

If isolated information in the map database is inaccurate, check the following:

- From any submap, select the inaccurate symbol, right-click with the mouse, and select `Object Properties, IP Map`. Write down the `System Object ID` number. Verify that the device supports SNMP (`isSNMPSupported=true`). Then, open the `oid_to_type` and `oid_to_sym` files to make sure there is an appropriate entry for that `sysObjectID` number. Also, check the registration files included in the *`install_dir`*`\symbols\` (`$OV_SYMBOLS/$LANG`) directory. Make any additions or corrections. Then, select the node's symbol on any submap, select `Fault:Network Connectivity->Capability Poll`. It may take some time before the map symbol updates. See Appendix D, "Changing All the Symbols for a Particular Device," on page 661 for more information.
- If changes to the underlying object's configuration have recently been made, select the device's symbol on any submap, then select the `Fault:Network Connectivity:Poll Node` menu item. This forces an immediate configuration check and updates NNM's databases to reflect your changes. You can also simply wait until the next polling cycle.

An SNMP device shows up on the map as a non-SNMP node

If NNM incorrectly identifies an SNMP node as a non-SNMP node, therefore displaying it as an unmanaged symbol:

- The problem may be that all of `netmon's` SNMP requests to a node failed. During SNMP requests, `netmon` asks for system information, interface table, IP address table, routing table, ARP cache, and possibly Bridge or Repeater MIB tables.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0823
3740
Doc:

If the node does not reply with a `sysObjectID`, `netmon` assumes that the node does not support SNMP. If, however, a configuration check succeeds, `netmon` assumes the node *does* support SNMP. Note that SNMP requests can fail if the transport is very busy. SNMP runs over UDP.

- The most common cause of this problem is that your SNMP GET- and SET-Community names may not be matching up with the settings on the management station. See "GET- and SET-Community Name and SNMP Port Issues" on page 145 for more information.
- Another common reason for failures is that the SNMP agent returns incorrect information. See "GET- and SET-Community Name and SNMP Port Issues" on page 145 for more information.

A host shows up on the map as a router

If you have a host that shows up as a router, it may be because the host has *multiple interfaces* and *IP forwarding,* therefore meeting the criteria of a router. To check the current configuration on the host:

1. From any submap, select the host's symbol and select the `Tools:SNMP MIB Browser` menu item and browse the following information:
   - IP Forwarding configuration (`.1.3.6.1.2.1.4.1`)

     `.iso.org.dod.internet.mgmt.mib-2.ip.ipForwarding`
   - Number of interfaces (`.1.3.6.1.2.1.2.1`)

     `.iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber`
2. From any submap, select the host's symbol and determine the device's System Object ID (`sysObjectID`) by using `Edit:Object Properties` and selecting `IP Map`. Use the `Edit:Find->Object By Attribute` menu item.

   Find all devices with the same `sysObjectID`.

   If all instances of this device are showing the same misbehavior on the map, see the *oid_to_type* reference page in NNM's online help (or the UNIX manpage) for information about the `M` parameter in the `oid_to_type` file that designates a device as a *multi-homed host* (not a gateway).

Some of my devices are missing from the map

There may be a problem with ICMP communication (`ping`):

- Select the `Fault:Network Connectivity:Ping` menu item and enter the missing IP address. If you can communicate directly with the device in this manner, it will automatically be added to the map.
- See "Interactively Expand/Limit Your Management Domain" on page 117.
- Check the device itself to ensure that it is not powered down.

The device may be in a network which is not yet *managed* by NNM:

- See "Interactively Expand/Limit Your Management Domain" on page 117.
- If you have several additional networks you need to add, consider creating a seed file to set multiple networks to *managed* all at once. See "Create a Seed File Specifying Multiple IP Networks to Manage" on page 120 for more information.

If initial discovery doesn't find many SNMP objects or if your SNMP community names are in disarray, the `netmon` jumpstart command (`-J` option) can force detected SNMP agents to generate ICMP broadcasts to populate their ARP tables, thus aiding the discovery process. See "Running netmon with the Jumpstart (-J) option" on page 152 for more information.

Devices are labeled with the IP address, when I have a name resolution system in place. What happened to the hostname

Check the DNS, NIS, or other name resolution configuration.

Use the `nslookup` tool that is included in the Windows or UNIX operating system. This utility can easily verify which part of the name-resolution configuration is incorrect. The reverse map must also work (`nslookup` must be able to resolve an IP address to a hostname, as well as resolve a hostname to an IP address). See your operating system's documentation for more information.

TIP Make sure that the case (use of uppercase and lowercase letters) is consistent in your hostnames.

Multi-homed hosts show up as separate devices

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0824
3740 Doc.

- The most common reason that `netmon` incorrectly identifies a multi-homed host as separate devices is that your SNMP GET- and SET-Community names may not be matching up with the settings on the management station. See "GET- and SET-Community Name and SNMP Port Issues" on page 145 for more information.
- Check the DNS, NIS, or other name resolution configuration.

  See also "Devices are labeled with the IP address, when I have a name resolution system in place. What happened to the hostname" on page 141 and "The name of a system running Windows is incorrect on the map" on page 143 for more information about name resolution.
- See the *oid_to_type* reference page in NNM's online help (or the UNIX manpage) and explore the `M` parameter setting for multi-homes hosts.

How does NNM decide which one of multiple hostnames to use for a device

NNM uses the hostname associated with the lowest numbered IP address which resolves to a name.

Devices have generic icons rather than manufacturer-specific icons

- The most common reason that devices display on the map with generic icons is that your SNMP GET- and SET-Community names may not be matching up with the settings on the management station. See "GET- and SET-Community Name and SNMP Port Issues" on page 145 for more information.
- From any submap, select the inaccurate symbol, right-click with the mouse, and select `Object Properties, IP Map`. Verify that the device supports SNMP (`isSNMPSupported=true`). Write down the `System Object ID` number. Then, open the `oid_to_type` and `oid_to_sym` files to make sure there is an appropriate entry for that `sysObjectID` number. Also, check the registration files included in the *`install_dir`*`\symbols\` (`$OV_SYMBOLS/$LANG`) directory. Make any additions or corrections. Then, select the node's symbol on any submap, select `Fault:Network Connectivity->Capability Poll`. It may take some time before the map symbol updates. See Appendix D, "Changing All the Symbols for a Particular Device," on page 661 for more information.

The name of a system running Windows is incorrect on the map

If an IP address to IP hostname lookup fails, the system attempts to resolve the address via NETBIOS. If the system with the IP address does not have a NETBIOS name that can be resolved back to the IP address in question, the symptoms described above can occur, as well as other communication problems with the target system.

To verify and correct the NETBIOS name on the target system, do the following:

1. On the remote system, access the Windows `Control Panel`.
2. Double-click on the `Network` icon; a dialog box will appear.
3. Correct the configured computer name.

NOTE Changing the name of the target system may affect other network connections for the system.

See also "Devices are labeled with the IP address, when I have a name resolution system in place. What happened to the hostname" on page 141 for more information about name resolution.

Addresses from two distinct nodes within a system running Windows are merged into a single node

See "The name of a system running Windows is incorrect on the map" on page 143 for information about resolving this.

DNS hostname is incorrect on map symbols for a system running Windows

See "The name of a system running Windows is incorrect on the map" on page 143 for information about resolving this.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0825
Doc: 3740

General IP Suggestions

Check NNM's Alarm Browser: Configuration Alarms

NNM's Alarm Browser sorts network alarms into useful categories for you. With your map open, notice the `Alarm Categories` window off to the side of your map. Click on the `Configuration Alarms` button to display the list of problems that NNM has discovered. Fix any problems before continuing. You will find information such as:

- Inconsistent subnet masks discovered on specific nodes (see "Subnet Mask Issues" on page 149).
- Duplicate IP addresses discovered on specific nodes.

Duplicate IP Address Errors

Duplicate IP addresses may cause the following NNM behavior:

- In an effort to keep the map current, NNM may continuously move the device symbol from one submap to a second submap and back again as it discovers the first device using the IP address and then discovers the second device using the same IP address.
- NNM's Alarm Browser may show multiple `Mismatched link-level address` alarms indicating that ARP tables on your network devices are continuously working to update based upon messages received from the two devices using the same IP address.

If within the alarm message NNM identifies the host name of the two devices, correct the problem on one of the two offending devices.

If within the alarm message NNM identifies the MAC address or link-level address of the two devices, use NNM's `Edit:Find->Object by attribute` feature to identify the two offending devices.

Routing Table Configuration

Make sure your network device's routing tables are configured properly. To check the routing table configuration on an SNMP-enabled device, select the device's symbol on any submap, then select `Configuration:Network Configuration->IP Routing Table`.

TIP NNM does not detect proxy ARP (an alternative to defining extensive routing tables). If you receive alarms about misconfigured subnet masks, proxy ARP may be the problem. If you wish to prevent these alarms from posting, highlight one of the alarms in the Alarm Browser and select `Action:Configure Event`. Then modify the event's configuration so that the alarm category is set to `Don't log or display`.

GET- and SET-Community Name and SNMP Port Issues

Community names are a security technique employed by SNMP agent software. If the network management software wants to communicate with the SNMP agent software, both the management station and the SNMP agent must know the current GET-community name and talk over the same port. By default, community names are often set to *public* and the port is set to 161. NNM assumes that these defaults are in use unless you inform it otherwise. Many network administrators change the GET-Community name so that hackers cannot obtain sensitive information about their devices. It is even more common for network administrators to change the SET-Community name, since knowing this community name enables others to make system configuration changes to the device itself.

In order to work, NNM depends upon successful communication with the SNMP agents installed on your network devices. If the GET-community names have been changed from *public* or the port changed from 161, you need to inform NNM of the new ones. (NNM cannot obtain these automatically because that would defeat the security feature.)

NOTE If you do not have access to the GET-Community names, for critical devices in your network, see "If Community Names are Unavailable" on page 148.

To inform NNM of the community naming scheme and ports in use on your network:

1. Open any submap and select the `Options:SNMP Configuration` menu item.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0826
3740

2. Enter the specific information about your community naming scheme for IP and IPX devices in this dialog box. For your convenience, you can use wildcard entries when indicating IP addresses. If no SET-Community name is defined, NNM uses the GET-Community name for SNMP SetRequests.

   In this same dialog box, you can indicate any SNMP proxies that you have set up for non-SNMP devices and indicate any nonstandard remote-port configurations that are in use by SNMP agent software on your network (default is port 161). Generally, a remote port is only specified for specialized proxy agents that do not listen to the standard SNMP port.

   Check NNM's online help from this dialog box for more information and directions.

For technical information, see the *ovsnmp.conf* reference page in NNM's online help (or the UNIX manpage).

You can also change these values using a command line interface. For more information, see the *xnmsnmpconf* reference page in NNM's online help (or the UNIX manpage). If you need to know the specific configuration settings for a particular device, use:

```
xnmsnmpconf -resolve device_name
```

For information about configuring SNMP for collection stations and management stations, refer to *A Guide to Scalability and Distribution*.

To determine which GET- and SET-Community name is currently configured in the SNMP agent on each device in your network, refer to the documentation that came with each SNMP agent software package.

If you change the community names on the agent, you also *must* configure the community names for that agent on the management station.

If the settings on both your management station and your SNMP device's agent software are correct and it still does not work, try the following and then contact the vendor of the SNMP agent software.

To verify that the problem resides in the device's SNMP agent, do one of the following. Then see if the information returned to you by the device's SNMP agent makes sense. Make sure common entries in these two tables match:

- On any submap, select the device's symbol and select the `Tools:SNMP MIB Browser` menu item. Then browse the following MIB tables:
  - interface table `.1.3.6.1.2.1.2.2` (`.iso.org.dod.internet.mgmt.mib-2.interfaces`)
  - IP address table `.1.3.6.1.2.1.4.20.1` (`.iso.org.dod.internet.mgmt.mib-2.ip.ipAddrTable`)
- From the command prompt using `snmpget` or `snmpwalk`, type:

```
snmpwalk nodename (or IP address) .1.3.6.1.2.1.2.2
snmpwalk nodename (or IP address) .1.3.6.1.2.1.4.20.1
```

Contact the vendor who supplied the SNMP agent software if the information returned to your request doesn't make sense.

Symptoms of incorrect community names include

- The default router is not discovered.
- Hosts appear to not support SNMP.
- `netmon` incorrectly identifies a router as a host.
- Node that supports SNMP as not supporting SNMP.
- The default router is shown as a host on the map.
- Error messages appear, such as "time-out" or "no such name."
- `netmon` incorrectly identifies a node that supports SNMP as not supporting SNMP.
- Multi-homed hosts show up as separate devices.

If the community name on the default router or the community name on nodes in the seed file does not match the configuration settings in NNM, `netmon` will not be able to get the information that it needs in order to discover the nodes on the network.

TIP

If NNM attempts to contact a node using SNMP and the SNMP request times out, NNM looks for a `netmon.cmstr` file that you can configure to contain additional community names for the node. If the `netmon.cmstr` file exists, and contains community names, the first community name from the netmon.cmstr file that results in a successful SNMP response is

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0827
3740
Doc:

stored in the SNMP configuration database for that node. See the *netmon.cmstr* reference page in NNM's online help (or the UNIX manpage) for more information.

If Community Names are Unavailable

If you need to manage critical devices, yet do not have access to their GET-community names, create a `hosts` file. This *optional* file allows NNM to identify multiple IP addresses as being within a single device (without obtaining this information from the device's SNMP agent). This file must be maintained manually, in the following format:

```
IPAddress       hostname       alias(optional)
```

If you are identifying multi-homed devices such as switches, you must implement alias assignments so that the hostnames of all boards within the device resolve to the same IP address.

```
IPAddress_1         hostname_1         hostname_2

IPAddress_2         hostname_1

IPAddress_3         hostname_1         hostname_3
```

Place your new `hosts` file in the following location. Make sure that the file does not have any extension, such as `.txt`:

- *Windows:* `\WinNT\system32\drivers\etc\hosts`
- *UNIX:* `/etc/hosts`

NOTE

Name resolution order issues:

Windows: The default behavior is to search the `hosts` file before checking DNS. If you have altered this default order, this technique may not work.

UNIX: Ensure that the hostname resolution order reads your new `hosts` file. Open the `/etc/nsswitch.conf` file and verify the contents.

Subnet Mask Issues

If the subnet masks on the management station or configured on your network devices are incorrect, discovery will fail. If the subnet mask is too restrictive, not enough is discovered. If the subnet mask is not restrictive enough, too much is discovered.

Symptoms of incorrect subnet masks may include:

- `netmon` discovers and adds nodes from the internet that are outside of your administrative domain. This is caused by an un-subnetted or incorrectly subnetted network.
- Nodes in your management domain do not show up on the map. This is caused by incorrect subnet masks on those nodes.
- Strange networks appear on the map, such as a network having a Class A, Class B, or Class C network number when you expect a subnetted network number. This is caused by incorrectly configured subnet masks on the nodes mapped to those strange networks.
- Many `Inconsistent subnet mask` alarms show up in your Alarm Browser. This is caused by incorrect subnet masks on the nodes identified in the alarm messages.

For networks to be discovered correctly, subnet masks must be correctly configured on all IP interfaces on the following:

- The management station
- All gateways
- Any nodes in a seed file for `netmon`
- Any SNMP-enabled node within your management domain

NOTE Non-contiguous subnet masks are not supported by NNM. Also, in hierarchical subnets, two subnets having the same IP subnet address but different subnet masks are not supported. See the white paper about subnet masks (page 75) for more information.

Proxy ARP (an alternative to defining extensive routing tables) is also not supported and will result in "misconfigured subnet mask" alarms. If you wish to prevent these alarms from posting, highlight one of the

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0828
3740
Doc:

alarms in the Alarm Browser and select `Action:Configure Event`. Then modify the event's configuration so that the alarm category is set to `Don't log or display`.

To identify the source of the problem caused by incorrect subnet masks, first check the management station to see which subnet masks it knows about, then check the subnet configuration on each network and each device that is causing the problem.

1. *Check the subnet mask information on the Management Station:* Check this information through both SNMP and non-SNMP tools to check for misconfigurations.

   - SNMP check:

     Use the `Edit:Find->Object by Selection Name` to locate the management station's symbol.

     Select the NNM management station's symbol and select `Configuration:Network Configuration->IP Addresses` to see which subnet masks are in use on the management station's interfaces.

   - Non-SNMP check using the tool provided by your operating system:

     — *Windows:* issue the `ipconfig /all` command

     `ipconfig /all` tells you how the system is actually configured; which may not be what the device's SNMP agent returns. For information, see your operating system documentation.

     — *UNIX:* issue the `ifconfig` *`interface`* command, where *`interface`* is usually `lan0`, `lan1`, and so forth. The `interface` command can be found in the `/usr/sbin/ifconfig` file.

2. *Check the subnet mask for each network:* If the subnet masks on the management system are correct (from the previous step), determine the subnet mask currently being used for each network. Do one of the following:

- Select a network symbol on any submap, then right-click on the symbol and select `Object Properties, IP Map`. Check to see that the subnet mask entry is correct. Repeat for each network symbol in question.
- From the command prompt, issue the `ovtopodump` command specifying each network. See the *ovtopodump* reference page in NNM's online help (or the UNIX manpage) for more information.

3. *Check the subnet mask on individual network devices:* To determine what subnet masks are returned to NNM from a device's SNMP agent, do one of the following:
   - On any node-level submap, select an interface board symbol, right-click on the symbol and select `Object Properties, IP Map`. Check the subnet mask entry.
   - On any submap, select the `Fault:Network Connectivity->Poll Node` menu item and type in the offending IP address and look at the results.
   - From the command prompt, type:

     `netstat -I nodename (or IP address)`

     Check the Windows operating system documentation or the UNIX manpage for more information about `netstat`.
4. To solve the subnet masks problems, follow these steps:
   a. Correct the problem with the subnet masks on the network objects that have the problem.

      Log into the network device itself and modify its network configuration to specify the correct subnet masks.
   b. Use the `Fault:Network Connectivity->Poll Node` menu item to verify that the new symbols have the correct subnet masks.

TIP If you discover a large number of inaccuracies, correct the problems and then redo discovery to reset NNM's databases ("Stop Everything and Start Discovery Over Again" on page 161).

ROS nº 03/2005 - CN - CPMI CORREIOS
Fls. Nº 0829
3740
Doc:

Running netmon with the Jumpstart (-J) option

The netmon jumpstart command (-J option) can force detected SNMP agents to generate ICMP broadcasts to populate their ARP tables, thus aiding NNM's discovery process. See the *netmon* reference page in NNM's online help (or the UNIX manpage) for more information.

CAUTION Generating ICMP broadcasts can cause a great deal of network traffic. Use this with caution.

netmon's default setting does not use the -J option. By default netmon generates, if necessary, just an ARP Request. There are several factors that determine whether netmon needs to generate an ARP Request:

- For nodes that are up but not on the same subnet with the management station, netmon generates just one ICMP echo request packet and gets back one response. In this case, no ARP Request is generated.

  Because the management station is on a different subnet, a request will go through a gateway. Gateways always have large ARP caches. netmon knows the gateway's link-level address and does not have to broadcast an ARP Request to that gateway. netmon only has to send one ICMP echo request through the gateway and gets back one response.

- For devices that are on the same subnet as the management station, netmon may generate just one ICMP echo request, or it may also generate one ARP Request as well. Because the nodes are on the same subnet, netmon does not have to go through a gateway. Broadcasting an ARP Request will depend on whether or not netmon already has the device's link-level address in the management station's own ARP cache.

- netmon will generate an ARP Request if the address that is being polled for status is not in the ARP cache of your management station.

  The presence of the address in the management station's ARP cache is affected by how many nodes are on the subnet and by how much physical memory is in your management station (some systems will automatically adjust the size of their ARP table).

If netmon is started with the -J option, netmon may cause a broadcast ICMP echo request on each subnet it discovers. These broadcasts will only be issued on a subnet if:

- No broadcast ICMP echo request has ever been issued on this subnet on behalf of this management station.
- An agent capable of issuing a broadcast ICMP echo request on netmon's behalf has been discovered on this subnet. All HP-UX SNMP agents have this capability.

IPX Discovery and Layout (Windows only)

- "General IPX Suggestions" on page 153
- "Network Issues with IPX" on page 154
  - "All IPX nodes are missing from my map" on page 154
  - "IP Network 0.0.0.0 Contains All IPX Nodes" on page 156
- "Router Issues with IPX" on page 156
  - "IPX routers are missing from my map" on page 156
- "Problems with Specific IPX Devices" on page 157
  - "Some IPX nodes are missing from my map" on page 157
  - "IPX nodes have incorrect names or labels" on page 157
  - "Nodes supporting both IP and IPX appear on the map as two separate nodes" on page 159
  - "Duplicate IP Address messages are in the Configuration Alarms list" on page 159

General IPX Suggestions

- Ensure that IPX is configured and installed correctly on the management station. See "Installing IPX Transport Software (Windows only)" on page 100. Pay particular attention to the Frame Type. All IPX nodes on the same IPX network must use the Frame Type configured on the IPX servers and routers.
- Ensure that nodes are running and responding to IPX diagnostic requests *and* SNMP requests. From the command prompt, issue the ipxping -b command. You should receive a response from each

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0830
3740

device configured to respond to IPX. If you don't receive any responses, your management station's IPX is probably not configured correctly. If a particular node does not respond, use `snmpget` and `snmpwalk` to check that device's configuration settings. Correct any problems that you discover.

- Ensure that the community name is configured correctly (see "GET- and SET-Community Name and SNMP Port Issues" on page 145).

  It may be necessary to add entries for the IP address and hostname in addition to the IPX address. The format for an IPX address is *<net>*`:`*<nodeaddr>*; for example, `00000100:080009ABCDEF`. You can drop the leading zeros of the *<net>* portion of the address in most cases. For example: `100:080009ABCDEF`.

- Ensure that the SNMP agent on the node is running.
- Ensure that the IPX objects are *managed* on your map.

Network Issues with IPX

All IPX nodes are missing from my map If NNM does not discover any IPX nodes when run for the first time, check the following:

- Make sure that IPX discovery is enabled via the `Options:Network Polling Configuration:IP/IPX` operation. Click the `IPX Discovery` tab and make sure that `Discover New Nodes` is checked. Also, if IPX discovery is configured for a particular time of day, no nodes will be discovered until that time.
- Make sure that the IPX transport is correctly configured and installed on your system. If `netmon` is started with IPX discovery enabled, but the IPX software is not installed, check the Alarm Browser window under the `Application Alert Alarms` category. You should see an application error event similar to `Could not get IPX RIP socket, disabling IPX discovery.`

  `netmon` will not perform IPX discovery until IPX is correctly configured and `netmon` is restarted.
- Check the Alarm Browser window under the `Application Alert Alarms` category for other errors that may indicate the problem. For example, an invalid license could prevent the system from starting.
- Verify that there is at least one server or router that will respond to the IPX RIP request.

1. Issue the following command at the command prompt:

   Windows: ***install_dir*\bin\ipxping -r -n 1 -d 5**

   This command sends one IPX RIP request and waits five seconds for responses. Responses will include the address of the responding server or router. Adding the -v option will include the IPX networks that can be reached from your management station.

   If you do not see a response and the management station is not also configured as an IPX/NetWare gateway, this indicates that there are either no servers or routers attached to this network, or there is a misconfiguration in your IPX Transport installation. In particular, verify that the IPX transport Frame Type is configured correctly, both on the management system and on the various servers and routers in the network.

   All nodes configured for the same IPX network must run the same Frame Type. For some installations, different IPX networks may be configured for different Frame Types on the same physical cable, but all nodes in the same IPX network must have the same Frame Type, which must match the types configured on the NetWare servers and IPX routers.

2. If the test above succeeded in producing RIP responses, verify that your system receives IPX diagnostic responses by issuing the following command:

   Windows: ***install_dir*\bin\ipxping -n 1**

   This command sends a single IPX diagnostic broadcast request to the local network. All NetWare clients and servers attached to the local network should respond. Lack of response indicates either there are no local NetWare clients, or there is a misconfiguration of the IPX transport on the management station or the target systems. Verify the IPX transport installation and configuration.

3. You can also verify communication with any given network by issuing the following command from the command prompt:

   Windows:
   ***install_dir*\bin\ipxping -n 1 -b <*IPX_net_addr*>**

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0831
Doc. 3740

For example: `bin\ipxping -n 1 -b 00000100` sends a single IPX broadcast diagnostic request to the IPX network 00000100. All NetWare clients and servers configured for the 00000100 network should respond.

IP Network 0.0.0.0 Contains All IPX Nodes If you are running this version of NNM on a collection station that forwards information to a management station running NNM 4.X, you may encounter errors on the management station's display of network information. NNM 4.X does not correctly handle IPX nodes and networks. All nodes with IPX interfaces end up in a single IP network with the IP address 0.0.0.0.

To avoid this, install a topology filter that includes *only* IP objects. You can find details on installing topology filters in *A Guide to Scalability and Distribution*. An example filter, `IPObjectsOnly`, is shipped with the system's filter configuration file for this purpose.

Router Issues with IPX

IPX routers are missing from my map

1. Verify connectivity with the router as described in "Some IPX nodes are missing from my map" on page 157.
2. If the router does not support IPX diagnostic protocols, you can expand the IPX discovery region beyond the router using the `Options:Network Polling Configuration` operation. Click the `IPX Discovery` tab, and use the controls to set the `Maximum Hops` to a larger value. Make sure the value is large enough to expand beyond the router, but not any larger than desired for your discovery purposes. To discover all IPX networks, set the value to 16—the maximum allowed by IPX (however, see note below).

NOTE Setting the maximum hops to 16 can cause a large number of nodes to be discovered rapidly, causing both short-term and long-term system performance problems. Unless you are sure your system is appropriately configured to handle the number of IPX nodes in your environment, Hewlett-Packard recommends that you expand your management domain slowly.

There is no way to add the router manually if it does not respond to IPX diagnostic requests.

3. If you increased your IPX hop count, but no nodes are being discovered in some or all of the IPX networks, check the following:

   - If the IPX networks exist on your map, verify that the target networks are managed. Use `Edit:Manage Objects` to manage the target networks.
   - If you have IPX discovery configured to run only at a certain time of day, new node discovery will not happen on the newly discovered networks until that time. You can verify your IPX discovery configuration using `Options: Network Polling Configuration:IP/IPX`

Problems with Specific IPX Devices

Some IPX nodes are missing from my map If NNM discovers some, but not all nodes that support IPX:

1. Verify the installation and configuration of the IPX transport on the nodes that are not responding. In particular, check the IPX Transport Frame Type, making sure that it is either set to `Auto Detected` or set to match the Frame Type of the management system and servers.
2. Systems must respond to IPX diagnostic requests in order for NNM to add them to the databases and map. The following systems are known not to respond to IPX diagnostic requests:

   - Some dedicated routers (that is, not NetWare servers) do not support IPX diagnostic protocols.
   - Windows systems, including the management station itself.

To verify that a system responds to IPX diagnostic packets, you must know its IPX address, which is a combination of the IPX network number and its node hardware address. Once you know the IPX address, you can test connectivity to that IPX address by issuing the ***install_dir*\bin\ipxping <*IPX_address*>** command. For example: *install_dir*\bin\ipxping 00000100:080009ABCDEF sends an IPX diagnostic packet to the node with a LAN hardware address of 080009ABCDEF in the IPX network 00000100.

IPX nodes have incorrect names or labels NNM uses the following rules to choose the label for an IPX node:

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0832
Doc: 3740

- If the node has an IP hostname, then truncate the IP hostname to just the basename and use that—preference is given to the IP name of an object.
- If the node is a NetWare server, use the NetWare server name as the label. Otherwise, take the network number of the internal server address (that is, remove the 00000000000, which is the same for every server).
- If the node supports SNMP and reports an SNMP `sysName` value, use that as the label.
- If the node supports IP, use the IP address.
- If the node supports IPX, use the host-address portion of the IPX address, formatted to translate the vendor of the hardware. (For example, `100:080009ABCDEF` gets a label of `HP-ABCDEF`).
- Otherwise, if the node has an LLA/MAC, use the hardware address as the label, formatting the hardware vendor if possible.

Based upon this information, troubleshoot naming problems by doing the following:

- If the node label is an IP address instead of a node name, update the IP address-to-hostname mapping. Verify the DNS configuration under the Network TCP/IP Configuration, and make sure your hostname resolution is configured correctly.
- If the node supports both IP and IPX and the label is incorrect, verify the IP address-to-hostname mapping as above.
- If the node is a Netware Server, verify that the correct server name is being propagated by the IPX network protocols by checking IPX SAP packets that show the server name, server type, and server address. You can check IPX SAP packets by doing either:
  - Listen for the information. Every server on the local network should broadcast a set of SAP packets once per minute. You can see the contents of these packets by typing the following at the command prompt:
    ***install_dir*\bin\ipxping -s -1**
  - Query for the information. You can obtain the information immediately by typing the following at the command prompt:
    ***install_dir*\bin\ipxping -sbgv**

If the name returned via either of the above methods does not match your expectations, you will need to reconfigure the IPX Server name.

- If the node supports SNMP, verify that the SNMP `sysName` is configured correctly on the target node. View the SNMP `sysName`, as determined by netmon, using `Edit: Object Properties`. Select the `IP Map` application and click `Edit Attributes`. The System Name attribute will be the SNMP `sysName` variable. If this name is blank, either the system does not have a `sysName` configured, or the SNMP configuration for the node is incorrect. Many nodes are shipped with a pre-configured SNMP `sysName` which may cause several nodes to have the same label.
- If the discovered label is a hardware address, but no vendor translation is occurring, check the contents of the following file: *`install_dir`*`\conf\physAddr.conf`

  Make sure the vendor is listed correctly; for example: `080009 HP`

Nodes supporting both IP and IPX appear on the map as two separate nodes If nodes that support both IP and IPX are showing up as two separate nodes on the map, verify your SNMP configuration for the IPX addresses of the node. The nodes can only be determined to be the same node if the node supports SNMP over IPX, and reports the MIB-II `ipAddrTable` correctly.

SNMP could be misconfigured over IPX. At the command prompt, type:
`snmpwalk IPXaddress system`

If you do not receive a response, verify the community name configuration (see "GET- and SET-Community Name and SNMP Port Issues" on page 145).

Duplicate IP Address messages are in the Configuration Alarms list Some IPX nodes are shipped with the IP address 192.0.0.192 preconfigured. This normally does not cause problems for IP discovery, but might for IPX discovery. If multiple nodes support SNMP over IPX, and report the 192.0.0.192 address as a valid address, `Duplicate IP Address` alarms will be generated.

To fix this problem, configure a correct IP address on each IPX node in question.

To configure NNM to simply ignore the problem and prevent these particular `Duplicate IP Address` alarms from showing up in your Alarm Browser, do the following:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0833
Doc 3740

1. From any submap, select `Options:Event Configuration`. Click the `OpenView` entry in the `Enterprises` section.
2. Select `OV_Duplicate_IP_Addr` from the event list.
3. From the `Event Configuration` window, use `Edit:Events->Copy` to make a copy of the event. A window will be displayed with the event information to be modified.
4. On the `Description` tab, enter a new event name; for example, **`Ignored_Dup_Addrs`**.
5. Click `Only specified sources`.
6. Click the `Sources` tab. Identify each node that is generating duplicate IP address alarms by doing one or more of the following:
   - Select each offending IPX node on the submaps and click the `[Add From Map]` button in the event configuration dialog box.
   - Type each node name or address into the `Source` entry area, and click `Add`. The source name should be the name listed in the `Source` column of the Alarm Browser.
   - Create an ASCII file listing the full host name or IP addresses of each offending IPX source, one per line. (Use of wildcard characters is allowed in this file.)

     Type the full path and name of this file into the `Source` entry area, and click `Add`.

   File names and sources can be intermixed in this list. See NNM's online help for more information.
7. Click the `Event Message` tab.
   a. Select either `Don't log or display`, or `Log only`.
   b. Click `[OK]`.
   c. Click `File:Save` to cause the event configuration to be updated.
   d. Click `File:Exit` to exit the `Event Configuration` window.

Stop Everything and Start Discovery Over Again

If a few aspects of your map do not look right, see "Troubleshooting Discovery" on page 131. However, if the entire map does not accurately represent your network or you decide to try discovering your network in a more limited fashion (page 124) and want to restart initial discovery, repopulate the databases, and generate a new map, do the following:

1. Stop all of NNM's services (background processes):

CAUTION

See *A Guide to Scalability and Distribution* for information about shutting down NNM in a distributed environment.

   - *Windows:*
     Select `Start:Programs:HP OpenView:`
     `Network Node Manager Admin->NNM Services - Stop.`
   - *UNIX:* As root, at the command prompt, type **`ovstop`**.

2. Since this step deletes NNM's topology, object, and map databases and your maps, you may wish to back up your existing databases before proceeding (see "Backup/Restore to Protect Your Investment of Time" on page 165).

   If you have customized NNM's configuration (discovery configuration, SNMP configuration, event configuration, or data collection and threshold monitoring, etc.) none of these configurations are affected by this step.

   Execute the following:

   - *Windows:* Use the Windows Explorer program to highlight the ***`install_dir`*`\databases\openview\`** directory. Select all of the contents of that directory and delete the contents.
   - *UNIX:* Type

     ```
     cd $OV_DB/openview
     rm -rf $OV_DB/openview/*/*
     ```

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0834
Doc: 3740

NOTE If you are using a database other than the one embedded in NNM, see NNM's online manual, *Reporting and Data Analysis*.

3. Optional: To remove the old error messages and start again, execute the following:

   - *Windows:* Use the Windows Explorer program to highlight the ***install_dir*\databases\eventdb** directory. Select all of the contents of that directory and delete the contents.
   - *UNIX:* Type

     ```
     cd $OV_DB/eventdb
     rm -rf $OV_DB/eventdb/*/*
     ```

NOTE If you are using a database other than the one embedded in NNM, see NNM's online manual, *Reporting and Data Analysis*.

4. Restart NNM's services. NNM runs initial discovery, populates the databases, and generates a new map:

   - *Windows:*
     Select `Start:Programs:HP OpenView: Network Node Manager Admin->NNM Services - Start`.
   - *UNIX:* At the command prompt, type:

     ```
     xnmsnmpconf -clearCache
     $OV_BIN/ovstart ovwdb
     $OV_BIN/ovw -fields
     $OV_BIN/ovstart
     ```

See "Discover the Network... Let NNM Do It" on page 103 to start again.

6 Preserve Your Sanity: Backup and Polling Configuration

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: Nº 0835
Doc: 3740

Before you begin to configure NNM to meet your team's needs, it is a good idea to make sure that the backup process for NNM is in place and working properly. For information about backing up NNM see page 165.

NNM monitors the devices on your network through standard network protocols. This means that network traffic is generated while accomplishing network management. NNM ships with a generic polling configuration already in place. Take time to learn about and customize the polling configuration to meet your particular business needs. For information about controlling the polling traffic generated by NNM see page 178.

Backup/Restore to Protect Your Investment of Time

Backing up NNM can be integrated into your regularly scheduled network backup scheme. The backup happens in the background while your team continues to monitor alarms on your network. NNM temporarily pauses all services (background processes) whose activities result in changes to the NNM databases (such as the `ovw`, `ovwdb` and `ovtopmd` databases), thus ensuring consistency among the NNM databases and minimizing the potential for database corruption.

After the synchronized files are copied to the backup directory, the services resume normal activity. Then the files that do not require services to be in a paused state are copied to the backup directory.

During the backup of synchronized information, your team's maps are frozen in time, but the Alarm Browser's list and all Data Collection & Threshold information stay current throughout the backup.

NOTE Do not initiate changes to NNM's configuration files from the command line during a backup. It may cause data corruption in the backup copies of the files.

You must ensure that the information copied to the backup directory is archived to the disaster-recovery media of your choice (such as tape).

Add NNM's backup command to your list of regularly scheduled maintenance jobs. This script needs to run prior to your regularly scheduled backup process:

- *Windows:* `install_dir\bin\ovbackup.ovpl`
- *UNIX:* `$OV_BIN/ovbackup.ovpl`

Add NNM's backup directory to the list of items in your regularly-scheduled backup procedure. The backup directory (staging area) on the management station is:

- *Windows:* `install_dir\tmp\ovbackup\`

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0836
3740
Doc:

- *UNIX:* `$OV_TMP/ovbackup/`

See the *ovbackup.ovpl* and/or *ovrestore.ovpl* reference pages in NNM's online help (or the UNIX manpages) for more information.

How Does the Backup Work?

The `ovbackup.ovpl` command encapsulates all the steps needed to create a backup copy of NNM's critical files. In addition, other HP OpenView programs may supply scripts to include their critical files in the backup process.

A backup consists of two phases. The purpose of these phases is to copy the directory structure and data to the backup staging area. Two distinct phases are required in order to ensure that NNM is paused for the shortest possible time.

- **Operational Phase**

  NNM runs each script located in the `pre_pause` directory. Affected applications take preparatory steps. Then, NNM broadcasts an `ovpause` command. *All* services configured to respond to NNM's `ovpause` command take appropriate action. In some cases, the service temporarily becomes inactive. In other cases, such as data collection (`snmpCollect`), the service is not completely inactive; data continues to be recorded in temporary files until the backup is complete.

  Once all services registered to respond to the pause have successfully paused, NNM runs each script located in the `operational` directory. Because all affected services are paused, the data copied during this phase is *synchronized*.

  Once all files are copied to the backup directory structure, NNM broadcasts the `ovresume` command to restart all services. Some services, such as the data collector (`snmpCollect`), then copy their data collected during the paused state from their temporary files to the regular files. In this way, even during a paused state, data collection is not interrupted. Finally, NNM runs each script located in the `post_resume` directory to return affected applications to an operational state.

- **Analytical Phase**

NNM runs each script located in the `analytical` directory. An affected service may or may not be paused and resumed during the backup process, depending on the settings in its local registration file. The backup scripts might also pause and resume affected applications, themselves.

It is your responsibility to ensure that your disaster recovery plan includes archiving NNM's backup directory during your regularly scheduled backup scheme.

CAUTION If you choose to run `ovbackup.ovpl`, you *must* deactivate the default `solid.ini` scheduled backup. Do not do both or neither. Running both programs will result in backups that may not restore properly. Running neither program may cause severe performance problems with the embedded database. See"Problem: Backup failed. SOLID Database Error 10019:Backup is already active" on page 175 or the *Reporting and Data Analysis with HP OpenView Network Node Manager* online manual for more information.

Backing Up and Archiving All Critical Files

Try the backup and archive procedure now, before you spend a lot of time customizing NNM! Then back up and archive NNM files periodically while you configure NNM for your specific site, and back up and archive NNM files regularly as part of your disaster recovery plan.

1. The scripts named `nnm_checkpoint.ovpl` back up all of NNM's critical data. Additional scripts could be provided by other HP OpenView application developers or by you. Backup scripts must be placed in one of the following directories:

   - *Windows:*

     install_dir`\conf\ovbackup\pre_pause` **or**
     install_dir`\conf\ovbackup\checkpoint\operational` **or**
     install_dir`\conf\ovbackup\checkpoint\analytical` **or**
     install_dir`\conf\ovbackup\post_resume`

   - *UNIX:*

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 167 0837
Doc: 3740

```
$OV_CONF/ovbackup/pre_pause or
$OV_CONF/ovbackup/checkpoint/operational or
$OV_CONF/ovbackup/checkpoint/analytical or
$OV_CONF/ovbackup/post_resume
```

TIP To prevent NNM from being paused for longer than necessary, scripts should be placed in the `analytical` directory unless the data needs to be synchronized with the NNM databases. Scripts placed in the `operational` directory are run while all services registered to respond to the `ovpause` command are paused. Scripts placed in the `analytical` directory pause and resume services one at a time or in groups, only if necessary. See "Custom Scripts" on page 176 for information about writing your own backup/restore scripts.

2. Check on disk space availability before backing up the databases.

   At a minimum, the destination directory must have space for the NNM data that `ovbackup.ovpl` copies. If additional scripts have been added by other applications or the administrator, then additional space is needed. To determine the minimum space requirements, calculate the sum of the space used by NNM in the directories listed in the following table.

TIP As soon as you install NNM, data collection begins on certain MIB objects. Data collection consumes disk space. Backing up data collection files consumes additional disk space. Disk space being consumed by any SNMP data collection as well as the back-up of these files needs to be managed. For more information on network performance data collection, see page 447.

Table 6-1 Directories Included in Backup

Windows	UNIX
Operational files: *install_dir*\databases\openview*.* *install_dir*\databases\eventdb*.* *install_dir*\log*.* *install_dir*\conf*.* *install_dir*\registration*.* *install_dir*\lrf*.* *install_dir*\fields*.* *install_dir*\symbols*.*	*Operational files:* $OV_DB/openview/* $OV_DB/eventdb/* $OV_LOG/* $OV_CONF/* $OV_REGISTRATION/* $OV_LRF/* $OV_FIELDS/* $OV_SYMBOLS/*
Analytical files: *install_dir*\databases\snmpCollect*.* *install_dir*\databases\analysis*.*	*Analytical files:* $OV_DB/snmpCollect/* $OV_DB/analysis/*

After the backup, the ovbackup directory contains a duplicate copy of all directory structures as well as individual files. The backup process does not compress data, so depending on the size of the original database, the directory could become very large:

- *Windows:* *install_dir*\tmp\ovbackup\
- *UNIX:* $OV_TMP/ovbackup/

You can specify a different directory with the `ovbackup.ovpl -d` option. See the *ovbackup.ovpl* reference page in NNM's online help (or the UNIX manpage) for more information.

TIP

The following *analytical data* directories are *not* included in NNM's backup scripts:

- *Windows:*

  install_dir\backgrounds
  install_dir\bitmaps
  install_dir\www\htdocs\bitmaps
  install_dir\www\registration

- *UNIX:*

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls.: Nº 0838
Doc: 3740

```
$OV_BACKGROUNDS
$OV_BITMAPS
$OV_WWW/htdocs/bitmaps
$OV_WWW_REG
```

If you make changes or additions to map backgrounds, bitmap files, or web registration files ensure that your new files are properly backed up. See "Custom Scripts" on page 176 for information about writing your own backup/restore scripts.

3. Decide how you will archive the backup copy of NNM's critical files. Implement measures to ensure that the files in the *install_dir*\tmp\ovbackup directory (`$OV_TMP/ovbackup`) are archived to the disaster-recovery media of your choice on a regular and timely basis *and NOT during the time that the NNM backup scripts are running*.

CAUTION

If you redirected the Data Warehouse storage from the SOLID database to another database of your choice: The information will not be included by the `ovbackup.ovpl` script. Be sure to back up the database files that are used by NNM's reporting feature and Data Warehouse feature. See your database provider's documentation for directions about backing up your data.

4. At the command line, type **`ovbackup.ovpl`** or create a script that issues the `ovbackup.ovpl` command at the scheduled time of your choice. Refer to the *ovbackup.ovpl* reference page in NNM's online help (or the UNIX manpage) for more information.

NOTE

Do not initiate changes to NNM's configuration files from the command line during a backup. It may cause data corruption in the backup copies of the files.

TIP

UNIX systems only issue: NNM's `ovw`, `ovwdb`, and `ovtopmd` databases use sparse files. Sparse files are RDBM files which are stored to disk with the NULs stripped out. Sparse files usually have the extension `.PAG`. NNM's backup program makes sure that sparse database files are *not* expanded. Do not use `tar` because it expands sparse files.

5. After the backup completes:
   a. Check the ASCII log file to ensure that NNM's critical files were copied successfully:
      - *Windows:* *`install_dir`*`\tmp\ovbackup.log`
      - *UNIX:* `$OV_TMP/ovbackup.log`
   b. At the command line, type **ovstatus** to verify that all NNM services were successfully restarted.
6. Copy the files to the disaster recovery media of your choice.
7. Verify that your archive process successfully ran to completion and that the files on your disaster-recovery media are valid.
8. Optional: to reclaim hard drive space on your management station, delete the archived files from *`install_dir`*`\tmp\ovbackup\*.*` (`$OV_TMP/ovbackup/*`).

Restoring All of NNM (procedures/options)

In the event of a disaster or equipment upgrade, you must restore NNM to the most recently backed up state:

1. Install NNM from the installation CD, if necessary, and install any patches.
2. Stop all of NNM's services (background processes):
   - *Windows:*
     Select `Start:Programs:HP OpenView:`
     `Network Node Manager Admin->NNM Services - Stop`.
   - *UNIX:* As root, at the command prompt, type **ovstop**.
3. Retrieve the latest NNM backup files from your disaster-recovery media and copy them to the management station's backup directory.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
FIS. Nº 0839
3740
Doc:

- *Windows:* *install_dir*\tmp\ovbackup\
- *UNIX:* $OV_TMP/ovbackup/

TIP

UNIX systems only issue: NNM's ovw, ovwdb, and ovtopmd databases use sparse files. Sparse files are RDBM files which are stored to disk with the NULs stripped out. Sparse files usually have the extension .PAG. Make sure that the software being used to copy the files from your disaster-recovery media to the NNM management station does not expand sparse database files. Do not use tar because it expands sparse files.

4. Type **ovrestore.ovpl** from the command line to run the script files that update NNM's databases, log files, and configuration information files.

   The scripts named nnm_restore.ovpl restore all files found in the ovbackup directory. Additional scripts could be provided by other OpenView application developers or by you. See "Custom Scripts" on page 176 for information about writing your own backup/restore scripts. These restore scripts must be placed in one of the following directories:

   - *Windows:*

     install_dir\conf\ovbackup\restore\operational
     install_dir\conf\ovbackup\restore\analytical

   - *UNIX:*

     $OV_CONF/ovbackup/restore/operational
     $OV_CONF/ovbackup/restore/analytical

5. Verify that your files are safely restored.

   Optional: to reclaim hard drive space on your management station, delete the archived files from *install_dir*\tmp\ovbackup*.* ($OV_TMP/ovbackup/*).

6. Start all of NNM's services (background processes):

   - *Windows:*
     Select Start:Programs:HP OpenView:
     Network Node Manager Admin->NNM Services - Start.
   - *UNIX:* As root, at the command prompt, type **ovstart**.

Restoring Part of NNM (procedures/options)

The `ovrestore.ovpl` command allows you to specify that only the operational data (that must remain in a synchronized state) or only the analytical data be restored. It is not recommended that you restore smaller segments of NNM than these two categories. In fact, doing so could introduce data corruption.

See the *ovrestore.ovpl* reference page in NNM's online help (or the UNIX manpage) for more information. Remember that the following steps apply:

1. Stop all of NNM's services (background processes):
   - *Windows:*
     Select `Start:Programs:HP OpenView:`
     `Network Node Manager Admin->NNM Services - Stop`.
   - *UNIX:* As root, at the command prompt, type **`ovstop`**.
2. Retrieve the latest NNM backup information from your disaster-recovery media and copy it to the management station's backup directory:
   - *Windows:* *`install_dir`*`\tmp\ovbackup\`
   - *UNIX:* `$OV_TMP/ovbackup/`

TIP

UNIX systems only issue: NNM's `ovw`, `ovwdb`, and `ovtopmd` databases use sparse files. Sparse files are RDBM files which are stored to disk with the NULs stripped out. Sparse files usually have the extension `.PAG`. Make sure that the software being used to copy the files from your disaster-recovery media to the NNM management station does not expand sparse database files. Do not use `tar` because it expands sparse files.

3. Type **`ovrestore.ovpl`** (along with the parameter specifying either operational or analytical data) from the command line to run the script files that replace NNM's databases, log files, and configuration information files with the backup copy.

   The scripts named `nnm_restore.ovpl` restore NNM-specific data in either the operational or analytical files found in the `ovbackup` directory. Additional scripts could be provided by other HP

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0840
3740
Doc:

OpenView application developers or by you. See "Custom Scripts" on page 176 for information about writing your own backup/restore scripts. These restore scripts must be placed in one of the following directories:

- *Windows:*

  install_dir\conf\ovbackup\restore\operational
  install_dir\conf\ovbackup\restore\analytical

- *UNIX:*

  $OV_CONF/ovbackup/restore/operational
  $OV_CONF/ovbackup/restore/analytical

4. Verify that your files are safely restored.

   Optional: to reclaim hard drive space on your management station, delete the archived files from *install_dir*\tmp\ovbackup*.* ($OV_TMP/ovbackup/*).

5. Start all of NNM's services (background processes):

   - *Windows:*
     Select Start:Programs:HP OpenView:
     Network Node Manager Admin->NNM Services - Start.
   - *UNIX:* As root, at the command prompt, type **ovstart**.

Troubleshooting Information

At the completion of the backup, ensure that the backup completed without the errors. This section describes some errors which can occur. Look at the last entry in NNM's backup log file:

- *Windows:* *install_dir*\tmp\ovbackup.log
- *UNIX:* $OV_TMP/ovbackup.log

Problem: The system is already in a paused state.

Solution: An error occurred while pausing the services. ovpause logs an error and generates a trap. The backup is aborted. From the command line, type **ovresume.ovpl** and then try the backup again. If you are experiencing time-out errors for a particular service during the pause process, double the length of its pause time-out by altering the affected service's lrf file. See the *lrf* reference page in NNM's online help (or the

UNIX manpage) for more information. You must use the `ovaddobj` command to update NNM's configuration, and then use `ovstop` and `ovstart` to force NNM to acknowledge the change.

Problem: `The backup failed due to a file copy error.`

Solution: The original databases are not disturbed; however, the backup files cannot be used for a recovery. Fix the copy failure condition and then restart the backup. If the copy failed due to insufficient space, free up space in the staging area or use the `ovbackup.ovpl -d` option to copy files to a different directory. See the *ovbackup.ovpl* reference page in NNM's online help (or the UNIX manpage) for more information.

Problem: `The system is not in a paused state. ovresume cannot continue.`

Solution: The backup script assumes that there will be no operator interaction during the backup. Should someone on your team execute `ovresume` from the command line prior to the backup completing, the backup process may not run to completion. The original databases are not disturbed; however, the backup files cannot be used for a recovery. Restart the backup.

Problem: `Resume attempt FAILED.`

Solution: Check the backup log file. If you also see "Resume time-out" errors, see the *ovresume* reference page in NNM's online help (or the UNIX manpage) for information about the `-t` parameter to extend the time-out interval. If you see "Resume Error" messages, call HP customer support.

Problem: `Backup failed. SOLID Database Error 10019:Backup is already active`

Solution: If you are using NNM's reporting feature or Data Warehouse feature, historical information about your network is being stored in the SOLID database. By default, the SOLID database conducts a discreet backup of its own at 11 p.m. nightly. If you see this error in the `ovbackup.log` file, it means that the `ovbackup` was scheduled to run shortly after the SOLID database backup began.

To correct this problem you must deactivate the default `solid.ini` scheduled backup. The process for doing this is:

1. Copy the `$OV_DB/analysis/default/solid.ini` file to `$OV_DB/analysis/default/solid.ini.old` file.
2. Edit the `$OV_DB/analysis/default/solid.ini` file.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0841
3740
Doc:

3. Comment out the `At=<time> backup` entry, by inserting a semicolon (;) at the beginning of the line. An example would be:

```
;At=23:00 backup
```

4. Save the `$OV_DB/analysis/default/solid.ini` file.

The embedded database will now be backed up only when the `ovbackup.ovpl` command is run. If the use of `ovbackup.ovpl` is stopped at a future time, the default backup should be reinstated by copying the `$OV_DB/analysis/default/solid.ini.old` back to `$OV_DB/analysis/default/solid.ini`.

Windows-only Problem: `WARNING: Could not do 'secure' copy for file <filename>.`

Solution: This is unavoidable when open files on the Windows operating system's NTFS are copied to the staging area. See the WARNINGS section of the *ovbackup.ovpl* reference page in NNM's online help for more information.

UNIX-only Problem: `WARNING: Symbolic link errors or warnings from <directory>.`

Solution: In most cases, this is not a problem and nothing needs to be done. It usually occurs when restore attempts to create a symbolic link for a file that is already there. See the WARNINGS section of the *ovbackup.ovpl(1m)* manpage for more information.

Custom Scripts

NNM's backup procedure and restore procedure are designed so that they can be extended by placing any executable script into the appropriate `operational` or `analytical` directory. The HP-supplied `nnm_checkpoint.ovpl` and `nnm_restore.ovpl` scripts all have the extension `*.ovpl`. The suffix means "OpenView Perl" and refers to a specific subset of the Perl language used to implement NNM automated backup. This subset is not supported for general use by HP customers.

You may use the scripts supplied by HP as a reference or example while creating your own Perl scripts. However, if you create your own Perl scripts, do not use the `*.ovpl` extension in your script's file name and do not invoke HP's unsupported subset of Perl. Instead, ensure that you have a complete version of Perl installed on your system and use that one.

If you have *specific files* that you wish to include in NNM's backup process, the simplest way is to:

- *Windows:* Write a `.BAT` file that copies your files to the backup staging area, *`install_dir`*`\tmp\ovbackup`. Make sure that you duplicate the directory structure to your files, if necessary.
- *UNIX:* Write a shell script that copies your files to the backup staging area, `$OV_TMP/ovbackup`. Make sure that you duplicate the directory structure to your files, if necessary.

After you place your script in the appropriate directory, NNM runs it during the next backup or restore process:

- *Windows:*

```
install_dir\conf\ovbackup\pre_pause or
install_dir\conf\ovbackup\checkpoint\operational or
install_dir\conf\ovbackup\checkpoint\analytical or
install_dir\conf\ovbackup\post_resume or
install_dir\conf\ovbackup\restore\operational or
install_dir\conf\ovbackup\restore\analytical
```

- *UNIX:*

```
$OV_CONF/ovbackup/pre_pause or
$OV_CONF/ovbackup/checkpoint/operational or
$OV_CONF/ovbackup/checkpoint/analytical or
$OV_CONF/ovbackup/post_resume or
$OV_CONF/ovbackup/restore/operational or
$OV_CONF/ovbackup/restore/analytical
```

CAUTION

If you write scripts to copy *specific files* to the backup staging area, you must either:

- Create scripts that restore those specific files to the correct location (upon execution of `ovrestore.ovpl`). Place the scripts in the appropriate restore directories.
- Remember to copy the files to their original locations after running `ovrestore.ovpl`.

Refer to the *ovbackup.ovpl* or *ovrestore.ovpl* reference page in NNM's online help (or the UNIX manpage) for more information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0842
Doc 3740

Controlling the Amount of Traffic Generated by NNM

NOTE When you configure performance reports using the NNM web Reporting interface, the data collector starts collecting data. This data collection increases network traffic. You cannot control when or how frequently the collections are taken. If you need to reduce the amount of network traffic, you can suspend the generation of the report. See the NNM online help for more information.

Network Node Manager software automatically generates intense polling traffic at first as the network monitoring process is discovering your network.

After NNM's initial discovery of you network, *you* are in control of NNM's polling based upon your business needs. There are five types of polling in NNM that you need to know about. You can customize polling, or you can turn polling off completely. There are benefits and consequences to your decisions: less polling means less network traffic; however, reducing the amount of polling traffic by lengthening polling intervals may delay real-tim map updates, resulting in a less accurate map and less timely alarm logs. Turning polling off completely disables proactive management of you network.

You adjust NNM's polling through two dialog boxes accessed with the map menu's `Options:SNMP Configuration` and `Options:Network Polling Configuration` menu items.

2709

Figure 6-1 Options:SNMP Configuration Dialog Box

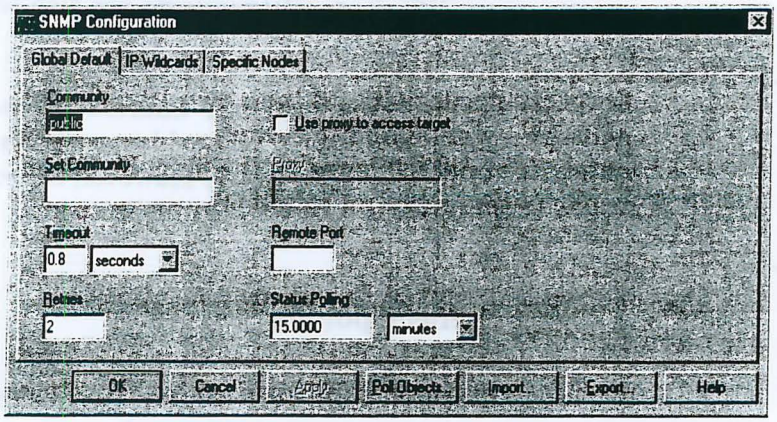
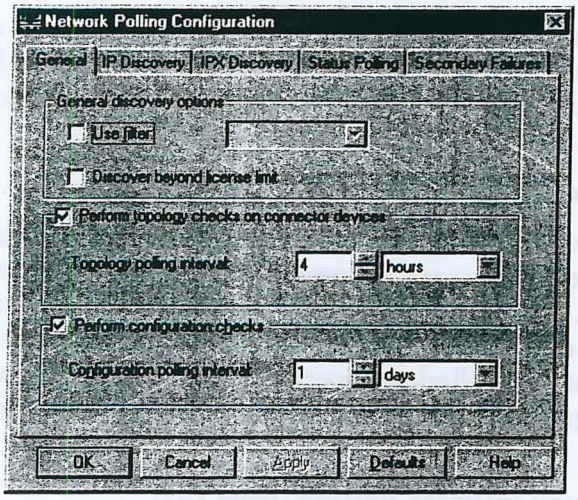


Figure 6-2 Options:Network Polling Configuration Dialog Box



Check the online help from these dialog boxes for more detailed information than you will find in this chapter. The five types of polling are:

- **Status polling** (See "Status Polling" on page 181)

  This is an ICMP `ping` sent to each interface of each managed device to verify if it is still accessible by the management station. In addition, a direct SNMP poll checks cached port tables on hubs and bridges to find the physical address listings of non-SNMP supported

ROS nº 03/2005 - CN - CPMI CORREIOS
Fls. Nº 0843
3740
Doc:

devices, and a direct SNMP poll updates the designated list of DHCP addresses. Status polling intervals are configurable as described in this section. *Only management stations running a Windows operating system:* IPX diagnostic requests are also sent.

TIP

Level-2 devices (without their own IP address) whose physical addresses were found in cached port tables are included in NNM's databases and displayed on the map. However, no network polling traffic is generated on behalf of these devices.

- **Configuration check polling** (page 183)

  This is an SNMP poll to gather current information about managed devices. This information is used by NNM to keep the maps current. The default interval is once-per-24-hours for each managed device.

- **Topology check polling of connecting devices** (page 184)

  This is an SNMP poll to verify the manner in which managed connective devices (bridges and hubs via the Bridge MIB, Repeater MIB, and proprietary HP MIBs) service other devices on the network. The default interval is 4 hours.

- **New node discovery polling** (page 184)

  There are two categories of new node discovery, IP and IPX. IP is an SNMP poll that scans for previously unknown devices and updates the map. The default interval is dynamic. *Only management stations running a Windows operating system:* if the IPX stack is configured as part of your Windows operating system, IPX issues RIP, SAP, and IPX diagnostic commands to detect additions to your management domain.

- **Secondary failures polling** (page 192)

  This status polling works in conjunction with the Event-Correlation feature provided with NNM. During a network failure, NNM now identifies the device causing the problem and correlates failure messages from all other affected devices. Through this setting, you control how long NNM ignores devices other than the primary failure. You can also instruct NNM to never ignore certain critical devices, even if they are a secondary failure in an event stream.

- Also see suggestions for fine-tuning all of these polling settings on page 193.

Status Polling

For each managed IP device, an ICMP `ping` is issued to verify if it is still accessible by the management station. The `Global Default` interval for IP devices is once every 15 minutes. Often, the `Global Default` interval setting for every device is not optimal. Refer to the list of mission-critical devices that you developed in Chapter 4, "Planning Your NNM Configuration." You will probably want to poll mission-critical devices more frequently. Some customers decide not to poll certain devices at all, such as end-user PCs or certain printers.

Dynamic Host Configuration Protocol (DHCP) allows IP addresses to be allocated on a temporary basis (a lease). When the lease for an IP address expires, the address can be reused by a different node. This is useful in environments supporting mobile users who connect to the network with a laptop from many different places.

You can specify the range of IP addresses that your network is configured to assign dynamically for mobile devices. The default is OFF (no filter in use). If this filter is enabled, NNM keeps the map clean and the Alarm Browser list free of unnecessary messages about devices within this address range as they are repeatedly attached and detached from your network. Addresses are defined through a *filter* that you write using Boolean logic. See *A Guide to Scalability and Distribution* for information about writing, testing, and implementing the DHCP filter.

You can control status polling in the following ways.

In the Options:SNMP Configuration dialog box

- Set polling intervals on specific nodes by IP address, IPX address, or hostname.

  For IP addresses only, you can set polling intervals using IP address wildcards for a group of IP nodes (for example, `15.122.*.*`). You can also import a file that contains your configuration preferences; see the online help in this dialog box for information about using a file. The IP address wildcard is useful; for example, when you want to configure different values for time-outs or the number of retries for Wide Area Networks (WANs).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0844
3740
Doc:

- Set the status polling interval to be used for any device not specifically listed. If you set it to 24-hours, polling begins at the time that you enter the setting. The actual time may drift depending on network conditions.
- Specify time-out and retry values. For example, you may want to increase the time-out and retry count values to prevent the management station from a premature time-out when making requests across a WAN because latency times are greater over WANs than LANs. Note that the time-out value is set in tenths of a second, and the time-out value doubles with each retry.
- Use filters to configure status polling by object classes. To view the current object class status polling interval configurations, click `Poll Objects` to open the `Status Polling Interval Configuration` dialog box. See the *OVfilterIntro* reference page (or the UNIX manpage) in NNM's online help for more information about defining filters. See the *netmon.statusIntervals* reference page (or the UNIX manpage) about modifying object-based status polling definitions.

NOTE

You may want to view or edit the current object class status polling interval configurations from a remote computer. To do this, use the following procedure:

1. Edit, as `root` (UNIX) or `Administrator` (Windows), the following file and follow the instructions contained in the file.
   - *Windows*:`install_dir\conf\remoteConfAllow.conf`
   - *UNIX*: `$OV_CONF/remoteConfAllow.conf`
2. From your remote computer, point your web browser to the following location:
   `http://hostname:3443/OvCgi/statusIntervalConf.ovpl`

In the Options:Network Polling Configuration dialog box

- Turn OFF/ON both IP and IPX status polling.
- Specify the interval of time that NNM should wait before deleting a "down node" from your maps. The default is 1 week.

- Identify your DHCP node list filter to specify a group of IP addresses that NNM should use for laptop computers. NNM handles this group of IP addresses differently, since devices will be connected and disconnected often from these addresses. Also specify the time interval that NNM should wait before deleting a disconnected node from your map.
- Designate your Discovery filter (if you created a filter of devices that should be excluded from polling). See "Create a Discovery Filter Identifying Which Devices to Include" on page 128.

NOTE One other status polling method, **SNMP status polling**, is used only in special cases to obtain device status information using SNMP queries. SNMP status polling is not configured to run automatically at installation and does not generate any network traffic until you configure it to run. SNMP status polling is covered in more detail on page 273.

Configuration-Check Polling

This type of polling gathers SNMP information about all currently managed devices for NNM's exclusive use. Configuration-check polling gathers information such as:

- Contact and location change
- Forwarding IP packets change
- Interface added
- Interface deleted
- Incorrect routing by a node
- Link address change
- Mismatch of link address
- Network mask change
- Node name change
- Object Identifier change
- Mismatches in link addresses
- World wide web capabilities

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0845
3740
Doc:

This information is used by NNM to keep the maps and databases current. The default interval is once-per-24-hours. This setting applies to all managed devices; it cannot be customized per node.

You can control configuration-check polling in the following ways.

In the Options:Network Polling Configuration dialog box

- Turn OFF/ON all configuration polling.
- Set the interval of time to wait between configuration polling, starting from the time that you set it. The time may drift depending on network conditions.

TIP To monitor status of devices outside your firewall, see "SNMP Status Polling" on page 273.

Connector Topology Polling

Connector topology polling monitors how hubs and bridges are connected in a network. All hubs and bridges are polled based upon the Bridge MIB (RFC1493), Repeater MIB (RFC2108), MAU MIB (RFC1515), and proprietary HP MIBs. You cannot set this polling on a per node basis. This setting helps keep your map current when you are moving devices around.

You can control connector topology polling in the following ways.

In the Options:Network Polling Configuration dialog box

- Turn it OFF/ON.
- Specify the interval of time. The default is 4 hours.

New Node Discovery Polling (IP, Level-2, and IPX)

New node discovery polling checks available ARP caches and Routing tables. This information is used to keep your maps current. This setting applies to all managed devices. It cannot be customized per node.

If you are running NNM on a Windows management station: For each managed IPX network, the following broadcasts occur for each discovery interval. The default interval is 6 hours:

- A single broadcast IPX Routing Information Protocol (RIP) request
- Two broadcast Service Advertising Protocol (SAP) requests
- Two broadcast IPX diagnostic requests per network, 10 seconds apart

You can control new node discovery polling in the following ways.

In the Options:Network Polling Configuration dialog box

For IP and Level-2 devices:

- Turn new node discovery polling OFF/ON. The default is ON for both IP and Level-2 devices. See "Controlling Level-2 Device Discovery and Layout" for more information about configuring NNM to discover level-2 devices.
- Select either the auto-adjust discovery interval or set your own polling interval. The default is auto-adjust, which is based upon the number of new nodes discovered. The range is between 15 minutes and 24 hours.

For IPX devices:

- Turn new-node discovery polling OFF/ON. The default is OFF.
- Set your polling interval or the desired specific time of day for polling.
- Specify the maximum number of sequential routers through which to poll. The default hop count is zero.

Controlling Level-2 Device Discovery and Layout

NNM discovers level 2 devices on both LANs and WANs and presents this information in a graphical format in the NNM map.

Table 6-2 on page 186 and Table 6-3 on page 190 summarize the information contained in this section. Table 6-2 shows the `netmon -k` keyword options and how these options work with the `Discover Level-2 Objects` check box to deliver the resulting NNM behaviors.

Table 6-3 shows how the `Discover New IP Nodes` check box and the `Discover Level-2 Objects` check box works with the `loadhosts` command to deliver the resulting NNM behaviors.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0846
Doc: 3740



See "Controlling Level-2 Discovery: Detailed Information" on page 188 for more in-depth information about controlling level-2 discovery and layout.

Table 6-2 Controlling Level 2 Discovery and Layout

netmon -k Option	Discover Level2 Object Check Box Status	NNM Behavior
bridgeMIB=true	Checked	Level 2 nodes and interfaces are discovered and added to the topology database. Bridge MIB layout is done. Existing level 2 interfaces in the topology are unaffected.
bridgeMIB=false	Checked	Level 2 nodes and interfaces are discovered and added to the topology database. No Bridge MIB layout is done. Existing level 2 interfaces in the topology are unaffected.
bridgeMIB=true	Not checked	Level 2 interfaces are discovered and added to the topology database. Level 2 nodes are not discovered. Bridge MIB layout is done. Existing level 2 interfaces in the topology are unaffected.
bridgeMIB=false	Not Checked	Level 2 nodes and interfaces are not discovered. No Bridge MIB layout is done. Existing level 2 interfaces in topology are unaffected.

Table 6-2 Controlling Level 2 Discovery and Layout (Continued)

netmon -k Option	Discover Level2 Object Check Box Status	NNM Behavior
discoverLevel2Nets=true	Checked	L2Nets are created between pairs of routers with such routes. All level 2 interfaces on routers are discovered and added to the topology db. Existing level 2 interfaces in the topology are unaffected.
discoverLevel2Nets=false	Checked	L2Nets are not created between pairs of routers with such routes. All level 2 interfaces on routers are discovered and added to the topology db. Existing level 2 interfaces in the topology are unaffected.
discoverLevel2Nets=true	Not checked	Routers are examined for non-IP interfaces. L2Nets are created between pairs of routers with such routes. All level 2 interfaces on routers are discovered. Only level 2 interfaces on routers needed for L2Nets are added to the topology. Existing level 2 interfaces in the topology are unaffected.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0847
3740

Table 6-2 Controlling Level 2 Discovery and Layout (Continued)

netmon -k Option	Discover Level2 Object Check Box Status	NNM Behavior
discoverLevel2Nets=false	Not Checked	Routers are not examined for non-IP interfaces. L2Nets are not created. No level 2 interfaces on routers are discovered. Existing level 2 interfaces in the topology are unaffected.

Controlling Level-2 Discovery: Detailed Information

NNM controls the discovery and layout of level 2 devices in the following manner:

- NNM discovers and adds views of level 2 devices that support the Bridge MIB (RFC 1493).
- NNM examines routers for non-IP interfaces and adds views of level 2 networks that exist between pairs of routers to the NNM map.

You can control the discovery and map layout of level 2 devices by using of the following NNM controls:

- Using the `netmon -k` options.
- By selecting the `Discover Level2 Objects` check box in the `IP Discovery` area of the `Network Polling Configuration` user interface.

You can use the `Discover Level2 Objects` check box together with the `netmon -k bridgeMIB` options to configure the following discovery and layout behaviors:

- If the `bridgeMIB` keyword is set to true (the default value) and the `Discover Level-2 Objects` check box is checked, the `netmon` process discovers level 2 interfaces and adds these interfaces to the topology database. The `netmon` process attempts to create new

segments for bridges and switches supporting the bridge MIB and places the devices on the NNM map. In some cases the netmon process creates and places level 2 nodes on the NNM map. The netmon process changes the names of these newly created level 2 nodes from MAC layer addresses to IP or IPX name references if it determines that the level 2 nodes are IP or IPX nodes. Existing level 2 interfaces in the topology are unaffected.

- If you change the bridgeMIB keyword to false and the Discover Level-2 Objects check box is checked, the netmon process discovers level 2 interfaces and adds these interfaces to the topology database. The netmon process will not attempt to create new segments for the bridges and switches supporting the bridge MIB nor will it place the devices on the NNM map. Existing level 2 interfaces in the topology are unaffected.
- If the bridgeMIB keyword is set to true and the Discover Level-2 Objects check box is not checked, the netmon process discovers level 2 interfaces and adds these interfaces to the topology database. The netmon process attempts to create new segments for bridges and switches supporting the bridge MIB and places the devices on the NNM map. The netmon process will not create nor will it place level 2 nodes on the NNM map. Existing level 2 interfaces in the topology are unaffected.
- If you change the bridgeMIB keyword to false and the Discover Level-2 Objects check box is not checked, the netmon process will not discover level 2 interfaces nor will it add these interfaces to the topology database. The netmon process will not create nor will it place level 2 nodes on the NNM map. The netmon process will not attempt to create new segments for bridges and switches supporting the bridge MIB, nor will it place the devices on the NNM map. Existing level 2 interfaces in the topology are unaffected.

See the ovtopofix reference page in NNM's online help (or the UNIX manpage) for information on reversing the effects of the bridgeMIB keyword. Look for information on the ovtopofix -l (el) and -I options.

You can use the Discover Level2 Objects check box together with the netmon -k discoverLevel2Nets options to configure the following discovery and layout behaviors:

- If the discoverLevel2Nets keyword is set to true (the default value) and the Discover Level-2 Objects check box is checked, the netmon process examines routers for non-IP interfaces and creates

RQS II 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0848
3740 . 0
Doc.



L2Nets between pairs of routers with non-IP interfaces. All level 2 interfaces on routers are discovered and added to the topology database.

- If you change the `discoverLevel2Nets` keyword to false and the `Discover Level-2 Objects` check box is checked, the `netmon` process will not examine routers for non-IP interfaces nor will it create L2Nets between pairs of routers with non-IP interfaces. All level 2 interfaces on routers are discovered and added to the topology database.
- If the `discoverLevel2Nets` keyword is set to true and the `Discover Level-2 Objects` check box is not checked, the `netmon` process examines routers for non-IP interfaces and creates L2Nets between pairs of routers with non-IP interfaces. All level 2 interfaces on routers are discovered. Only level 2 interfaces on routers needed for L2Nets are added to the topology. Existing level 2 interfaces in the topology are unaffected.
- If you change the `discoverLevel2Nets` keyword to false and the `Discover Level-2 Objects` check box is not checked, the `netmon` process will not examine routers for non-IP interfaces nor will it create L2Nets between pairs of routers with non-IP interfaces. No level 2 interfaces on routers are discovered. Existing level 2 interfaces in the topology are unaffected.

When the `Discover New IP Nodes` check box is not checked, the `Discover Level-2 Objects` check box is grayed-out, but still impacts NNM behavior. Table 6-3 shows the resulting NNM behavior when the `Discover New IP Nodes` check box is not checked and new nodes are added by using the `$OV_BIN/loadhosts` command, netmon's seedfile, or when manually adding symbols to the map. The discovery of level 2 interfaces on these nodes is still controlled by the `Discover Level-2 Objects` check box.

Table 6-3 Discovery Impact of Using `loadhosts` Command or a Seed File

Discover Level-2 Objects Check Box Status	Discover New IP Nodes Check Box Status	NNM Behavior
Checked	Not checked	Adds both IP interfaces and level 2 interfaces

Table 6-3 **Discovery Impact of Using `loadhosts` Command or a Seed File (Continued)**

Discover Level-2 Objects Check Box Status	Discover New IP Nodes Check Box Status	NNM Behavior
Not checked	Not checked	Adds only IP interfaces

Changing `netmon -k` Options

You can use the following procedure to modify the netmon -k options:

1. Log in as:
   - *Windows*: Administrator
   - *UNIX*: root
2. Open the netmon local registration file in the ASCII editing software of your choice:
   - *Windows*: *install_dir*`\lrf\netmon.lrf`
   - *UNIX*: `$OV_LRF/netmon.lrf`
3. Add the text shown in bold to set the keyword to the stated value:
   - To set bridgeMIB= true:

```
netmon:netmon:

OVs_YES_START:ovtopmd,pmd,ovwdb:-P -k segRedux=true -k
bridgeMIB=true:OVs_WELL_BEHAVED:15:PAUSE::
```

   - To set bridgeMIB=false:

```
netmon:netmon:

OVs_YES_START:ovtopmd,pmd,ovwdb:-P -k segRedux=true -k
bridgeMIB=false:OVs_WELL_BEHAVED:15:PAUSE::
```

   - To set DiscoverL2Nets=true:

```
netmon:netmon:

OVs_YES_START:ovtopmd,pmd,ovwdb:-P -k segRedux=true -k
discoverLevel2Nets=true:OVs_WELL_BEHAVED:15:PAUSE::
```

   - To set DiscoverL2Nets=false;

```
netmon:netmon:
```

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0849
Doc: 3740

```
OVs_YES_START:ovtopmd,pmd,ovwdb:-P -k segRedux=true -k discoverLevel2Nets=false:
OVs_WELL_BEHAVED:15:PAUSE::
```

4. Turn off the netmon service (background process). At the command prompt, run **ovstop -c netmon.**
5. Force NNM to acknowledge the change. At the command prompt, run:
   - *Windows*: **ovaddobj *install_dir*\lrf\netmon.lrf**
   - *UNIX*: **ovaddobj $OV_BIN/ovaddobj $OV_LRF/netmon.lrf**
6. Turn on the netmon service (background process): At the command prompt, run: **ovstart -c netmon**

See the *netmon* reference page in NNM's online help (or the UNIX manpage) for more information; look for the -k keyword parameter and the bridgeMIB and discoverLevel2Nets keyword arguments.

Secondary Failure Polling

This setting allows you to fine-tune the behavior of the connector-down correlation circuit. The default is ON. See "NNM's Event Reduction Capabilities" on page 352 and "Connector Down Correlation" on page 361 for more information about the event correlation feature.

You can control secondary failure polling in the following ways.

In the Options:Network Polling Configuration dialog box

- Turn secondary failure polling OFF/ON.
- Specify the factor by which the normal polling interval should be extended for secondary devices during a failure.
- Designate the section that you wrote in the `filters` file that specifies which critical devices should always be excluded from the secondary status list regardless of their location during a failure event.

  See the *OVfilterIntro* reference page (or the UNIX manpage) in NNM's online help for more information about defining filters. See also *A Guide to Scalability and Distribution* for information about creating filters.
- Control the behavior of the map and event log during a failure event.

Fine-Tuning the Polling Services

The amount of network management traffic generated by status polling depends on your network's configuration, including:

- How many nodes are up and how many are down?
- How many nodes are on the same subnet?
- How many nodes are on other subnets?
- How large is the permanent ARP cache?
- How probable is it that a particular IP address can be found in the permanent ARP cache?

Polling is controlled by NNM's `netmon` service (background process). Because automatic polling is based upon managed nodes, you can reduce the amount of network-management traffic by unmanaging nodes. Simply select the node or nodes on the map, and then select the `Edit:Unmanage Objects` menu item. You can add nodes and change nodes from unmanaged to managed. It may take a while for polling changes to take effect. Polling is scheduled on a per node basis, but the `netmon` service can fall behind schedule if its polling load exceeds capacity limits.

TIP

To automatically set specific types of devices to unmanaged, such as all printers or all end-user systems, see the *oid_to_type* reference page in NNM's online help (or the UNIX manpage). See also "Modify the oid_to_type File to Unmanage Devices by Type" on page 129.

To determine if the polling process is overloaded, select the `Performance:Network Polling Statistics` menu item. If "Seconds until next status poll" or "Seconds until next SNMP poll" is a negative number, then the polling queue is overloaded and running behind.

If polling is continually running behind, you may want to change the startup parameter settings in the `netmon.lrf` file for queue length (`-q` controls the ICMP queue length, `-Q` controls the SNMP queue length, and `-x` controls the IPX queue length). The default queue setting is 3 on a management station running the Windows operating system and 20 on a management station running a UNIX operating system. Increasing queue length affects the management station's use of system resources and use of network bandwidth for network management.

DOC 1.99/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0850
3740
Doc:

For information about parameter choices available to you for configuring NNM's polling service:

- See the *netmon* reference page in NNM's online help (or the UNIX manpage) for a wealth of choices about controlling polling from the command line and start-up parameter settings. The information in this reference page lists the parameters allowed in the `netmon.lrf` file. See "Create a Seed File Specifying Multiple IP Networks to Manage" on page 120 for information about the process of changing the `netmon.lrf` file (the seed file requires a modification to the `netmon.lrf` file).
- See the *xnmpolling* reference page in NNM's online help (or the UNIX manpage) for information about how to change polling configuration from the command line.
- See NNM's online help available from within the `Options:SNMP Configuration` dialog box and the `Options:Network Polling Configuration` dialog box for more information.

Information that is gathered during polling is stored in NNM's `ovsnmp.conf_db` database.

Watching NNM's Polling Queue

You can automate NNM to notify you whenever the `netmon` service is falling behind in the polling queue.

Use NNM's Data Collection & Thresholds feature (see page 447) to monitor two MIB values from HP's netmon MIB (provided on NNM's installation CD; use Load/Unload MIBs to access the `netmon` MIB):

- `nnmICMPSecsUntilNextPoll (.1.3.6.1.4.1.11.2.17.4.4.1.1.3)` and
- `nnmSNMPSecsUntilNext Poll (.1.3.6.1.4.1.11.2.17.4.4.1.2.3)`

Set the threshold configuration to generate a trap each time the polling queue falls behind to the negative amount that you specify.

Then use NNM's Event Configuration feature (page 422) to set up Automatic Action instructions for that trap instructing NNM to email a message to you or to page you each time that trap is received.

Running NNM Without Network Polling

It is possible to run NNM without the netmon service (background process) that polls your network to generate the map and detect changes. This may be useful if the only applications you have running under NNM do not rely on netmon's discovery functionality or if you are relying on collection stations to perform discovery and monitoring.

NOTE See *A Guide to Scalability and Distribution* for information about collection stations and how to proceed with this step when using collection stations.

To run NNM without automatic IP discovery, configuration checking, and polling by netmon, follow these steps:

1. Stop the currently running netmon service (background process). From the command line, type **ovstop -v netmon**
2. Remove netmon from NNM's start-up options. At the command prompt, type:

   Windows: **ovdelobj *install_dir*\lrf\netmon.lrf**

   UNIX: **ovdelobj $OV_LRF/netmon.lrf**

NOTE If you change your mind and want to restart netmon at a later time:

1. Add netmon to NNM's start-up options. At the command prompt, type:

   Windows: **ovaddobj *install_dir*\lrf\netmon.lrf**

   UNIX: **ovaddobj $OV_LRF/netmon.lrf**

2. Start the netmon service (background process):

   Windows: Select `Start:Programs:HP OpenView:Network Node Manager Admin->NNM Services - Start`.

   UNIX: As root, at the command prompt, type **ovstart**.

The pmd, ovwdb, and ovtopmd services must also be running before netmon can work properly. To generate a list showing the status of each of NNM's services:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0851
3740
Doc:

- *Windows:* Select `Start:Programs:HP OpenView:Network Node Manager Admin->NNM Services - Status`.
- *UNIX:* At the command line prompt, type **`ovstatus -c`**.

If any of the processes are not successfully running, see Appendix A, "NNM Services and Files," on page 539 for information about troubleshooting NNM's services before continuing.

2691

7 Map Making Fundamentals

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0852
3740
Doc:

The following concepts are useful to understand before you start creating your own customized maps:

- maps versus submaps (page 199)
- objects versus symbols (page 203)

Maps versus Submaps

You can think of the relationship between maps and submaps as being much like the relationships between an atlas and its pages. The atlas is the map. The pages of the atlas are the submaps where you may view a particular continent, country, state, city, or even specific parts of a city. In NNM, when you view a part of your network map, you are actually viewing a submap. The view may be presented in a high-level submap that represents your entire network that spans the world, or in a more detailed submap of any portion of the network.

Maps

A **map** is a set of related objects, symbols, and submaps that provides a graphical and hierarchical presentation of your network and its systems. You can create multiple maps, but only one map is open at a time for any given session of NNM.

You do not view a map directly; instead, you always view the submaps that comprise the map. You can display multiple submaps at any given time. Submaps are typically organized hierarchically to show an increasing level of detail.

Different maps can be used for defining different management regions, or for different presentations of the same management region. Different maps can be tailored to the needs of individual users.

You can create multiple maps and customize how information about objects is displayed on each map. Different maps can display information about the same object because maps obtain their information from the same source, the object database. In NNM, you can create new maps, delete maps, and choose the map to display from existing maps.

When you start NNM, a map is automatically opened. You can specify a map by name, or you can let the ovw service open a default map. While a map is open for display, it is simply called an "opened map."

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0853
3740
Doc:

Pros/Cons of Multiple Maps

You can view your various maps through multiple NNM SESSIONS. HOWEVER, Only one map can be opened in a single session at any given time. A single user can open multiple maps by opening multiple NNM sessions. Different users can open the same map (at the same time) through different NNM sessions.

When multiple users access the same map, all users except the first one to access the map are limited to Read-Only access. This means that only the first users will be able to create map snapshots or access any modification features that you, the map administrator, made available to them.

Submaps

When you open a map, you actually view submaps of the map.

A **submap** is a particular view of the network environment. It consists of related symbols that are displayed in a single window. Each submap displays a different perspective of your map. NNM creates a root submap for each map. The root submap provides a standard, top-level submap for every map. Submaps are often organized in a hierarchical fashion for a given map, with the root submap at the top. You can also create independent submaps that are not associated with a hierarchy.

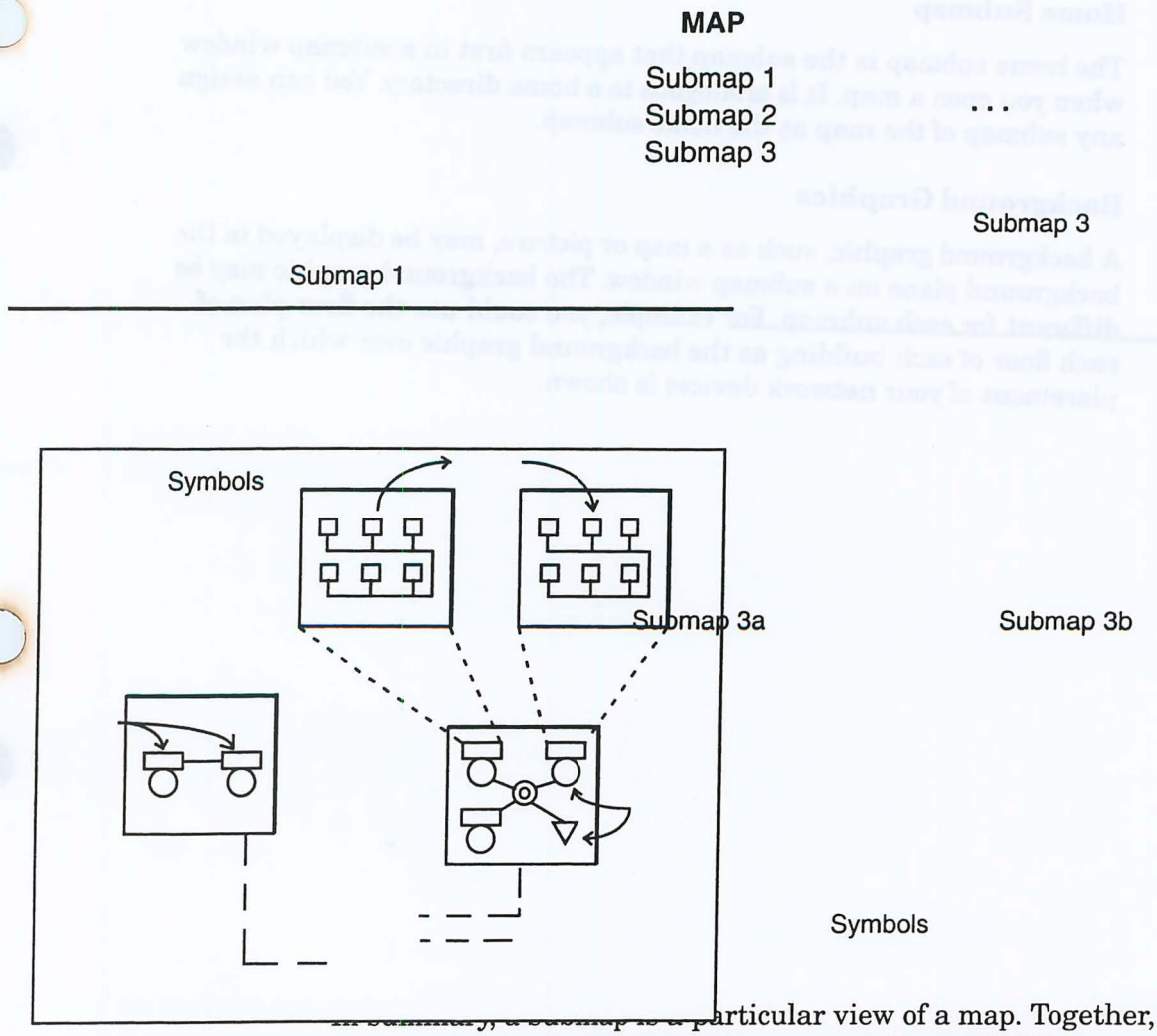
You can open and display multiple submaps of the open map at any given time, either by listing all the submaps of the open map and selecting the submaps to open, or by navigating from one submap to another. You can navigate among the submaps of the open map by double-clicking the mouse on explodable symbols. Double-clicking on an explodable symbol opens a submap that displays a more detailed view.

The hierarchical relationship of submaps creates a parent-child relationship between them. A submap may have several child submaps. The hierarchical relationship of submaps enables you to view your network from a distance, or to choose a more detailed view. For example, consider a submap that contains a single symbol that represents an entire organization. From this high-level view of the map, you can double-click on the symbol to open a child submap. The child submap may display a view of your network map from the perspective of a particular location. From there, you can select a specific department,

then a specific node. You can customize the organization of submaps in a map to suit your purposes; for example, to reflect the organization of your company.

The following figure shows how submaps and their symbols can be used to graphically display network or system management information in a network map.

Figure 7-1 Symbols and Submaps in a Map



In summary, a submap is a particular view of a map. Together, symbols, submaps, and maps make up the presentation of NNM.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0854
3740
Doc:

Root Submap

The root submap is the highest-level submap of the map. The first time a map is opened, the root submap is set as the default home submap.The root submap is a system-created submap that allows for the placement of very high-level objects by multiple applications. The root submap cannot be deleted. You can easily return to the root submap at any time by pressing the Home toolbar button.

Home Submap

The home submap is the submap that appears first in a submap window when you open a map. It is analogous to a home directory. You can assign any submap of the map as the home submap.

Background Graphics

A background graphic, such as a map or picture, may be displayed in the background plane on a submap window. The background graphic may be different for each submap. For example, you could use the floor plan of each floor of each building as the background graphic over which the placement of your network devices is shown.

Understanding Objects versus Symbols

An **object** represents a particular entity or resource in a networked systems environment. An object might represent a physical piece of equipment on the network, the components of a node on the network, or parts of the network itself. The object represents the resource by modeling the characteristics (attributes) of the resource. An object exists on a map by virtue of being represented by a symbol on a submap in a map.

A **symbol** is a graphical representation of an object. A single object can be represented by multiple symbols. Multiple symbols for the same object can exist on the same submap, on multiple submaps of the same map, or on submaps of different maps. This enables multiple users on different maps to view a symbol of the same object at the same time. A symbol never represents more than one object at a time.

In addition to representing objects, symbols have other functions:

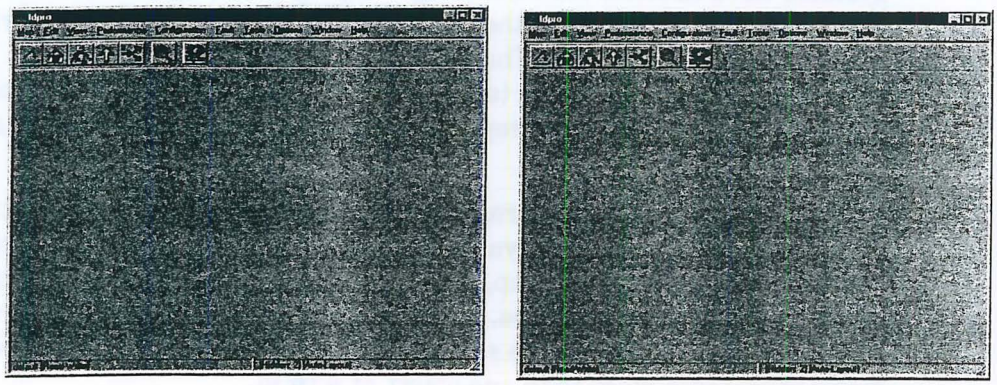
- Symbols let you navigate through the submaps of a map. Most symbols are explodable—when you double-click on an explodable symbol, a new submap window opens to let you "look inside" the object represented by the symbol.
- Some symbols execute actions. When you double-click on an executable symbol, a predefined action is executed on a predefined target.
- Symbols can be configured to reflect the status of the object that they represent or of objects in child submaps.

The following figure shows how symbols and objects are related. This figure contains two submaps that contain different symbols. Object Y is represented by a single symbol in the root submap, while Object X is

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0855
3740
Doc:

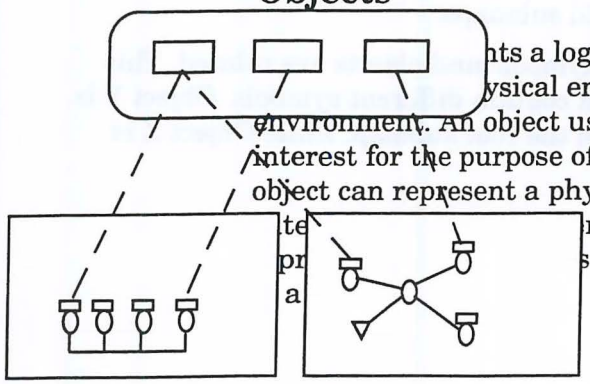
represented by symbols in both the root submap and submap2. Changes made to object X, such as a change in status, can be displayed in both symbols in the two submaps.

Figure 7-2 Object-Symbol Relationships





Objects



nts a logical or physical entity or resource, or a group of ysical entities or resources that exist in a network environment. An object usually represents any particular thing of interest for the purpose of doing network or systems management. An object can represent a physical item (such as a PC, a workstation, a te rface card, or an RS-232 connection), or it can pr such as a group of PCs, all 486 PCs, or all nodes a

Object Attributes/Properties

Each object stored in the map database contains attributes that define the object. An **attribute** is a characteristic of an object to which values can be assigned.

You can think of an attribute as a field that has a specific value. In an application dialog box that displays certain attributes of an object, the labeled fields represent the object' s attributes, and the data in the fields are the object's attribute values, such as:

- hostname
- address
- status
- description
- owner

Every object has a special attribute called a **selection name**. The selection name is a textual name that uniquely identifies the object. An object can have multiple names, but each name must be unique for its name space. For example, an object might have a hostname (for TCP/IP networks) and a fully distinguished name (for OSI networks). Either name could be used as the selection name.

The phrase **selection list** appears throughout this manual and relates to objects. The selection list is a list of objects that are represented by the symbols selected by the user. The selection list is one of the primary ways that you pass arguments to NNM.

The attributes of an object are displayed via the `Edit:Object Properties` dialog box. This dialog box displays the selection name of the object and displays any comments that you, or another user, may have entered about this object.

In the `Edit:Object Properties` dialog box, there is a list of attribute categories, such as General and Capabilities. These categories are accessed by applications that may be managing or monitoring certain attributes about the object. Applications may also add their own attribute category. You can view/modify the object attributes in each category.

- The `General Attributes` dialog box provides a place for applications and users to display attributes in one common location. The `General Attributes` dialog box may display attributes of an

IRQ Nº 03/2005 - CN -
CPMI - CORREIOS
IPIS. Nº 0856
Doc. 3740

object from multiple applications. These fields may also be displayed in application-specific dialog boxes. The specific fields that are displayed in this dialog box depend on the applications that register a field for this dialog box. Check NNM's online help in this dialog box for more information.

You can set the values of these attributes from the dialog box. Note that values set in this dialog box are not verified. Applications or users may add additional fields to this dialog box by setting a general flag for the field in the field registration file.

- The `Capabilities` dialog box includes the object attributes that determine menu graying. The capabilities of the objects on the current selection list determine which menu items are enabled or disabled. All attributes displayed in the `Capabilities` dialog box are read-only.

  The default for this dialog box is that unset capability fields are not displayed. You can change the behavior of this dialog box so that the unset fields *are* displayed by modifying your Windows system registry or UNIX `$APP_DEFS/OVw` file and changing the value of `showUnsetCapabilitiesFields` to `TRUE`.

The same information is available in the `Edit:Add Object` dialog box. This enables you to assign attribute values during object creation.

Operations on Objects

Check NNM's online help for information about the operations you may commonly perform on objects, such as:

- adding an object
- selecting one or more objects
- locating objects
- adding attributes to an object
- changing an object's description
- changing the vendor and SNMP agent values
- deleting an object
- hiding an object
- showing a hidden object

Symbols

A symbol provides a graphical representation of a particular object. NNM uses two varieties of symbols for display on the map: icon symbols and connection symbols.

- *Icon symbols*, usually referred to simply as a symbol, consists of a geometric shape. A symbol graphic, or icon, usually appears inside the shape.
- *Connection symbols* connect two icon symbols or an icon symbol and a backbone. On a submap, connection symbols appear as lines. However, connection symbols are not merely lines. They represent objects and can display status. NNM uses connection symbols to show the current state of connections between resources on your network.

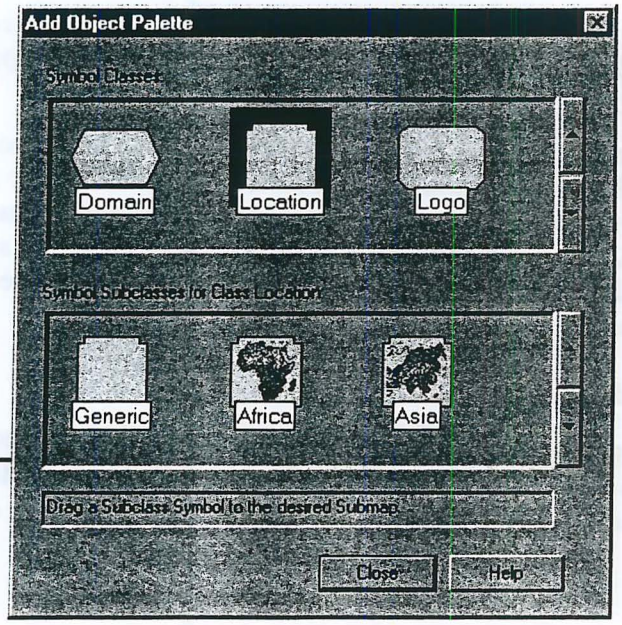
Icon Symbols

Icon symbols include many symbol types. A symbol type consists of the symbol class and symbol subclass. The symbol class is indicated by the outside shape of the symbol. Each symbol class is further divided into

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0857
3740
Doc:

subclasses. Figure 7-3 displays the palette as it appears when you select the `Location` class. The subclasses of the selected symbol class are displayed in the lower portion of the palette.

Figure 7-3 **Subclasses in the Location Class**



NNM contains a variety of predefined symbols. You can view the available symbols by browsing through the palette or by looking at the `Display Legend` dialog box. To view the legend, select `Help:Display Legend` from the menu bar. The classes and respective subclasses that are registered by NNM are listed in the `Add Object Palette`.

Connection Symbols

A connection symbol is a line that graphically connects two icon symbols or an icon symbol and a backbone (a bus or a ring backbone) on a submap. The connection symbol displays the status of a connection between two objects. Connection symbols behave like icon symbols in the following ways:

- A connection symbol represents an object, just like an icon symbol.
- Connection symbols may reside on the application plane or the user plane.

- You can display a symbol pop-up menu for the connection, and open the `Symbol Properties` dialog box to view or change symbol characteristics.
- You can assign a label to the connection symbol.
- You can change the type of a connection symbol.

Like an icon symbol, the connection symbol may be explodable or executable.

Symbol Characteristics

The following list discusses characteristics of symbols.

Symbol Variety — Symbols come in two varieties: the icon symbol and the connection symbol.

Symbol Type — Symbol type consists of the symbol class and subclass.

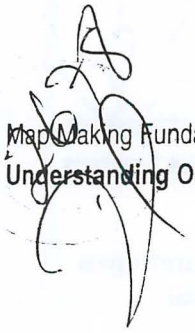
- **Class** — You can distinguish the symbol class by the outer shape of the symbol. For example, a circle, square, diamond, and so on.
- **Subclass** — A subclass is a further definition of the class. Each symbol class has a unique set of subclasses.

Status — NNM displays status information by changing the color of the class (or outer shape) of the symbol. The ten status states are categorized as either administrative or operational (see page 270).

Label — You can label each symbol that appears on your network map. The label appears below the symbol. You can choose whether or not to display the label of a symbol.

Location — A symbol can reside on one of two planes: the application plane or the user plane. If an object is not managed by any application, then symbols of that object reside on the user plane of the submap and have a box displayed around them. If an object is managed by one or more applications in a particular submap, then symbols of that object reside on the application

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0858
3740
Doc:



plane of that submap. This enables you to visually distinguish between objects that are being managed by applications and those objects that are not.

Behavior	Behavior defines how the symbol behaves when you double-click on the symbol. A symbol may behave in one of two ways. It may open a child submap (explode the child submap), or it may execute an application.
Status Source	A symbol may present status information from one of three sources (see page 273). This characteristic enables applications to have more control over the presentation of status. In general, you do not need to change these settings.

Operations on Symbols

Check NNM's online help for information about the operations you may commonly perform on symbols. Many of these symbol operations can be performed from the symbol pop-up menu:

- Adding a connection symbol
- Adding an executable symbol
- Adding an icon symbol
- Changing symbol behavior
- Changing a symbol label
- Changing a symbol type
- Cutting and pasting symbols
- Copying a symbol

See also Appendix D, "Changing All the Symbols for a Particular Device," on page 661.

8 Map Customization

RQS nº 03/2005 - CN
CPMI - CORREIOS
0859
Fls. Nº
3740
Doc:

Putting It All Together

After you create the initial map and clean up any network problems that were identified, you have the *default* map. (See Chapter 5, Initial Network Discovery: Options and Troubleshooting, if you need to create the default map.) The purpose of the default map is to display a map of your network quickly when you first run NNM. Now you are ready to create copies of the default map and customize the copies for your specific needs.

You can create multiple maps and customize the way in which information about objects is displayed on each map. This enables you to distribute resources over your map to better match how your network and/or team is organized. Multiple maps can display information about the same object because all maps obtain their information from the same source, the object database.

Which Maps for Which Users

In Chapter 4, Planning Your NNM Configuration, you identified the groups or individuals within your organization who need access to the maps. You also identified which aspects of your network each group or individual needs to see on their maps.

Identifying the Purpose of Each Map

As you develop your custom maps, keep in mind the type of problem each group or individual is trying to prevent or solve by using the map. Design their map so that the amount of information displayed is limited to the minimum relevant information and that the information is presented in such a way that it makes their job easier. For example: the map for printer maintenance may show only printers and print servers with backgrounds showing actual floor plans to aid quick response efforts; the map for network troubleshooters might need to contain network infrastructure devices across the entire company; and the map for upper-management to use during client visits might need to show everything possible to look large and impressive.

Determining How Many People Need Access to Each Map

In Chapter 4, you built a model of your customer base and network support team to understand how NNM can be customized to most effectively help your team.

Can any of the groups that you identified share a map, or do their information needs require completely different maps?

Keep in mind that a number of people can view one map simultaneously or multiple maps by using remote console access (see *A Guide to Scalability and Distribution* for information) or by using NNM's new web access (see Chapter 14, NNM on the Web,). When multiple people are accessing a single map, only the first user to open the map has read-write permission (provided that they have read-write permission to the map file), which means that only one person will be able to make changes to the map. However, everyone accessing NNM can acknowledge/delete alarms from the Alarm Browser as issues are resolved.

The number of remote access logins that can be supported is dependent upon a number of factors. See the *Performance and Configuration Guide* that was included with NNM's installation package.

Planning Your Efforts

The remainder of this chapter presents a series of possible map customizing changes. Focus on customizations that help your team meet a business need. After initial map customizing, NNM users tend to use the Alarm Browser on a day-to-day basis and only use the map while troubleshooting a specific network alarm. So keep map customizations to a workable minimum. The customizing options are:

- "Copying the Default Map" on page 215
- "Controlling the Display of Devices Attached to Switches or Bridges" on page 217
- "Giving Your Network Symbols Meaningful Names" on page 221
- "Turning Connection Labels on or off" on page 223
- "Configuring Trunking and Meshing" on page 225
- "Establishing Submap Persistence Settings" on page 229
- "Controlling Which Devices Appear on the Map" on page 232

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0860
Fls: Nº
3740
Doc:

- "Changing/Adding Object Attribute Fields" on page 235
- "Making the Maps Look Like Your World" on page 240
- "Creating Your Own Map Symbols" on page 263
- "Specifying the Placement and Size of the Submap Windows" on page 266
- "Miscellaneous Configuration Changes" on page 268
- "Controlling Symbol Status" on page 270
- "Creating New NNM Features to Meet Your Team's Needs" on page 278

Customizing the maps requires a substantial time commitment and should be done by someone who understands NNM and your network. To protect your efforts, you may want to remove functionality from the maps so that your team cannot accidentally make changes to your customizations. See Chapter 9, "Controlling Map Access," on page 283.

Copying the Default Map

When you start NNM, the default map is automatically opened with the home submap displayed. You can create multiple maps and specify which map NNM displays initially. Only one map can be opened in a single session at any given time. Different users can open the same map (at the same time) through different NNM sessions, although only the first session opened would include read-write capabilities (provided that they have read-write permission to the map file). All other instances of the same map would be set to read-only.

The `Map:Save As` menu item copies only the currently *open* map and saves it under the new name you specify. Do this when you want to:

- Create multiple maps with similar characteristics.
- Create a specific map for each user. By copying one map, they all initially have similar or identical characteristics; although as changes are made, the maps will diverge.
- Create a writable version of the current map if the currently open map is set to `read-only`.

See the NNM online help if you need more information. See also the *ovw* reference page in NNM's online help (or the UNIX manpage) for information about command line options for copying maps.

The new map is not automatically opened. You can open the new map by selecting the `Map:Open` menu item and selecting the map name that you specified.

Copy the default map now and open the copy before you start making customizations. You can always return to your default map if you make a mistake.

Your Map Strategy

Refer to your worksheets from Chapter 4, Planning Your NNM Configuration, where you identified which maps were needed by your organization. This chapter leads you through the map customization process. Think about how you might leverage your work from one map to another to keep this process as simple as possible. For example, first

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0861
3740
Doc:

make customizations that are common to all required maps. Then make multiple copies of that map before making the finishing touches for each department.

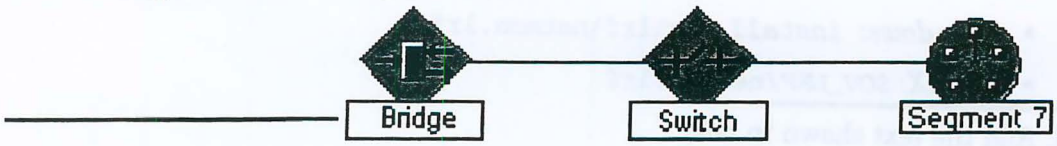
You can set a different Home submap for each user of the map, if you wish (page 287).

Controlling the Display of Devices Attached to Switches or Bridges

NNM has two methods for displaying the devices that are directly attached to ports on switches or bridges:

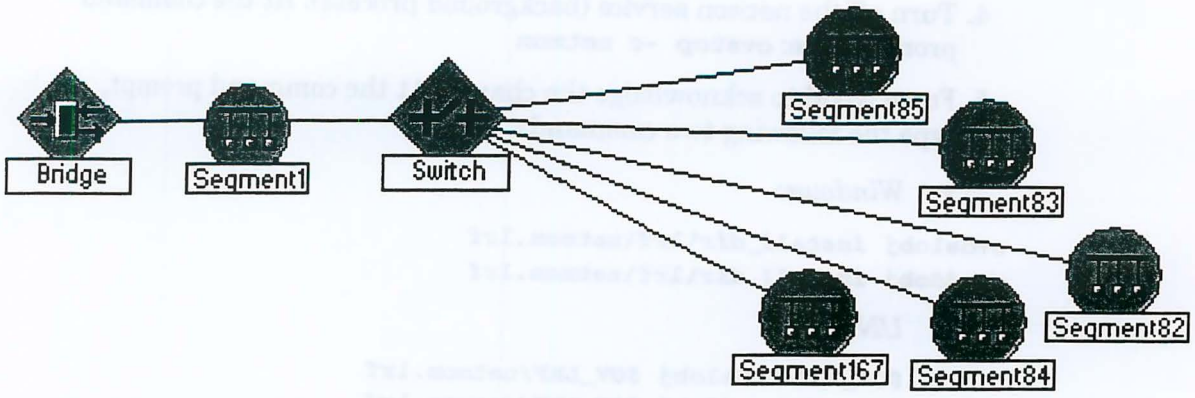
1. Each attached device is presented as part of a star configuration. You double-click on the star segment icon that is attached to a switch or bridge to display all attached devices on one submap. The star segment presentation is the recommended choice. Your map is less cluttered and easier to use when troubleshooting problems.

Figure 8-1 SegRedux On



2. Each attached device is presented as a separate bus segment. You can check the status of each device on its own separate bus segment.

Figure 8-2 SegRedux Off



RQS nº 03/2005 - CN - CPMI - CORREIOS
217
Fls. Nº 0862
3740

Turning On Star Configuration for Attached Devices

If you installed NNM for the first time, devices that are directly attached to ports on switches or bridges are automatically displayed in the star configuration. If you *upgraded* NNM from a previous version, you need to take the following steps in order to update your map and NNM's databases so that devices directly attached to ports on switches or bridges are displayed in the star configuration.

1. Log in as:
   - *Windows:* `Administrator`
   - *UNIX:* `root`
2. Open the `netmon` local registration file in the ASCII editing software of your choice:
   - *Windows:* *`install_dir`*`\lrf\netmon.lrf`
   - *UNIX:* `$OV_LRF/netmon.lrf`
3. Add the text shown in bold:

```
netmon:netmon:
OVs_YES_START:ovtopmd,pmd,ovwdb:-P -k segRedux=true:OVs_WELL_BEHAVED:15:PAUSE::
```

   See the *netmon* reference page in NNM's online help (or the UNIX manpage); read about the `-k` keyword parameter and the `segRedux` keyword argument for more information.
4. Turn off the `netmon` service (background process). At the command prompt, type: **`ovstop -c netmon`**
5. Force NNM to acknowledge the change. At the command prompt, type the following two commands:
   - *Windows:*

```
ovdelobj install_dir\lrf\netmon.lrf
ovaddobj install_dir\lrf\netmon.lrf
```

   - *UNIX:*

```
$OV_BIN/ovdelobj $OV_LRF/netmon.lrf
$OV_BIN/ovaddobj $OV_LRF/netmon.lrf
```

6. Turn on the `netmon` service (background process). At the command prompt, type: **`ovstart -c netmon`**

NNM now displays all devices that are directly attached to the ports on a switch or bridge in one star segment submap.

Turning Off Star Configuration for Attached Devices

If you want to turn off this feature, you need to take the following steps in order to update your map and NNM's databases.

1. Log in as:
   - *Windows:* `Administrator`
   - *UNIX:* `root`
2. Open the netmon local registration file in the ASCII editing software of your choice:
   - *Windows:* *install_dir*`\lrf\netmon.lrf`
   - *UNIX:* `$OV_LRF/netmon.lrf`
3. Change the *true* to *false* (or delete the text shown in bold):

```
netmon:netmon:
OVs_YES_START:ovtopmd,pmd,ovwdb:-P -k segRedux=true:OVs_WELL_BEHAVED:15:PAUSE::
```

   See the *netmon* reference page in NNM's online help (or the UNIX manpage); read about the `-k` keyword parameter and the `segRedux` keyword argument for more information.
4. Turn off the `netmon` service (background process). At the command prompt, type: **`ovstop -c netmon`**
5. Force NNM to acknowledge the change. At the command prompt, type the following two commands:
   - *Windows:*

```
ovdelobj install_dir\lrf\netmon.lrf
ovaddobj install_dir\lrf\netmon.lrf
```

   - *UNIX:*

```
$OV_BIN/ovdelobj $OV_LRF/netmon.lrf
$OV_BIN/ovaddobj $OV_LRF/netmon.lrf
```

6. Clean up NNM's databases to update the configuration information. At the command prompt, type:
   - *Windows:* **`ovtopofix -l`**

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0863
Doc: 3740

- *UNIX:* **`$OV_BIN/ovtopofix -l`**

See the *ovtopofix* reference page in NNM's online help (or the UNIX manpage); read about the `-l` parameter for more information.

7. Turn on the `netmon` service (background process). At the command prompt, type: **`ovstart -c netmon`**

   NNM displays a separate bus segment for each device directly attached to a port on a switch or bridge.

Giving Your Network Symbols Meaningful Names

You can easily provide meaningful names for your network symbols, rather than their IP addresses; for example, Finance, R&D, or Manufacturing. Simply make additions to the list in the following file:

- *Windows:* `\WinNT\system32\drivers\etc\networks`
- *UNIX:* `/etc/networks`

Follow the directions at the top of this ASCII file. Make a list of all your network IP addresses and the corresponding names that would be most meaningful to your team. To force NNM to acknowledge the change, at the command prompt type:

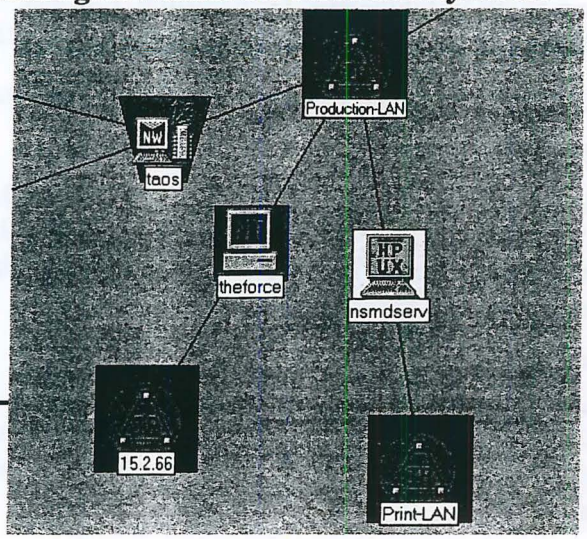
```
ovstop netmon
ovstart netmon
```

Once NNM synchronizes, the new names appear on your maps. Your changes to this file are preserved when applying NNM patches or upgrades.

RQS nº 03/2005 - CN - CPMI - CORREIOS
221
Fls. Nº 0864
3740
Doc:

NOTE This change is visible from remote consoles and web access after the map is reloaded or refreshed on each system.

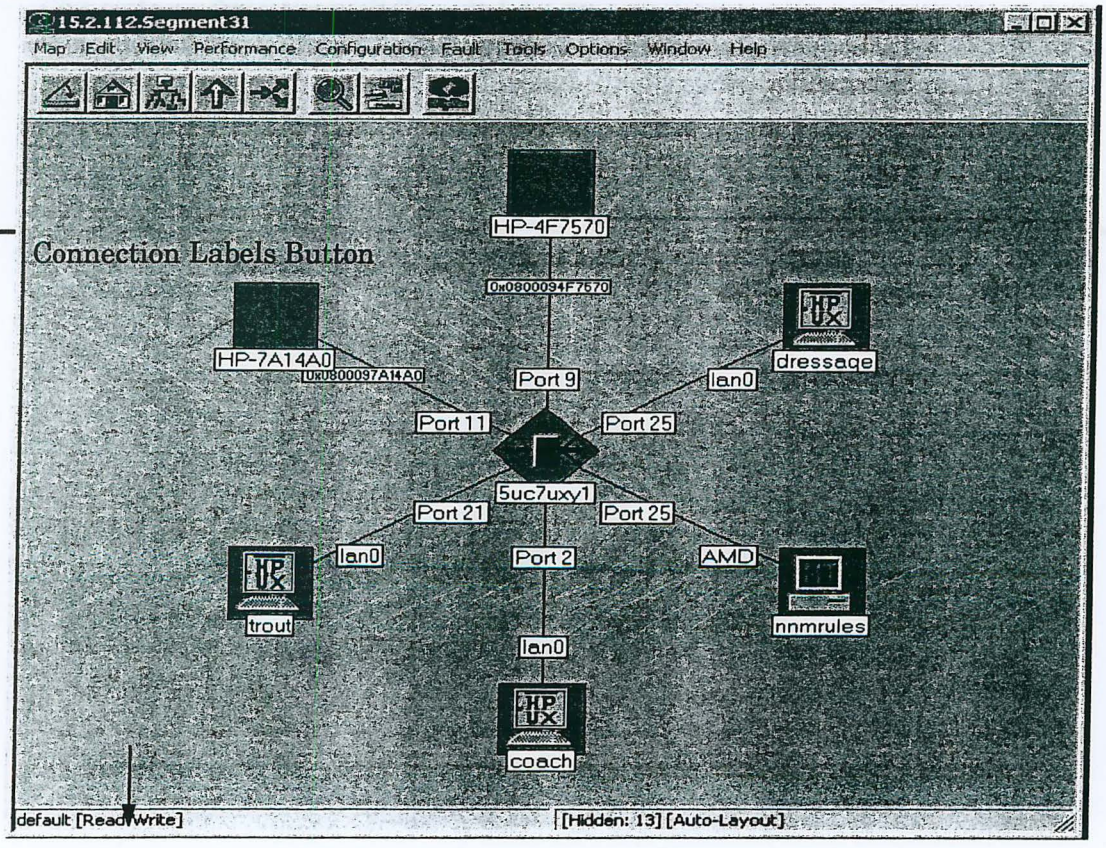
Figure 8-3 Meaningful Names for Network Symbols



Turning Connection Labels on or off

Connection labels indicate the port used to connect one network interface to another. Use either the `View:Show Connection Labels` menu item or the `Connection Labels` button to turn this feature on or off. On a Windows operating system you can control the connection label feature through the `View` tab contained in the `Map:Properties` or `Submap:Properties` pull-down menus.

Figure 8-4 Show Connection Labels Enabled



NNM labels each end of a connection unless one end is a container object such as a segment, network, or location. Connection labels are created from information made available by equipment manufacturers. Since

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0865
3740
Doc:

devices return information in varying formats, connection labels vary from device to device. If NNM cannot read or understand the information from a device, it will not label the connection.

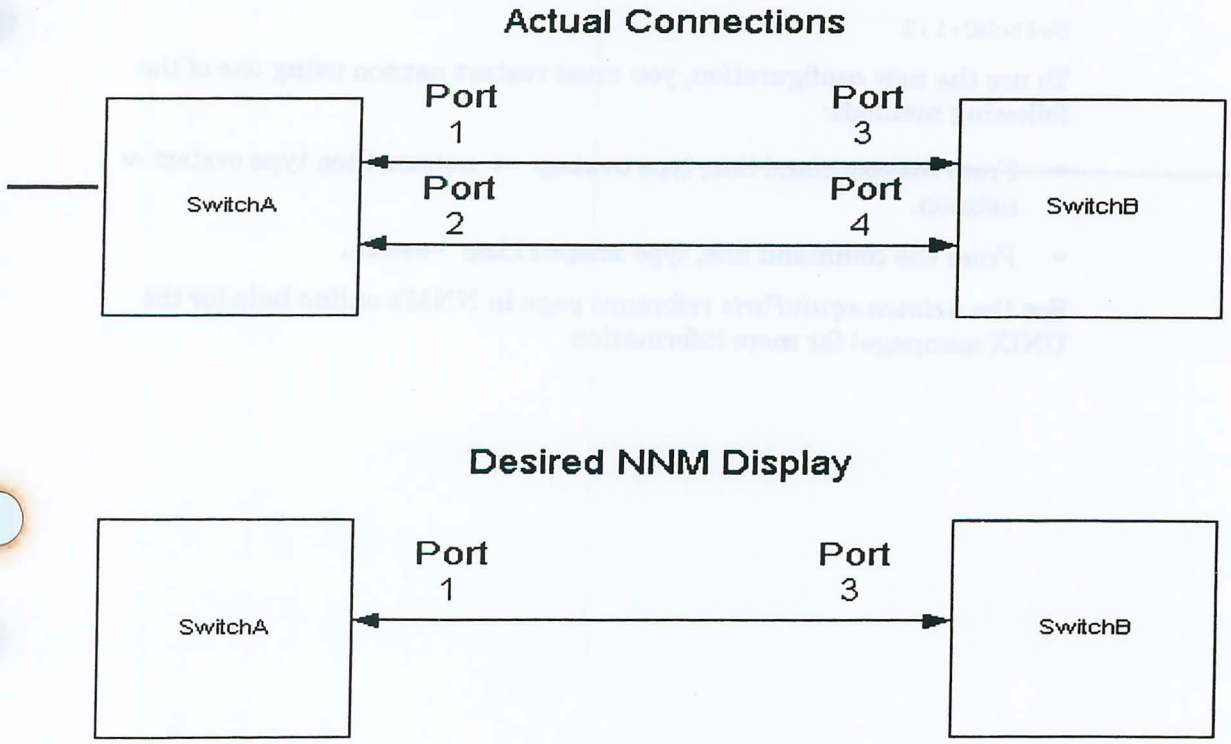
For devices that do not respond to SNMP requests, the connection label usually defaults to the IP address of the node. One common cause of devices not responding to SNMP requests is a mismatched community name. If you suspect that your GET-Community names are not matching up with the settings on your management station, see"GET- and SET-Community Name and SNMP Port Issues" on page 145.

The connection label depends on information gathered during discovery and may be updated during a configuration poll. Changes on the devices may not appear on the connection label until the next configuration poll. To force an update of the connection labels, at the command prompt, type **`ovtopofix -U`**.

Configuring Trunking and Meshing

Configuring two or more ports between two network devices into a single group is referred to as **port trunking**. This is done to increase the available bandwidth between two devices. For example, look at the actual connections diagrammed in Figure 8-5. The available bandwidth between switches A and B increases when ports 1 and 2 on switch A and ports 3 and 4 on switch B are connected in a trunk configuration.

Figure 8-5 A Port Trunking Example



NNM is unable to detect port trunking and meshing automatically. For example, NNM will move devices around on your map depending on which port in the trunk or mesh configuration it last heard the device. To control NNM's representation of this topology, you can enter port trunking configuration information into the following file:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0866
3740
Doc:

To specify a mesh, add a line in the `netmon.equivPorts` file for each switch participating in the mesh. The `netmon.equivPorts` file consists of parameters in the format *`host`*`:`*`port-spec`*`:`*`port-spec`*`:[`*`port-spec`*`]` where *`host`* is an object identifier such as a host name, IP address, or MAC address, and *`port-spec`* is a combination of *`group_number`*, *`port_number`*.

When labeling any of the ports participating in a mesh relationship, NNM labels the object with the first *`port-spec`* parameter from the `netmon.equivPorts` device line entry.

For example, to achieve the results shown in Figure 8-6, the `netmon.equivPorts` file would have the following entries:

```
SwitchB:1:2

SwitchC:1:2
```

To use the new configuration, you must restart `netmon` using one of the following methods:

- From the command line, type **`ovstop -v netmon`** then type ovstart -v netmon.
- From the command line, type **`xnmpolling -event`**.

See the *netmon.equivPorts* reference page in NNM's online help (or the UNIX manpage) for more information

Establishing Submap Persistence Settings

The persistence settings allow you to control the number of submaps that are retained in memory (RAM) so that they are available at all times, rather than generated upon demand. There are several of things to keep in mind when making your choices:

- Persistent submaps display faster.
- The greater the number of persistent submaps, the greater the need for RAM on the management station.
- Only those submaps that are persistent are included when a map snapshot is created.
- Only those submaps that are persistent are included in the initial scoping pane list for NNM's web access.
- You can set persistence by logical level of network structure (such as internet level, network level, or segment level).
- You can establish a persistence filter that specifies making persistent all submaps that contain certain devices, that you specify (page 230).
- Any time that you make an editing modification directly to a l all related parent submaps up to the internet level become persistent; for example, turn off auto-layout, set window geometry, add a background graphic, or add an

NOTE If you add background graphics to your submaps, they automatically become persistent. Keep in mind that graphic files are quite large and may significantly increase the amount of memory required to keep the submap in RAM.

NNM's default setting for this feature:

- *Windows:* Only the Internet level and the containment realm of the map are persistent.
- *UNIX:* All levels of the map are persistent.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0867
3740
Doc:

NOTE The selection that you make affects remote consoles and the web display after the map is reloaded or refreshed on each system.

By Logical-level of Your Network's Structure

If you choose to set the persistence by logical level, select the `Map:Properties` menu item, select the `Applications` tab, and double-click the `IP Map` entry. The level to which submaps should be persistent can be one of the following values:

`Unset` — *Windows:* Same as `Internet Level`.

UNIX: Same as `All Levels`.

`All Levels` — Specifies all submaps as persistent.

`Segment Level and Higher` — Specifies that Segment-, Network-, and Internet-level submaps are persistent.

`Network Level and Higher` — Specifies that Network- and Internet-level submaps are persistent.

`Internet Level` — Specifies that Internet-level submaps are persistent.

By Presence of Specific Devices

A persistence filter describes which specific network devices should have their submaps retained in memory (RAM) at all times.

This may be useful if you want to use the snapshot feature (see Appendix B, "Network Troubleshooting Tools," on page 553 or NNM's online help) as part of your normal business procedures and need to make sure the snapshots always include information about specific critical devices. It may also be a useful way to keep the number of submaps retained in memory (RAM) to a minimum when you are using an HP OpenView program that requires the submaps containing certain devices to remain present in RAM.

The persistence filter is defined in the `filters` file (the same file that contains any discovery filters, DHCP filters, etc.):

- *Windows:* `install_dir\conf\C\filters`
- *UNIX:* `$OV_CONF/C/filters`

NNM includes a predefined persistence filter section for your convenience as a starting point, or you may define your own. For detailed information about how to develop a filter, refer to *A Guide to Scalability and Distribution*.

After you create your persistence filter:

- Select the `Map:Properties` menu item, select the `Applications` tab, and double-click the `IP Map` entry.
- Click on `Persistence Filter` and type the name of the section in NNM's `filters` file that you just created.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
231
Fls. Nº 0868
3740
Doc:

Controlling Which Devices Appear on the Map

You can control which devices are visible on a particular map. It is important to remember that all maps derive their information from the same database, so *deleting* an object (specific device) from the database eliminates it from all maps (until the next discovery polling interval). Rather than using delete, consider the following choices:

- Map Filter:

  A map filter allows you to remove nodes from view on the map. You write the map filter using Boolean logic and place it in the `filters` file with all the other NNM filters. You can create multiple map filters and assign a unique filter to each map.

- Hide Feature:

  The hide feature enables you to modify which group of symbols is displayed on any submap in an interactive way (without needing to write a filter using Boolean logic).

NOTE These changes are visible from remote consoles and web access after the map is reloaded or refreshed on each system.

Creating a Map Filter

A map filter allows you to remove certain nodes from view on the map while continuing to monitor them and receive alarms from them in the event/alarm portion of NNM. Map filters are defined in the `filters` file (the same file that contains any discovery filters, DHCP filters, and so on):

- *Windows:* `install_dir\conf\C\filters`
- *UNIX:* `$OV_CONF/C/filters`

See *A Guide to Scalability and Distribution* for information about creating filters.

You can create multiple map filters and assign a unique filter to each map. See the `filters` file for predefined examples as a starting point. Your filter can be applied/changed at any time by opening the map, selecting `Map:Properties`, selecting the `Applications` tab, and opening the configuration dialog box for `IP Map`.

Testing Your Filter

See *A Guide to Scalability and Distribution* for information about testing and troubleshooting your filters.

Using the Hide Feature

The hide feature allows you to customize individual submaps as well as all submaps in a map. For example, you may wish to hide everything except printers to create a special set of submaps specifically for monitoring printers, or hide everything except routers to create a special submap specifically for monitoring routers. Because all maps derive their information from the same database, if you delete all instances of any symbol, the underlying object in the database is also deleted. The hide feature enables you to modify the group of symbols displayed on any submap in an interactive way (without needing to learn Boolean logic in order to write a filter).

NOTE If the submap is transient, it becomes persistent when you hide a symbol. (Use the map filter if you wish to hide symbols without effecting persistence.)

If devices are hidden on a particular submap:

- `[Hidden:#]` appears on the right side of the status bar giving notice about how many devices are hidden (# = number of hidden objects).
- There is no way to determine which devices are hidden, only how many are hidden.
- If you wish to show a hidden object on a particular submap, you must show all hidden objects. There is no way to specify which hidden objects to show.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0869
3740
Doc:

To hide a symbol, select the symbol or symbols that you wish to hide, select `View:Hidden Objects`, and select `Hide Selected From This Submap` or `Hide Selected From All Submaps`. You can use the Find feature in partnership with the Hide feature to hide groups of symbols such as all routers.

Testing and Troubleshooting

If you choose to hide a symbol from all submaps but change your mind later, to undo the action you must show ALL hidden symbols on ALL submaps.

To display hidden symbols on individual submaps, open each affected submap and select `View:Hidden Objects->Show Hidden On This Submap`.

To display hidden symbols on all submaps, open any submap and select `View:Hidden Objects->Show Hidden On All Submaps`.

Backing Up Your Efforts

The next time NNM's backup process runs, your modifications will be included.

Changing/Adding Object Attribute Fields

You may wish to modify or add object attribute field definitions so that your team can search on custom criteria when resolving network problems or so that a new application can manage the object.

NOTE You can only add fields, you cannot delete them. Adding fields does not affect submap persistence.

An NNM object represents a logical or physical entity or resource, or a group of such logical or physical entities or resources that exist in a network environment. In NNM, an object usually represents any particular thing of interest for the purpose of doing network or systems management. An object can represent a physical item (such as a PC, a gateway, a router, or an interface card) or it can represent a logical item (such as a group of PCs, all 486 PCs, or all nodes in a single department). An object is represented on the map graphically by a symbol.

An object is constructed of individual characteristics that are called attributes. Attributes include the name of the object and various characteristics that are used to classify the object. An object, for example, might have the name `IP Hostname` and an attribute such as `isDevice`.

To view the attributes assigned to any object, select any symbol that represents the object and then display the `Edit:Object Properties` dialog box. A list of attribute categories is displayed, such as `Capabilities`, `General Attributes`, and application-specific categories such as `IP Map` (an application included in NNM). Select any category to display its list of attribute names and values.

The attribute names represent fields in the NNM object database, and the data in the fields are the object's attribute values. Possible modifications/additions to the information in the object database:

- Change the current value in an attribute field through the object properties' `General Attributes` dialog box.
- Change a symbol's *type* in order to switch to a different set of attribute fields.

RQS nº 03/2005 - CN - CPMI - CORREIOS
235
Fls. Nº 0870
3740
Doc:

- Add underlying definitions of attribute fields by editing field registration files (FRF).

These changes are visible from remote consoles and NNM's web interface after the map is reloaded or refreshed on each system.

TIP

The following *analytical data* directories are *not* included in NNM's backup scripts:

- *Windows:*

  ```
  install_dir\backgrounds
  install_dir\bitmaps
  install_dir\www\htdocs\bitmaps
  install_dir\www\registration
  ```

- *UNIX:*

  ```
  $OV_BACKGROUNDS
  $OV_BITMAPS
  $OV_WWW/htdocs/bitmaps
  $OV_WWW_REG
  ```

If you make changes or additions to map backgrounds, bitmap files, or web registration files ensure that your new files are properly backed up. See "Backup/Restore to Protect Your Investment of Time" on page 165 for more information.

Changing the Value in an Attribute Field

You can change the description of an object by modifying the values assigned to its attributes (characteristics) in the `General Attributes` dialog box. See NNM's online help for more information.

To change object attribute values:

- *Windows:* Select a symbol; then select `Edit:Object Properties`. Alternately, right-click the a symbol and select `Object Properties` from the pop-up menu. The values in the `General Attributes` dialog box can be modified. To edit these values, click on the attribute name.

- *UNIX:* Select a symbol; then select `Edit:Object Properties`. Alternately, click mouse button 3 on a symbol and select `Object Properties` from the pop-up menu. The values in the `General Attributes` dialog box can be modified. To edit these values, click on the attribute name.

For example, clicking on `isSNMPSupported` will toggle the value between `TRUE` and `FALSE`; clicking on `SNMPAgent` will pop-up a dialog box from which you can choose the SNMP agent.

NOTE This change is visible from remote consoles and the web interface after the map is reloaded or refreshed on each system.

Changing Symbol Type to Switch Attribute Sets

You can assign a new set of attributes to an object by changing the symbol type of the object.

NOTE This step adds fields, but does not delete or change values in existing fields.

l and select `Change Symbol Type` from the pop-up menu.

UNIX: Click mouse button 3 on a symbol and select `Change Symbol Type` from the pop-up menu.

NOTE This change is visible from remote consoles and the web interface after the map is reloaded or refreshed on each system. Changing the symbol type forces the submap to become persistent.

See NNM's online help for more information about changing symbol type. See also the *OVwRegIntro* reference page in NNM's online help (or the UNIX manpage) for more information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0871
3740
Doc:

NOTE

The `ipmap` service automatically assigns a symbol type and label based upon information it receives from the `netmon` service. This means that if you modify the symbol label or symbol type of an object that is managed by NNM, your changes will be replaced by the values assigned by NNM the next time configuration polling runs.

You can turn off this `ipmap` capability by setting the environment variable `IPMAP_NO_SYMBOL_CHANGES=TRUE`. See the *ipmap* reference page in NNM's online help (or the UNIX manpage) for information about the `-u` parameter.

Alternately, you can modify the `oid_to_sym` file to specify that a different symbol be associated with a specific *type* of device (determined by `sysObjectID`). See the *oid_to_sym* reference page in NNM's online help (or the UNIX manpage) for more information. See "Changing All the Symbols for a Particular Device" on page 661 for a complete example.

Adding Attribute Fields in the Object Database

If you want to add a specific attribute field that is not yet defined in the object database, you simply create or modify the field registration files (FRF):

- *Windows:* *install_dir*`\fields\C\*.*`
- *UNIX:* `$OV_FIELDS/$LANG/*`

See NNM's online manual, *Creating and Using Registration Files*, for complete information about changing fields or adding fields.

See the *OVWRegIntro* reference page in NNM's online help (or the UNIX manpage) for more information.

TIP

Set the `Locate` and `General` flag for the field when you define it. `Locate` enables your new field to appear in the `Edit:Find->Object by Attribute` dialog box. `General` enables the field to show up in the `Object Properties, General Attributes` category.

After you have modified the field registration files:

1. Display a list of currently running sessions. At the command prompt type:

   ovstatus -v ovuispmd

   You may want to print out this information so that you have the hostnames and session IDs for restarting the sessions later. You may wish to notify those users who are currently accessing NNM to warn them about the shutdown.

2. Stop all sessions. At the command prompt, type:

   ovstop -c ovuispmd

   (This terminates any sessions and stops only the `ovuispmd` service--the maps are all closed, but your network is still being monitored by NNM.)

3. Force NNM to update the field definitions in the object database. At the command prompt, type:

   ovw -fields

4. To start new NNM sessions, at the command prompt, type:

   ovstart -c ovuispmd

5. Open NNM's user interface to begin one or more sessions.

parsed for correctness and checked for errors which are reported to:

- *Windows:* The error message pop-up `Console` window. Messages are always appended to the end of the Console file. It is a good idea to clear the contents of this file (`Edit:Clear`) each time that you see it.
- *UNIX:* `stderr`

Close the NNM interface and reopen the maps to view your changes (see "Closing All Current Sessions" on page 319).

NOTE These changes are visible from remote consoles and web access after the map is reloaded on each system.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0872
3740
Doc:

Making the Maps Look Like Your World

Review the worksheet from Chapter 4, Planning Your NNM Configuration, where you identified the maps that your organization needs and the network devices that need to be present on each map. Now customize the look of each map to meet the needs of your team. When you edit a map, your changes affect only the *open* map. If you want the same customizations on multiple maps, make the changes once, then copy the modified map. A map can be customized in the following ways:

- By controlling the placement of the symbols on your map.
  By default, NNM controls how symbols are placed on your submaps, but you can take control of how symbols are placed on individual submaps. You can also turn off auto-layout for the whole map.
- By adding your own submaps:
  - *Partitioned Internet* submaps (child submaps at the Internet-level) to break the Internet symbols into smaller groups of information, such as by country, city, building, department, or floor by using container objects (location symbols). These changes (*and these changes only*) can be copied to other maps using the `Map:Export` and `Map:Import` feature.
  - *Child* submaps (at the Network-, Segment-, or Node-level) to add more information to an explodable symbol.
  - *Meta-connection* submaps automatically created by NNM whenever there are multiple connections between two symbols. Double-click on the connecting line to explode a submap showing each connecting-line symbol.
  - *Independent* submaps to create your own custom hierarchy of submaps that is independent of the hierarchy automatically created.
- By adding background graphics such as map images, site-specific images, or floor plans ("Background Graphics" on page 260). Use *.GIF files to ensure that the background graphics are visible over web access.

NOTE These changes are visible from remote consoles after the map is reloaded or refreshed on each system. These changes are immediately visible in NNM on the web.

Controlling the Placement of the Symbols on Your Map

NNM's auto-layout controls the placement of symbols on the maps (see "Automatic Discovery and Layout" on page 56 for more information about how auto-layout works). If you want to make changes to the placement of symbols, you must first turn off auto-layout. Auto-layout can be turned `On/Off` for a single submap or for all submaps in the open map.When auto-layout is turned off, the `[Auto-Layout]` message at the bottom of each affected submap disappears, and the `New Object Holding Area` appears across the bottom of the submap. Any time a new object is discovered, a map symbol is moved to another submap, a bridge or hub is moved within a network submap, or a hidden object is set to show on your network, the affected symbols will show up in the `New Object Holding Area` to await your decision about placement.

TIP When accessing NNM over the web, there is no `New Object Holding Area`. However, the status bar notifies you if objects are currently in the `New Object Holding Area`.

Auto-Layout Algorithms (Default Layout Rules)

The layout algorithm for a submap is set when the submap is created. If an application (such as NNM) creates the submap, it specifies a layout algorithm. NNM's default layout algorithm for a submap is based upon the symbol type of the parent object and cannot be changed after the submap is created.

The possible layout algorithms are:

- None. Symbols are arranged by the user or are left in the `New Object Holding Area`.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0873
Doc: 3740

- Point To Point. Symbols are arranged as an arbitrarily interconnected set of nodes and connections.
- Row/Column. Symbols are arranged in rows and columns.
- Bus. Symbols are arranged along a snake-like backbone representing the linear array of nodes on a segment.
- Star. Symbols are arranged in a star consisting of a circle and a center symbol. You can set the star center using the symbol pop-up menu.
- Ring. Symbols are arranged in a circle.

If automatic layout is enabled:

- `[Auto-Layout]` appears on the right side of the status bar.
- When a new symbol is added to the submap, NNM places the symbol on the submap according to the assigned layout algorithm.
- Although you can move the symbols in the submap, all symbols in the submap snap back to their original position when the `ipmap` service checks for changes.

By default, auto-layout is turned on. If you turned it off and change your mind, to turn auto-layout on:

- *Windows:*

  For all submaps, select `Map:Properties` and access the `View` tab.

  For one submap, select `Map:Submap->Properties` from that submap and access the `View` tab. Select the `Auto Layout` field.

- *UNIX:* Select either:

```
View:Automatic Layout->On For All Submaps
View:Automatic Layout->On For This Submap
```

Do-It-Yourself Layout

If you want to create a customized placement (for example, to place symbols on a background graphic that shows their geographical location), you need to turn off automatic layout for the submap you want to customize.

NOTE If the submap is transient, it becomes persistent when you turn off auto-layout.

If automatic layout is disabled:

- A `New Object Holding Area` is created in the lower portion of the submap. Symbols in the `New Object Holding Area` are shown without their connections. Connections are automatically added when you remove the symbol from the holding area and place it on the map.
- Symbols added to the submap are placed in the `New Object Holding Area`. You can move symbols from the `New Object Holding Area` to the submap.
- You can move symbols within the submap window by dragging and dropping them with the mouse.
- You cannot move a symbol from the submap to the `New Object Holding Area`.
- You can arrange symbols in the submap according the assigned layout algorithm by selecting `View:Redo Layout`.
- When hidden symbols are unhidden, they are placed in the `New Object Holding Area`.

To disable auto-layout:

- *Windows:*

  For all submaps, select `Map:Properties` and access the `View` tab.

  For one submap, select `Map:Submap->Properties` from that submap and access the `View` tab. Deselect the `Auto Layout` field.

- *UNIX:* Select either:

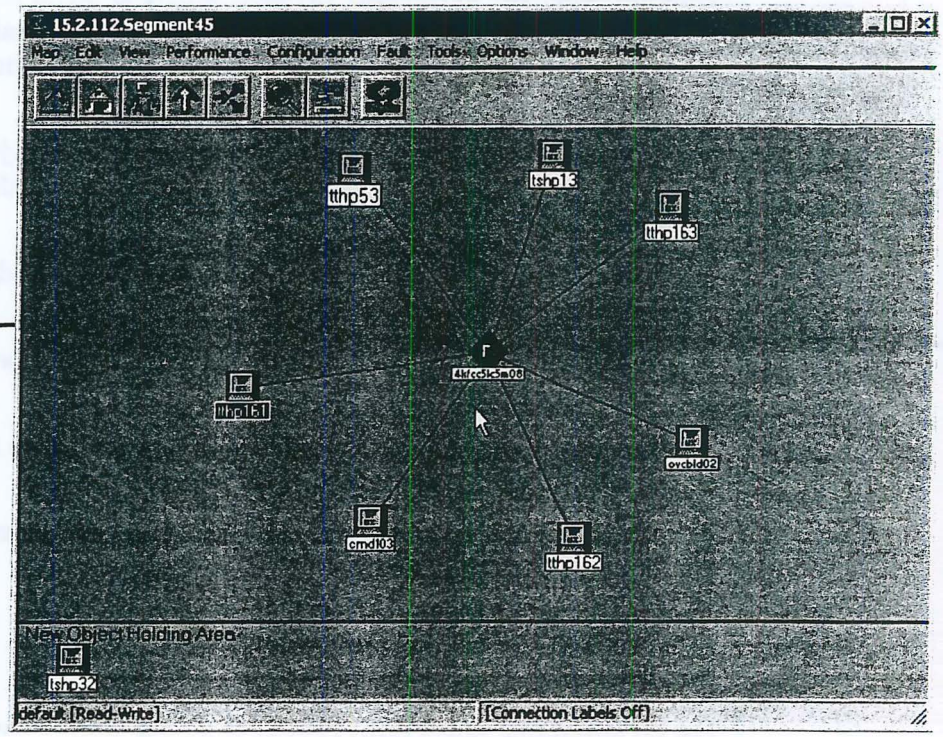
```
View:Automatic Layout->Off For All Submaps
View:Automatic Layout->Off For This Submap
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0874
3740
Doc:

New Object Holding Area

A `New Object Holding Area` (Figure 8-7) appears on the lower portion of each submap window if the submap has no layout algorithm or if the assigned layout algorithm is disabled (automatic layout is turned off). Symbols in the `New Object Holding Area` are shown without their connections.

Figure 8-7 **The New Object Holding Area**



New Object Holding Area

Adding Your Own Submaps

You can create submaps that show a particular view of some aspect of your network. For example, you may create one submap to show all the nodes on a particular network segment, and create another submap that shows all the software subsystems of a particular node.

Child Submap or Independent Submap?

The method you use to create a new submap determines whether the submap is a *child submap* or an *independent submap*.

- A *child submap* is related to a parent object. To create a child submap, double-click on an explodable symbol. If no child submap exists, you are prompted to create one (for example, when you create a new container object).
- An *independent submap* is created from the `Map:Submap->New` menu item. The submap has no associated parent object and is independent of any existing hierarchy of submaps. To display an independent submap, select a submap entry in the `Edit:Find->Submap` dialog box.

TIP You cannot open the independent submap by double-clicking on a symbol unless you manually add a symbol to the root-level submap that invokes your independent submap.

An independent submap can be used as the beginning of a new submap hierarchy. You must create any child submaps starting from the independent submap to build an additional submap hierarchy into the map. NNM cannot automatically generate these child submaps for you. NNM also cannot update your independent hierarchy as new nodes are discovered or changes occur to the connections.

The map must be open with read-write access before you can create a submap.

Meta-Connection Submaps (for multiple connections)

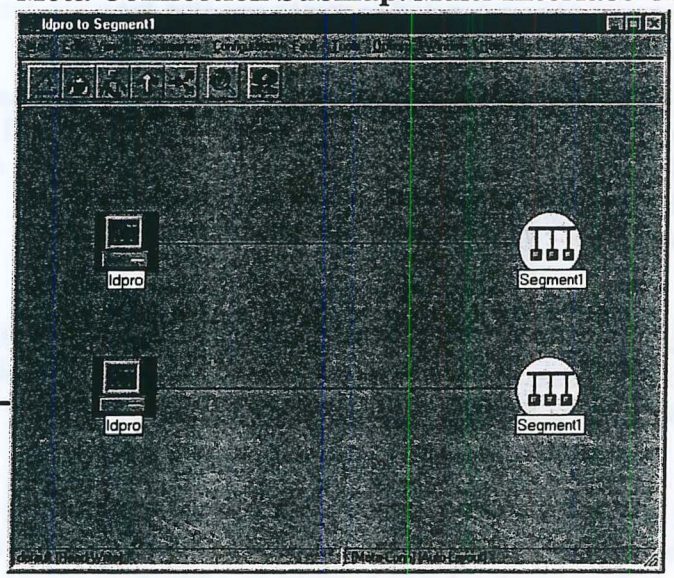
If two devices represented by symbols on your map communicate over *multiple* connections, you can double-click upon the connecting line to display a meta-connection submap. The meta-connection line (symbol) on your submap looks the same as a regular line on your map (connection symbol).

NNM does not display multiple lines between the two objects; instead, each individual connection between the two symbols is displayed on the line's meta-connection submap. NNM automatically creates a meta-connection submap when you (or an application) add a connection.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0875
3740

symbol between two symbols in a regular submap that already have a connection. You can add an unlimited number of connections between two symbols in a regular submap. Each of these connections is automatically added to the meta-connection submap with the two symbols as end points.

Figure 8-8 Meta-Connection Submap: Multi-Interface Connections



A *meta-connection submap* displays the status of each connection between two symbols or a symbol and a backbone. Compound status colors from the meta-connection's submap are propagated to their parent submap differently as compared to regular submaps (page 274). The meta-connection symbol in the parent submap displays the compound status of the multiple connections in the meta-connection submap. Any unconnected objects in the meta-connection submap also contribute to compound status. However, the connected icon symbols in a meta-connection submap do not propagate their status. Their status is maintained by the symbols in the parent submap above the meta-connection submap. (Meta-connection submaps are not accessible over NNM's web interface.)

You can:

- Create a child submap from a meta-connection submap by double-clicking on any of the objects in the meta-connection submap. Therefore, the meta-connection submap can be a parent of other regular submaps.

- Select objects in the meta-connection submap.
- Add unconnected objects to a meta-connection submap.
- Add connections at the parent level submap. (You cannot add connections directly on a meta-connection submap.)
- Delete the meta-connection submap by deleting the last object from the meta-connection submap.

Customizing the Internet Level of Your Network Map

As a result of the initial discovery process, NNM displays one Internet symbol on the root submap *and creates one Internet submap*. Within the Internet submap are symbols representing IP and IPX networks, and IP- and IPX-addressable gateways (routers). This section provides definitions and procedures that you can use when editing the internet level of your network map (for information about editing the network, segment, or node levels, see page 256). In order to understand your options, you need to know:

- What are container objects.
- rnet submaps.
- What is the containment realm.
- How to expand the single Internet submap into multiple partitioned internet submaps.
- the partitioned internet submaps.

NOTE To manage IPX networks, you must be running NNM on a management station using a Windows operating system. If you are running NNM on a management station using a UNIX operating system, you can configure a system that uses the Windows operating system to serve as a collection station that forwards IPX information to the UNIX system. This requires another copy of NNM to be running on the system with the Windows operating system. See *A Guide to Scalability and Distribution* for information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 247
0876
Doc 3740

Container Objects to Hold Part of Your Map

You can group the symbols on the Internet-level submap into logical submaps that reflect the physical or logical reality of your network and working style.

First, you add symbols called *container objects* to the Internet submap. The container objects allow you to create maps by location, building, department, or whatever makes sense to you. Each container object explodes into a new submap called a *partitioned internet submap*. Container objects can be either the Internet symbol (in the Network class) or any of the symbols in the Location class (see NNM's online help Display Legend for a quick look at your choices).

Partitioned internet submaps can contain gateway router symbols and subnet symbols. To maintain the map hierarchy, partitioned internet submaps are only allowed between the Internet-level submap and the Network-level submap. NNM maintains the connection between devices as you create the partitioned internet submaps.

Partitioned Internet Submaps

The symbol of a container object opens a special submap called a partitioned internet submap. You can add symbols from the Location class and the Internet symbol from the Network class to any partitioned internet submap. Thus, you can create a hierarchy of partitioned internet submaps as many levels deep as you wish. For example, you may want to subdivide your management domain by continent, then by country, then by city, showing your IP and IPX networks, and IP and IPX-addressable gateways (routers) only at the city level.

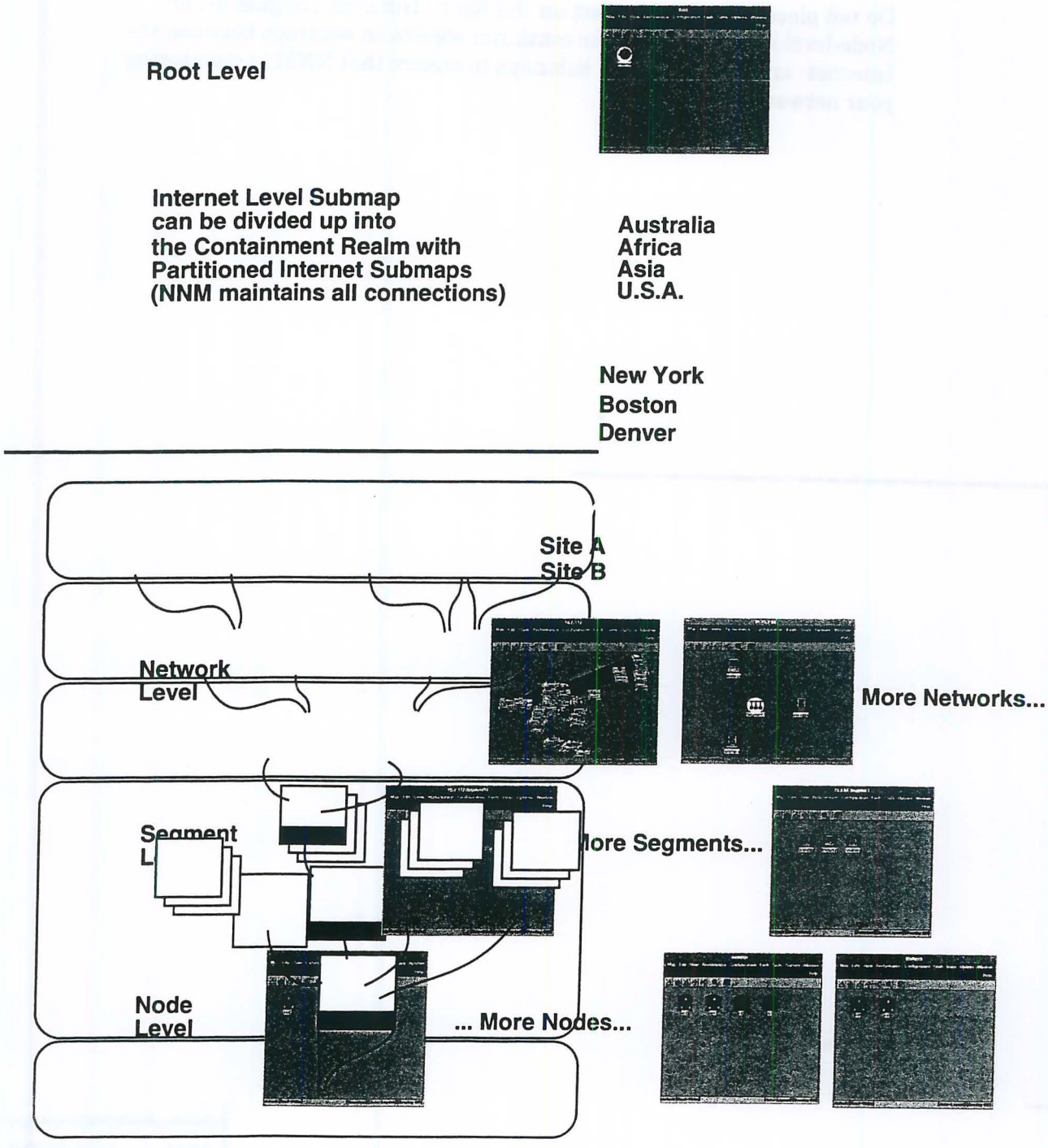
The Internet submap always remains at the top of your hierarchy of partitioned internet submaps and is opened whenever the Internet symbol is selected from the root map.

You can create multiple levels of partitioned internet submaps to rearrange how your network map is displayed. NNM maintains the connections and monitors the devices placed within a container object as long as the container objects are on submaps between the Internet-level submap and any Network-level submaps. If you use container objects at other levels of the map, NNM cannot manage the devices that are contained in the submaps, so connections are lost and status is not updated.

NOTE Do not place a container object on the Root-, Network-, Segment-, or Node-level submaps. Only use container objects on submaps between the Internet- and Network-level submaps to ensure that NNM is monitoring your network devices.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 249
0877
3740
Doc:

Figure 8-9 Containment Realm: Partitioned Internet Submaps



2639

Creating a Partitioned Internet Submap

To create a partitioned internet submap, add the Internet symbol from the Network class or any of the symbols from the Location class to the Internet submap or any partitioned internet submap. The new symbol represents a special object, called a container object. Symbols of container objects open into a partitioned internet submap. You can then cut and paste IP and IPX network and gateway (router) objects from your Internet submap into your partitioned internet submap. NNM maintains all connections between your IP and IPX network and gateway (router) objects.

NOTE It is important to follow these directions *exactly*.

To add a container object to an Internet or partitioned internet submap:

1. Select the `Edit:Add Object` menu item. The `Add Object Palette` appears.
2. From the `Add Object Palette`, select either:
   - the `Network Class`'s Internet symbol
   - the `Location Class` (any symbol)

   Drag the symbol onto the Internet submap or the partitioned internet submap of your choice. The `Add Object` dialog box appears.
3. Specify your choices in the `Add Object` dialog box.
4. Click on `[OK]`. The newly added symbol resides on the submap, and an empty child submap (partitioned internet submap) for that symbol is automatically created. To open the new partitioned internet submap, double-click on the new symbol.

NOTE Until you add objects to your new partitioned internet submap, the container symbol displays an unknown status. In the new container symbol's `Object Properties` dialog box, `IP Map` is not listed as a configurable application because the `IP Map` service does not require any information about the container object.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 251
3-740
Doc:

5. Use `Edit:Cut` and `Edit:Paste` to place the desired IP and IPX network and gateway (router) objects into the new partitioned internet submap.

All submaps, objects, symbols, and connections that are contained under a cut-and-pasted symbol remain intact. Symbol behavior and status are maintained. For example, if the symbol you paste onto a map explodes into a child submap, that capability also exists for the new symbol.

The Containment Realm

The Internet submap and the hierarchy of partitioned internet submaps make up the **containment realm**. You can populate a manually created partitioned internet submap by cutting and pasting IP and IPX network and gateway (router) symbols from the Internet submap to a partitioned internet submap. Only one symbol is allowed for each IP and IPX network and gateway (router) symbol; however that symbol can be placed in any location within the containment realm.

Within the containment realm, when you cut and paste these symbols the hierarchical and topological relationship between symbols is maintained. When you cut these symbols from the Internet submap and paste them on a partitioned internet submap, the hierarchical [illegible] wn the map hierarchy. In other words, that symbol's child submaps along with all associated symbols and objects are [illegible]

In addition to the hierarchical relationship, all topological relationships between symbols are maintained. NNM maintains the connections between symbols after they are pasted onto a partitioned internet submap by redrawing their connections to the symbol of the container object.

Editing Guidelines

NOTE You must follow these directions *exactly* in order to maintain the connections between devices on your map as you work and in order to maintain NNM's monitoring of your network devices.

This section discusses the types of editing operations you can perform in the containment realm *while maintaining the connections between symbols*.

To maintain connections between symbols in the containment realm:

Use `Edit:Cut/Edit:Paste` or drag-and-drop.

However, you must also follow these guidelines:

- You can cut and paste symbols between the Internet submap and any partitioned internet submap.
- You *cannot* cut from and/or paste symbols onto the Root submap or the Network, Segment, and Node submaps. In other words, cut/paste is only allowed on the Internet or containment realm level.
- You *cannot* cut and paste or drag and drop container symbols themselves. If you paste a container object on one of these submaps, the containment information is broken; that is, the symbol will no longer maintain its relationship to other symbols. Connections between that symbol and other symbols are also broken.

Once a cut and paste or drag and drop operation has been made between submaps, IP Map will need to resynchronize. You cannot perform any other operations until this resynchronization is complete.

Example of an Internet Submap

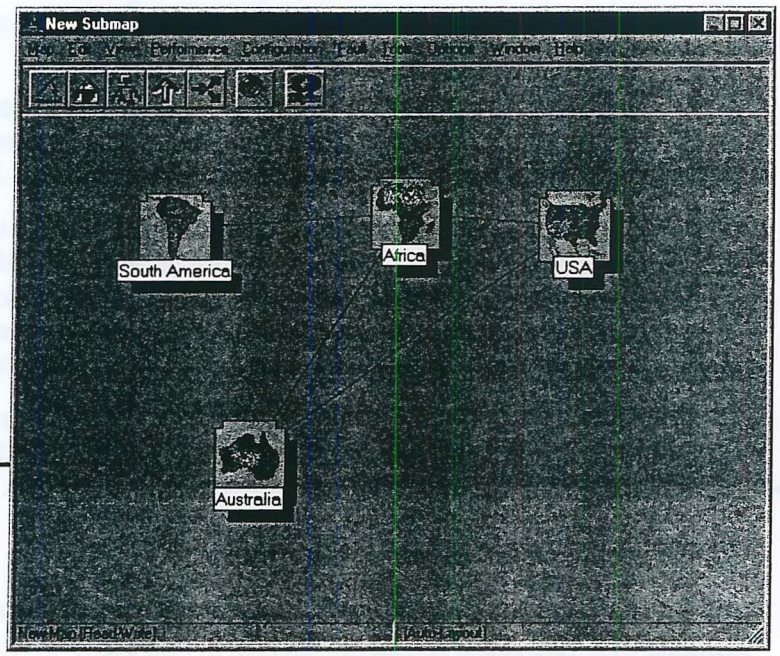
On the Internet submap, you can place a map of the world and add symbols that represent container objects of countries or continents. Each container object opens into its own submap. You can then cut symbols that represent your resources in a particular country or continent from the Internet submap and paste them into the appropriate partitioned internet submap.

The following figure shows an Internet submap in which four container objects were added. The symbols of the container objects represents Australia, U.S.A., South America, and Africa. In addition, all symbols of objects discovered by NNM have been cut from the Internet submap and pasted in lower-level partitioned internet submaps. NNM maintains the

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls.: Nº 253 0879
3740
Doc:

connections between the symbols of discovered objects in the lower-level submaps. Also, NNM creates the proper connections between the symbols of the container objects.

Figure 8-10 **IP Internet Submap**

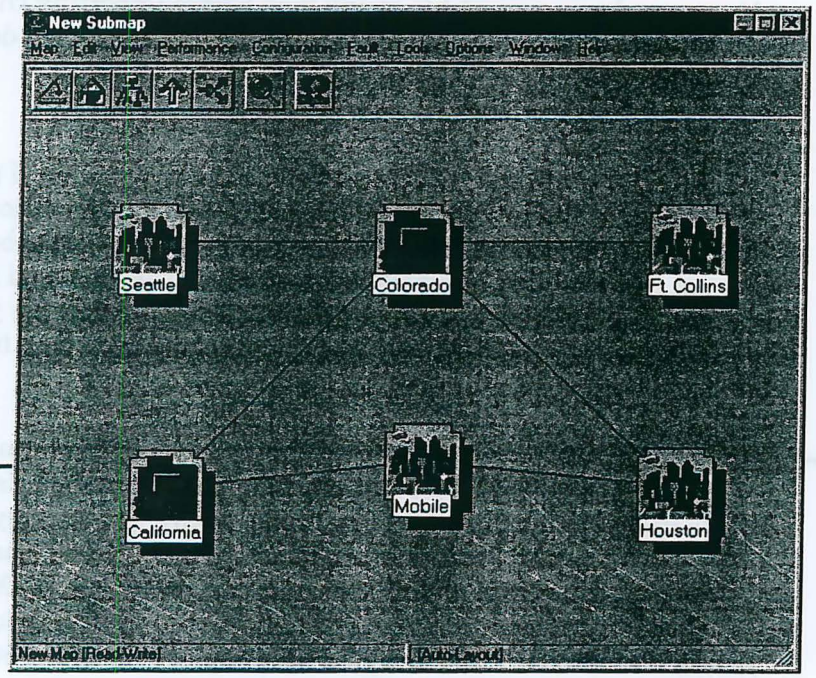


Example of Partitioned Internet Submap

The following figure shows the U.S.A. submap. Six container objects have been created in this submap. This submap may also contain symbols representing IP and IPX networks or gateways. From this submap, you can double-click on any of the six container objects and open a

partitioned internet submap, which may display an additional partitioned internet submap containing other container objects or symbols that represent IP and IPX networks and gateways.

Figure 8-11 Partitioned Internet Submap of the USA



Maintaining the Containment Realm

As you customize your submaps, NNM tracks any editing changes you make to the open map. The Internet submap and all partitioned internet submaps make up the containment realm. NNM continues to manage objects that have been moved within the containment realm with the network monitoring process (netmon).

If new IP- and IPX-addressable resources are added to the network, NNM discovers these resources, creates objects for them, and adds a symbol for each object to the appropriate submap or submaps. NNM always places IP- and IPX-addressable gateways (routers) and networks that have been discovered on the original, highest-level Internet submap.

You can maintain the customized organization of your network map by distributing these symbols ("Editing Guidelines" on page 252) to the partitioned internet submap of your choice.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0880
3740
Doc:

When creating multiple maps on one management station, using the `Map:Import` and `Map:Export` feature is an easy way to copy your *containment-realm customization* changes from map to map.

CAUTION Always make an export file of any map before importing changes from another map. This enables you to undo the changes if you don't like what happened.

All your container objects as well as the objects that NNM automatically placed at the internet level are included. Changes to the lower-levels of the map (network/segment/node) and any executable symbols (page 279) are not included in the export/import nor are they affected in any way by the import/export. If you need multiple maps that include your customizations to *all* levels of the map, use `Map:Save As` instead.

TIP The `Map:Export/Map:Import` feature *may* be useful if you are configuring NNM on a test machine and plan to move changes to a production machine at a later time. Make sure that exactly the same HP OpenView and 3rd party products are installed on both machines to ensure a successful map export/import operation. See NNM's online help for more information about Map Import/Map Export. If you need to move customization at all levels of your map, rather than just at the Internet and containment realm levels, use NNM's backup and restore feature instead (page 165).

Customizing Network-, Segment-, or Node-Level Submaps

Editing the lower-level network submaps enables you to distribute resources over your map to better match how your network is organized. You can:

- Copy or move symbols within or between submaps.
- Add symbols to your submaps.

Copying or Moving Symbols

Copying or cutting and pasting are convenient ways to edit your network map. The cut and paste operation is the means for changing a symbol's location from one submap to another, and is essentially a move operation. You can cut and paste multiple symbols simultaneously.

If you cut and paste symbols at the network, segment, or node levels, NNM will *not* maintain the previous connections between these symbols. Therefore, after cut and paste operations, you must add a connection between the desired symbols. Use the dialog box accessed through `Edit:Add Connection`.

The sections that follow show you how to add network, segment, node, and interface objects to your network map so that they can be managed by NNM.

Changing Symbol Location on One Submap After auto-layout is turned off, simply select the symbol and, while holding down the left or center mouse button, drag the symbol to the new location within the submap.

Copying/Moving Symbols from Submap to Submap You can easily copy or move symbols from one submap into any other submap in the open map. Select the symbols, then:

- To copy the symbols, select the `Edit:Copy` menu item and `Edit:Paste` menu item. The copy operation does not remove the symbols or selected objects from their original location.
- To move the symbols, select the `Edit:Cut` menu item and `Edit:Paste` menu item.

  Sometimes the cut (or delete) operation applies only to a symbol or set of symbols, without affecting the object or objects represented by the symbols. Sometimes the cut operation applies to the object as well as the symbol. When you cut a symbol, if the object that the symbol represents is represented by another symbol, in any map, the symbol is cut, but the object is not deleted from the database. If the symbol is the only symbol that represents the object, the object is cut (or deleted) along with the symbol.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0881
3740
Doc:

NOTE If you are using NNM for UNIX operating systems, you can also move the symbol by dragging and dropping symbols from one submap to another.

Adding Object Symbols to Your Submaps

You can add segment, node, or interface objects to your maps.

Adding a Segment Object If NNM can identify which network segment a node is on, it places the node on that segment. If NNM cannot identify the segment, it places the node on the default segment submap for that network. The default segment submap for each network is the first submap created by the `ipmap` service when NNM ran initial discovery (named Segment 1). If this submap has been deleted, the oldest segment submap (lowest segment number) becomes the default segment submap.

NOTE You may wish to check the oldest segment submap for each network (Segment 1) periodically to check for stray objects.

NNM discovers new nodes on segments attached to connector devices that support the Bridge MIB (RFC1493) and Repeater MIB (RFC2108), as well as HP SNMP bridges and multi-port repeaters (hubs) that have IP or IPX addresses.

A Network submap may contain symbols in the Network and Connector classes. NNM recognizes the following symbols on a Network submap.

Table 8-1 Symbols Managed on a Network Submap

Class	Symbol
Network	Bus
Network	Star
Network	Token Ring
Network	FDDI Ring

Table 8-1 Symbols Managed on a Network Submap (Continued)

Class	Symbol
Connector	Gateway (Router)
Connector	Bridge
Connector	Repeater
Connector	Multi-Port (Hub)
Connector	Switch (supplied by vendors)

You can add a segment object to a Network submap. When you add a segment, an empty Segment submap is created. Double-clicking on the symbol opens the Segment submap. See NNM's online help for more information.

Adding a Node Object You can add an object that represents a node or a network device to your Segment submap by placing one of the supported symbols on a Segment submap. Double-clicking on the node symbol opens a Node submap. NNM manages the following symbols from the Computer, Connector, and Net Device classes in a Node submap. See NNM's online help for more information.

Table 8-2 Symbols Managed in a Segment Submap

Class	Symbol
Computer	Generic
Computer	PC
Computer	Workstation
Computer	Mini
Computer	Main Frame
Connector	Bridge
Connector	Gateway (Router)
Connector	Repeater
Connector	Multi-port (Hub)

RQS nº 03/2005 - CN
CPMI - CORREIOS
FLS. Nº 0882
3740
Doc:

Table 8-2 Symbols Managed in a Segment Submap (Continued)

Class	Symbol
Net Device	Analyzer
Net Device	Modem
Net Device	X.25
Net Device	PBX

Adding an IP or IPX Interface Object You can add an interface to a Node submap by placing an interface symbol on the Node submap. To do this, enter the address of the interface in the `Add Object` dialog box. See NNM's online help for more information.

Table 8-3 Symbols Managed in a Node Submap

Class	Symbol
Cards	IP Interface
Cards	IPX Interface

Background Graphics

A background graphic, such as a map or picture, may be displayed in the background plane of a submap window. The background graphic may be different for each submap. NNM includes an extensive collection of background graphics for your convenience. You can also create your own background graphics.

Keep in mind that graphic files are quite large and may significantly increase the time required to open each submap and significantly increase the amount of memory required to view a submap. If the submap is transient, it becomes persistent when you add a background graphic. Supported file formats for background graphics are as follows:

- *NNM for all platforms:*
  - GIF (CompuServe Graphics Interchange Form)
- *NNM for a Windows or UNIX operating system:* Supports these graphic file formats (not displayed when accessing NNM over the web):

2629

  - BMP (Bitmap)
  - TIFF (Tag Image File Format)

- *NNM for UNIX operating systems only:* Supports these graphic file formats
  (not displayed in NNM for Windows or NNM on the web):
  - XBM (X11 monochrome bitmap format)
  - PCX
  - Image
  - Starbase
  - XPM (X Pixmap format)
  - XWD (X Window Dump)
- *NNM for UNIX and NNM on the web only:* Supports these graphic file formats (not displayed in NNM for Windows):
  - JPEG (Joint Photographics Experts Group)

TIP

The following *analytical data* directories are *not* included in NNM's backup scripts:

```
install_dir\backgrounds
install_dir\bitmaps
install_dir\www\htdocs\bitmaps
install_dir\www\registration
```

- *UNIX:*

```
$OV_BACKGROUNDS
$OV_BITMAPS
$OV_WWW/htdocs/bitmaps
$OV_WWW_REG
```

If you make changes or additions to map backgrounds, bitmap files, or web registration files ensure that your new files are properly backed up. See "Backup/Restore to Protect Your Investment of Time" on page 165 for more information.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
FIS. Nº 0883
3740
Doc:

Adding or Replacing a Background Graphic

You can add a graphic to the background of a submap or replace a graphic with a new graphic. Background graphics shipped with NNM are stored in:

- *Windows:* `install_dir\backgrounds\*.*`
- *UNIX:* `$OV_BACKGROUNDS`

A graphic can serve as a background for the symbols in a submap. A graphic helps provide contextual information such as a floor plan for systems, a map of geographically diverse sites, and so on. Both users and applications can specify a background graphic for a submap.

The map must be open with read-write access to choose a new background graphic. Select `Map:Submap->Properties` and specify the name of the graphic file that you wish to use.

NOTE When using a background graphic, symbols cannot be placed outside the dimensions of the background graphic.

Creating Your Own Map Symbols

You can create your own symbols to use on maps. You might want to do this to customize the appearance of existing symbols, or you might need a symbol to represent a new object. Each symbol is comprised of two graphic elements: the class that determines the background shape of the symbol and changes color according to current status, and the subclass that determines the graphic displayed within the background shape. Several steps are required. See "Changing All the Symbols for a Particular Device" on page 661 for a detailed example of these steps:

- Create a set of *.GIF images according to the specifications in NNM's online manual, *Creating and Using Registration Files*.
- Create a symbol registration file to define the characteristics and appearance of the new symbol.
- Develop custom online help information about the your new symbol. This online help information will be available through the symbol's pop-up menu. See NNM's online manual, *Creating and Using Registration Files*.

NOTE These changes are visible from remote consoles and web access after the map is reloaded or refreshed on each system. Your new symbol will also display in `Help:Display Legend`.

What Is a Symbol

A **symbol** is a graphical representation of an object (page 203). A single object can be represented by multiple symbols. Multiple symbols of the same object can exist on the same submap, on multiple submaps of the same map, or on submaps of different maps.

In addition to representing objects, symbols have other functions:

- Most symbols are explodable--when you double-click an explodable symbol, a new submap opens to let you "look inside" the object representing the symbol.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
263
Fls. Nº 0884
3740
Doc:

- Some symbols are executable. When you double-click on this type of symbol, a predefined action is carried out on a predefined target.
- Symbols can reflect the status of the object that they represent or of objects in child submaps.

When you create a new symbol type you can define the following characteristics:

Symbol Variety Symbols come in two varieties: the icon symbol and the connection symbol.

- **Icon Symbol** These symbols represent the objects or groups of objects managed by NNM.
- **Connection Symbols** These symbols represent logical connections between devices that are managed by NNM. Connection symbols do not represent actual physical connectors.

Symbol Type Symbol type consists of the symbol class and subclass (see Note on page 265):

- **Class** You can distinguish the symbol class by the outer shape of the symbol. For example, a circle=a network, square=a computer, diamond=a connective device, and so on.
- **Subclass** A subclass is a further definition of the symbol that is represented by a bitmap within the outer shape that represents the class.

Status Source A symbol may present status information from one of three sources. This characteristic allows applications to have more control over the presentation of status. See "Controlling Symbol Status" on page 270 for more information. In general, Hewlett-Packard recommends that you do not change these settings.

Label A label may appear below each symbol. This label is simply a name to help you identify a specific symbol. (see Note on page 265).

Behavior	Behavior defines how the symbol behaves when you double-click the symbol. A symbol may behave in one of two ways: it may open a child submap (explode), or it may execute an action (execute).
Default Layout	When an explodable symbol opens a new submap, its default layout specifies the layout algorithm (Ring, Bus, Star, Point to Point, or Row/Column) for the submap.

NOTE

The `ipmap` service automatically assigns a symbol type and label based upon information it receives from the `netmon` service.

This means that if you modify the symbol type or symbol label of an object that is managed by NNM, your changes will be replaced by the values assigned by NNM the next time configuration polling runs.

You can turn off this `ipmap` capability by setting the environment variable `IPMAP_NO_SYMBOL_CHANGES=TRUE`. See the *ipmap* reference page in NNM's online help (or the UNIX manpage) for information about changing this environment variable.

Alternately, you can modify the `oid_to_sym` file to specify that a different symbol be associated with a specific *type* of device (determined by `sysObjectID`). See the *oid_to_sym* reference page in NNM's online help (or the UNIX manpage) for more information. See "Changing All the Symbols for a Particular Device" on page 661 for a complete example.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0885
3740
Doc:

Specifying the Placement and Size of the Submap Windows

You can control the size and placement of the submap windows through the menu choices `Window Geometry` and `Submap Overlay`. The choices you make here affect the way that the submaps are displayed on the management station and on remote consoles, but not through web access.

Window Geometry

NOTE Window geometry settings are visible from remote consoles when the map is reloaded on each system. This change does not impact maps accessed over the web.

Select `View:Window Geometry` to explicitly save the size and placement of submap windows so that they are consistent each time they are opened. This feature allows you to override any settings that an application may specify for the size and placement of its submap

When you specify the size or placement of a submap window in a read-write map, those settings will be used in that session and in all subsequent sessions. You cannot change window geometry on read-only maps.

If the submap is transient, it becomes persistent when you save its window geometry.

Submap Overlay

NOTE Submap overlay settings are visible from remote consoles when the map is reloaded on each system. This change does not impact maps accessed over the web.

Select `View:Submap Overlay` to minimize the number of windows on your screen during submap navigation. By default, NNM automatically reuses submap windows. Each new submap that you access by double-clicking on it is placed in the window from which you accessed it. This eliminates the display of submaps that you are merely passing through as you navigate the hierarchy. By using submap window overlay, you no longer have to close unneeded submaps that are on your display.

You can change this behavior so that a new window is presented whenever you access a new submap. The overlay feature is set on a per-submap basis. You cannot change submap overlay on read-only maps.

If the submap is transient, it becomes persistent when you turn off overlay.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0886
3740
Doc.

Miscellaneous Configuration Changes

A variety of configurable settings are stored in:

- *Windows:* The system registry.
- *UNIX:* The X Windows resource files (page 269).

The changes discussed in this section affect only the local management system's display of NNM or the local remote console's display of NNM. NNM accessed over the web is not affected.

Windows Operating System

See the *app-defaults* reference page in NNM's online help for detailed information about which NNM settings can be controlled through the Windows system registry.

You can customize the appearance and behavior of NNM by editing the Windows system registry. Check your Windows operating system documentation for more information about editing the system registry files.

Changing the Windows system registry on the management station affects *only* the sessions run on the management station. Each management station and each remote console could have different settings.

Possible settings include:

- Map fonts
- Status colors for symbols and map background color

These settings are stored in the registry under the following keys:

- `\HEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\Network Node Manager\OVw\Map Fonts`
- `\HEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\OpenView\Network Node Manager\OVw\Map Colors`

TIP After making your changes, check `Help:Display Legend` to verify that your color choices are working successfully.

UNIX Operating Systems

You can also customize the appearance and behavior of NNM by editing the application defaults files and the X resources files used by your X Windows resource manager.

Open the `$APP_DEFS/OVw` file and read the instructions within the file.

Changing the `$APP_DEFS/OVw` file on the management station affects *only* the sessions run on the management station. Each management station and each remote console could have different settings. Each user on the system can have a private X resources file that can override the `$APP_DEFS/OVw` file.

The UNIX `$APP_DEFS/OVw` file for NNM lets you customize things such

- Map background color
- Status colors for symbols
- Submap window height and width
- Timers for response to requests to close a map
- Timers for queries
- Keyboard focus policy
- Fonts for dialog boxes

To change general X Windows behavior and color, refer to the online help for the window manager that is being used on your computer. Refer to documentation on your window manager for the location of the X resources file for that window manager.

TIP After making status color changes, check `Help:Display Legend` to verify that your color choices are working successfully.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0887
3740
Doc:

Controlling Symbol Status

You can customize the status color and status propagation of the symbols:

- Control the colors used to indicate the status of network objects.
- Control the way in which critical status is propagated up the map's network hierarchy ("Compound Status" on page 274).
- Monitor the status of router interfaces outside of your firewall ("SNMP Status Polling" on page 273).

Object Status Colors

NNM displays status conditions via the colors of the symbols. The colors used to display status in NNM's web interface cannot be changed. However the colors used to display status in NNM for a Windows or UNIX operating system can be changed; colors used for both device symbols and connection symbols are defined and documented in:

- *Windows:* The system registry.
- *UNIX:* $APP_DEFS/OVw

You can view the current colors using `Help:Display Legend`.

Someone on your team may need to change their colors, for example to address color blindness issues. Keep in mind that your changes affect *only the local display* of the management station or remote console, and must be redone each time you upgrade NNM.

TIP After making your changes, check `Help:Display Legend` to verify that your color choices are working successfully.

To change the colors, see "Miscellaneous Configuration Changes" on page 268.

Symbol Status

Status is displayed by a symbol on a submap. There are two categories of status conditions: administrative and operational. These two categories are important because they interact with the status propagation schemes in very different ways.

In the **status propagation** schemes, rules are used to determine how the status of a symbol in a child submap is transmitted to the symbols of objects in parent submaps. Administrative status conditions are ignored by the propagation schemes, which means that status information from a child submap is not transferred to a parent symbol. Operational status conditions, on the other hand, may indicate problems that must be propagated through the use of the schemes.

NNM recognizes ten status conditions, shown in the following table:

Table 8-4 Default Status Conditions

Category	Status Condition	Meaning of Status
Administrative	Unmanaged	Users can set this value, which indicates that the object should not be monitored and that the operational status should be ignored.
Administrative	Testing	An application sets the status to "testing" when an object is undergoing temporary diagnostic or maintenance procedures.
Administrative	Restricted	An application sets the status to "restricted" when an object is functioning normally, but it may not be available to all users.
Administrative	Disabled	An application sets the status to "disabled" when an object is inactive (although there may not be anything necessarily wrong with the object).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0888
3740
Doc:

Table 8-4 Default Status Conditions (Continued)

Category	Status Condition	Meaning of Status
Operational	Unknown	An application sets the status to "unknown" when the status of an object cannot be determined.
Operational	Normal	An application sets the status to "normal" when the object is in a normal operational state.
Operational	Warning	An application sets the status to "warning" when an object may face a potential problem.
Operational	Minor/Marginal	An application sets the status to "minor/marginal" when an object has a minor problem; the device itself may continue to operate normally.
Operational	Major	An application sets the status to "major" when an object has serious problems; the device itself probably no longer operates normally.
Operational	Critical	An application sets the status to "critical" when the device represented by the object is not functioning.

The status of a particular symbol represents an application's interpretation of the status of certain object attributes, or characteristics, as defined in NNM's object database.

For example, the `ipmap` service determines the status of a node object based upon the operational status of IP and IPX interfaces installed in the node. If all of its IP or IPX interfaces are down, then NNM determines that the node's state is critical. From the perspective of the `ipmap` service, the node is nonfunctional. However, another application may consider the same node functional because that application

monitors a different protocol, and it finds that the interfaces for that protocol are fully functional. Multiple symbols for the node object could be used to represent these status states separately.

Status Source

Status may be obtained from three possible sources. This feature is mainly used by applications so that they can set the status of specific symbols. In general, Hewlett-Packard recommends that you do not change the status source of a symbol. The status source of a symbol is automatically set depending on the application that manages the object.

The three sources of status are:

Symbol Status Source This source of status is used by applications that may want to set status on a particular symbol of the object. This allows other applications to set states for other symbols of the same object.

Object Status Source This source of status is used by applications that want to set and display the same status state among all the symbols of a particular object.

Compound Status Source NNM determines the status state of the symbol based upon compound status rules. Compound status determines how status propagates from symbols in child submaps to symbols in parent submaps.

The following subsections discuss the significance of each status source.

NOTE If you change symbol source, the submap containing the symbol is forced to become persistent.

SNMP Status Polling

In some cases a router may have interfaces to which the NNM management station has no route (for example, interfaces located outside of a firewall). You can obtain status information from the SNMP agent for the device, just as you can for layer-2 interfaces, via SNMP queries for `ifAdminStatus` and `ifOperStatus`.

To configure an IP interface for SNMP status polling, use the following procedure.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0889
3740
Doc:

1. If the file `netmon.snmpStatus` file does not exist you will need to create it in the location listed below.
   - *Windows:* `install_dir\conf\netmon.snmpStatus`
   - *UNIX:* `$OV_CONF/netmon.snmpStatus`
2. Add a line to the `netmon.snmpStatus` file with the IP wildcards you want to have SNMP status polled.
3. To make your changes take effect, do one of the following.
   - From the command line, type **`ovstop -v netmon`** then type ovstart -v netmon.
   - From the command line, type **`xnmpolling -event.`**
   - Click `Apply` in the `Options:Network Polling Configuration` dialog box.

See the `netmon` and `netmon.snmpStatus` reference pages in NNM's online help (or the UNIX manpages) for more information.

Compound Status

NNM uses compound status to propagate the status of a symbol in a low-level submap up to parent submaps, to alert you about a problem. Note that status propagation occurs only when a symbol is given one of the six operational status conditions (unknown, normal, warning, minor, marginal, major, or critical). The administrative status conditions (unmanaged, testing, restricted, and disabled) are not propagated.

You can set compound status in the `Status Propagation` section of the `Map Properties` dialog box.

NOTE The selections that you make affect remote consoles and the web display after the map is reloaded or refreshed on each system.

From the perspective of a compound status scheme, a symbol is either:

- **unknown**: a symbol's current status has not yet been determined by an application.
- **normal**: a symbol is functioning as intended and responding appropriately when contacted by an application.

- **abnormal**: a symbol is given one of the four abnormal status conditions (warning, minor/marginal, major, or critical), and is either potentially or currently having problems.

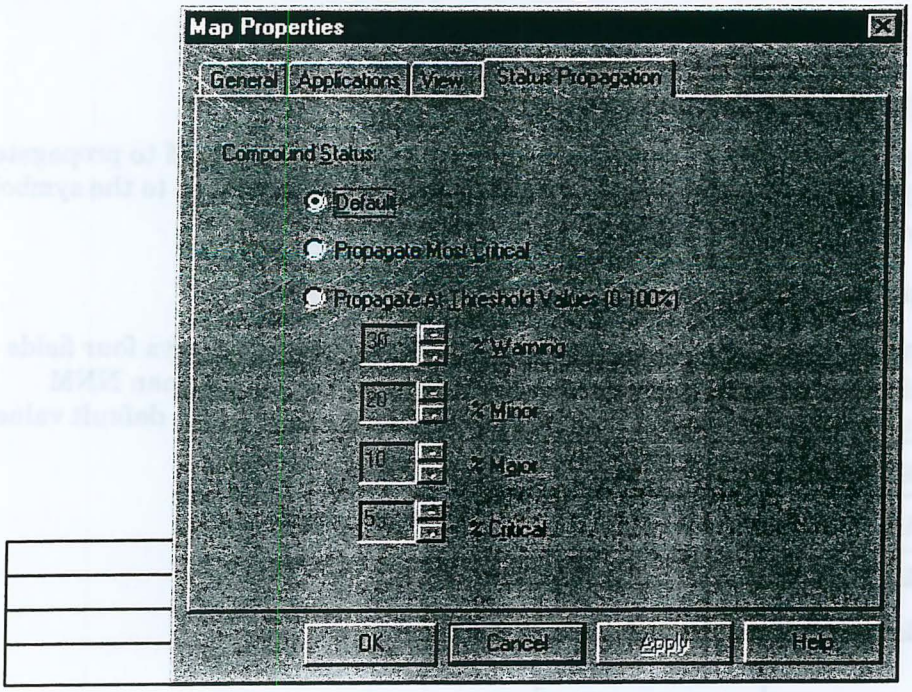
The mapping of the compound status categories to the operational status conditions is described in the following table.

Table 8-5 Compound Mapping

This Compound	Maps to This Operational Status Condition
Unknown	Unknown
Normal	Normal
Abnormal	Warning, Minor/Marginal, Major, or Critical

The following subsections discuss each of the three compound status schemes: default, propagate most critical, and propagate at threshold value.

Figure 8-12 Status Propagation Settings



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3740
Doc:

Default

Selecting the default propagation scheme causes NNM to propagate status according to the algorithms described in the following table:

Table 8-6 Default Status Propagation

Condition of Symbols in Child Submap	Status of Symbols of Parent Object
No symbols are normal and no symbols are abnormal.	Unknown
All symbols are normal.	Normal
One symbol is abnormal; all other symbols are normal.	Warning
More than one symbol is abnormal and more than one other symbol is normal.	Minor/Marginal
One symbol is normal; all other symbols are abnormal.	Major
All symbols are abnormal.	Critical

Propagate Most Critical

Selecting the propagate most critical scheme causes NNM to propagate the status of the most critical symbol in the child submap to the symbols of the parent object.

Propagate At Threshold Value (0 - 100%)

Selecting the propagate at threshold value scheme displays four fields that enable you to set threshold values that determine when NNM propagates status. The number shown for each field is its default value.

% warning	30
% minor	20
% major	10
% critical	5

The specified value indicates the minimum percentage of symbols that must be in that status state in order for that status state to be propagated. If the percentage is met or exceeded in more than one status state, then the most severe of those states is propagated.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
277
Fls. Nº 0891
3740
Doc:

Creating New NNM Features to Meet Your Team's Needs

Adding to NNM's Menu Structure

You can add your own choice of features to NNM's pull-down menus, pop-up menus, and tool bars. This is useful for providing quick access to commonly used tools or to specific network management scripts that your team developed. You may wish to designate a menu location where you post tools developed by team members as a way to share best practices, or designate a menu location to post software tools provided by specific vendors.

There are two ways to make additions to NNM's menu choices:

- NNM provides an easy way to add menu access to MIB-based applications that are written using NNM's MIB Application Builder program. See "Using the MIB Application Builder" on page 443 for more information.
- You can also make modifications to NNM's registration files to add any menu or toolbar items that you want. Complete information about registration files is available in NNM's online manual, *tration Files*.

NOTE The changes that you make using these two options appear on the management station and from remote consoles. They do not show up when NNM is accessed over the web. See Chapter 14, "NNM on the Web," for information about modifying NNM's web user interface.

TIP You can develop your own *context* settings for your new menu items to make them appear on only specific submaps. See "Using the Context Feature to Control Menu Choices" on page 296. You can also establish *selection rules* that make the menu item unavailable unless an

appropriate device is selected on the map. See NNM's online manual, *Creating and Using Registration Files* for complete information about establishing selection rules.

Creating Executable Symbols with Custom Behaviors

Symbol Behavior

The setting for a symbol's behavior defines how the symbol behaves when you double-click on it. A symbol may behave in one of two ways. It may explode into a submap, or it may execute an action.

A single object may be represented by both an explodable and an executable symbol. Note that when you change an existing explodable symbol to executable, you can open the child submap only from the `Map:Submap->Open` dialog box, or from another explodable symbol of the parent object.

Explodable Symbols

If a symbol's behavior is set as explodable (the default), the symbol enables you to view the components of an object. When you double-click on an explodable symbol, NNM opens another submap, called a child submap. The contents of this child submap may be determined by you or an application.

For example, NNM creates a child submap for a node that contains the IP interfaces installed in the node. If you double-click on a computer workstation managed by NNM, a node submap is opened that displays symbols of the node's IP and/or IPX interfaces.

If no child submap exists for the object, when you double-click on the symbol you are prompted to create a child submap. See "Making the Maps Look Like Your World" on page 240 for information about creating child submaps.

Executable Symbols

You can distinguish executable symbols from explodable symbols by the three dimensional appearance of each executable symbol. A square appears around the symbol indicating that it is executable (button-like). If a symbol's behavior is set as executable, the symbol enables you to

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0892
3740
Doc:

associate the double-click with an action other than opening a child submap. For example, by double-clicking on a conveniently placed symbol, you could:

- Launch a management tool.
- Open a window for remote login on a particular workstation.
- Execute a script that checks the disk space available on a selected system's hard drive and causes a message to display with the results of the check.

You can choose one or more objects as the target objects of the action from among the objects represented on the map. The chosen target objects must be appropriate for the action selected.

TIP *NNM over the web:* You will see the executable symbol with a box around it; however, you cannot run the executable.

Creating an Executable Symbol

Using NNM for a Windows or UNIX operating system, you can create a new executable symbol that performs an action. You can copy and paste a symbol, then change the duplicate symbol's behavior so that it executes some action. Or you can change the behavior of an existing symbol from explodable to executable.

When you add an executable symbol to your map, you must select the action that the symbol will execute and the target objects on which it will act. You can choose an action from among the actions supplied:

- `Edit:Add Object` dialog box, choose the `Executable` setting.
- Right-click on a symbol, choose `Symbol Properties`, select the `Executable` setting.

Or you can designate your own action by setting up an application registration file (ARF). The application registration file defines the action and adds it to the list in the `Add Object` dialog box and the `Symbol Properties` dialog box.

For more information about establishing your own custom actions:

- See NNM's online help.
- See NNM's online manual, *Creating and Using Registration Files*.

NOTE If an executable symbol is placed on a submap, that submap becomes persistent.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 281
0893
3740
Doc:

9 Controlling Map Access

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 283
0894
Doc.

Customizing the maps requires a substantial time commitment and a level of expertise in the intricate workings of NNM. To protect your efforts, you may want to remove functionality from some maps so that inadvertent detrimental changes cannot be made.

As you are setting up maps for various users/groups, you need to decide how much control you want to maintain over the map. If you allow your team to maintain the map, provide training (see page 286). If you want to maintain control over changes to the map, there are several choices for controlling how NNM looks and functions for each user or group:

- "Setting User Preferences Within NNM" on page 287.

  Simply log in as each user/group and set their options. NNM tracks these options by user/group and invokes them each time that user/group accesses NNM. Keep in mind that your team can change these settings if they wish.

- "Using Command Line Startup Options" on page 289.

  To use the command line options, you need to develop scripts for each user/group that enforce your choices. Your team member runs the script rather than the regular `ovw` command to open NNM's interface.

- "Using Operating-System Level File Permissions for the Map" on page 292.

  You control access to specific maps through setting operating system level permissions on the `snapinfo.dir` file within each map's directory.

- "Using the Context Feature to Control Menu Choices" on page 296.

  Control which features are accessible through the menus by selecting from predefined "context" identifiers or defining your own. Keep in mind that your team can change these settings if they wish.

- "Using ARF Files to Control Menu Choices" on page 299.

  Control which features are accessible through the menus by modifying the underlying application registration files (ARFs). The example provided makes NNM "fool-proof" by removing all access to configuring NNM, yet without limiting the use of NNM. This choice provides you with the ultimate control.

- "Allowing Others to View NNM from Many Computers" on page 317. Learn how to set up multiple systems to run the NNM interface while accessing the common database on the management station. You can set up remote consoles and/or web access.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0895
3740
Doc:

Establishing and Communicating a Process for Requesting Changes to the Map

Now that your maps are set up just the way you want them, think about how you will handle ongoing changes to the maps.

Not Allowing Team Members to Make Changes

Provide procedures for your team members to follow when requesting changes to their maps. Who should your team members contact and how. Designate one person to maintain the maps.

Allowing Team Members to Make Changes

If you are allowing your team members to have access to editing features, think about what training they will need in order to understand how NNM works and make wise decisions as they use the map. For example:

- All maps use the same database information. Don't delete symbols from the map. Use the hide feature.
- If more than one person uses a particular map, only the first person to open the map will have read/write permissions. Identify which team member has read-write permission for each map.
- If you are viewing a map in read-only mode, use `Map:Refresh` to display the most recent changes.
- Explain what to do when symbols show up in the `New Object Holding Area`. Explain why this might happen, such as when a new device added to your network.
- If they are allowed to modify their submaps, provide information about how to edit maps so that the connections between devices are maintained, and/or how to reestablish connections that are lost from the map.

Setting User Preferences Within NNM

You can define the following user preferences for each user/group. Simply log into the system as each user/group and set the preferences. NNM keeps track of each user's settings. These settings can be changed by each team member. You may want to simply provide training about these choices and leave it up to each team member, or you may wish to set them up for each team member and then remove the menu choices that allow changes (see page 299):

- Set the default map.
- Set a home submap.
- Set the toolbar to be hidden or displayed.
- Create a list of frequently accessed submaps by adding symbols to the Quick Navigator (this is customized per map rather than per user).

Table 9-1 User Preference Settings

User Preference	Setting
The **home** submap is the first submap that appears when you open a map. The home submap is always persistent.	Define the home submap: 1. Open the submap you want to be displayed each time you open the current map. 2. Select `Map:Submap->Set This Submap as Home` (Not available in NNM on the web.)
The map that NNM first displays upon startup is called the **user default map**.	Define the user's default map: 1. Select `Map:Open`. 2. Select a map name. 3. Click `Set User Default`.
The toolbar provides quick access to frequently-used menu items.	*UNIX only:* Display or hide the tool bar by selecting `View:Toolbar`

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0896
3740
Doc:

Table 9-1 User Preference Settings (Continued)

User Preference	Setting
The Quick Navigator provides quick access to frequently used submaps.	• Add a submap symbol to the Quick Navigator: 1. Open the submap you want to access from the Quick Navigator. 2. Select `Edit:Add to Quick Navigator->Add This Submap`. • Remove a submap symbol from the Quick Navigator: 1. Select the symbol in the Quick Navigator and display the symbol pop-up menu. 2. Select `Delete Symbol` from the pop-up menu. Remember that your team members can change these settings at any time unless you remove the menu choices for making those changes (see page 299).

Using Command Line Startup Options

This section discusses details about the ovw command that you may use to start NNM from the command line prompt. You can write scripts for each user/group that specify their specific startup options.

TIP It may be useful to enter these into each user's login script. For security purposes, remove the *write* permissions to the login scripts after you are done.

These commands may be useful for customizing NNM per user group or useful when running multiple sessions of NNM at the same time.

Options

The ovw command contains the following options. See the *ovw* reference page in NNM's online help (or the UNIX manpage) for more information.

```
ovw [-ro|-rw][-map map_name][-submap submap_name][-propagation
scheme][-server][-verify][-fields][-copyMap source_map_name
destination_map_name ...][deleteMap map_name] [mapcount]
```

Table 9-2 Startup Options for NNM

Option	Meaning
ovw -ro	Open all maps as read-only.
ovw -rw	Open all maps as read-write if possible. *UNIX:* This is the default. It is necessary only if the X resources specify read-only as a default behavior.
ovw -map *map_name*	Open map *map_name*. Create the map, *map_name*, if it does not exist.
ovw -submap *submap_name*	Open *submap_name* as the initial submap if it exists on the map being opened. If *submap_name* does not exist, then NNM initially opens the home submap of the map being opened.

RQS nº 03/2005 - CN - CPMI - CORREIOS
289
Fls. Nº 0897
Doc: 3740

Table 9-2 Startup Options for NNM (Continued)

Option	Meaning
`ovw -propagation` *scheme*	Sets the propagation scheme for a new map or changes the scheme for an existing map. The propagation schemes are default, most critical, and threshold.

Examples

Table 9-3 provides examples that show you various ways you can use the `ovw` command to start NNM from a command line prompt.

Table 9-3 Using the ovw Command to Start NNM

Command Entered	Effects
`ovw`	Runs NNM and opens the map assigned as the user default map.
`ovw -map Admin_Map`	Runs NNM and opens the map named `Admin_Map`. `Admin_Map` does not need to be the user default map.
`ovw -map world -propagation threshold:40:30:20:5`	Runs NNM and creates a new map named `world` using the threshold propagation scheme with a warning threshold of 40%, a minor threshold of 30%, a major threshold of 20%, and a critical threshold of 5%.
`ovw -ro`	Runs NNM and opens the map assigned as the user default map. The user default map, and all maps subsequently opened during this session, are opened with read-only access.
`ovw -ro -map Europe2`	Runs NNM and opens the map called `Europe2`. All maps during this session of NNM are opened with read-only access.
`ovw -rw`	Runs NNM and opens the map assigned as the user default map. Maps can be opened with read-write access if permissions allow. The `-rw` option is the default and is necessary only if read-only is specified as the default behavior.

0599

Table 9-3 Using the ovw Command to Start NNM (Continued)

Command Entered	Effects
`ovw -map Admin_Map -submap Main`	Runs NNM and opens map named `Admin_Map`, and first displays the submap named `Main` instead of the home submap.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0898
Doc. 3740

Using Operating-System Level File Permissions for the Map

Two factors determine whether a map is opened with read-write access or with read-only access when a map is opened. First, only one user can have a specific map opened with read-write access at any one time (the first person to access the map). Second, you can use the file system to purposely allow specific users read-write or read-only access to a map by setting permission to the files.

TIP If you want several users to have simultaneous read-write access, make copies of the map for each user. See "Copying the Default Map" on page 215. Keep in mind that if your team members make changes to their map, it will then be out of sync with the other maps. To prevent team members from making changes to the map, see page 299.

Possible permission settings are:

Read-write Access A map opened with read-write access is completely editable. You can add objects, add connections, create submaps, and change object attribute values. Only one user can have a specific map open with read-write access at any one time. If another user has the map open with read-write access, when you open the same map, you have read-only access to it. This is the case even if you have read-write permission from the operating system.

Read-only Access A map opened with read-only access is not editable by the user, although the map still can receive status from applications. In a map open with read-only access, you can view status changes, perform locate operations on objects, and update topological changes using the `Map:Refresh Map` menu item. However, you cannot add, delete, or modify items in the map, including symbols, objects, submaps, and map snapshots.

CAUTION: Using `Map:Open` or `Map:Save as`, it may be possible to navigate to a read-write map.

You can use command line options to make *all* maps read-only (page 289) or remove these menu choices (page 299).

No Access — You cannot open a map that is set with No Access.

Windows: Setting Permissions

User access to maps is governed by the file permissions of the snapinfo.dir file in each individual map directory. If NNM is installed on:

- *FAT file system*, you can make each map read-only or read-write for *everyone* on the system. HP recommends that you install NNM on an NTFS file system if more individualized map access permissions are a concern.
- *NTFS*, you have a fine level of control over access to maps. For example, using the Windows Explorer's `Security` tab, you can adjust the permissions so that specific users/groups have write access to specific maps only.

FAT file systems

CAUTION Close the NNM interface before changing map permissions (see "Closing All Current Sessions" on page 319). NNM checks permissions only when it opens the map. If, for example, you change permissions for an open map from read-write to read-only, you risk map database corruption.

Each NNM map is comprised of a group of files. NNM needs to be able to make continuous changes to these files. A special file that controls users' access to the map files themselves is provided for each map. You can set individual maps to `read-write` or `read-only` by setting the attributes on the following file:

install_dir`\databases\openview\mapdb\`*mapname*`\snapinfo.dir`

Log in as Administrator. Use the Windows Explorer to access the file properties of the `snapinfo.dir` file. When you set this file to `read-only`, all the files that comprise the map are read-only protected for *all* users. The next time the map is opened, your changes take affect.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 293
0899
3740

NTFS

CAUTION Close the NNM interface before changing map permissions (see "Closing All Current Sessions" on page 319). NNM checks permissions only when it opens the map. If, for example, you change permissions for an open map from read-write to read-only, you risk map database corruption.

Each NNM map is comprised of a group of files. A special file that controls users' access to the map files themselves is provided for each map. You can set customized permissions for each user/group on individual maps. Set `read-write` or `read-only` attributes on the following file:

`install_dir``\databases\openview\mapdb\`*`mapname`*`\snapinfo.dir`

Log in as Administrator. Access the file properties of the `snapinfo.dir` file and use the Windows Explorer's `File:Properties-> Security` tab. Set the appropriate permissions for each user or group that accesses this file. When you set this file to `read-only`, all the files that comprise the map are read-only protected for *the specific user/group*. The next time the map is opened, your changes take affect.

UNIX: Setting Permissions

CAUTION Close the NNM interface before changing map permissions (see "Closing All Current Sessions" on page 319). NNM checks permissions only when it opens the map. If, for example, you change permissions for an open map from read-write to read-only, you risk map database corruption.

Each NNM map is comprised of a group of files. A special file that controls user's access to the map files themselves is provided for each map. You can set customized permissions for each user/group on individual maps. Set `read-write` or `read-only` attributes on the following file:

`$OV_DB/Openview/mapdb/`*`mapname`*`/snapinfo.dir`

To change map permissions, log in as root. Use the commands provided by NNM. *Do not use the UNIX file permission commands* (`chmod`, `chgrp`, `chown`) *from your operating system.*

NNM provides several commands to let you change permissions:

`ovwchmod`	Changes the mode of individual maps.
`ovwchgrp`	Changes the group ownership of individual maps.
`ovwchown`	Changes the ownership of individual maps.
`ovwperms`	Lists the available maps and their current permissions.

See the *ovwperms* reference page in NNM's online help (or the UNIX manpage) for more information.

To change permissions of *other* NNM configuration files and database files, use the UNIX `chown`, `chmod`, and `chgrp` commands. You may need to stop and start NNM's services (background processes) in order to force NNM to acknowledge the changes. You do not need to stop and start any services to force NNM to acknowledge the change in *map* permissions. The next time the map is opened, your changes take affect.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0900
Doc: 3740

Using the Context Feature to Control Menu Choices

NOTE This feature is not available when accessing NNM over the web.

If you want to remove completely a menu choice from all submaps rather than from specific submaps, see page 299.

If you want to add menu choices, the context feature allows you to control in which submaps your new choices display. See "Creating New NNM Features to Meet Your Team's Needs" on page 278, and see also "Using the MIB Application Builder" on page 443.

This feature allows you to remove or display specific *groups* of pull-down menu items and pop-up menu items on a submap-by-submap basis.

There are two components to the context feature:

- Application Registrations Files (ARFs)

  Menu items are defined in application registration files. Each menu item is set to display in one or more *contexts*.

- `Map:Submap->Properties / Context` tab

  Each submap is configured to display one or more *contexts*.

NNM provides multiple predefined *contexts* for your use. You can also create your own *contexts*.

Anyone with read-write access to the map can change the contexts assigned to a submap.

Using NNM's Predefined Contexts

NNM's predefined context identifiers that are provided for your convenience are:

- `isInternet`

  Displays menus, toolbar buttons, and commands pertaining to an Internet network.

- `isIP`

  Displays menus, toolbar buttons, and commands pertaining to an Internet Protocol (IP) network.

- `isIPX`

  Displays menus, toolbar buttons, and commands pertaining to an Internet Packet Exchange (IPX) network.

- `isNetwork`

  Displays menus, toolbar buttons, and commands pertaining to network management.

- `isNode`

  Displays menus, toolbar buttons, and commands pertaining to node management.

You can add and remove these predefined context identifiers through the `Context` tab in the `Map:Submap Properties` dialog box or the New Submap Wizard. See NNM's online help from these dialog boxes for more information.

NOTE If you see the `NoGeneric` or `NoDefault` context identifier in a submap's properties, do not change it. These are special contexts utilized by application developers.

Creating Your Own Contexts

Contexts are specified on a menu-item by menu-item basis in the application registration files (ARFs) that control HP OpenView or third-party applications. (See page 305 for an example ARF file.)

To create your own context IDs:

- See NNM's online manual, *Creating and Using Registration Files,* for details about editing application registration files (ARFs).
- See the *OVwRegIntro* reference page in NNM's online help (or the UNIX manpage) for more information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0901
3740
Doc:

NOTE If you don't want a menu item to show up everywhere, delete the `AllContexts` identifier associated with that menu item in the ARF file, and replace it with a more specific context identifier.

Close the NNM user interface (ovw service) and reopen it to force NNM to acknowledge changes to the ARF files.

Using ARF Files to Control Menu Choices

NOTE These changes do not affect NNM over the web. NNM's web-based user interface is read-only for all maps, so you do not need to do anything to prevent team members who have web access from making changes to the map.

You can configure NNM so that your team cannot accidentally change your map customizations while accessing maps from remote consoles or on the management station itself. In this example, all features that allow access to modifying NNM are removed *without* setting the map to read-only. By leaving the read-write access to the map, your team retains full use of NNM and can still make map snapshots as needed. You are left in complete control over how NNM operates. Your team can use NNM, but cannot change any configuration settings. All access to configuration settings is removed from your team's view of the software, but remains in your view of the software.

See NNM's online manual, *Creating and Using Registration Files*, for details about editing application registration files (ARFs).

1. Establish *login accounts* for each user/group on your team. NNM needs to be able to differentiate between them in order to provide customized menu selections.
2. Create a unique directory for each user/group to hold their custom registration files. For example:
   - *Windows:* You should be the only user with read-write access:

     ```
     install_dir\registration\connectivity_reg\C\*.*
     install_dir\registration\printers_reg\C\*.*
     install_dir\registration\servers_reg\C\*.*
     ```

   - *UNIX:*

     ```
     /etc/opt/OV/share/registration/connectivity_reg/C/*
     /etc/opt/OV/share/registration/printers_reg/C/*
     /etc/opt/OV/share/registration/servers_reg/C/*
     ```

     (Set your new directories and the files that you place within them to have at least permissions of `r-xr-xr-x`.)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0902
Doc: 3740

TIP Placing your custom registration files in this location ensures that your work is included in the NNM backup and restore process.

3. *Copy* NNM's default registration directory to the new empty directories. NEVER MODIFY THE ORIGINAL FILES:

   - *Windows:* in Windows Explorer, select the contents of *install_dir*\registration\C*.* and paste it into each new directory that you created in the previous step.
   - *UNIX:* repeat the following command for each new directory that you created in the previous step.

```
# cd $OV_REGISTRATION/C
# find .| cpio -pdumv $OV_REGISTRATION/each new directory/C/
```

4. Delete the following files from each new directory that you just populated:

   - `dataWarehouse`

     To disable access to NNM's data warehouse feature that exports the NNM database contents to a relational database.

   - `xnmpolling`

     To disable access to NNM's polling configuration settings.

   - `ovsnmp/xnmbuilder`

     To disable access to NNM's Application Builder program.

   - `ovsnmp/xnmcollect`

     To disable access to setting up or changing data collection and threshold monitoring.

   - `ovsnmp/xnmloadmib`
     To disable access to changing the SNMP MIBs loaded on your system.

   - `ovsnmp/xnmsnmpconf`

     To disable access to customizing NNM's record of your network's SNMP configuration settings such as GET- and SET-community names and port settings.

   - `ovsnmp/xnmtrap`



TIP Placing your custom registration files in this location ensures that your work is included in the NNM backup and restore process.

3. *Copy* NNM's default registration directory to the new empty directories. NEVER MODIFY THE ORIGINAL FILES:
   - *Windows:* in Windows Explorer, select the contents of `install_dir\registration\C\*.*` and paste it into each new directory that you created in the previous step.
   - *UNIX:* repeat the following command for each new directory that you created in the previous step.

```
# cd $OV_REGISTRATION/C
# find .| cpio -pdumv $OV_REGISTRATION/each new directory/C/
```

4. Delete the following files from each new directory that you just populated:
   - `dataWarehouse`

     To disable access to NNM's data warehouse feature that exports the NNM database contents to a relational database.
   - `xnmpolling`

     To disable access to NNM's polling configuration settings.
   - `ovsnmp/xnmbuilder`

     To disable access to NNM's Application Builder program.
   - `ovsnmp/xnmcollect`

     To disable access to setting up or changing data collection and threshold monitoring.
   - `ovsnmp/xnmloadmib`
     To disable access to changing the SNMP MIBs loaded on your system.
   - `ovsnmp/xnmsnmpconf`

     To disable access to customizing NNM's record of your network's SNMP configuration settings such as GET- and SET-community names and port settings.
   - `ovsnmp/xnmtrap`

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: 0903
3740
Doc:

To disable access to customizing NNM's event configuration settings.

5. In each of the new directories that you just created, open the following application registration file (ARF): ...\C\ovw

   Use an ASCII editor program and comment out or delete the following blocks of code that provide potentially destructive functionality to the user interface. To comment out a section, use the /* characters at the beginning and the */ characters at the end of the section that you wish NNM to ignore. Although you can delete these sections, for the convenience of troubleshooting and changing your mind later, it is better to simply comment them out.

TIP Never place comments within comments.

The ARF file controls which menu choices show up in the NNM interface. If you find it confusing to read the file, refer to the NNM user interface for clues about what you are seeing. Refer to the *OVwRegIntro* reference page in NNM's online help (or the UNIX manpage) for information about the syntax of the file.

- In the `MenuBar <100> "Map" _M` section, delete or comment out the following sections to remove Map pull-down menu items from the user interface (see the example ARF file on page 305):

```
"New..."
"Open..."
"Save As..."
"Export..."
"Import..."
"Delete..."
"Properties..."
"Submap..."
```

```
Menu Submap
"New..."
"Open..."
"Delete..."
"Delete This Submap"
"Set This Submap As Home"
"Make This Submap Persistent"
"Properties..."
"Close
```

- In the `MenuBar <100> "Edit" _E` section, delete or comment out the following sections to remove Edit pull-down menu items from the user interface (see the example ARF file on page 305):

```
"Add Object..."
"Add Connection..."
"Cut"
"Copy"
"Paste"
"Delete"
"Manage Objects"
"Unmanage Objects"
"Object Properties..."

Menu Delete
"From This Submap"
"From All Submaps"
```

- In the `MenuBar <100> "View" _V` section, delete or comment out the following sections to remove View pull-down menu items from the user interface (see the example ARF file on page 305):

```
"Hidden Objects"
"Automatic Layout"
"Redo Layout"

Menu "Hidden Objects"
"Hide Selected From This Submap"
"Hide Selected From All Submaps"
"Show Hidden On This Submap"
"Show Hidden On All Submaps"
```

- In the `Menu Find` section, delete or comment out the following sections to remove Find menu items from the user interface (see the example ARF file on page 305):

```
"Submap..."
```

- Delete or comment out all of the following to disable access to NNM customization through the pop-up menus (see the example ARF file on page 305):

```
"Change Symbol Type"
"Symbol Properties"
"Delete"
"Hide"
"Set Star Center"
```

6. Verify that your changes are valid. At the command prompt, type:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0904
3740
Doc:

ovw -verify

7. In each of the new directories that you just created, open the following application registration file (ARF): ...\C\ipmap

   Use an ASCII editor program and comment out or delete the following blocks of code that provide potentially destructive functionality to the user interface. To comment out a section, use the /* characters at the beginning and the */ characters at the end of the section that you wish NNM to ignore. Although you can delete these sections, for the convenience of troubleshooting and changing your mind later, it is better to simply comment them out.

TIP Never place comments within comments.

   The ARF file controls which menu choices show up in the NNM interface. If you find it confusing to read the file, refer to the *OVwRegIntro* reference page in NNM's online help (or the UNIX manpage) for information about the syntax of the file.

   In the `MenuBar "Map"` section, delete or comment out the following sections to remove pull-down menu items from the user interface:

```
"Import..."
"Export..."
```

8. Verify that your changes are valid. At the command prompt, type:

   ovw -verify

9. Set the ovw environment variable `OVwRegDir` in each user/group's path so that the new registration files are used each time this user logs in:

   - *Windows:* Edit the system registry files:

     a. Select `Start:Run` and type **regedit**.

     b. Add a new string value to `HKEY_USERS\`*`S-id#`*`\Environment`. For example:

        Name: **OVWRegDir**

        Data: **c:*install_dir*\registration\printers_reg\C**



NOTE If you are unsure which `S-id#` (systemID number) is the correct `user id#`, you can reference the registry entry and check the `ProfileImagePath` data. Look at the last 3 or 4 digits in the `S-id#`: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\current version\ProfileList\S-id#`.

- *UNIX:*
  C shell users, enter the following in each `.cshrc` file; for example:

```
setenv OVwRegDir=/etc/opt/OV/share/registration/printers_reg/C/
```

  Borne and Korn shell users, enter the following in each `.profile` file; for example:

```
export OVwRegDir=/etc/opt/OV/share/registration/printer_reg/C/
```

10. Log in as the user you just established, and test the look and feel of the user interface to make sure you obtained the results that you had in mind. Try out several submaps with a variety of context settings.

TIP If it isn't working as you expected, you can always return to the untouched original files. In a Windows operating system, however, the registry entries will not be automatically reset.

11. When everything is working as you planned, set the file permissions on your custom registration files as follows:

    - *FAT file system in Windows*, you can set individual files to `read-only` for *everyone* on the system. Log in as Administrator. Use the Windows Explorer to access the file properties of each file in the custom registration directory. Set these files to `read-only` to prevent all users from changing your customizations.

TIP As a workaround for the limited user-level permissions in FAT, consider creating an NTFS partition on your hard drive. Then use the partitioned space for your customized registration

FOS nº 03/2005 - CN - CPMI - CORREIOS
0905
3740
Doc:

directory in order to gain more control over access security. However, if you do this, your customized registration files are no longer automatically included in NNM's backup routine.

- *NTFS in Windows*, you have a fine level of control over file permissions. Log in as Administrator. Using Windows Explorer's `File:Properties->Security` tab, set up the appropriate permissions for the *directory* that holds your customized registration files. Be sure to select both `Replace Permissions on Subdirectories` and `Replace Permissions on Existing Files`. Set the permissions to `read-only` for each user/group to prevent them from changing your customizations.
- *UNIX:* set the appropriate permissions on each file using the standard UNIX `chmod` and `chown` commands. For example:

```
# chmod -R 500 /etc/opt/OV/share/registration/printers_reg/C
# chown -R printers /etc/opt/OV/share/registration/printers_reg/C
# chgrp -R bin /etc/opt/OV/share/registration/printers_reg/C
```

ARF File Modifications Example

The following is a printout of the `ovw` ARF file with bold type showing the sections discussed in the previous section. Place comment symbols /* */ around all the sections in bold type to implement the suggested changes on your management station.

TIP Do not place comments within comments.

```
/*
**
**  @(#)HP OpenView Windows Menu Registration
**
**  $Revision: /main/PULSAR/5 $
**  $Date: 1998/07/06 18:43 UTC $
*/
Application "OpenView Windows"
{
    Description {
        "HP OpenView"
```



```
        "Application registration fiel for various menu items",

        "which present themselves from the ovw menu bar."

    Version "Network  Node Manager X.X (copy_proot modifies)";
    Copyright {
        "Copyright (c) 1990-19XX Hewlett-Packard Company (copy_proot modifies)",
        "All rights reserved."
    }
    }
#ifndef NT
    HelpDirectory "OVW";
#endif /* NT */

    /*
    **
    ** OVw Menu Bars
    **
    */
    MenuBar <100> "Map" _M
    {
#ifndef SPECIAL_EDITION

        <100>   "New..."                _N      Ctrl<Key>N
                Context (AllContexts || WantMapMenus)
                f.new_map;
        <100>   "Open..."               _O      Ctrl<Key>O
                Context (AllContexts || WantMapMenus)
                f.avail_maps;
        <100>   "Refresh"               _f
                Context (AllContexts || WantMapMenus)
                f.refresh_map;
        <100>   "Save As..."    _A      Ctrl<Key>S
                Context (AllContexts || WantMapMenus)
                f.save_map;

        /* 99 is used for ipmap and map customization */

        <98>    "Delete..."             _D
                Context (AllContexts || WantMapMenus)
                f.avail_maps;
#endif /* !SPECIAL_EDITION */
        <98>    "Properties..."         _r
                Context (AllContexts || WantMapMenus)
                f.map_desc;
```

RQS nº 03/2005 - CN - CPMI - CORREIOS
FLS. Nº 0906
3740
Doc:

```
        <98>    "Separator 1"
                Context (CantTouchThis)
                        f.separator;
#ifndef NT
        <98>    "Print Window"  _P              Ctrl<Key>P
                        Context (AllContexts || WantMapMenus)
                        f.action Print_Window;
#endif /* !NT */
        <98>    "Submap"                _S
                        Context (AllContexts || WantMapMenus)
                        f.menu "Submap";
#ifndef SPECIAL_EDITION
        <98>    "Snapshot"              _h
                        Context (AllContexts || WantMapMenus)
                        f.menu "Snapshot";
#endif /* !SPECIAL_EDITION */
        <0>             "Exit"                  _x
                        Context (CantTouchThis)
                        f.exit;
    }
#ifndef NT
        Action "Print_Window" {
                Command "printwindow";
        }
#endif /* NT */
    Menu Submap
    {
        <100>   "New..."                        _N
                        Context (AllContexts || WantMapMenus)
                        f.new_submap;
        <100>   "Open..."                       _O
                        Context (AllContexts || WantMapMenus)
                        f.list_submaps;
        <100>   "Delete..."                     _D
                        Context (AllContexts || WantMapMenus)
                        f.list_submaps;
        <100>   "Delete This Submap"    _T
                        Context (AllContexts || WantMapMenus)
                        f.delete_smap;
        <100>   "Set This Submap As Home"       _H
                        Context (AllContexts || WantMapMenus)
                        f.set_home_submap;
#ifndef NT
        <100>   "Make This Submap Persistent"   _M
                        Context (AllContexts || WantMapMenus)
                        f.persistify;
```

```
#endif /* !NT */
        <100>   "Properties..."          _r
                        Context (AllContexts || WantMapMenus)
                        f.submap_desc;
    <1>         "Close"              _C      <Key>Escape
                        Context (AllContexts || WantMapMenus)
                        f.close_smap;
        }
#ifndef SPECIAL_EDITION
    Menu "Snapshot"
    {
        <100>   "New..."                 _N
                        Context (AllContexts || WantMapMenus)
                        f.create_snap;
        <100>   "Open..."                _O
                        Context (AllContexts || WantMapMenus)
                        f.avail_snaps;
        <100>   "Delete..."              _D
                        Context (AllContexts || WantMapMenus)
                        f.avail_snaps;
        <100>   "Properties..."          _r
                        Context (AllContexts || WantMapMenus)
                        f.snap_desc;
        <100>   "Close"                  _C
                        Context (AllContexts || WantMapMenus)
                        f.close_snapshot;
    }
#endif /* !SPECIAL_EDITION */

    MenuBar <100> "Edit" _E
    {
        <100>   "Add Object..."          _A
                        Context (AllContexts || WantEditMenus)
                        f.add_obj;
        <100>   "Add Connection..."      _n
                        Context (AllContexts || WantEditMenus || WantEditObjs)
                        f.add_conn;
        <100>   "Separator 1"
                Context (CantTouchThis)
                        f.separator;
        <100>   "Cut"                    _t     Ctrl<Key>X
                        Context (AllContexts || WantEditMenus || WantEditCut)
                    f.cut_obj_smap;
        <100>   "Copy"                   _C     Ctrl<Key>C
                        Context (AllContexts || WantEditMenus || WantEditCut)
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0907
Doc 3740

```
                f.copy_obj_smap;
    <100>   "Paste"                 _P      Ctrl<Key>V
                Context (AllContexts || WantEditMenus || WantEditCut)
                f.paste;
    <100>   "Delete"                _D
                Context (AllContexts || WantEditMenus || WantEditObjs)
                f.menu Delete;
<100>   "Selected Objects List..."      _L      Ctrl<Key>L
                Context (AllContexts || WantLocateMenus)
                f.sel_objs;
    <100>   "Find"              _F
        Context (AllContexts || WantEditMenus || WantLocateMenus)
                f.menu Find;
    <50>    "Separator 2"
            Context (CantTouchThis)
                f.separator;
    <50>    "Manage Objects"        _M
                Context (AllContexts || WantMapMenus)
                f.manage_objects;
    <50>    "Unmanage Objects"      _U
                Context (AllContexts || WantMapMenus)
                f.unmanage_objects;
    <1>         "Object Properties..."      _r
                Context (AllContexts || WantEditMenus || WantEditObjs)
                f.obj_desc;
    }

Menu Delete
{
    <100>   "From This Submap"      _T
                Context (AllContexts || WantEditMenus || WantEditObjs)
                f.delete_obj_smap;
    <100>   "From All Submaps"      _A
                Context (AllContexts || WantEditMenus || WantEditObjs)
                f.delete_obj;
}
Menu Find
{
    <100>   "Submap..."                 _S
                Context (AllContexts || WantLocateMenus)
                f.list_submaps;
    <100>   "Object By Selection Name..."   _N      Ctrl<Key>F
                Context (AllContexts || WantLocateMenus)
                f.locate_name;
    <100>   "Object By Attribute..."        _A      Ctrl<Key>A
                Context (AllContexts || WantLocateMenus)
```

```
                        f.locate_attr;
        <100>   "Object By Comment..."          _C
                        Context (AllContexts || WantLocateMenus)
                        f.locate_comment;
        <100>   "Object By Status..."   _u
                        Context (AllContexts || WantLocateMenus)
                        f.locate_status;
        <100>   "Object By Symbol Type..."      _T
                        Context (AllContexts || WantLocateMenus)
                        f.locate_type;
        <100>   "Object By Label..."    _L
                        Context (AllContexts || WantLocateMenus)
                        f.locate_label;
    }
    MenuBar <100> "View" _V
    {
        <100>   "Highlights"            _H
            Context (AllContexts || WantEditMenus )
                        f.menu Highlights;
        <100>   "Hidden Objects"                        _n
                        Context (AllContexts || WantEditMenus || WantEditHide)
                        f.menu "Hidden Objects";
#ifdef NT
        <100>   "Toolbar"               _T
                        Context (AllContexts || WantViewMenus)
                        f.submap_toolbar_toggle;
        <100>   "Status Bar"            _S
                        Context (AllContexts || WantViewMenus)
                        f.submap_status_toggle;
#else /* NT */
        <100>   "Toolbar"               _T
                        Context (AllContexts || WantViewMenus)
                        f.toolbar_toggle;
#endif /* NT */
        <100>   "Pan and Zoom"          _Z
                        Context (AllContexts || WantViewMenus)
                        f.show_panner;
#ifndef NT
        <100>   "User Plane"    _U
                        Context (AllContexts || WantViewMenus)
                        f.user_plane;
        <100>   "Automatic Layout"      _A
                        Context (AllContexts || WantViewMenus)
                        f.auto_layout;
        <100>   "Submap Overlay"        _O
                        Context (AllContexts || WantViewMenus)
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0908
3740
Doc:



```
                        f.overlay_toggle;
#else /* NT */
        <100>   "Submap Overlay"        _O
                        Context (AllContexts || WantViewMenus)
                        f.nt_overlay_toggle;
#endif /* NT */
        <100>   "Window Geometry"       _G
                        Context (AllContexts || WantViewMenus)
                        f.menu "Window Geometry";
        <100>   "Redo Layout"           _R
                        Context (AllContexts || WantViewMenus)
                        f.redolayout;
    }
    Menu Highlights
    {
        <100>   "Select Highlighted"    _S   Ctrl<Key>H
                        Context (AllContexts || WantEditMenus)
                        f.select_highlighted;
        <100>   "Clear Highlighted"     _C
                        Context (AllContexts || WantEditMenus)
                        f.clear_highlights;
    }
    Menu "Hidden Objects"
    {
        <100>   "Hide Selected From This Submap"        _T
                        Context (AllContexts || WantEditMenus || WantEditHide)
                        f.hide_obj_smap;
        <100>   "Hide Selected From All Submaps"        _A
                        Context (AllContexts || WantEditMenus || WantEditHide)
                        f.hide_obj;
        <100>   "Show Hidden On This Submap"    _S
                        Context (AllContexts || WantEditMenus || WantEditHide)
                        f.unhide;
        <100>   "Show Hidden On All Submaps"    _O
                        Context (AllContexts || WantEditMenus || WantEditHide)
                        f.unhide_all;
        }

        Menu "Window Geometry"
        {
                <100>   "Save For This Submap"  _T
                        Context (AllContexts || WantViewMenus)
                        f.geometry_smap;
                <100>   "Save For All Open Submaps"     _A
                        Context (AllContexts || WantViewMenus)
                        f.geometry_all;
```

```
                <100>   "Clear For This Submap" _S
                        Context (AllContexts || WantViewMenus)
                        f.geometry_smap_off;
                <100>   "Clear For All Open Submaps"    _O
                        Context (AllContexts || WantViewMenus)
                        f.geometry_all_off;
        }
    MenuBar <100> "Performance" _P
    {
    }
    MenuBar <100> "Configuration" _C
    {
    }

    MenuBar <100> "Fault" _F
    {
    }
    MenuBar <100> "Accounting" _A
    {
    }
    MenuBar <100> "Security" _S
    {
    }
    MenuBar <100> "Tools" _T
    {
    }
    MenuBar <100> "Options" _O
    {
    }
    MenuBar <100> "Window" _W
    {
        <100>   "Separator 1"
                Context (CantTouchThis)
                        f.separator;
#ifdef NT
        <100>   "Cascade Submaps"               _C
                        Context (AllContexts || WantLocateMenus)
                        f.cascade_submaps;
        <100>   "Separator 2"
                Context (CantTouchThis)
                        f.separator;
#endif /* NT */
        <100>   "Root"                          _R
                        Context (AllContexts || WantLocateMenus)
                        f.goto_root;
        <100>   "Home"                          _H
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fl. Nº 0909
Doc: 3740

```
                Context (AllContexts || WantLocateMenus)
                f.goto_home;
        <100>   "Parent"                        _P
                Context (AllContexts || WantLocateMenus)
                f.goto_parent;
        <51>    "Separator 3"
                Context (CantTouchThis)
                f.separator;
    }
    MenuBar <0> "Help" _H
    {
        <90>    "Display Legend"        _D
                Context (AllContexts || WantHelpMenus)
                f.disp_legend;
#ifndef NT
        <80>    "Mouse and Keyboard"    _M
                Context (AllContexts || WantHelpMenus)
                f.help_browser "ovw:mousenkeyboard";
        <80>    "On Window"
                Context (AllContexts || WantHelpMenus)
                f.help_browser "ovw:overv";
        <60>    "Using Help"                    _H
                Context (AllContexts || WantHelpMenus)
                f.on_help;
    <50>    "Misc"              _i
            Context (AllContexts || WantHelpMenus)
            f.menu "Misc Help";
#endif /* !NT */

        <43>    "Release Notes" _L f.action "ReleaseNotes";

        <40>    "About HP OpenView..."      _A
                Context (AllContexts || WantHelpMenus)
                f.about_ovw;
    }
    Action "ReleaseNotes"
    {
       Command "ovweb -ReleaseNotes README.html";
    }
#ifndef NT
    Menu "Misc Help"
    {
        <98>    "Tasks"                 _T
            Context (AllContexts || WantHelpMenus)
                f.task_index;
        <98>    "Functions"             _F
```



```
            Context (AllContexts || WantHelpMenus)
                    f.function_index;
    }
#endif /* !NT */

    /*
     *  OVw Popup menu
     */
    PopupItem <100> "Open" Context (AllContexts || WantPopupMenus)
                    TargetSymbolType ANY f.open_symbol;
    PopupItem <100> "Change Symbol Type..." Context (AllContexts ||
WantPopupMenus)
                    TargetSymbolType ANY f.change_symbol;
    PopupItem <100> "Symbol Properties..." Context (AllContexts ||
WantPopupMenus)
                    TargetSymbolType ANY f.sym_desc;
    PopupItem <100> "Delete" Context (AllContexts || WantPopupMenus)
                    TargetSymbolType ANY f.delete_symbol;
    PopupItem <100> "Hide" Context (AllContexts || WantPopupMenus)
                    TargetSymbolType ANY f.hide_symbol;
    PopupItem <100> "Set Star Center" Context (AllContexts || WantPopupMenus)
                    TargetSymbolType ANY f.star_center_symbol;
    PopupItem <100> "PopupSeparator1" Context (AllContexts || WantPopupMenus)
                    TargetSymbolType ANY f.separator;
    PopupItem <100> "Object Properties..." Context (AllContexts ||
WantPopupMenus)
                    TargetSymbolType ANY f.obj_desc;



    /*
     *  Toolbar buttons with text
     */

#ifndef SPECIAL_EDITION
    /* Uncomment these for text buttons */

/*  ----  Remove this line for text buttons on the toolbar ----

    ToolbarButton <100> "Close" Context "AllContexts" f.close_smap;
    ToolbarButton <100> "Home" Context "AllContexts" f.goto_home;
    ToolbarButton <100> "Root" Context "AllContexts" f.goto_root;
    ToolbarButton <100> "Parent" Context "AllContexts" f.goto_parent;
    ToolbarButton <100> "TBAR_SEP1"  Context "AllContexts" f.separator;
    ToolbarButton <100> "Pan" Context "AllContexts" f.show_panner;
    ToolbarButton <100> "TBAR_SEP2"  Context "AllContexts" f.separator;
```

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0910
3740
Doc:

```
    ToolbarButton <100> "Open View" Context "AllContexts" f.about_ovw;

    ----  Remove this line for text buttons on the toolbar ----  */
#endif /* !SPECIAL_EDITION */
    /*
     *  Toolbar buttons with icons - icon paths are relative to OV       bitmaps
     *  directory.
     */
    ToolbarButton <100>
#ifdef NT
                @"toolbar/close.bmp,Close"
#else /* NT */
        @"toolbar/close.24.pm:toolbar/noclos.24.pm"
#endif /* NT */
                Context "AllContexts" f.close_smap;

    ToolbarButton <100>
#ifdef NT
                @"toolbar/home.bmp,Home"
#else /* NT */
                @"toolbar/home.24.pm:toolbar/nohome.24.pm"
#endif /* NT */
                Context "AllContexts" f.goto_home;
    ToolbarButton <100>
#ifdef NT
                @"toolbar/root.bmp,Root"
#else /* NT */
                @"toolbar/root.24.pm:toolbar/noroot.24.pm"
#endif /* NT */
                Context "AllContexts" f.goto_root;
    ToolbarButton <100>
#ifdef NT
                @"toolbar/parent.bmp,Parent"
#else /* NT */
        @"toolbar/parent.24.pm:toolbar/noparent.24.pm"
#endif /* NT */
                Context "AllContexts" f.goto_parent;
    ToolbarButton <90> "TBAR_SEP1" Context "AllContexts" f.separator;
    ToolbarButton <90>
#ifdef NT
                @"toolbar/pan.bmp,Pan && Zoom"
#else /* NT */
        @"toolbar/pan.24.pm:toolbar/nopan.24.pm"
#endif /* NT */
                Context "AllContexts" f.show_panner;
    ToolbarButton <0> "TBAR_SEP2" Context "AllContexts" f.separator;
```

```
    ToolbarButton <0>
#ifdef NT
                @"toolbar/hpov.bmp,About HP OpenView"
#else /* NT */
        @"toolbar/hpov.24.pm:toolbar/nohpov.24.pm"
#endif /* NT */
                Context "AllContexts" f.about_ovw;
}
```


RJS nº 03/2005 - CN - CPMI - CORREIOS
Fls. 0911
3740
Doc:



Allowing Others to View NNM from Many Computers

There are two ways to access NNM from multiple computers while it is running on your management station.

- Remote consoles

  Allows multiple people to use NNM as if they were sitting at the management station.

- NNM's web interface

  Allows multiple people to have read-only access to the maps and limited read-write access to the alarm tracking system. The web interface updates dynamically to display current network activity.

- Microsoft Terminal Services

  Allows multiple people to use NNM as if they were sitting at the management station.

Remote Consoles

A number of people can view one map simultaneously or multiple maps by using remote console access (see *A Guide to Scalability and Distribution* manual for information). Remote consoles access the NNM services (background processes) and databases running on the management station, yet run NNM's user interface locally.

This is a great way to distribute the work load among your team. The map and alarms browser list are updated dynamically so everyone on your team knows the current network status. Everyone accessing NNM can acknowledge/delete alarms from the Alarm Browser as issues are resolved.

The number of remote access logins that can be supported is dependent upon a number of factors. See the *Performance and Configuration Guide* that was included with NNM's installation package.

Keep in mind that each remote station generates some network traffic in order to operate.

NNM's Web Interface

Your team can remotely access the NNM session that is running on the management station through the web interface. See Chapter 14, "NNM on the Web," for more information.

Microsoft Terminal Services

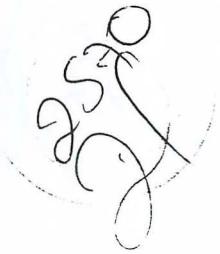
In the Terminal Server multiuser environment, a terminal emulator allows a user to locally display the Windows 2000 desktop of a remote server and manage NNM on that remote server. To enable this functionality, the server must have Microsoft Terminal Services enabled and the local workstation must have Microsoft Terminal Services Client installed. See the *Installation Guide* for more information.

The Terminal Server machine becomes a core server that allows multiple users the ability to connect and display its desktop on their local machines via a Terminal Services Client application. A user can connect (via Terminal Services Client) to multiple Terminal Servers, or connect multiple times to the same Terminal Server and locally display multiple desktops.

The Microsoft Terminal Services client is a small executable that resides on each client workstation. Its function is to display the remote Windows 2000 user interface to the user.

See *A Guide to Scalability and Distribution* manual for more information.

RQS II 03/2005 - CN - CPMI - CORREIOS
FLS. N 0912
Doc: 3740



Closing All Current Sessions

Sometimes, in order to configure, update, or troubleshoot NNM, it is necessary to stop and start the NNM user interface (you *don't* need to stop all the services/background processes). To close all sessions (local, remote, and web) that your team is currently using, do the following:

1. To display a list of currently running sessions, at the command prompt, type:

   ```
   ovstatus -v ovuispmd
   ```

   You may want to print out this information so that you have the hostnames and session IDs for restarting the sessions later. You may wish to notify users who are currently accessing NNM to warn them about the shutdown.

2. To stop all sessions, at the command prompt, type:

   ```
   ovstop -c ovuispmd
   ```

   (This terminates any sessions and stops the `ovuispmd` service--the maps are all closed but your network is still being monitored by NNM services/background processes.)

3. To start new NNM sessions, at the command prompt, type:

   ```
   ovstart -c ovuispmd
   ```

4. Now open NNM's user interface to begin one or more sessions.

2569

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0913
Doc. 3740



10 Keeping Up with Events on Your Network: Beyond the Maps



Once you have verified the accuracy of NNM's maps of your network, you can be sure that communications are established with all important devices. It is now time to turn your attention to the second aspect of NNM, the event system.

In this chapter, you will find:

- *Background Information* (page 323).
  An explanation about how the NNM event system works.
- *NNM's Alarm Browser Overview* (page 329).
  The Alarm Browser provides a convenient central location for your team to monitor critical events on your network.
- *Alarm Browser Customization* (page 342).
  You can control the way the Alarm Browser looks and operates.

See Chapter 11, "Event Reduction Capabilities: Getting to the Root Cause," for information about the event reduction tools that are included with NNM. Also learn how you can use event correlation and the de-duplication feature to automatically determine the root cause of a problem, eliminate unuseful alarms, and in response to a pattern of events, generate new alarms that contain exactly the data you need for troubleshooting.

See Chapter 12, "Customizing Events: Doing It Your Way," for an explanation about how you can implement your own custom event monitoring strategies using NNM's Event Configuration, Application Builder, and Data Collection & Threshold features. You will also learn how to utilize vendor-specific MIBs and MIFs using NNM's MIB Load/Unload, MIB Browser, and DMI Browser features.

See Chapter 13, "Using Event Data," for an explanation about how you can take advantage of the information that has been gathered. NNM provides tools for using this information for analytical purposes and allows you to port the data to the application of your choice. You will learn about NNM's MIB Grapher and the data warehouse features.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0914
3740
Doc:

How NNM's Event System Works

Many services (background processes) within NNM and other HP OpenView compatible programs, gather information and generate **events** that are forwarded to NNM. Events can also be emitted from agents on managed nodes, or from management applications residing on the management station or on specific network nodes. Unsolicited SNMP events or notifications are called **traps**. NNM provides one centralized location, the Alarm Browser, where the events and traps are visible to your team. You can control which events and traps are considered important enough to show up as **alarms**. You and your team can easily monitor the posted alarms and take appropriate action to preserve the health of your network. Examples of alarms include:

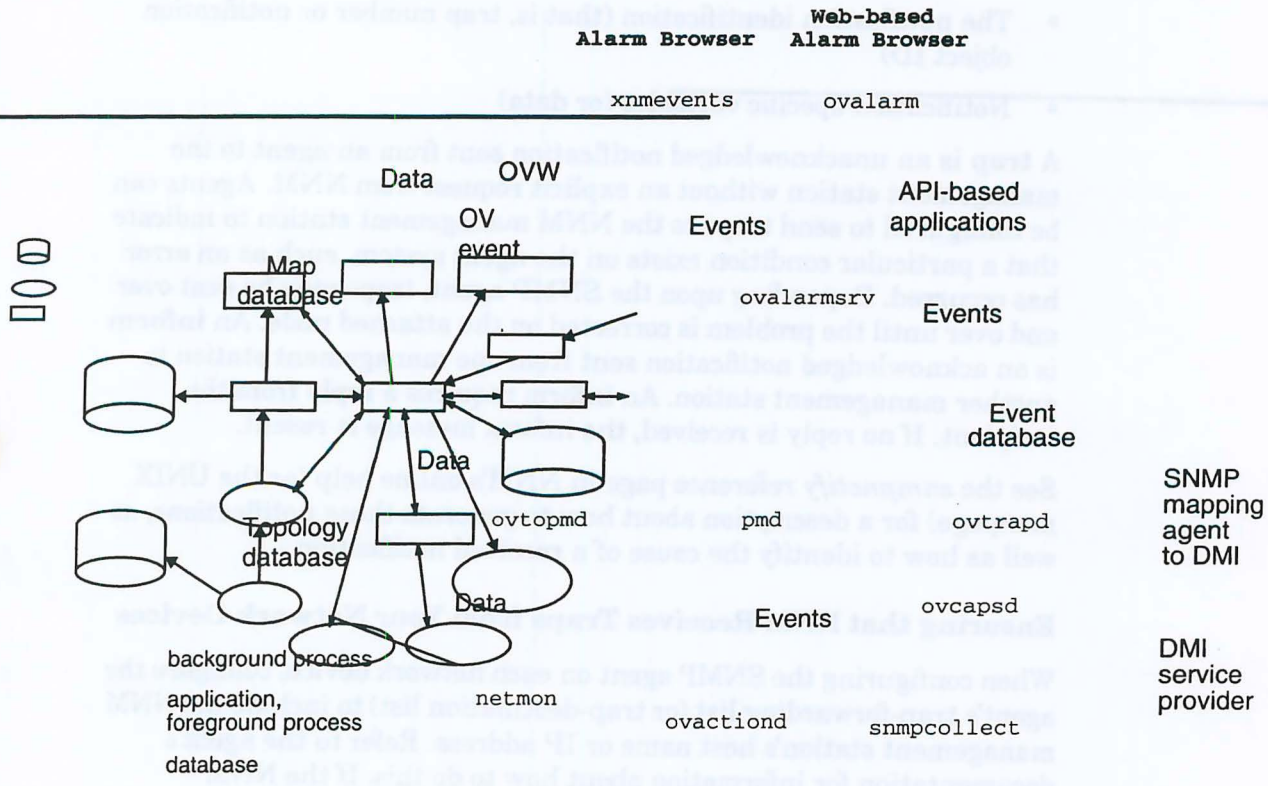
- A critical router exceeded its threshold of traffic volume that you configured in NNM's Data Collection & Thresholds feature (`snmpCollect` service).
- The shell script that you wrote or the MIB application that you created using NNM's Application Builder feature gathered the specific information you needed and posted it to the Alarm Browser.
- An unauthorized network topology change was detected (`netmon` or `ovrepld` services).
- At 3 a.m., you receive a page notifying you that one of your mission-critical servers is using its UPS battery power. You received this page because of the way you configured the underlying DMI event `dmtfUPSBatteryUtilityPowerLostSystemOnBattery` (`ovcapsd` service and `ovactiond` service).
- The theft of a network printer was detected during NNM's regularly scheduled polling cycle (`netmon` service).
- An SNMP agent on a managed critical server forwarded a trap to NNM (`ovtrapd` service) because it was overheating and about to fail.

All events are passed to NNM's `pmd` service, which then logs them in the event database and sends them on to all applications that subscribe to them. For example, the Alarm Browser subscribes to all events configured to *display in a category* of the Alarm Browser.

NOTE Alarms are not received by or displayed in the Alarm Browser if the pmd service is not running. See "Make Sure NNM's Services Are Successfully Running" on page 106 for information about how to verify that pmd is running. Refer to Appendix A, "NNM Services and Files," on page 539 for more information about these services (background processes).

If additional actions were configured to automatically execute upon the pmd services' receipt of a certain alarm (such as dialing a pager or sending an email message), the alarm is also forwarded to NNM's ovactiond service.

Figure 10-1 pmd Interactions with Other NNM Services



By default, NNM's Event Configuration feature includes preconfigured definitions for all standard traps. However, by default not all definitions are configured to post alarms into the Alarm Browser. Use NNM's Event

Configuration feature to specify which traps are important to you and should, therefore, be posted in the Alarm Browser category of your choice (see "Event Configuration Overview" on page 422).

SNMPv1 Traps / SNMPv2c Traps and Informs

An SNMP notification is a message sent from an agent to notify another system of an event on the local system. The notification may either be acknowledged (SNMPv2c `InformRequest`) or unacknowledged (SNMPv1 `TrapResponse` or `SNMPV2cTrap`).

NNM provides you with useful troubleshooting information each time a notification is received:

- The name or address of the node from which the notification came (also called an agent address)
- The notification identification (that is, trap number or notification object ID)
- Notification-specific variables (or data)

A **trap** is an unacknowledged notification sent from an agent to the management station without an explicit request from NNM. Agents can be configured to send traps to the NNM management station to indicate that a particular condition exists on the agent system, such as an error has occurred. Depending upon the SNMP agent, traps may be sent over and over until the problem is corrected on the attached node. An **inform** is an acknowledged notification sent from one management station to another management station. An inform requires a reply from the recipient. If no reply is received, the inform message is resent.

See the *snmpnotify* reference page in NNM's online help (or the UNIX manpage) for a description about how to generate these notifications, as well as how to identify the cause of a received notification.

Ensuring that NNM Receives Traps from Your Network Devices

When configuring the SNMP agent on each network device, configure the agent's trap-forwarding list (or trap-destination list) to include the NNM management station's host name or IP address. Refer to the agent's documentation for information about how to do this. If the NNM management station is included on the trap-forwarding list, NNM receives notice from the agent when something goes wrong (even if the device does not show up on your NNM maps).

If your network device is using the HP SNMP EMANATE agent, NNM's `netmon` service automatically updates the agent's trap-forwarding list upon initial discovery, provided your network's SET-community names are configured within NNM. See "GET- and SET-Community Name and SNMP Port Issues" on page 145.

NOTE For your convenience, NNM lets you view the currently configured trap-forwarding list on remote HP 9000 or Sun SPARCstations running the HP OpenView SNMP Agent software. On any submap, select the symbol for the HP 9000 or Sun SPARCstation running the HP OpenView SNMP Agent software, then do one of the following:

- Select the `Configuration:SNMP Trap Recipients` menu item.
- Use NNM's MIB Browser and the HP-UNIX MIB's object:
  `.1.3.6.1.4.1.11.2.13.1.2`

(You must first configure your correct community names. See "GET- and SET-Community Name and SNMP Port Issues" on page 145.)

Sending SNMP Traps from the NNM Management Station

To forward SNMP trap and inform messages originating from the NNM management station to another location of your choice, you must configure the SNMP agent on the NNM management station to include the destination host name or IP address in its trap-forwarding list. You must also manually configure the protocol versions that the destination supports. Use the `xnmsnmpconf -setVersions` command to configure this feature. Refer to the *xnmsnmpconf* reference page in NNM's online help (or the UNIX manpage) for more information.

For example, to configure protocol versions SNMPv1 and SNMPv2C for the default port for system `robert`, use the following command:

```
xnmsnmpconf -setVersions robert/162 1,2C
```

NOTE For information about forwarding alarms from one management station to another management station, see *A Guide to Scalability and Distribution*.

RQS nº 03/2005 - CN - CPMI - CORREIOS
0916
3740
Doc:

DMI Events (Indications)

The Desktop Management Interface (DMI) is a parallel management strategy to SNMP. DMI standards were developed by the Desktop Management Task Force (DMTF). Although DMI is entirely independent from the SNMP protocol, there are many similarities:

- The DMI **client** is similar to the SNMP management station.
- The DMI **service provider** is similar to the SNMP agent and must be running on each remote DMI device.
- The DMI **MIF** (Management Information Format) file is similar to the SNMP MIB file and defines the management information that can be provided by the service provider (event) or requested by the client (get/set).
- The **DMI event** is similar to the SNMP trap.

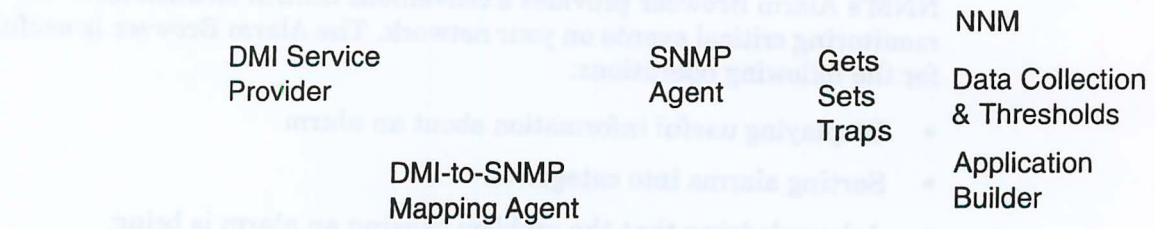
If your management station is running NNM on a Windows operating system, during discovery polling, NNM subscribes to receive DMI events from all managed systems running DMI version 2.0. All DMI events are received by NNM's ovcapsd service (background process) and converted to SNMP traps as specified in the Desktop Management Task Force's DMI to SNMP Mapping Standard. See the *ovcapsd* reference page in NNM's online help for more information.

NOTE

If your management station is running NNM for a UNIX system, you must communicate with the DMI service provider indirectly through an SNMP agent installed on the remote DMI-enabled device itself along with a DMI-to-SNMP mapping agent (such as Intel's). See the following figure.

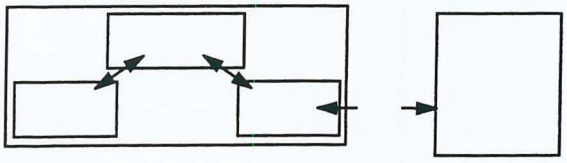
The SNMP agent then handles all communications. Therefore, NNM doesn't need to subscribe to the DMI service provider in order to receive DMI events from this node.

Figure 10-2 Remote DMI Enabled Node



All of the Desktop Management Task Force's standard DMI events that were available at the time of NNM's release are preconfigured in NNM's event system to post automatically to the Alarm Browser. You can customize the behavior of these events in the same manner that you can customize any SNMP event (see "Event Configuration Overview" on page 422 for information about customizing event configurations).

In addition to the DMTF's standard DMI MIF definitions, third-party vendors may have developed custom MIFs with their own custom events. NNM will receive these custom events and translate them to a generic DMI Event Received message until the vendor-specific DMI-to-SNMP mapping is configured in NNM. See "Loading DMI-to-SNMP Event Mappings" on page 419 for information about configuring a DMI-to-SNMP mapping for a custom MIF file.



RQS nº 03/2005 - CN - CPMI - CORREIOS
0917
3740
Doc.

Alarm Browser Overview

NNM's Alarm Browser provides a convenient central location for monitoring critical events on your network. The Alarm Browser is useful for the following operations:

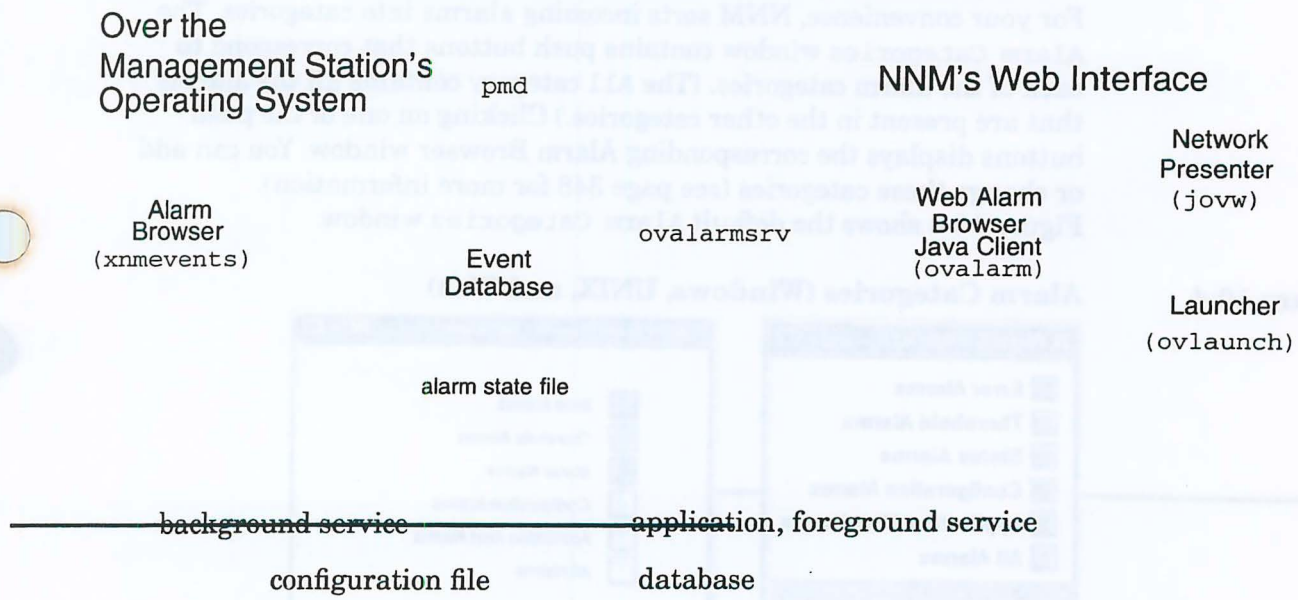
- Displaying useful information about an alarm.
- Sorting alarms into categories.
- Acknowledging that the problem causing an alarm is being addressed.
- Dynamically filtering the alarm list in multiple ways to make the information more useful; for example, by specific node.
- Deleting alarms from the list after they are resolved.
- Specifying additional actions that can be executed upon selected alarms.

There are actually two NNM Alarm Browser programs:

- one that runs under the management station's operating system
- one that runs within NNM's Java-based web interface

Both programs *share* the event database and configuration files for alarms as shown in the following figure. Therefore, no matter which Alarm Browser you use, the displayed list of alarms remains current at all times. Whenever someone acknowledges an alarm, deletes an alarm, or changes severity for an alarm everyone on the team sees the change.

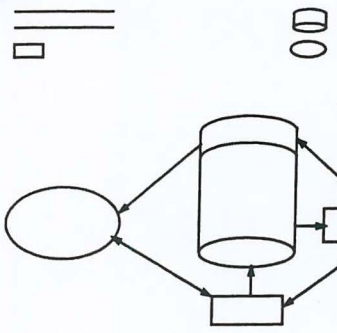
Figure 10-3 Relationship Between the Two Alarm Browsers



Displaying Alarms

To view alarms, open the NNM user interface, then:

- *Windows or UNIX:* Either,
  - In the `Alarm Categories` window, click on the button that corresponds to the category you wish to view.
  - In any submap, select the `Fault:Alarms` menu item to display the `All Alarms Browser` window. If any symbols are selected on your map, the alarm list is *filtered* to show only alarms related to the selected symbols.
- *Java-based web interface:* Either,
  - In the Launcher, select the `Tools` tab, then select `NNM:Alarm Browser`. In the `Alarm Categories` window, click on the button that corresponds to the category you wish to view.
  - In Network Presenter, select the `Fault` menu, then select `Alarm Browser`. In the `Alarm Categories` window, click on the button that corresponds to the category you wish to view.



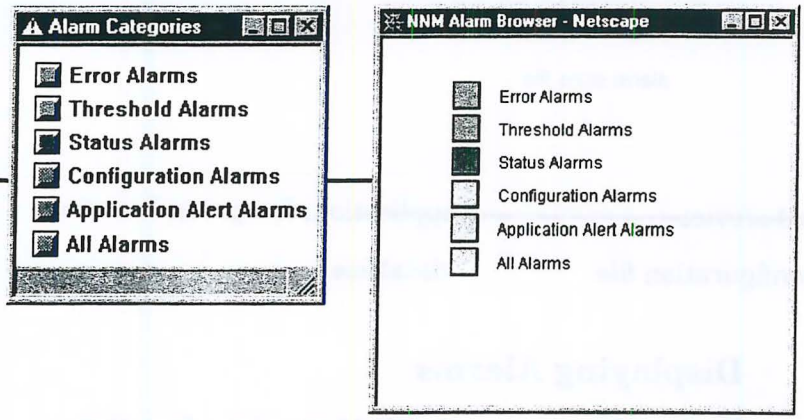
RQS nº 03/2005 - CN - CPMI - CORREIOS
0918
3740
Doc:

To exit any of the Alarm Browser windows, select `File:Close`.

Alarm Categories/Alarm Browser Windows

For your convenience, NNM sorts incoming alarms into categories. The `Alarm Categories` window contains push buttons that correspond to each of the alarm categories. (The `All` category contains all the alarms that are present in the other categories.) Clicking on one of the push buttons displays the corresponding Alarm Browser window. You can add or change these categories (see page 348 for more information). Figure 10-4 shows the default `Alarm Categories` window.

Figure 10-4 **Alarm Categories (Windows, UNIX, and Web)**



The push buttons in this window change color to indicate that alarms have been received. The color of the push button reflects the most severe unacknowledged alarm in the category, or it remains the background color if no alarms are present or all alarms are acknowledged. By default, alarm severity is indicated by the following colors:

Normal	Green
Warning	Cyan
Minor	Yellow
Major	Orange
Critical	Red
No alarms	Background color
All alarms acknowledged	White

When you select a category, the corresponding Alarm Browser window is displayed. The Alarm Browser window contains a scrollable list of alarms belonging to the associated category. The Alarm Browser window also displays status about the number of alarms in the window and their severity. Figure 10-6 shows the `All Alarms Browser` window.

To view details about alarms:

- *Windows or UNIX:*
  - Click the right mouse button on any alarm message to display a pop-up window that contains a summary.
  - Select the `Actions:Alarm Details` for complete details.
- *Java-based web interface:*
  - Click on the  button for complete details.
  - Select the `Actions:Alarm Details` for complete details.

It is possible to sort the alarm list:

- *Windows or UNIX:* Select `Actions:Additional Actions` for sorting choices.

- *Java-based web interface:* Click once or twice on any column heading.

Figure 10-5 All Alarms Browser Window (Windows or UNIX)

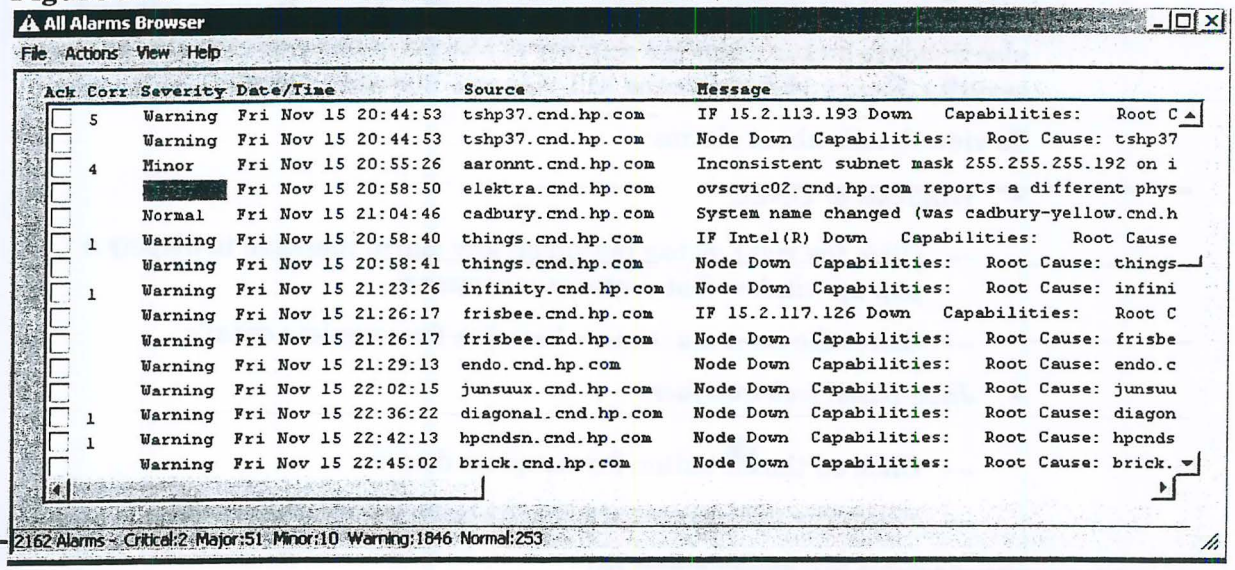
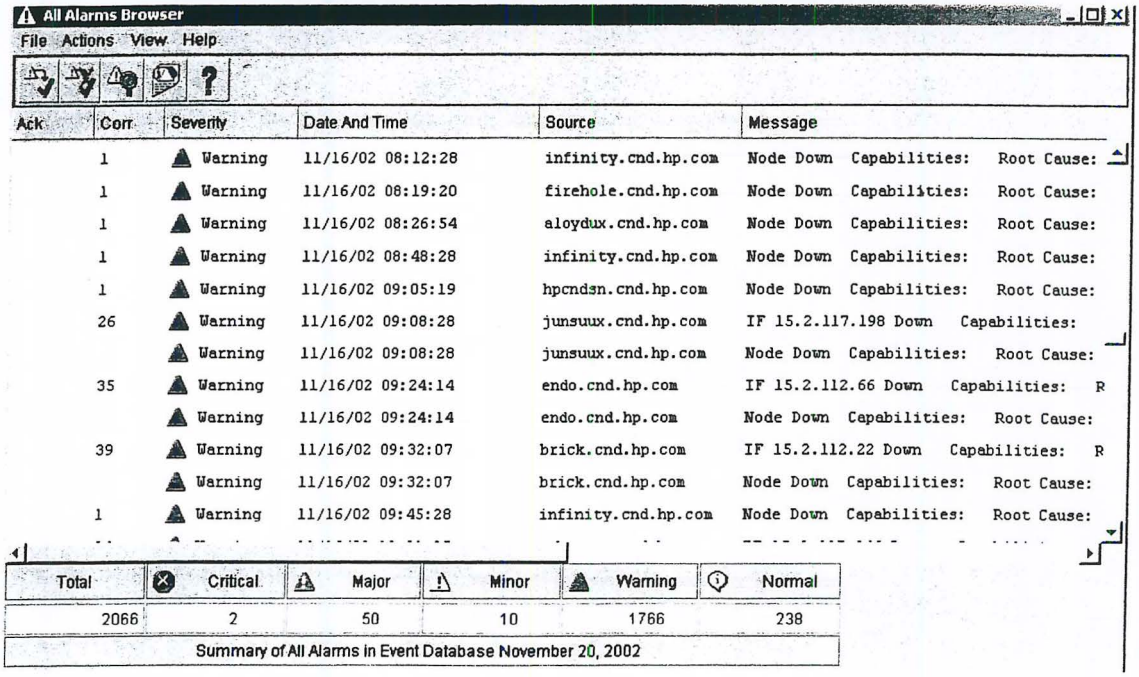


Figure 10-6 All Alarms Browser Window (Web)





The Alarm Browser window lists all undeleted alarms for the indicated category. By default, the alarms are in chronological order with the most recent event at the *bottom* of the list.

For each alarm, the list displays the following:

`Ack`	A check mark indicating whether the alarm is acknowledged or unacknowledged.
`Corr`	A number in this column indicates that this is a primary (root cause) alarm for a group of alarms identified by the Event Correlation System. This number represents the quantity of related or duplicate events correlated beneath the most recent alarm. If you double-click on this number, NNM displays all of the events nested under the alarm.
`Severity`	The severity of the alarm.
`Date/Time`	The day of the week, date, and time when the alarm was received.
`Source`	An identifier (such as a node name) for the network object where the alarm originated.
`Message`	A brief description of the alarm.

Acknowledging Alarms

In order to keep track of which alarms are being worked on, members of your team can acknowledge an alarm, yet not delete it. When an alarm is acknowledged, everyone who has access to the Alarm Browser sees the change. This is a great way for your team to communicate about which issues are being addressed.

Once acknowledged, an alarm remains visible but does not affect the color propagated into the `Alarm Categories` window. To acknowledge selected alarms:

- *Windows and UNIX:*
  Either select the `Actions:Acknowledge` menu item or click in the `Ack` field.
- *Java-based web interface:*
  Either select the `Actions:Acknowledge` menu item or click the  button.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 3740
Doc:

Filtering Alarms

Filtering allows you to limit the number of alarms displayed. You display only the alarms that are meaningful to your particular troubleshooting efforts at the time; for example, all alarms related to a specific node. Your filtering choices do not affect the Alarm Browser lists being viewed by other members of your team. When you close any Alarm Browser window, the filters are automatically cleared.

Each person using NNM can dynamically filter their displayed alarm list based upon one or more criteria. The criteria must all be true for an alarm to display in the list:

- Severity level
- Source IP addresses or use wildcards to specify a range of IP addresses or node names
- Acknowledged or unacknowledged alarms
- Alarm time span
- Message string word search
- Event type

Filters are available from any Alarm Browser window under `View:Set Filters`.

- *Windows or UNIX:*
  If filtering is on, the status message at the bottom of the Alarm Browser window indicates that filtering is applied.

  Each Alarm Browser window can use unique alarm filter settings. Only one filter dialog box can be displayed at a time. The title bar of the filter dialog box indicates which Alarm Browser window is currently affected. If the filter dialog box is displayed and the `View:Set Filters` menu item is selected from a different Alarm Browser window, the name in the filter dialog box title bar changes and the filter settings in the dialog box change to reflect current filter settings for that Alarm Browser window.

  You can perform operations based upon the filtered alarms, the selected alarms, or all the alarms in the category. For example, to see all the `Critical` alarms, pick the `All Alarms` category. From the `All Alarms Browser` window pick `View:Set Filter`, then ensure that only `Critical` severity is selected and click `[Apply]` or `[OK]`. The filter modifies the list of alarms currently displayed in the Alarm

2553

Browser window. You now see all the critical alarms. After resolving all these alarms, delete them using `Actions:Delete->Filtered Alarms`. The category light in the `Alarm Category` window changes from red to the next most severe color.

You can save and restore the filters you have set by using the `[Save]` and `[Restore]` buttons in the `Set Filters` dialog box (not available in the web-based Alarm Browser).

- *Java-based web interface:*
  If filtering is on, the status message at the bottom of the Alarm Browser window indicates that filtering is applied.

  You can perform operations based upon the filtered alarms and the selected alarms. For example, to see all the `Critical` alarms, pick the `All Alarms` category. From the `All Alarms Browser` window pick `View:Set Filter`, then ensure that only `Critical` severity is selected and click `[Apply]` or `[OK]`. The filter modifies the list of alarms currently displayed in the Alarm Browser window. You now see all the critical alarms. After resolving all these alarms, delete them using `Actions:Delete->All in Browser`. The category light in the `Alarm Category` window changes from red to the next most severe color.

  Each Alarm Browser window can use unique alarm filter settings. Select the `View:Set Filters` menu item from any Alarm Browser window to set its filter.

NOTE Two additional alarm filters are available on a user-by-user basis; they need to be implemented on each management station and each remote console. These filters are not available through NNM's web interface:

- `filterByMap`
  Display only alarms that apply to devices on the current map.
- `filterByMapManaged`
  Display only alarms that apply to managed devices on the current map.

These two filters are invoked through settings in:

- *Windows:* The system registry settings for `xnmevent`
  See the *app-defaults* reference page in NNM's online help.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0921
Doc: 3740

- *UNIX:* `$APP_DEFS/XNmevents` file
  See the comments within this ASCII file.

Deleting Alarms

Alarms remain visible in an Alarm Browser window until someone deletes them or until the specified maximum number of alarms for the browser has been reached. If you do not delete (or acknowledge) alarms, each button in the `Alarm Categories` window will continue to show status color for all alarms, and you may not know when new alarms occur. When an alarm is deleted, it is removed from everyone's alarm list.

You can delete alarms either individually or all at once, using choices under the `Actions:Delete` menu item in each Alarm Browser window. Whenever you delete alarms, a confirmation window pops up.

Once deleted, the same alarm instance does not reappear. You need only delete the alarm in one Alarm Browser window. This clears the alarm from every Alarm Browser window in which it appears.

See "Controlling the Size of the Alarm Browser's State File" on page 344 for information about controlling the maximum number of alarms; the

NOTE

If you want to turn off the confirmation dialog box:

- *Windows:* In the system registry, set `XNevents/warnOnDelete` to false. See the *app-defaults* reference page in NNM's online help.
- *UNIX:* In the `$APP_DEFS/XNevents` file, set `warnOnDelete` to false. See the comments in this ASCII file for more information.

The confirmation dialog box does not appear over the web-based interface.

TIP

If you plan to delete a large number of alarms and wish to be able to undo the delete, see "Copy or Restore the Alarm Browser's State File" on page 347.

NNM's Map and the Alarm Browser

The map and the Alarm Browser are tightly integrated. When you double-click on an alarm from the Alarm Browser, NNM displays the source node in the submap, zooms to the highlighted object, and displays the panner window. Conversely, from a submap, NNM makes it easy to display all alarm messages related to selected symbols.

Highlighting an Alarm Message and Displaying the Relevant Submap

NOTE Selecting alarm messages in an Alarm Browser window does not affect the current object selections on your map.

To jump directly from an alarm message to the corresponding submap, select the alarm in the Alarm Browser window. Select:

- *Windows or UNIX:* `Actions:Highlight Source on Map` or simply double-click on the alarm message. The submap containing the source of the alarm is displayed. The label for the source object is *highlighted*. Any map symbols that were previously highlighted or *previously selected* remain so.
- *Java-based web interface:* `Actions:Show Node in Network Presenter`. If accessing a map other than the *default* map, you must type in the correct map name before proceeding. A new instance of the Network presenter is started. Any previously running instance of the Network Presenter is closed. The submap containing the source of the alarm is displayed. Only the symbol for the source object is *selected*.

On the submap, use NNM's menu items to obtain more information to help you resolve the problem that has caused the alarm.

TIP You may receive alarms for nodes that do not appear on the map. For example:

- If an SNMP agent is not in your management region, but is configured to send traps to the NNM management station, the Alarm Browser receives alarms for that agent (for example, when it starts up).

RQS nº 03/2005 - CN - CPMI - CORREIOS
0922
3740
Doc.



- If you are displaying a map's snapshot, the alarms are for the current map itself, not the snapshot.

Selecting Map Symbols and Displaying Associated Alarm Messages

To access alarm information about objects on the map:

- *Windows or UNIX:* Select the objects on the map and then select `Fault:Alarms`. The `All Alarms Browser` window displays automatically filtering out all alarms except those associated with the selected objects.
- *Java-based web interface:* From any submap, select the `Fault:Alarms` menu item; or select an object on the map, then right-click and select `Alarm Browser`. The `Alarm Category` window is displayed. To view alarms for specific devices, open the All Alarms list and use `View:Set Filters` to limit the alarm list.

Specifying Additional Actions on Alarms

You can select alarms and pipe the alarms into user-written programs (shell commands via standard input), using the menu item `Actions:Additional Actions`. The output of the command will be displayed.

NOTE This feature is not available in the web-based Alarm Browser.

Only one `Additional Actions` dialog box can be displayed at a time. The `Additional Actions` dialog box affects alarms in the browser that is indicated in its title bar. If this dialog box is displayed and the `Actions:Additional Actions` menu item is selected in a different Alarm Browser window, the name in the title bar changes to reflect the alarm category for the most recently selected browser.

Specify the scope of the action. You can select one of five different scopes for the action. These are:

- Selected Alarms
- Filtered Alarms



- Acknowledged Alarms
- Unacknowledged Alarms
- All Alarms in Category

Clicking `[Describe]` when an action is highlighted provides a description of the action, including what command is executed, and how long NNM waits for the command to complete before terminating the command.

See the *trapd.conf* reference page in NNM's online help (or the UNIX manpage) for an explanation about how to write additional action commands. The command is a program that expects input in a predefined format. See "Defining Additional Actions" on page 441, which describes how to define additional actions.

Launching Specific Views or URLs from Alarms

You can configure up to 50 URLs in the `xnmeventsExt.conf` file for the `Actions:Views` menu. These URLs can be one of the NNM views or any other URL that you prefer. NNM views are available from NNM's `Tools` menu.

To configure an alarm to launch a specific URL, edit the following file:

- *UNIX*:`$OV_CONF/$LANG/xnmeventsExt.conf`
- *Windows:* `install_dir\conf\C\xnmeventsExt.conf`

Editing instructions are included in the file.

After you modify xnmeventsExt.conf, do the following for the changes to take effect:

1. Close the NNM Alarm Browser.
2. Stop the `ovalarmsrv` process:
   - *Windows*: Run the `install_dir\bin\ovstop ovalarmsrv` command.
   - *UNIX*: As root, run the `$OV_BIN/ovstop ovalarmsrv` command.
3. Start the `ovalarmsrv` process:
   - Windows: Run the `install_dir\bin\ovstart ovalarmsrv` command.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0923
3740
Doc:

- UNIX: As root, run the `$OV_BIN/ovstart ovalarmsrv` command.

4. Run the `xnmevents` command to restart the NNM Alarm Browser:
   - *Windows*: Run the *`install_dir`*`\bin\xnmevents.exe` command.
   - *UNIX*: Run the `$OV_BIN/xnmevents.exe` command.
5. Restart any web-based Alarm Browsers to view the new menu items.
6. Use the `Fault:Alarms` menu item to open the Alarm Browser. The `Actions:Views` menu in the Alarm Browser should contain the new menu items.

See *Using Network Node Manager Extended Topology* for more information.

Configuring the Alarm Browser

You can configure the Alarm Browser in the following ways:

- Set the maximum size of the event database (default is 16MB).
- Set the maximum number of alarms in the Alarm Browser's state file (default is 3500).
- Set the number of alarms that should be deleted each time the state file reaches maximum capacity.
- Copy or restore the Alarm Browser's state file.
- Control the look and behavior of the Alarm Browser.
- Assign alarm categories:
  - Moving alarms from one category to another.
  - Changing the default alarm category for a specific MIB object.
  - Creating new alarm categories and assigning alarms to the new category.

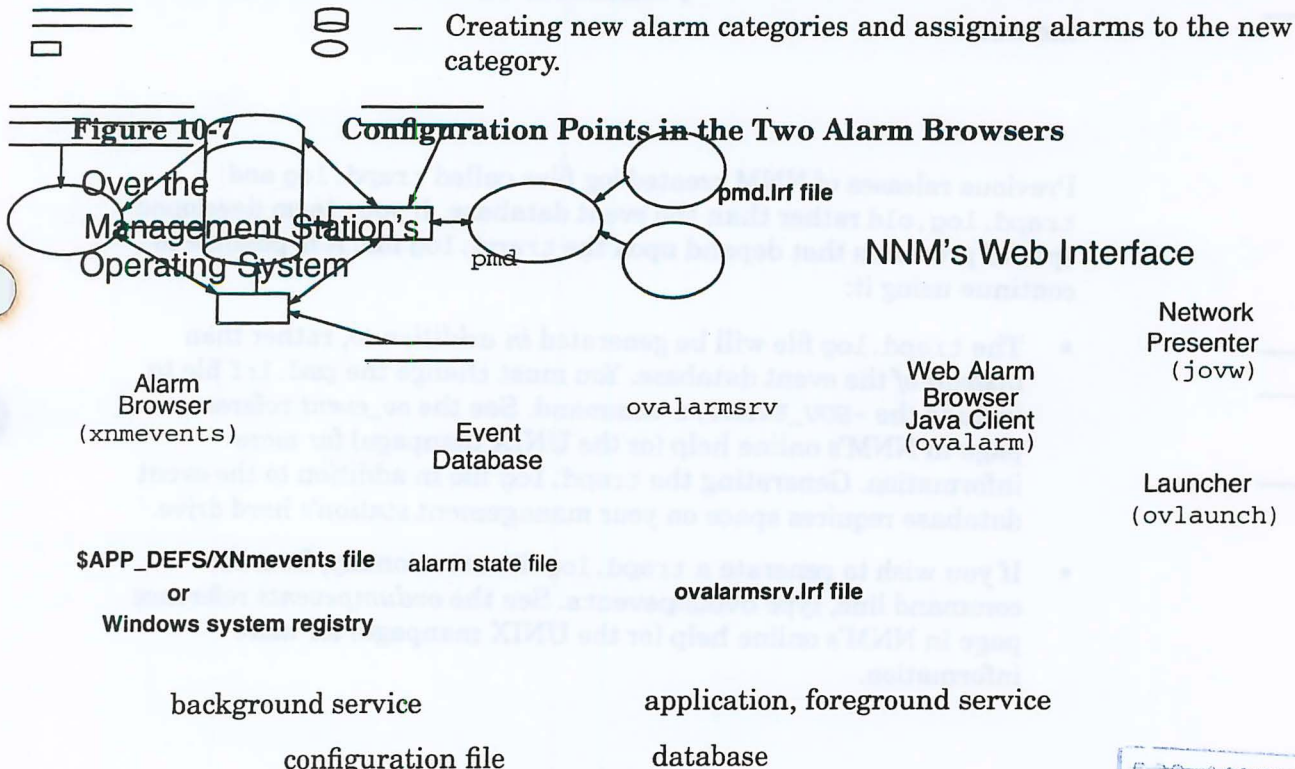


Figure 10-7 Configuration Points in the Two Alarm Browsers

Controlling the Size of the Event Database

All events are entered into the event database. The most important ones are posted to the Alarm Browser. Many NNM services rely upon the information stored in the event database. The default maximum size setting is 16MB. The event database is divided into four files. In the default configuration of 16MB, this means that each file has a maximum size of 4MB. When all four files are full, the oldest log is truncated and new events are written into the reclaimed space.

You can change the amount of disk space that is reserved on the management station for the event database by setting the `b` parameter in the `pmd.lrf` file. See the *ov_event* and *pmd* reference pages in NNM's online help (or the UNIX manpages) for information about changing this setting. Information from the event database can be archived into the data warehouse for trend analysis by selecting the menu item `Tools:Data Warehouse->Export Events`.

NOTE The event database is accessed by all versions of NNM running on your management station: NNM for Windows *or* NNM for UNIX, and NNM on the web.

TIP Previous releases of NNM created log files called `trapd.log` and `trapd.log.old` rather than the event database. If your team developed special processes that depend upon the `trapd.log` file, it is possible to continue using it:

- The `trapd.log` file will be generated *in addition to*, rather than *instead of* the event database. You must change the `pmd.lrf` file to include the `-SOV_EVENT;t` command. See the *ov_event* reference page in NNM's online help (or the UNIX manpage) for more information. Generating the `trapd.log` file in addition to the event database requires space on your management station's hard drive.
- If you wish to generate a `trapd.log` file occasionally, from the command line, type `ovdumpevents`. See the *ovdumpevents* reference page in NNM's online help (or the UNIX manpage) for more information.



Controlling the Size of the Alarm Browser's State File

Events that are configured to post as alarms in the Alarm Browser are sent to the Alarm Browser's state file. The contents of this state file provides the starting point for displayed alarms each time you open the NNM interface. The state file maintains all user edits to the alarm list, such as acknowledgments or deletes.

To modify the number of alarms being stored and displayed, you must change the setting in two places.

- The `-a` parameter in the `ovalarmsrv.lrf` file.
  Changes in the `ovalarmsrv.lrf` file control what is stored in the state file. Remember that this setting affects all users who have access to NNM. Consider RAM and hard drive space on your management station when changing this setting.
- The `maxEvents` setting.
  This parameter is in the UNIX's `$APP_DEFS/XNmevents` file or in the Windows system registry's `xnmevents` entry. It controls how many messages display in the Alarm Browser window itself (independent of the number stored in the underlying state file).

To change the `ovalarmsrv.lrf` file setting that controls the state file:

1. Make your changes to the `-a` parameter and save your changes:
   - *Windows:* *`install_dir`*`\lrf\ovalarmsrv.lrf`
   - *UNIX:* `$OV_LRF/ovalarmsrv.lrf`

   See the *lrf* reference page in NNM's online help (or the UNIX manpage) for more information.
2. Update NNM's configuration file. At the command prompt, type:
   `ovaddobj ovalarmsrv.lrf`
3. To force NNM to acknowledge the change, at the command prompt, type:
   `ovstop ovalarmsrv`

TIP This causes the Alarm Browser to close in all currently running NNM sessions.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0925
3740
Doc:

Then at the command prompt, type:
ovstart.

To change the `maxevents` setting that controls the display of messages, on each management station and each remote console (not required for the web-based Alarm Browser):

1. Make your changes to the `maxEvents` parameter and save your changes:
   - *Windows:* The system registry
     `MKEY_LOCAL_MACHINE:SOFTWARE:Hewlett-Packard:OpenView:Network Node Manager:xnmevents:maxEvents`
   - *UNIX:* `$APP_DEFS/XNmevents` file
2. To force NNM to acknowledge your changes, simply close the Alarm Browser; then reopen the Alarm Browser.

See the *ovalarmsrv, app-defaults,* and *xnmevents* reference pages in NNM's online help (or the UNIX *ovalarmsrv* and *xnmevents* manpages) for more information.

TIP Previous releases of NNM used per-user state files (`xnmevents.user`). Do not try to restore these old state files into this version of NNM.

Controlling How Many Alarms to Delete Automatically

Each time the Alarm Browser's state file reaches maximum capacity, the oldest alarms (at the top of the list) are deleted to make room for the new ones.

To control the number of alarms deleted each time, you must change the setting in two places.

- The `-d` parameter in the `ovalarmsrv.lrf` file.
  Remember that this setting affects all users who have access to NNM. Consider the frequency of pause time required to rewrite the state file's alarm list if you change this setting. The higher the number the less frequent the pause.

- The `deleteNumber` setting.
  This parameter is in UNIX's `$APP_DEFS/XNmevents` file or in the Windows system registry's `xnmevents` entry. It controls how many messages are deleted each time the Alarm Browser window itself reaches maximum size (independent of the number stored in the underlying state file).

To change the `ovalarmsrv.lrf` file setting that controls the state file:

1. Make your changes to the `-d` parameter and save your changes:
   - *Windows:* *`install_dir`*`\lrf\ovalarmsrv.lrf`
   - *UNIX:* `$OV_LRF/ovalarmsrv.lrf`

   See the *lrf* reference page in NNM's online help (or the UNIX manpage) for more information.
2. Update NNM's configuration file. At the command prompt, type:

   `ovaddobj ovalarmsrv.lrf`
3. To force NNM to acknowledge the change, at the command prompt, type:

   `ovstop ovalarmsrv`

TIP This causes the Alarm Browser to close in all currently running NNM sessions.

Then at the command prompt, type:

`ovstart`

To change the `deleteNumber` setting that controls how many messages are deleted from the Alarm Browser display window, on each management station and each remote console (not required for the web-based Alarm Browser):

1. Make your changes to the `deleteNumber` parameter and save your changes:
   - *Windows:* In the system registry, add the following parameter and specify the number:
     `MKEY_LOCAL_MACHINE:SOFTWARE:Hewlett-Packard:OpenView:Network Node Manager: xnmevents:deleteNumber`

CPMI - CORREIOS
FIS.N° 0926
Doc: 3740



- *UNIX:* `$APP_DEFS/XNmevents` file

2. To force NNM to acknowledge your changes, simply close the Alarm Browser; then reopen the Alarm Browser.

See the *ovalarmsrv*, *app-defaults*, and *xnmevents* reference pages in NNM's online help (or the UNIX *ovalarmsrv* and *xnmevents* manpages) for more information.

Copy or Restore the Alarm Browser's State File

The state file records all actions that have been applied to specific alarms, such as acknowledging an alarm, deleting an alarm, changing an alarm's category, or changing an alarm's severity rating. Remember that the state file affects all users who access NNM (unlike the filtering or sorting of alarm messages, which is controlled by each individual user).

There may be times when you want to delete a large number of alarms, yet be able to change your mind and undo the deletion. This is possible if you first save the state file.

NNM provides a tool for you to use that makes sure all services (background processes) are in the correct state, then copies or restores the state file for you.

See the *ovalarmadm* reference page in NNM's online help (or the UNIX ut copying and restoring the Alarm Browser's state file.

CAUTION

Do not work directly with the encoded binary state file:

- *Windows:* `install_dir\databases\eventdb\statelog`
- *UNIX:* `$OV_DB/eventdb/statelog`

All changes to this file are made through the Alarm Browser.

Controlling How the Alarm Browser Looks

If there are compelling reasons that you need to change aspects of the Alarm Browser such as the color used to indicate the severity of alarms, Explore the possibilities in:

- *Windows:* The system registry
  See the *app-defaults* reference page in NNM's online help for more information.
- *UNIX:* `$APP_DEFS/XNmevents` file
  See the information included in this ASCII file for more information.

Assigning Alarm Categories

You can control the category into which an alarm message is displayed by:

- Moving an existing alarm message to another category (affecting only that instance of the particular alarm).
- Changing the default category for alarms received from a specific MIB object.
- Creating an entirely new alarm category and assigning alarms to the new category.

Moving an Existing Alarm Message to Another Category

To move an alarm to a different category, in any Alarm Browser window, select the alarms that you want to recategorize. Then select `Actions:Assign Category` from the menu bar. Refer to the online help if you need more information.

This change only affects the selected instances of the alarms. Future alarms of the same type will continue to be posted in the old category's list, unless you reconfigure the alarm as described next.

Changing the Default Category for an Alarm

NOTE You cannot do this through NNM's web interface.

To permanently change the category assignment for a specific alarm message, you must change the configuration settings for the specific underlying event's MIB object. Access the `Event Configuration` dialog box:

RQS nº 03/2005 - CN
CPMI - CORREIO.
Fls. Nº 0927
3740
Doc:

- From any Alarm Browser window, select the alarm you wish to reconfigure, and select the `Actions:Configure Event` menu item. The `Event Configuration` dialog box displays the underlying event's current configuration.
- From any submap, select the `Options:Event Configuration` menu item. It is up to you to navigate to the MIB object that defines the event you wish to reconfigure.

Prerequisites are:

- The MIB for which you want to configure events must be loaded into NNM's MIB database. The `Options:Load/Unload MIBs:SNMP` operation lists all MIB modules currently in NNM's MIB database. If the enterprise-specific MIB is not loaded, see "Loading MIBs in the MIB Database" on page 413 for more information.
- Make sure you understand the enterprise-specific MIB. To configure events, you need to understand the trap definitions for the device and what they do. Most device vendors include documentation about their enterprise-specific traps with their product. This documentation typically describes the trap and when the trap is generated. In addition, some vendors include overview information describing strategies for how to manage their specific device. The vendor documentation can give you the conceptual understanding that you need to configure effective event formats and actions.

Refer to "Event Configuration Overview" on page 422 for information about reconfiguring an event to always post its alarm into a specific category of the Alarm Browser.

Creating a New Alarm Category

NOTE You cannot create a new alarm category through NNM's web interface. However, once you establish a new alarm category, it will show up in the web-based Alarm Browser.

You can configure NNM's Alarm Browser to contain custom categories that fit your organization's needs.

For example, you could add a category called `Link Address Alarms`. Once added, you could change all SNMP link address events so that new alarms of this type are posted into the new category.

To add a new category:

1. Access the `Event Configuration` dialog box from either any Alarm Browser window (`Actions:Configure Event`) or from any submap (`Options:Event Configuration`).
2. From the `Event Configuration` menu bar, click `Edit:Alarm Categories`. The `Alarm Categories` window appears.
3. Check NNM's online help that is available within the `Alarm Categories` window for more information.
4. In the `Event Configuration` window, click `File:Save` to save the changes you have made. The new event category appears in the `Alarm Categories` window.

NOTE You must now assign specific SNMP events (associated with specific MIB objects) to this new category; otherwise, it will remain empty. For information about assigning specific events to this category, see "Event Configuration Overview" on page 422.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0928
3740
Doc:

11 Event Reduction Capabilities: Getting to the Root Cause



NNM's Event Reduction Capabilities

Event reduction is the process by which NNM can identify relationships between events. Once identified, a smaller number of new events with the same or higher information content can be generated. This simplifies diagnosing network faults. There are three event reduction strategies within NNM:

- "De-Duplication of Alarms" on page 358

  Multiple, identical alarms are often sent to the NNM Alarm Browser. NNM can retain these alarms, but not display all of them by using *de-duplication* to nest the duplicate alarms beneath the most recent alarm. By reducing the quantity of alarms displayed in the Alarm Browser, you can easily determine the important alarms. You control which events are nested in this manner by making entries in the `dedup.conf` file.

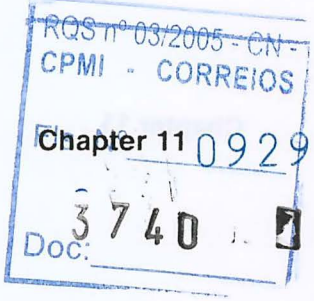
- "ECS Correlations" on page 360

  NNM includes built-in event correlation logic that evaluates incoming events and nests certain related events under a single meaningful alarm. Event correlation helps you quickly identify the primary cause of the problem. For example, you don't need to sift through hundreds of alarms to identify the root cause when a router goes down. High-speed correlation minimizes network bandwidth utilization and improves the quality of customer network services. The fundamental design principle is to correlate events in real-time.

- "Correlation Composer Correlators" on page 386

  NNM provides additional built-in event correlation logic, called correlators, through the Correlation Composer. The Correlation Composer provides a new easier-to-use interface for configuring and creating correlation rules.

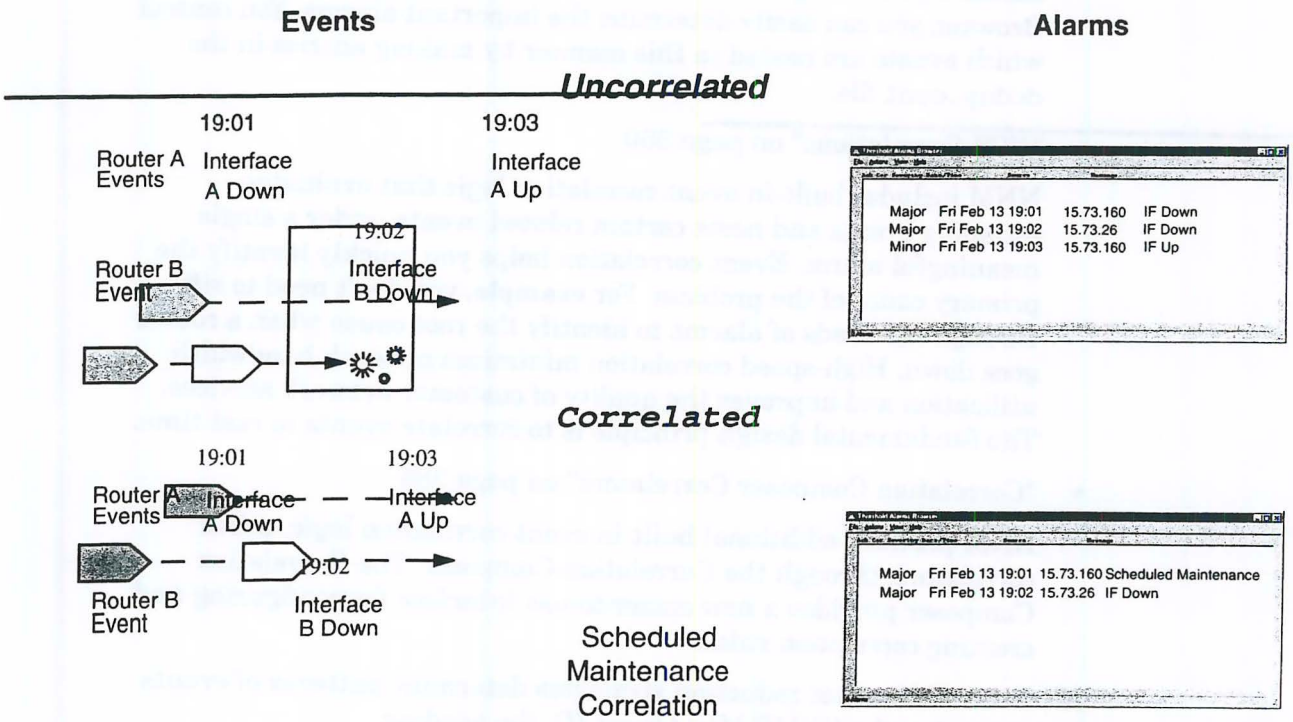
All three of the event reduction strategies determine patterns of events by monitoring the *SNMP MIB Object ID*, the sending *SNMP-agent/IP-address*, and a specific combination of *SNMP variable-binding values*. See "What is an SNMP Variable-Binding and How Do I Identify One?" on page 404 to learn about determining SNMP variable-binding values.



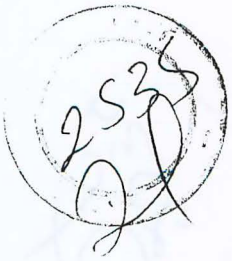
Event reduction modifies the flow of events by recognizing patterns of events, then either nesting related events in the Alarm Browser, discarding the events, or replacing the events with fewer more meaningful events. Event reduction strategies can dramatically reduce the number of alarms and improve the value of alarms displayed in your Alarm Browser. Instead of displaying the whole event storm typically generated by equipment and link failures, a correlated event stream displays only the most meaningful alarms, resulting in faster and easier identification of network problems.

For example, one of the correlations included with NNM is called the `ScheduledMaintenance` correlation. Once configured, it suppresses router events generated during routine maintenance.

Figure 11-1 With/Without Scheduled Maintenance Correlation



In Figure 11-1 on page 353, Router A is undergoing planned maintenance (for example, it is being moved to a new rack). The `ScheduledMaintenance` correlation has been configured to post a Scheduled Maintenance alarm notification and suppress all other events



generated by this device during the maintenance period. Because the device has powered down within the maintenance period, the correlation suppresses both events from Router A. However, the Interface Down event from Router (Interface) B is passed through because it is not one of the devices specified for maintenance. The result is two events instead of three, and a higher confidence level that the alarm represents a real problem requiring attention from your team.

This simple correlation eliminates false alarms caused by maintenance activities. Where previously an automated paging facility would have resulted in unnecessary pages, with event correlation it may be feasible to generate meaningful pages.

As illustrated by this example, a single correlation recognizes event patterns caused by a particular fault type. Once you understand how a correlation works, you can modify its parameter values.

A detailed description of each of the supplied correlations and correlators is provided. Before changing any parameter settings, carefully read the description in the configuration window to learn how each correlation and correlator works, its effect, and its deployment requirements.

Correlation Concepts

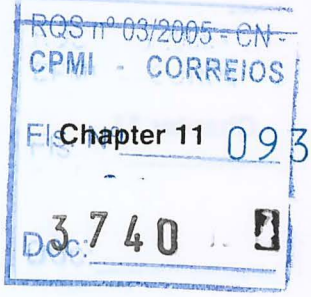
This section discusses the following concepts:

- "Enabling/Disabling Event Correlations" on page 354.
- "Static and Dynamic Parameters" on page 355.
- "Multiple Correlations and Correlators" on page 355.
- "Event Streams" on page 356.
- "Recommendations" on page 356
- "Event Reduction in Distributed Environments" on page 357.

Enabling/Disabling Event Correlations

When you install NNM, several correlations and correlators are loaded and **enabled**, meaning that they are actively filtering incoming events.

Correlations and correlators can be enabled and disabled at any time through the `ECS Configuration` window and `Correlation Composer` window.



Many correlations work by comparing incoming events with the previously gathered history of those events. When a correlation is first enabled, it has no history and takes a certain amount of time to build one. In the meantime, events that would otherwise be suppressed may be passed through, and events that would normally be modified or generated may not be. When a correlation is first enabled, a certain amount of time is required before the internal tables fill with events so that the correlation can work consistently. This is called **settling time**.

NOTE Some correlations do not provide any benefit until they are configured. For example, the `ScheduledMaintenance` correlation doesn't do anything until you specify the devices involved and a time span.

Static and Dynamic Parameters

Parameters are classified as either static or dynamic. The distinction is not important when you are changing the parameters of a disabled ECS correlation. However, if the ECS correlation is already enabled, then the distinction affects the way in which the changes are applied.

When changes to **static** parameters are applied, the correlation is disrupted because the correlation must be disabled and re-enabled, and you must allow for settling time before the correlation is effective. On the other hand, changes to **dynamic** parameters take effect as soon as they are applied.

NOTE The parameters of correlators within the Correlation Composer are all *dynamic*. Changes take effect as soon as they are applied.

Multiple Correlations and Correlators

When multiple correlations and correlators are enabled in the *default* stream (see next section), an incoming event will be posted into the Alarm Browser only if *all correlations and correlators* that are configured to receive that event, pass that particular event through. In other words, if *any* correlation or correlator filters out the incoming event, then that event will not appear in the Alarm Browser, even if another correlation or correlator would otherwise have posted it as an alarm.

2533

This point is especially important when you introduce a new correlation or correlator. You must make sure that the new one does not break any existing event reduction configurations: de-duplication, ECS correlations, and Correlation Composer correlators.

Event Streams

A **stream** is a logically separate flow of events. All streams originate from a common source (the postmaster, pmd service). However, each stream can have a different set of correlations applied to it and is directed to a different destination.

NNM listens only to the *default* stream. You may wish to establish separate streams for special network management applications that you add to your OpenView suite. The ECS correlations can be used on the new streams. However, the Correlation Composer correlators only work on the default stream; do not enable them on any other stream.

If you configure NNM's ECS feature with multiple streams, you can choose different combinations of your correlations for each stream. Each correlation can be enabled only once on a selected event stream. However, you can enable the same correlation on several different event streams. *The configuration settings for the correlation remain the same across all streams.* Refer to the *ecsmgr* reference page in NNM's online help (or the UNIX manpage) for more information.

Recommendations

The most detailed source of information about each correlation or correlator is the descriptive information displayed in each correlation's configuration window. Review this information before using the correlation or correlator.

To minimize disruption to the event reduction service, it is suggested that you:

- Plan changes ahead of time where possible.
- Choose a time when network activity is low.
- Do not make ad hoc changes to static parameters.
- Avoid inconsistent states by applying all parameter modifications at the same time, rather than applying each individual parameter change.
- Avoid changing static parameters in the middle of an event storm.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0931
3740
Doc:

- Test the effect of the event reduction strategy to be sure it does what you expect.
- Ensure that all members of your team know which event reduction strategies are in effect.

Event Reduction in Distributed Environments

The NNM correlation engine feeds information for all event reduction features into the ECS default event stream. In a distributed environment this has two main benefits:

- The correlation processing load is distributed over several collection stations.
- Network traffic is reduced.

See *A Guide to Scalability and Distribution* manual for further information about distributed network management concepts.



De-Duplication of Alarms

NNM de-duplication affects only those alarms listed in the `dedup.conf` file. The *newest* de-duplicated alarm always becomes the parent alarm, visible in the Alarm Browser. Only those alarms that are displayed in the Alarm Browser are monitored by de-duplication. In other words, de-duplication runs on alarms after they have passed through the event correlation system.

NOTE

All de-duplication configurations, correlators defined within Correlation Composer, and all correlations defined within ECS must *work well together* on your NNM management station. Before you begin, it is critical that you print out and read the following white paper:

`Developing_NNM_Event_Reduction.pdf`

- *Windows: NNM_install_dir*`\Doc\WhitePapers\`
- *UNIX:* `$OV_DOC/WhitePapers/`

This information explains how to ensure that you do not break existing implementations.

You *might* need to install the white papers on Windows-based NNM management stations. See "White Papers" on page 75.

You can modify the `dedup.conf` file to change the list of affected alarms. For example, if you have multiple, identical alarms that you want to nest under the most recent instance of the alarm, do the following:

1. Open the `dedup.conf` file from the following location:
   - *Windows*: *install_dir*`\conf\dedup.conf.`
   - *UNIX*: `$OV_CONF/dedup.conf.`
2. Make the following changes to increase de-duplication:
   - Add the SNMP MIB Object ID of the alarm.
   - Add the event SNMP-agent/IP-address source pair (optional).

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0932
3740
Doc:

- Add the specific SNMP variable-binding (optional). See "What is an SNMP Variable-Binding and How Do I Identify One?" on page 404 for more information about SNMP variable-bindings.

See the *dedup.conf* reference page in NNM's online help (or the UNIX manpage) for more information about how to edit the `dedup.conf` file.

NOTE If you need to disable the de-duplication feature, remove the # from the following line of the `dedup.conf` file.

```
#DEDUPLICATION=OFF
```

To deploy any changes you made to the `dedup.conf` file, you must restart the `ovalarmsrv` process. This causes NNM to read the contents of the `dedup.conf` file. To restart the `ovalarmsrv` process, use the following procedure:

1. Stop the `ovalarmsrv` process.
   - *Windows:* As administrator, run `ovstop ovalarmsrv`.
   - *UNIX:* As root, run `ovstop ovlarmsrv`.
2. Start the `ovalarmsrv` process.
   - *Windows:* As administrator, run `ovstart ovalarmsrv`.
   - *UNIX:* As root, run `ovstart ovlarmsrv`.

Once you complete this process, alarms that were already posted to the Alarm Browser before you implemented the de-duplication are not removed. The de-duplication feature nests all new matching alarms as they arrive. The *newest* de-duplicated alarm always becomes the parent alarm, visible in the Alarm Browser.

ECS Correlations

NNM's Built-In Correlations

NNM includes a set of event correlations (the Bundled Edition correlations):

- Connector Down Correlation System (page 361)
  This feature encompasses more than event correlation. NNM's map processes and alarm monitoring processes have been enhanced to help you speed up the task of identifying the source of a problem on your network as it occurs.
- Frame Relay Correlation (page 365)
  This correlation detects and reports specific problems with virtual connections. It distinguishes between failures within the provider network and failures within the local network.
- ManageX Server Down Correlation (page 369)
  When certain ManageX services become unavailable, this correlation combines HP OpenView ManageX events with NNM's topology events, creates new high level ManageX messages, and forwards them to the ManageX message reader. These messages explain why ManageX services are unavailable. Events sent to NNM by ManageX appear in the NNM Alarm Browser. Enable this correlation only if ManageX and NNM will be used together.
- Pair Wise Correlation (page 371)
  This correlation matches a *parent* event to one or more previously occurring *child* events; for example, an Interface Down alarm (OV_IF_Down) followed by an Interface Up alarm (OV_IF_Up) within a designated time frame. You can configure the behavior of alarms passing through this correlation.
- Repeated Event Correlation (page 375)
  This correlation identifies multiple duplicate alarms which are associated with a single physical event and bundles them together under a single alarm.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0933
3740

- Scheduled Maintenance Correlation (page 379)
  When conducting planned network maintenance that requires multiple devices to be off-line for a certain amount of time, this correlation allows you to exclude events generated because of the maintenance activity.

Connector Down Correlation

Use of this correlation can prevent event storms when a router (or other connector device) goes down. In the event of a network failure, NNM automatically determines:

- Which device is malfunctioning.
- Which other network devices are impacted by this failure. That is, which functional network devices are now *inaccessible to the management station* over the network because of the failing device. These inaccessible devices are referred to as *secondary failures*.
- Which *inaccessible* network devices are *important* to the productivity of the organization and thus should be given high priority.

Behavior NNM automatically determines the route to a node that is down and checks each connector device along the path to that node to determine the primary malfunction.

Only the alarm about the primary device is logged to the Alarm Browser, making it easy for you to determine the root cause of the problem. To view the error messages regarding devices considered secondary failures:

- From the Alarm Browser, select the correlated alarm's message and select `Actions:Show Correlated Events` or double-click on the correlated column.
- From the web-based Alarm Browser, select the correlated alarm's message and select `Actions:Alarm Details` and select the `Correlations` tab.

NNM slows down polling traffic to all affected devices (i.e. devices considered secondary failures other than the primary malfunction) until the primary device is recovered. The map automatically updates to indicate the primary failure and the affected secondary failures below the primary failure.

You can establish a list of mission-critical devices (Important Node filter) that are never considered secondary failures.

Setting Parameters There are several configuration parameters for the `ConnectorDown` correlation contained within the correlation, itself. However, the `ConnectorDown` correlation is mainly controlled by NNM rather than the Event Correlation Service. It is recommended that you do not modify the correlation itself.

To set parameters for the `ConnectorDown` correlation, from any NNM submap, select `Options:Network Polling Configuration`.(See "Secondary Failure Polling" on page 192 for instructions.)

Make sure that the `Secondary Failures Polling Options` field is enabled because this field determines whether the `ConnectorDown` correlation is being used. The settings in the other fields are up to you (see the following examples for information about the behavior of different choices).

- Important Node Filter
  Designate the name of the filter you created which lists all nodes that are mission-critical and should, therefore, never be placed in secondary-failure status. In the case of a failure resulting in devices contained in the list becoming inaccessible, alarm messages pertaining to these devices would continue to appear in the Alarm Browser window. (See "Router/Switch Health" on page 390 for information about the correlation of alarms from nodes listed in the Important Nodes filter.)

  This filter resides in the same file that contains any discovery filters, DHCP filters, etc.:

  — *Windows:* `install_dir\conf\C\filters`

  — *UNIX:* `$OV_CONF/C/filters`

  See the *OVfilterIntro* reference page (or the UNIX manpage) in NNM's online help for more information about defining filters. See also *A Guide to Scalability and Distribution* for information about creating filters.

- Important Node Behavior
  Designate which status change you prefer to receive for the devices listed in the important-node filter: Down (red on map) or Unknown (blue on map).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0934
3740
Doc:

- Secondary Node Polling Multiplier
  To prevent the generation of unnecessary polling traffic, specify a multiplier by which any scheduled polling should be extended during the failure for devices designated as secondary devices.
- Secondary Node Behavior
  Designate which status change you prefer to receive for devices determined to be secondary failures: Down (red on the map), Unknown (blue on the map), or Unchanged (no change reflected on the map).
- Secondary Failure Alarm Suppression
  Designate whether or not you want to prevent alarm messages about secondary failures from being posted to the Alarm Browser's main categories. If this function is selected, the secondary devices' alarm messages are displayed by selecting the primary alarm message in the Alarm Browser window and selecting the `Actions:Show Correlated Events` menu item.

NOTE See *A Guide to Scalability and Distribution* for information about configuring this feature on collection stations and their corresponding management station.

The following examples illustrate how these settings affect the behavior of NNM.

Example 11-1 Example 1 Default Settings without Using a Filter

```
Important Node Filter File: None
Important Node's Failure Status: Down (irrelevant because no devices are
identified in the filter)
Secondary Node Failure Status: Unknown (blue on the map)
Suppress Alarms for Secondary Failures: True
Secondary Node Polling Multiplier: 2
```

During a network failure:

- The node determined to be the primary cause of the failure appears as a red (critical) symbol on the map, an alarm message is posted in the Alarm Browser, and polling intervals remain constant.
- Since no filter has been specified, no secondary nodes are considered important.



- All secondary-failure nodes are displayed as blue symbols (unknown) on the map. The alarm messages for all secondary devices do not appear in the Alarm Browser list. To view secondary alarm messages, select the corresponding primary alarm and select the `Actions:Show Correlated Events` menu item. Once a node is identified as a secondary failure, its polling intervals are doubled.

Example 11-2 Example 2 Default Settings with a Filter

```
Important Node Filter File: YourFilterName
Important Node's Failure Status: Down (red on the map)
Secondary Node Failure Status: Unknown (blue on the map)
Suppress Alarms for Secondary Failures: True
Secondary Node Polling Multiplier: 2
```

During a network failure:

- The device determined to be the primary cause of the failure appears as a red (critical) symbol on the map, an alarm message is posted in the Alarm Browser, and polling intervals remain constant.
- Any affected device that is specified as an important device in your filter file appears as a red symbol (critical) on the map, polling intervals remain constant, and alarm messages are posted in the Alarm Browser window.
- All secondary-failure interfaces on all nodes are displayed as blue symbols (unknown) on the map. The alarm messages for all secondary devices do not appear in the Alarm Browser list. To view secondary alarm messages, select the corresponding primary alarm and select the `Actions:Show Correlated Events` menu item. Once a node is identified as a secondary failure, it's polling intervals are doubled.

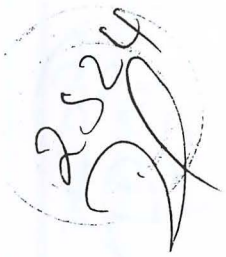
Example 11-3 Example 3 Minimum Network Traffic During Event Correlation

```
Important Node Filter File: YourFilterName
Important Node Behavior: Unknown (blue on the map)
Secondary Node Behavior: Ignore (no change on the map)
Secondary Failure Alarm Suppression: True
Secondary Node Polling Multiplier: 10
```

During a network failure:

- The device determined to be the primary cause of the failure appears as a red (critical) symbols on the map, an alarm message is posted in the Alarm Browser, and polling intervals remain constant.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0935
Doc: 3740



- Any affected device that is specified as an important device in your filter file appears as a blue symbol (unknown) on the map, polling intervals remain constant, and alarm messages are posted in the Alarm Browser window.
- All secondary-failure interfaces on all nodes are ignored, no change is reflected on the map. No alarm messages are generated for secondary devices. Once a node is identified as a secondary failure, its polling intervals are multiplied by 10.

Example 11-4 **Example 4 Behavior Like Previous Releases of NNM**

To disable the *secondary device* strategy and configure NNM to consider all devices as primary, deselect the `Secondary Failures Polling Options` field to disable the Connector Down correlation. This will have the following effect.

```
Important Node Filter File: None
Important Node Behavior: (irrelevant because no devices identified in the filter)
Secondary Node Behavior: Down (red on the map)
Secondary Failure Alarm Suppression: False (all alarms posted)
Secondary Node Polling Multiplier: 1 (no change)
```

During a network failure:

- The device determined to be the primary cause of the failure appears as a red (critical) symbol on the map, an alarm message is posted in the Alarm Browser, and polling intervals remain constant.
- Since no filter has been specified, no secondary nodes are singled out as important nodes.
- All secondary-failure interfaces on all nodes are displayed as red symbols (critical) on the map. The alarm messages for all secondary devices are sent directly to the Alarm Browser list. No polling intervals are changed.

Frame Relay Correlation

The `FrameRelay` correlation detects and reports problems with frame relay virtual connections. This correlation narrows the troubleshooting area for frame relay problems and reduces the number of events in the Alarm Browser by reporting only one alarm that represents all affected virtual connections.

Behavior

NOTE The `FrameRelay` correlation detects and analyzes `frDLCIStatusChange` traps from devices that support the circuit state changes described in RFC2115.

This correlation begins when a frame relay device generates several `frDLCIStatusChange` traps as shown in Example 11-5 on page 366. Notice that each `frDLCIStatusChange` trap contains an SNMP variable-binding named `state` that is set to `active`, `inactive`, or `invalid`. The `FrameRelay` correlation counts each time a `frDLCIStatusChange` trap's `state` value changes from `invalid/inactive` to `active`.

The `FrameRelay` correlation counts two state transitions for the traps shown in Example 11-5: the first at 10:10:10 and the second at 10:10:30. Two minutes after the first state change, the `FrameRelay` correlation generates an `OV_FrameRelayReset` event. Two minutes is the default `Window` setting and can be modified. See "Setting Parameters" on page 368 for more information.

Example 11-5 The frDLCIStatusChange Trap

```
01/01 10:10:00 frDLCIStatusChange: ifIndex=1, DLCI=401, state=inactive
01/01 10:10:10 frDLCIStatusChange: ifIndex=1, DLCI=401, state=active
01/01 10:10:20 frDLCIStatusChange: ifIndex=1, DLCI=401, state=invalid
01/01 10:10:30 frDLCIStatusChange: ifIndex=1, DLCI=401, state=active
```

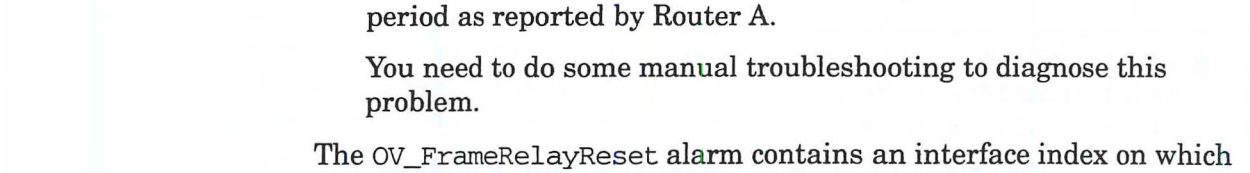
The `frDLCIStatusChange` trap indicates a problem with the PVC or the local equipment. NNM further analyzes this trap and reports whether the problem's root cause is located within the local network or the provider network.

To use the `FrameRelay` correlation you must enable SNMP trap forwarding on the frame relay routers and enable the `FrameRelay` correlation as shown in "Setting Parameters" on page 368. The router must support RFC2115.

Below are three examples of how to use the `FrameRelay` correlation to help you diagnose problems.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls.! Nº 0936
Doc. 3740

Figure 11-2 The Frame Relay Network



Example 11-6 NNM Reports a Problem with an Abnormal State Change Frequency

Refer to Figure 11-2 for this example. The following steps illustrate when NNM would generate an `OV_FrameRelayReset` event:

1. Router A generates a large number of `frDLCIStatusChange` traps within a configurable period of time.
2. The `FrameRelay` correlation counts several state transitions after analyzing the `frDLCIStatusChange` traps.
3. NNM generates an `OV_FrameRelayReset` event, indicating that there is a problem with either the frame relay network or the local router serial interface.

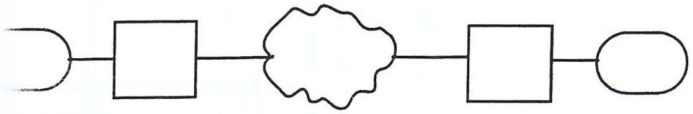
   The `OV_FrameRelayReset` event indicates that a problem exists due to a number of state transitions occurring within a certain time period as reported by Router A.

   You need to do some manual troubleshooting to diagnose this problem.

The `OV_FrameRelayReset` alarm contains an interface index on which the virtual connections are layered. This alarm reports the interface index along with the affected DLCIs and the number of times a reset occurs within the time period. For example, if an `OV_FrameRelayReset` alarm message contains `[(401, 2), (402, 1)]`, this indicates there were two resets for DLCI 401 and one reset for DLCI 402.

Example 11-7 NNM Reports a Problem with a Local Router Interface

Refer to Figure 11-2 on page 367 for this example. The following steps illustrate when NNM would generate an `OV_FrameRelayLocalCircuitProblem` event:



1. Router A generates a large number of `frDLCIStatusChange` traps within a configurable period of time. The status is currently `inactive`, and is toggling between `active` and `inactive`.
2. Either before or after the `frDLCIStatusChange` traps occur, router A sends a `link_Down` trap with the *`ifLocalReason`* variable-binding set to `LMI failed`. That indicates a possible LMI failure on Router A.
3. NNM generates an `OV_FrameRelayLocalCircuitProblem` event, indicating that there is a router serial interface failure on Router A.

   You need to troubleshoot the serial interface on Router A.

Example 11-8 NNM Reports a Problem with the Frame Relay Network

Refer to Figure 11-2 on page 367 for this example. The following steps illustrate when NNM would generate an `OV_FrameRelayCarrierProblem` event:

1. Local Router A generates a large number of `frDLCIStatusChange` traps within a configurable period of time.
2. The `frCircuitState` variable-binding within the `DLCIStatusChange` trap is invalid for the DLCIs generating the `DLCIStatusChange` events.
3. NNM generates an `OV_FrameRelayCarrierProblem` event, indicating that there is a problem with the frame relay network.

   You need to call your service provider.

Setting Parameters Complete the following steps if you want to view more information about or modify the `FrameRelay` correlation.

TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0937
3740
Doc:

3. If you want to enable or disable the `FrameRelay` correlation: from the `ECS Configuration` window, highlight the `FrameRelay` correlation, then select either `Enable` or `Disable`.
4. From the `ECS Configuration` window, highlight the `FrameRelay` correlation and select `Describe` to review the correlation description.
5. From the `ECS Configuration` window, highlight the `FrameRelay` correlation and select `Modify` to bring up the `FrameRelay-Modify` screen.

   The `Window` parameter, used as a time window for counting status transitions from the `frDLCIStatusChange` trap, is the only configurable parameter for the `FrameRelay` correlation.
6. To view the parameter description or modify the configurable parameter, select the parameter, then select `View/Modify`.

NOTE If you modify the `Windows` parameter, set the parameter to a value between two and five minutes. As you set the value higher, the `FrameRelay` correlation consumes more memory resources.

ManageX Server Down Correlation

The `MgXServerDown` correlation analyzes the network health, generates new high level ManageX messages, and delivers these messages to the ManageX message reader. The resulting messages explain why certain ManageX services are unavailable. ManageX messages also appear in the NNM Alarm Browser once this correlation is configured and enabled.

The message information is of value to the ManageX system administrator as it explains what portions of the network are interfering with ManageX operation. This information eliminates the need for the ManageX administrator to contact the network administrator and improves the efficiency of both the network administrator and the system administrator.

Behavior ManageX console events are picked up by the *NNM Lights Out policy* (nnmIntegration.mxc) and converted to an SNMP trap which is sent to NNM. These events route through the ECS `MgXServerDown` correlation for evaluation by NNM.

2519

If NNM discovers that a ManageX device is down, the ECS `MgXServerDown` correlation will determine if the interface-down event is due to a problem on a connector device (router interface, switch, etc.). The result of the analysis is encapsulated in an event that NNM converts into an SNMP trap and sends to the ManageX NNM WMI policy (nnmWmiEventPolicy.mxw) where it is converted into a ManageX console message for display in the ManageX message reader.

Setting Parameters There are numerous configurable parameters contained in the `MgXServerDown` correlation. Complete the following steps if you want to review parameter definitions or modify parameters contained within the `MgXServerDown` correlation.

TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

`Options:Event Configuration`. This launches the `Event Configuration` window.

2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.
3. From the `ECS Configuration` window, highlight the `MgXServerDown` correlation and select `Describe` to review the correlation description.
4. From the `ECS Configuration` window, highlight the `MgXServerDown` correlation and select `Modify` to bring up the `MgXServerDown-Modify` screen.
5. To view parameter descriptions or modify any of the configurable parameters, select the parameter, then select `View/Modify`.

TIP From the `View/Modify` window, select `Help` for general information on making correlation modifications.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 0938
Doc: 3740

Pair Wise Correlation

This correlation matches a *parent* event to one or more previously occurring *child* events. You can configure child events to:

- Display in the Alarm Browser while awaiting arrival of a parent event, or
- Only display in the Alarm Browser if the specified time window is exceeded without the arrival of a matching parent event,
- Upon arrival of a parent event, be removed from the Alarm Browser and nested beneath the parent event, or set to Acknowledged.

For example, consider several repeated OV_IF_Down events followed by an OV_IF_Up event within a designated time frame. This correlation could be configured to either remove or acknowledge the OV_IF_Down events upon arrival of the OV_IF_Up event. The OV_IF_Down events are nested under the OV_IF_Up alarm message in the Alarm Browser.

You can add SNMP traps and events to the `PairWise` correlation, provided that you know how the source that is sending the trap is identified. The SNMP MIB Object ID (OID) works in combination with one of the following to specify the source. The combination being used is determined by the developer of the underlying MIB. You must know the appropriate combination in order to configure additional events into this correlation:

- `agent-addr` attribute
- Any source wildcard (your choice)
- SNMP variable-binding name
- SNMP variable-binding position

Behavior You control the behavior of this correlation. The following three examples explain some of your choices. Remember that in order for an event to be displayed within the Alarm Browser, the event's configuration must *not* be set to:

- Don't log or display
- Log only

See "Event Configuration Overview" on page 422 for information about setting an event's configuration.

Example 11-9 Don't Display the Child Events or the Parent Event

```
ChildEventImmediateOutput = False
InhibitParentOfInhibitedChild = True
```

The correlation monitors the defined event parent/child relationships in the background. You never see the parent or any child events in the Alarm Browser unless the time of the defined window period is exceeded and no parent event arrives. If no parent is received, the child events are displayed in the Alarm Browser.

Example 11-10 Display the Parent Event, Nest Child Events Beneath Parent

```
ChildEventImmediateOutput = False
InhibitParentOfInhibitedChild = False
```

The correlation monitors the defined event parent/child relationships in the background. When the parent event is received, the parent event is displayed in the Alarm Browser with the child events nested beneath. If no parent is received within the defined window period, the child events are displayed in the Alarm Browser.

Example 11-11 Display Both the Parent and Child Events in the Alarm Browser

```
ChildEventImmediateOutput = True
InhibitParentOfInhibitedChild = ignored (True or False)
```

Child events are displayed in the Alarm Browser upon arrival. The correlation monitors the defined event parent/child relationships, and when the parent event is received, the parent event is displayed in the Alarm Browser with the child events nested beneath. You choose whether the child events are removed from the Alarm Browser list or set to Acknowledged upon arrival of the parent event.

To view nested child alarms:

- From the Alarm Browser, select the parent alarm message and select `Actions:Show Correlated Events` or double-click on the correlated column.
- From the web-based Alarm Browser, select the parent alarm message and select `Actions:Alarm Details` then select the `Correlations` tab. You can also select the parent alarm message, click on the view button and then select the `Correlations` tab.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0939
3740
Doc:

Setting Parameters Complete the following steps if you want to review parameter definitions or modify parameters contained within the `PairWise` correlation.

TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.
3. From the `ECS Configuration` window, highlight the `PairWise` correlation and select `Describe` to review the correlation description.
4. From the `ECS Configuration` window, highlight the `PairWise` correlation and select `Modify` to bring up the `PairWise-Modify` screen.
5. To view parameter descriptions or modify any of the configurable parameters, select the parameter, then select `View/Modify`.

TIP From the `View/Modify` window, select `Help` for general information on making correlation modifications.

This correlation allows configuration of the following parameters.

These two tables define which events are being monitored by the correlation and define the parent/child relationships:

- The `InputEventTypeListStringSources` table is used when the event source is a simple string which is not an IP address. This table is used to set event types for input into the correlation and determine the parent and child event sources.

- The `InputEventTypeList` table is used when the event source is an IP address. This table is used to set event types for input into the correlation and determine the parent and child event sources.

The following two parameters control when alarms appear in the Alarm Browser:

- The `ChildEventImmediateOutput` parameter determines whether the `PairWise` correlation outputs child events immediately or if it holds onto child events for further processing and possible cancellation by a parent event.

  `False` = The `PairWise` correlation holds onto child events for the duration of the `PairedTimeWindow`. If the `PairWise` correlation receives a matching parent event from the same source, within the appropriate amount of time, the child event is nested beneath the parent event in the Alarm Browser. If the `PairWise` correlation does not receive a matching parent event within the `PairedTimeWindow`, the child event is displayed in the Alarm Browser.

  `True` = Child events are displayed in the Alarm Browser upon arrival. Child events may be deleted or acknowledged in the Alarm Browser at a later time if a matching parent event arrives.

- The `InhibitParentOfInhibitedChild` parameter determines whether parent events are displayed in the Alarm Browser.

  `ateOutput` is true, the `PairWise` correlation ignores the `InhibitParentOfInhibitedChild` parameter and sends parent events to the Alarms Browser immediately.

  `True` = The correlation monitors the defined event parent/child relationships in the background. You never see either parent or child alarms in the Alarm Browser unless the time of the defined window period is exceeded and no parent event arrives. If no parent is received, the child events are displayed in the Alarm Browser.

  `False` = The parent event is displayed in the Alarm Browser upon arrival, with all child events nested beneath.

The following parameters fine tune the correlation:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0940
Doc 3740

- The `DeleteOrAcknowledge` parameter determines whether a child event is deleted or acknowledged from the Alarm Browser once it is matched to a parent event (assuming that `ChildEventImmediateOutput = True`).
- The `PairedTimeWindow` is the maximum time that the child event waits for a parent event. However, the `PairWise` correlation has a built in *pattern delete* feature. If a parent event arrives outside of the defined window, the Alarm Browser is scanned for any defined child events from the same source as the parent event.
- The `IgnoreSecondaryFailureEvents` parameter determines whether this correlation monitors events from devices identified as secondary failures. When set to `True`, secondary failures are monitored by the `ConnectorDown` correlation (page 361), and not by the `PairWise` correlation.

Repeated Event Correlation

This correlation allows multiple alarms which are associated with a single physical event to be bundled together and replaced by a single alarm in NNM's Alarm Browser.

For example, the OpenView `OV_PhysAddr_Mismatch` alarm is one of several alarms that are configured and active by default. When the physical address of a device changes, NNM generates multiple events as neighboring systems discover the change and NNM reads this conflicting information. The `RepeatedEvent` correlation suppresses the multiple instances of the physical address change alarms and correlates them into one alarm for any particular node. You specify the time interval; for example, after receipt of the first of many repeated alarms, suppress duplicates for 2 hours. Then generate another alarm and resume suppression of duplicate alarms for two more hours.

You can add other SNMP traps to the `RepeatedEvent` correlation for suppression of duplicate alarms, provided that you know the following information. Event Identifiers (MIB OIDs) work in combination with one of the following to specify how to obtain the source of the incoming trap:

- `agent-addr` attribute
- Any source wildcard (your choice)
- SNMP variable-binding name
- SNMP variable-binding position

2513

The combination being used is determined by the developer of the underlying MIB. You must know the appropriate combination in order to configure additional events into this correlation.

Behavior In NNM's Alarm Browser, all traps with the same key identifier [OID +source specifier] are nested under the first trap received for the specified time period. Only the first alarm in the series is posted into the Alarm Browser's main list. To view the rest of the alarms:

- From the Alarm Browser, select the primary message and select `Actions: Show Correlated Events` or double-click on the correlated column.
- From the web-based Alarm Browser, select the primary message and select `Actions:Alarm Details`, then select the `Correlations` tab. You can also select the primary message, click on the view button and then select the `Correlations` tab.

Setting Parameters Complete the following steps if you want to review parameter definitions or modify parameters contained within the `RepeatedEvent` correlation.

TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit: Event Correlation`. This brings up the `ECS Configuration` window.
3. From the `ECS Configuration` window, highlight the `RepeatedEvent` correlation and select `Describe` to review the correlation description.
4. From the `ECS Configuration` window, highlight the `RepeatedEvent` correlation and select `Modify` to bring up the `RepeatedEvent-Modify` screen.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0941
3740
Doc:



5. To view parameter descriptions or modify any of the configurable parameters, select the parameter, then select `View/Modify`.

TIP From the `View/Modify` window, select `Help` for general information on making correlation modifications.

The `RepeatedEvent` correlation contains the following parameters:

- The *`HoldFirstEventTime`* parameter sets an overall maximum time that initial events are held for later correlation with future events.
- The *`MaxHoldFirstEvents`* parameter sets an overall maximum number of first events to hold for later correlation with future events.
- The `InputEventTypeList` is a table that specifies the event types and event source identifiers that are input to this correlation. The following `Generic Trap Strings` and `Input Event OID` descriptions are included as event types in the `InputEventTypeList` table.

  `Generic Trap String`: The following generic trap names are contained within the correlation. Valid generic trap names are:

  coldStart

  warmStart

  linkDown

  linkUp

  authenticationFailure

  egpNeighborLoss

  By default, all of the generic traps are set to false (event not enabled) and are not evaluated by the `RepeatedEvent` correlation.

  `Input Event OID`: The Specific Event Types (Input Event `OID`) specify the trap `OID`. Two Input Event `OID`s are set to true (by default):

  `OV_PhysAddr_Mismatch (1.3.6.1.4.1.11.2.17.1.0.58982401)`

  `OV_Node_Added (.1.3.6.1.4.1.11.2.17.1.0.58785794)`

Enabling a particular row in the `InputEventTypeList-Modify` screen allows the event to be used as an input event into the correlation.

TIP Make sure that the Event Configuration settings for the trap you are enabling is *not* set to either of the following. If it is, your correlated alarm will never show up in the NNM Alarm Browser:

— Don't log or display

— Log only

See "Event Configuration Overview" on page 422.

- The `RepeatedTimeWindow` parameter sets an overall maximum time to correlate duplicate events. This value is used for both fixed (`RollingWindow=false`) and rolling (`RollingWindow=true`) time windows.

- The `CreateUpdateEvent` parameter allows you to specify whether or not to delete the original alarm from the Alarm Browser and create a new summary event when the time limit for this correlation is exceeded. If `CreateUpdateEvent` is true, the `RepeatedEvent` correlation creates a new, identical summary event that contains a count of the correlated events. If `CreateUpdateEvent` is false, the original alarm is not deleted from the Alarm Browser and no update event is created.

- Setting the `RollingWindow` parameter to true means that the time window is not fixed to a set time duration. The rolling time window resets each time the correlation receives another duplicate event.

  For example, the `RepeatedTimeWindow` parameter is set to 10 minutes with the `RollingWindow` parameter set to true. An event reports a conflicting MAC layer address. A second identical event arrives (repeats) within 10 minutes of the initial event. The time window for the correlation extends for another 10 minutes and the event is nested beneath the initial event in the Alarm Browser.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0942
Doc 3740

Scheduled Maintenance Correlation

Computer nodes and network segments are occasionally scheduled for maintenance. Such an occurrence typically results in a number of SNMP traps or HP OpenView events being generated. The `ScheduledMaintenance` correlation prevents unnecessary alarms during maintenance.

Behavior When the `ScheduledMaintenance` correlation detects the first event from a specified node or network segment within the specified time range, an event is generated and posted in the NNM Alarm Browser with the message: `Scheduled Maintenance`. The triggering event and all subsequent matching events are nested beneath the Scheduled Maintenance alarm. To view the nested alarms:

- From the Alarm Browser, select the primary message and select `Actions:Show Correlated Events` or double-click on the correlated column.
- From the web-based Alarm Browser, select the primary message and select `Actions:Alarm Details` and select the *Correlations tab.*

Setting Parameters Complete the following steps if you want to configure and enable the `ScheduledMaintenance` Correlation.

TIP

There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the [?] tab. Click Tasks, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.
3. If you want to enable or disable the `ScheduledMaintenance` correlation: from the `ECS Configuration` window, highlight the `ScheduledMaintenance` correlation. Then select either `Enable` or `Disable`.



4. From the `ECS Configuration` window, highlight the `ScheduledMaintenance` correlation and select `Describe` to review the correlation description.
5. From the `ECS Configuration` window, highlight the `ScheduledMaintenance` correlation and select `Modify` to bring up the `ScheduledMaintenance-Modify` screen.
6. To view or modify the affected network devices, or set the name of the planned outage, or activate/deactivate a planned outage: select `MaintenanceList` from the `ScheduledMaintenance-Modify` window and click on `View/Modify`.
7. To view or modify the date, time, and duration of a planned outage: Select `OutageTimeSpecification` from the `ScheduledMaintenance-Modify` window and click on `View/Modify` to make changes. It's important to note that a time window name is specified and configured in the `OutageTimeSpecification-Modify` window. This time window name is then referenced in the `MaintenanceList` definition.
8. To view any other parameter descriptions or modify any of the other configurable parameters, select the parameter, then select `View/Modify`.

TIP From the `View/Modify` window, select `Help` for general information on making correlation modifications.

Command Line Control

You can enable, disable, and control correlations from the `Options:Event Configuration` or `Edit:Event Correlation` menu item. However, if you need to debug a test correlation or enable tracing or logging for support purposes, use the `ecsmgr` command line utility. Possible tasks include:

- Starting or stopping event logging.
- Configuring error logging and trace logging.
- Creating a new stream.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0943
3740

See the *ecsmgr* reference page in NNM's online help (or the UNIX manpage) for more information.

Correlation File Structure

Each correlation is comprised of four files. Correlations are stored in the following directory:

- *Windows:* `install_dir\conf\ecs\circuits\*.*`
- *UNIX:* `$OV_CONF/ecs/circuits/*.*`

Do not edit these files directly. Only the `*.ds` file can be altered by using the `Options:Event Configuration`, or `Edit:Event Correlation` menu items.

Table 11-1 Correlation File Structure

correlation.eco	Compiled correlation file (not editable).
correlation.ds	Data Store file containing externally configurable parameter values (text).
correlation.fs	Optional Fact Store file containing topological or other information describing relationships (text).
C/*correlation*.param or $LANG/*correlation*.param	Parameter file that describes the parameters configurable by the ECS Event Configuration window (text).

Troubleshooting

Correlation Not Displayed

If the correlation you want is not displayed:

- In the ECS Event Configuration window, click `[Update View]` to refresh the list display. Updates made by other users and updates made from the command line are not reflected in the list of correlations until you click `[Update View]`.
- The correlation may not have been loaded (installed).

Correlation Status Incorrect

If the Status of the correlation appears to be incorrect:

- In the ECS Event Configuration window, select the appropriate stream. Correlations are enabled in the selected stream only and the correlation status reflects the status for the selected stream only. A correlation may be enabled in one stream and disabled in others.
- Click `[Update View]` to refresh the list display.

ECS Event Configuration Window Hangs

If the ECS Event Configuration window appear to hang when you click `[Verify Table]` or `[OK]` after modifying a parameter value:

- Wait until the server responds. Verification is performed on the server and can take some time if the server is very busy.
- Check that the connection with the server has not been severed.

Too Many Alarms Are Showing Up

Did you change the NNM Event Configuration default settings for any events from "log-only" to display in the NNM Alarm Browser? Consider changing some of them back to "log-only" For example, you do not need to display the Link Down events received from your Cisco router because NNM is already monitoring status. The NNM `OV_IF_Down` event is the same as the hardware's Link Down trap.

Expand the configuration of de-duplication to include any repetitive events (see "De-Duplication of Alarms" on page 358).

Obtaining Additional Event Correlations

NNM includes several **Bundled Edition** correlations. No additional license or software is required to use these correlations. HP tests and supports these correlations.

There are three additional sources for correlations that can run in NNM:

- **Contributed Edition** correlations are provided by HP OpenView Partners. Check the HP OpenView web page for links (also check OpenView partners' web sites for access to these correlations). No

RQS nº 03/2005 - CN
CPMI - CORREIOS
0944
Fls. Nº
3740
Doc:

additional license or software is required. HP does not test or support the Contributed Edition correlations. They are tested and supported by the partner.

- **Extended Edition** correlations can be obtained from system integrators, such as HP Consulting Service (see "HP Consulting Service" on page 76) and others. They are tested and supported by the supplier.
- **Designer Edition** correlations are written by you. You must purchase and use the HP OpenView ECS Designer product. HP does not test or support the Designer Edition correlations. They must be tested and supported by you.

If you add correlations to NNM, they must be installed and their initial parameter values configured. When a correlation is enabled, its memory tables must fill with events before correlation becomes effective. Like the correlations supplied with NNM, you can then make further modifications to the parameter values while the correlation is enabled.

So You Want To Develop Your Own Correlation?

Developing your own event correlations is a powerful option but a non-trivial task. You should consider carefully whether this is something you want to do or whether it might be quicker, simpler, and cheaper to contract with a specialist to supply the correlation or correlations you need.

If you need only one or two special correlations, then it is probably not worthwhile developing them yourself. Instead, you should consider contracting a specialist to develop them for you. Contact HP Consulting Service (see "HP Consulting Service" on page 76) or other system integrators for assistance.

To develop a correlation you need to:

- Purchase the HP OpenView ECS Designer product, a separately licensed component.
- Learn to develop correlations (ECS Designer training, and/or documentation).
- Design and debug the correlation, data store file, and parameter file.
- If required, develop processes to use the ECS Annotation and/or Event I/O APIs, as described in the *HP OpenView ECS Developer's Guide*.

- Deploy the correlation to each management station and collection station, as described in the documentation that you received when you purchased ECS Designer.

When to Design Your Own Event Correlations There are several key factors which indicate that a new correlation is required, or that an existing correlation needs to be reconstructed:

- No existing correlation provides the correlation you need.
- Parameters of an existing correlation need to be set to values that are outside the minimum and maximum allowed in the ECS Event Configuration window.
- The correlation requires access to external data (for example, to look up an inventory database) and therefore needs to use ECS annotation.
- Special event I/O requirements exist.

What is Involved

NOTE

All de-duplication configurations, correlators defined within Correlation Composer, and all correlations defined within ECS must *work well* ement station. Before you begin, it is critical that you print out and read the following white paper:

`Developing_NNM_Event_Reduction.pdf`

- *Windows:* `NNM_install_dir\Doc\WhitePapers\`
- *UNIX:* `$OV_DOC/WhitePapers/`

This information explains how to ensure that you do not break existing implementations.

You *might* need to install the white papers on Windows-based NNM management stations. See "White Papers" on page 75.

To design an effective correlation, you must:

- Understand typical network event patterns and what they mean.
- Know the architecture of your network management system.
- Identify external data access (ECS Annotation) requirements.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0945
Doc: 3740

- Define the problem concisely in terms of filtering and time-related if-then statements.
- Determine if all data is available from the events themselves. If not determine if:
  - — The external data is subject to change or is relatively stable.
  - — The required data is small enough to store in memory.
  - — The access speed and reliability is sufficient when extracting from your database (particularly if the database is remote).

Then, to develop the correlations, in addition to purchasing the HP OpenView ECS Designer product, you need to:

- Set up a test platform.
- Obtain or develop sample logs of events (perhaps use NNM backup files).
- If Event I/O or Annotation is required, refer to the *HP OpenView ECS Developer's Guide* (provided and obtain an ANSI C/C++ compiler.
- If ASCII events must be correlated, use the ASCII Module of the HP OpenView ECS Designer product.

2503

Correlation Composer Correlators

NNM's Built-In Correlators

NNM includes a set of correlators:

- "Cisco Chassis Failure" on page 387.
  Monitors Cisco traps for three error conditions: temperature, fan failure, and power supply fault. Generates a new alarm if the condition persists for the specified time period.
- "Router/Switch Intermittent Status Changes" on page 393.
  Listens for `OV_IF_Down` alarms from routers and switches, and creates a new alarm when more than *N* interface-down events are received within *M* minutes from a specific interface (defaults N=5, M=30min). Only the new `OV_Intermittent` alarm appears in the NNM Alarm Browser.
- "Router/Switch Health" on page 390.
  (actually a group of three correlators) Correlates Interface status alarms with their related router or switch Node status alarm. `OV_IF_Unknown` and `OV_IF_Down` status alarms from interfaces within routers or switches are suppressed and nested beneath the Node-status alarm.
- "Multiple Reboots on Routers/Switches" on page 388.
  Listens for `coldStart` and `warmStart` traps and creates a new alarm when more than *N* `coldStart/warmStart` traps are received within *M* minutes from a specific SNMP-agent/IP-address pair (defaults N=4, M=5min).
- "HSRP Group Health" on page 394.
  (actually a group of 6 correlators on UNIX only) If you purchased the NNM Extended Topology product, this group of six correlators analyzes an HSRP group status change and notifies you of the results by generating an `OV_HSRP_`*x* status alarm, with related alarms nested beneath.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0946
Doc: 3740

Cisco Chassis Failure

Correlates events forwarded from switches supporting the `CISCO-STACK-MIB.my` MIB.

Behavior Certain Cisco and HP routers and switches that support the CISCO-STACK MIB can be configured to send traps that report chassis error conditions to the NNM management station. This correlator monitors the SNMP variable-binding data within the Cisco traps that provides information about the reasons for a failure.

If a *temperature*, *fan failure*, or *power supply* fault condition persists for a period longer than the configured time interval, one of the following events is generated and sent to the NNM Alarm Browser:

- `OV_Chassis_Temperature` (.1.3.6.1.4.1.11.2.17.1.0.58982424)
- `OV_Chassis_FanFailure` (.1.3.6.1.4.1.11.2.17.1.0.58982425)
- `OV_Chassis_PowerSupply` (.1.3.6.1.4.1.11.2.17.1.0.58982426)

Conditions that persist for a time less than the specified Window Period are discarded.

Setting Parameters Complete the following steps if you want to review parameter definitions or modify parameters contained within the `OV_Chassis_Cisco` correlator.

TIP

There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.
3. From the `ECS Configuration` window, select the `'default'` stream. Then, highlight `Composer` in the correlation table and select `Modify`. The `Correlation Composer` window appears in your web browser.

4. In the `Correlation Composer` window, right-click the `OV_Chassis_Cisco` correlator and select `Modify` to display the `Description` tab.
5. Carefully read the information in the `Description` tab. Do not change any parameters other than the one specifically listed:
   - Window Period
6. Click the `Definition` tab to access the parameter settings. Click `[Help]` for information about each field.
7. After making the desired changes, close the correlator configuration window and return to the `Correlation Composer` main window.
8. Exit the `Correlation Composer` main window.
9. Save your changes when prompted to do so. This updates the NNM correlator fact store file.

Multiple Reboots on Routers/Switches

The Multiple Reboots correlator detects and reports problems with routers and switches that reboot multiple times within a specified time window.

Behavior The ECS `PairWise` correlation (page 371) suppresses `OV_Node_Down` alarms when the corresponding `OV_Node_Up` alarm arrives. Therefore, you may never see these events in the NNM Alarm Browser. This `OV_MultipleReboots` correlator detects a repetitive down/up situation within routers and switches and generates an `OV_Multiple_Reboots` alarm to warn you of a potential problem.

If a `coldStart` or `warmStart` trap arrives and no such traps have previously been seen for this SNMP-agent/IP-address pair, a new interval is started. If `coldStart` or `warmStart` traps already exist for this system, a counter is updated and checked to see if the number of counts exceeds the configured threshold. If the count exceeds the threshold and the trap is still within the current interval for this system, an `OV_Multiple_Reboot` alarm is posted in the NNM Alarm Browser. All further `coldStart` or `warmStart` traps within the specified time interval are nested under the `OV_Multiple_Reboot` alarm.

Once the interval expires, the sequence begins again.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0947
Doc: 3740

Setting Parameters Complete the following steps if you want to review parameter definitions or modify parameters contained within the `OV_MultipleReboots` correlator.

TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.
3. From the `ECS Configuration` window, select the `'default'` stream. Then, highlight `Composer` in the correlation table and select `Modify`. The `Correlation Composer` window appears in your web browser.
4. In the `Correlation Composer` window, right-click the `OV_MultipleReboots` correlator and select `Modify` to display the `Description` tab.
5. Carefully read the information in the `Description` tab. Do not change any parameters other than those specifically listed:
   - Count
   - Window Period
6. Click the `Definition` tab to access the parameter settings. Click `[Help]` for information about each field.
7. After making the desired changes, close the correlator configuration window and return to the `Correlation Composer` main window.
8. Exit the `Correlation Composer` main window.
9. Save your changes when prompted to do so. This updates the NNM correlator fact store file.

2489

Router/Switch Health

Suppresses interface status alarms from devices other than routers or switches so that these alarms never appear in the NNM Alarm Browser. The assumption is that you do not wish to see end-node interface status alarms.

Displays, in the NNM Alarm Browser, the important interface status alarms from your routers and switches. Suppresses the unimportant interface status alarms from those same routers and switches.

Router/switch health is actually determined by a group of three correlators:

- OV_NodeIf_NodeDown
- OV_NodeIf_NodeNotConnector
- OV_NodeIF_PrimaryIFUnknown

Behavior Suppresses interface status alarms from devices other than routers or switches.

Suppresses interface status alarms from unused (unconnected) ports within routers or switches.

Addresses the following failure scenarios that the ECS `ConnectorDown` correlation (page 361) doesn't detect:

- If fewer than *all* the interfaces on a router or switch fail, the interface status alarms display in your Alarm Browser. Intermediate node status alarms (`OV_Node_Warning`, `OV_Node_Marginal`, or `OV_Node_Major`) are configured as *log-only*, so they never appear in your Alarm Browser.
- If *all* the interfaces on a router or switch fail, `OV_Node_Down` alarm displays in your Alarm Browser with the interface alarms nested underneath.
- If a router or switch failure is a secondary failure (for example a Switch B is inaccessible due to a Switch A failure), then the ECS `ConnectorDown` correlation suppresses all of the events associated with Switch B. The suppressedInterface alarms are nested under the primary Switch A `OV_Node_Down` alarm.

  However, if the Secondary Failure Polling configuration identifies Switch B as an **Important Node** (listed in your Important Node filter, see page 361 and page 192) the Switch B secondary failure

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0948
3740
Doc.

events are not suppressed by the ECS ConnectorDown correlation. In this case, the Switch B OV_Node_Unknown alarm is displayed in the NNM Alarm Browser. The OV_NodeIf group of correlators nest the associated Interface status alarms beneath the parent node alarm. The Switch B OV_Node_Unknown alarm is not nested under the Switch A alarm.

Setting Parameters Complete the following steps if you want to review parameter definitions or modify parameters contained within the OV_IF_NodeDown correlator.

TIP There are several ways to access the event correlation features. For more information, from any submap, select Tools:HP OpenView Launcher. Select the [?] tab. Click Tasks, Event Correlation Management. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select Options:Event Configuration. This launches the Event Configuration window.
2. From NNM's Event Configuration window, select Edit:Event Correlation. This brings up the ECS Configuration window.
3. From the ECS Configuration window, select the 'default' stream. Then, highlight Composer in the correlation table and select Modify. The Correlation Composer window appears in your web browser.
4. In the Correlation Composer window, right-click the OV_IF_NodeDown correlator and select Modify to display the Description tab.
5. Carefully read the information in the Description tab. Do not change any parameters other than the one specifically listed:
   - Window Period
6. Click the Definition tab to access the parameter settings. Click [Help] for information about each field.
7. After making the desired changes, close the correlator configuration window and return to the Correlation Composer main window.
8. Exit the Correlation Composer main window.



9. Save your changes when prompted to do so. This updates the NNM correlator fact store file.

Disabling the OV_NodeIF Correlator Group In releases prior to NNM 6.31, *node-status-events* were displayed in the Alarm Browser, and *interface-status-events* were configured as log-only so that they never displayed in the Alarm Browser. In this release of NNM, interface status events are usually displayed unless a catastrophic failure is detected (all interfaces within a node are down). If a catastrophic event is detected, the node alarm is displayed with the interface alarms nested beneath.

This procedure explains how to return to the old NNM behavior, if desired:

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. Select `OpenView`.
3. Sort the events using the `View:Sort->Sort by Event Name` command.
4. Edit the `OV_IF_Unknown` and `OV_IF_Down` events and change the `Category` field to `Log only`.
5. Edit the following events and change the `Category` field to `Status Alarms` instead of `Log only`:
   - OV_Network_Major
   - OV_Network_Critical
   - OV_Segment_Major
   - OV_Segment_Critical
   - OV_Node_Warning
   - OV_Node_Marginal
   - OV_Node_Major
   - OV_Remote_Mgr_Up
6. Select `[OK]`.
7. Save your changes using the `File:Save` command.
8. Exit using the `File:Exit` command.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº
0949
Doc: 3740

Once you have the events reconfigured, complete the following to disable the group of three OV_NodeIF correlators:

1. From any NNM submap, select Tools:HP OpenView Launcher. Select the [?] tab. Click:
   - Tasks
   - Event Correlation Management
   - Correlation Composer
   - Read the information in the *Disabling a Correlator* topic.
2. Access the Correlator Composer main window and disable the following three correlators. You must disable *all* of them:
   - OV_NodeIf_NodeDown
   - OV_NodeIf_NodeNotConnector
   - OV_NodeIF_PrimaryIFUnknown

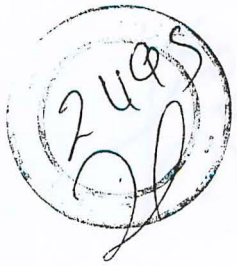
Router/Switch Intermittent Status Changes

Identifies routers or switches that are reporting intermittent up/down status.

Behavior If an interface is continuously going down and then coming up, the ECS PairWise correlation (page 371) cancels the OV_IF_Down event when the OV_IF_Up event arrives. Therefore, you would never see these events in the NNM Alarm Browser.

This correlator (OV_Connector_IntermittentStatus) detects a repetitive interface down/up situation within a router or switch and generates an OV_Intermittent alarm if the OV_IF_Down event occurs the specified number of times (Count) during the specified time (Window Period).

Setting Parameters Complete the following steps if you want to review parameter definitions or modify parameters contained within the OV_Connector_IntermittentStatus correlator.



TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.
3. From the `ECS Configuration` window, select the `'default'` stream. Then, highlight `Composer` in the correlation table and select `Modify`. The `Correlation Composer` window appears in your web browser.
4. In the `Correlation Composer` window, right-click the `OV_Connector_IntermittentStatus` correlator and select `Modify` to display the `Description` tab.
5. Carefully read the information in the `Description` tab. Do not change any parameters other than those specifically listed:
   - Count
   - Window Period
6. Click the `Definition` tab to access the parameter settings. Click `[Help]` for information about each field.
7. After making the desired changes, close the correlator configuration window and return to the `Correlation Composer` main window.
8. Exit the `Correlation Composer` main window.
9. Save your changes when prompted to do so. This updates the NNM correlator fact store file.

HSRP Group Health

If you purchased the NNM Extended Topology product, six correlators work together to monitor HSRP group status within your networking environment. These six HSRP correlators are only provided with NNM management stations installed on a UNIX operating system. All six are required to calculate HSRP group health:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº. 0950
3740
Doc:

- OV_HSRP_StatusChange
- OV_HSRP_If
- OV_HSRP_NewNNMEtTopo
- OV_HSRP_ProcessIfEvent
- OV_HSRP_ProcessTrap
- OV_HSRP_Trap_DrillDown

Behavior The following sequence is followed:

1. Listens for any *interface-status-change* alarms from an interface that is assigned to an HSRP group. If detected, initiates an `OV_Force_If_Group_Status_Polling` event for the identified HSRP group.

   Also, listens for any HSRP *trap*. If detected, initiates an `OV_Force_If_Group_Status_Polling` event for the identified HSRP group.

2. Runs the correlator logic to calculate the health of the HSRP group being monitored by using the results of the `OV_Force_If_Group_Status_Polling`. Posts one of the following alarms in the NNM Alarm Browser reporting the results:

   - `OV_HSRP_Up`
     An HSRP group is completely normal, and providing routing functionality.
   - `OV_HSRP_State_Transition`
     An HSRP group has changed either its active router or standby router or both.
   - `OV_HSRP_Marginal`
     An HSRP group has all interfaces in either Unknown or Normal status only, with at least one in each status.
   - `OV_HSRP_Warning`
     An HSRP group has all interfaces with Unknown status, except for one with Normal status.
   - `OV_HSRP_Unknown`
     An HSRP group has all interfaces in Unknown IP status. Network problems exist between the management station and all the interfaces. This HSRP group is providing routing only if an



interface with an Unknown IP status is actually functioning, but due to other network problems, cannot be reached from the NNM management station.

- `OV_HSRP_Major`
  An HSRP group has one or more interfaces with Critical IP status, and one or more interfaces with Unknown IP status. There are no interfaces with a Normal IP status. This HSRP group is providing routing functionality only if an interface with an Unknown IP status is actually functioning, but due to other network problems, cannot be reached from the NNM management station.
- `OV_HSRP_Down`
  An HSRP group is completely down. No active or standby interfaces in this HSRP group could be identified.

3. Nests all related *interface-status-change* alarms, from members of an HSRP group, under the relevant `OV_HSRP_x` status alarm.

   Also, nests all related HSRP *traps* under the relevant `OV_HSRP_x` status alarm.

4. Restarts the HSRP analysis process if any change is detected within the NNM Extended Topology database during the time that the ated.

Setting Parameters Complete the following steps if you want to review parameter definitions or modify parameters contained within the lator. This is the *only* correlator within the HSRP group of correlators that can be modified.

TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº: 0951
3740
Doc:

3. From the ECS Configuration window, select the 'default' stream. Then, highlight Composer in the correlation table and select Modify. The Correlation Composer window appears in your web browser.
4. In the Correlation Composer window, right-click the OV_HSRP_StatusChange correlator and select Modify to display the Description tab.
5. Carefully read the information in the Description tab. Do not change any parameters other than the one specifically listed:
   - NetmonGroupPollWaitTime (in seconds)
6. Click the Definition tab to access the parameter settings. Click [Help] for information about each field.
7. After making the desired changes, close the correlator configuration window and return to the Correlation Composer main window.
8. Exit the Correlation Composer main window.
9. Save your changes when prompted to do so. This updates the NNM correlator fact store file.

Correlator Fact Store File

The correlators, themselves, are all stored within one file. You should never edit this file directly; only make changes through the Correlator Composer window. The file is automatically included when ovbackup and ovrestore are run (see "Backup/Restore to Protect Your Investment of Time" on page 165). If you are planning to make experimental changes to the correlator parameter settings, you may wish to make a backup of this file before proceeding.

All correlator configurations are stored within one NNM fact store file. No other correlator fact store files are allowed within NNM:

Windows: `\NNM_install_dir\conf\ecs\circuits\Composer.fs`

UNIX: `$OV_CONF/ecs/circuits/Composer.fs`

Troubleshooting

For troubleshooting information about the Correlation Composer, see the following references:

2491

- Access the following pdf format manual from the NNM main window, select `Help:Documentation:`

  — *HP OpenView Correlation Composer's Guide*

- Access the following pdf-format white paper file: `Developing_NNM_Event_Reduction.pdf`

  — *Windows:* `NNM_install_dir\Doc\WhitePapers\`

  — *UNIX:* `$OV_DOC/WhitePapers/`

  This information explains how to ensure that you do not break existing event reduction implementations. It also explains the process required for carefully merging your new correlators into the NNM correlator fact store file.

  You *might* need to install the white papers on Windows-based NNM management stations. See "White Papers" on page 75.

- The `TroubleshootingEventReduction.txt` file explains how to create event logs and play them back into the NNM event correlation system for testing purposes:

  — *Windows:* `NNM_install_dir\contrib\ecs\`

  — *UNIX:* `$OV_CONTRIB/ecs/`

  You *might* need to install the contib files on Windows-based NNM management stations. See "The contrib Directory" on page 74.

Creating Additional Correlators

NOTE

All de-duplication configurations, correlators defined within Correlation Composer, and all correlations defined within ECS must *work well together* on your NNM management station. Before you begin, it is critical that you print out and read the following white paper:

`Developing_NNM_Event_Reduction.pdf`

- *Windows:* `NNM_install_dir\Doc\WhitePapers\`
- *UNIX:* `$OV_DOC/WhitePapers/`

This information explains how to ensure that you do not break existing implementations.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0952
3740
Doc:

You *might* need to install the white papers on Windows-based NNM management stations. See "White Papers" on page 75.

Correlation Composer provides templates for the most commonly used correlation logic. These templates make it easy for you to develop your own:

- **Enhanced**
  Used to trigger the creation of one or more new alarms or to augment the information content of an alarm.
- **MultiSource**
  Used to define a relationship between an arbitrary number of alarms, potentially from different sources, that together form a logical set that identifies a problem. The set of alarms must all arrive within a defined time period. Upon completion of the set, the alarms can be discarded, modified, or a new more meaningful alarm can be generated.
- **Rate**
  Used to measure the number of incoming events within a defined time period. When a specified number is received, you can choose to discard the alarms and generate a new more meaningful alarm.
- **Repeated**
  Used to either discard duplicate alarms within a defined time period, or generate a new alarm each time an additional alarm is received so that the current number of alarms received can be specified in the alarm message text.
- **Suppress**
  Used when a specific category of alarms needs to be discarded, so that they never appear in the NNM Alarm Browser.
- **Transient**
  Used to detect a defined number of paired event occurrences within a defined time period, such as node up/node down. The paired events can be discarded, and a new more meaningful alarm can be generated.

2489

NOTE Support for the correlator template named **User Defined** is not included. If you wish to use the Correlation Composer **User Defined** template, contact HP to purchase a Partner Care Extended support contract before beginning.

Correlators can be chained together to accomplish complex tasks (see "Router/Switch Health" on page 390 and "HSRP Group Health" on page 394 for examples of correlator groups).

If you wish to use external calls, contact HP to purchase a Partner Care Extended support contract before beginning.

Print out and read the following reference materials:

- Access the following pdf format manual from the NNM main window, select `Help:Documentation:`
  - — *HP OpenView Correlation Composer's Guide*
- Find the *csmerge* reference page in NNM's online help (or the UNIX manpage) for information about Correlation Composer's tool for merging new correlators (that are developed and tested in an isolated environment) back into the NNM correlator fact store file on your production NNM management station.
- Access the following pdf-format white paper file: `Developing_NNM_Event_Reduction.pdf`
  - — *Windows:* `NNM_install_dir\Doc\WhitePapers\`
  - — *UNIX:* `$OV_DOC/WhitePapers/`

  This information explains how to ensure that you do not break existing event reduction implementations. It also explains the process required for carefully merging your new correlators into the NNM correlator fact store file.
- The `TroubleshootingEventReduction.txt` file explains how to create event logs and play them back into the NNM event correlation system for testing purposes:
  - — *Windows:* `NNM_install_dir\contrib\ecs\`
  - — *UNIX:* `$OV_CONTRIB/ecs/`

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0953
Doc 7 4 0

2488

Developing your own event correlators is a powerful option, but a non-trivial task. You should consider carefully whether this is something you want to do or whether it might be quicker, simpler, and cheaper to contract with a specialist to supply the correlator or correlators you need. Contact HP Consulting Service (see "HP Consulting Service" on page 76) or other system integrators for assistance.

To develop a correlator you need to:

- Learn to develop correlators through Correlation Composer training and/or documentation.
- Design and debug the correlator on an isolated test machine.
- Deploy the correlator to each NNM management station and collection station, as described in the `Developing_NNM_Event_Reduction.pdf` white paper.

When to Design Your Own Event Correlators

There are several key factors which indicate that a new correlator is required, or that an existing correlator needs to be reconstructed:

- No existing correlator provides the correlation you need.
- Parameters of an existing correlator need to be set to values that are outside the minimum and maximum allowed.
- The correlator requires access to external data (for example, to look up an inventory database) and therefore needs to use ECS annotation.
- Special event I/O requirements exist.

What is Involved

To design an effective correlator, you must:

- Understand typical network event patterns and what they mean.
- Know the architecture of your network management system.
- Identify external data access (ECS Annotation) requirements.
- Define the problem concisely in terms of filtering and time-related if-then statements.
- Determine if all data is available from the event's variable-bindings. If not determine if:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0954
Doc: 3740

— The external data is subject to change or is relatively stable.

— The required data is small enough to store in memory.

— The access speed and reliability is sufficient when extracting from your database (particularly if the database is remote).

Then, to develop the correlators, you need to:

- Set up a test platform.
- Develop sample logs of events. See the following file for information about how to create log files of events, and how to feed them into the NNM event correlation system in your test environment:

  — *Windows:*

  NNM_install_dir\contrib\ecs\TroubleshootingEventReduction.txt

  — *UNIX:*

  $OV_CONTRIB/ecs/TroubleshootingEventReduction.txt

- Your NNM support contract includes coverage for the use of the following Correlation Composer templates (provided that you do not invoke calls to APIs, libraries, scripts, or programs that are not included as part of the Correlation Composer product embedded within NNM):

  — Enhanced

  — MultiSource

  — Rate

  — Repeated

  — Suppress

  — Transient

  If you wish to use external calls, contact HP to purchase a Partner Care Extended support contract before beginning.

2486

NOTE

Support for the correlator template named **User Defined** is not included. If you wish to use the Correlation Composer **User Defined** template, contact HP to purchase a Partner Care Extended support contract before beginning.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0955
3740
Doc:

What is an SNMP Variable-Binding and How Do I Identify One?

When an SNMP event or trap is generated, a group of *variables* are included in the data. These variables are defined within the MIB file from which the event or trap originates. These variables are often referred to as *var-binds* because they are bound to a particular instance of the SNMP event or trap. The *SNMP variable-binding list* associated with a particular trap or event can provide a wealth of valuable information for you to use when creating your own event reduction strategies using NNM de-duplication, ECS correlation, or Correlation Composer correlator. This section explains a couple of ways to determine the available SNMP variable-bindings:

- "Look within the MIB File" on page 404.
- "Check the Alarm Message Text in the Alarm Browser" on page 405.

This section also explains the SNMP variable-bindings contained within the NNM *interface-status* and *node-status* alarms on page 405, because they can be very useful when defining event reduction implementations.

Look within the MIB File

The most direct way to determine the available SNMP variable-bindings is to locate the MIB file, open the MIB file with an ASCII editor, and look up the variable list for that particular trap or event. Check the documentation that came with your router or switch to locate the MIBs currently in use. If you do not have a copy of the MIB file, try using the MIB Depot web site. It may be a good resource for obtaining MIBs:

`http://www.mibdepot.com`

Otherwise, contact the vendor who created that particular MIB to obtain a copy.

See also "Exchanging Management Information" on page 27 for more information about MIB files.

2487

Check the Alarm Message Text in the Alarm Browser

The alarm messages that display within the NNM Alarm Browser are controlled by the NNM Event Configuration settings. Usually the alarm message text includes a specified subset of available SNMP variable-binding values, as defined through the NNM `Event Configuration` window.

NOTE

For more information about NNM's Event Configuration feature and the choices for controlling alarm message text, see "Event Configuration Overview" on page 422. The event configuration settings are stored in the `trapd.conf` file.

You can easily modify the alarm message configuration settings. See "Variables and Special Characters Allowed" on page 436 for information about alarm message configuration choices. Some very useful alarm message variables are:

$# = prints out the total number of SNMP variable-bindings defined within the originating MIB of the incoming trap

$* = prints out the value passed with each of the defined SNMP variable-bindings

You can use the alarm message information as a starting point for your event reduction strategy, even if you do not have a copy of the MIB.

Any incoming traps whose MIBs have not been loaded into NNM (see "Loading MIBs in the MIB Database" on page 413) are displayed as generic traps called `EnterpriseDefault` (.1.3.6.1.4.1.*). The alarm message for the "generic" trap is defined as follows:

```
no format in trapd.conf. $# args: $*
```

Special SNMP Variable-Bindings within NNM Interface and Node Status Alarms

The OpenView interface and node status events include a wealth of information transported in SNMP variable-bindings. They are of particular interest when developing new de-duplication configurations, correlations, and correlators.

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0956
Doc: 3740

NOTE The first variable in the SNMP variable-binding list is traditionally considered to be var-bind "1" (one). If you are developing a Correlation Composer correlator, the first variable in the SNMP variable-binding list is var-bind "0" (zero).

OpenView Interface Status Variable Bindings

- **Var-Bind 1:** The ID of application sending the event.
- **Var-Bind 2:** The hostname of the node that caused the event.
- **Var-Bind 3:** The HP OpenView object identifier of the node that caused the event.
- **Var-Bind 4:** The database name, if applicable.
- **Var-Bind 5:** A time stamp for when the event occurred.
- **Var-Bind 6:** The HP OpenView object identifier of the interface that caused the event.
- **Var-Bind 7:** The name or label for the interface that caused the event.
- **Var-Bind 8:** The IP address for the interface that caused the event, or "0" if unavailable.
- **Var-Bind 9:** The NNM management station ID.
- **Var-Bind 10:** Event correlation event UUID which identifies the primary failure.
- **Var-Bind 11:** Number of bits in the subnet mask of interface.
- **Var-Bind 12:** Locale neutral description of the interface (typically `ifAlias`). Note that the regular label for the interface is transmitted in var-bind 7 and so the presence of this new variable-binding allows the interface name (for example, lan0) and the interface `ifAlias` to be displayed simultaneously.
- **Var-Bind 13:** Locale neutral comma separated list of capabilities of the interface. For example, `isSwitch,isIPRouter`. Not all capabilities are included that may be available in NNM. The primary purpose of this interface is to identify connector devices within event reduction implementations.

- **Var-Bind 14:** Name of the primary failure host if available.
- **Var-Bind 15:** Name of the primary failure entity if available.
- **Var-Bind 16:** The HP OpenView object identifier of primary failure entity if available.
- **Var-Bind 17:** Locale neutral description of the primary failure entity if available.
- **Var-Bind 18:** Locale neutral comma separated list of capabilities of the primary failure entity if available.

Variable-binding 14 through 18 describe the primary failure. For example, node C may be inaccessible due to a failure on router R. Node R would be the primary failure and node C would be the secondary failure. If node R is a primary failure then variable-binding 12 through 15 will describe node R and all the other variable-binding describe node C. If node C is a primary failure then all the SNMP variable-bindings describe node C. See "Connector Down Correlation" on page 361 and "Secondary Failure Polling" on page 192 for more information about designating primary and secondary failures.

OpenView Node Status Variable Bindings

- **Var-Bind 8:** Locale neutral comma separated list of capabilities of the entity. For example, `isSwitch`, `isIPRouter`.
- **Var-Bind 9:** Name of the primary failure host if available.
- **Var-Bind 10:** Name of the primary failure entity if available.
- **Var-Bind 11:** The HP OpenView object identifier of primary failure entity if available.
- **Var-Bind 12:** Locale neutral description of the primary failure entity if available.
- **Var-Bind 13:** Locale neutral comma separated list of capabilities of the primary failure entity if available.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0957
Doc: 3740

What is an SNMP Variable-Binding and How Do I Identify One?

12 Customizing Events: Doing It Your Way

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0958
3740
Doc:

NNM allows you to take control of the event system through the use of several built-in applications. This chapter explains the purpose and use of each of these standard NNM applications:

- *SNMP MIB Browser* (page 412) and *Load/Unload MIBs* (page 413). Allows you to load and explore the functionality of the MIBs of your choosing. Once the MIB is loaded, you can query to determine the remote device's status, configuration, and available resources. You can also *set* MIB object values, provided you configured your network's community names into NNM.
- *DMI Browser* (page 417) and mapping MIFs (page 419). *NNM for the Windows operating system only:* Allows you to explore and access the functionality of a network device's Desktop Management Interface (DMI) service provider to which NNM subscribes. You can query to determine the remote device's status, configuration, and available resources.
- *Event Configuration* (page 422). Allows you to customize events, such as changing standard wording of MIB-generated error messages to more meaningful messages for your organization. You can control which Alarm Browser category the event is assigned to and also configure:
  - Automatic Actions, such as dialing a pager, that execute whenever NNM receives a specific event. An Automatic Action command is tied to a particular event and can be limited to a specified list of IP hostnames and/or IPX addresses.
  - Additional Actions that provide access to batch files or executables that your team uses occasionally. You configure the additional actions to show up in NNM's menu bar. Additional Actions can be applied to any alarm or specified groups of alarms.
- Information gathering applications:
  - *MIB Application Builder* (page 443). Allows you to set up new menu items within NNM that provide access to your choice of useful MIB objects on an as-needed basis.

2474

— *Data Collection & Thresholds* (page 447).
Allows you to configure NNM to gather your choice of SNMP-MIB objects automatically (scheduling specific collections, establishing threshold monitoring of devices, and controlling what shows up in the Alarm Browser as a result).

— *MIB Expressions* (page 460).
You can create MIB expressions (mathematical formulas using MIB objects for analysis) to be used by Data Collection & Thresholds.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0959
3740
Doc:

SNMP MIB Browser

The SNMP MIB Browser is available from any submap under `Tools:SNMP MIB Browser`. The SNMP MIB Browser is useful for:

- Exploring your MIBs and their objects to become familiar with the network management capabilities that they provide. It serves as a useful reference tool. Type in any MIB number and view the description of what it is intended to do. Click on any leaf in any loaded MIB tree to view the MIB object's description.
- Querying MIB objects and viewing the returned instances for a network device that you selected on the submap or specified by typing in the IP address. You can view real-time MIB values for a selected node. You can also collect multiple instances by specifying a time interval for queries and display a graph of the results. The node for which you want to view MIB objects must support SNMPv1 or SNMPv2C.
- Setting MIB values on a network device. Prerequisites are:
  - The selected node on which you want to set MIB objects must support SNMPv1 or SNMPv2C.
  - The SNMP agent on the selected node must be configured to respond to SNMP SetRequests.
  - You must know the agent's SET-community name.

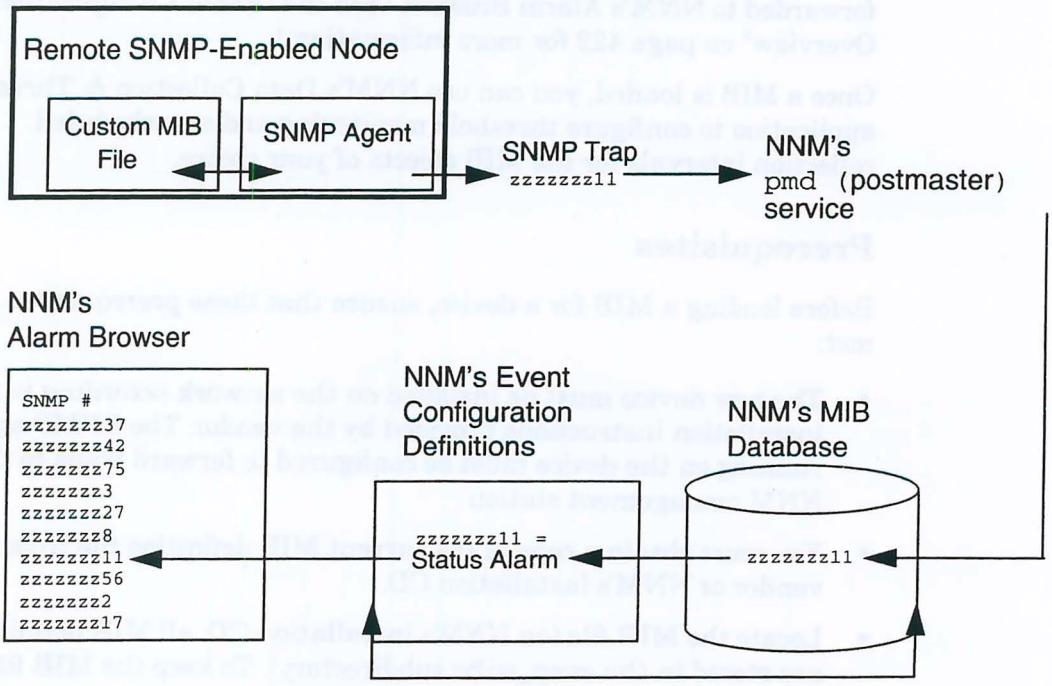
For more information about what you can do with NNM's SNMP MIB Browser, see the online help available within the SNMP MIB Browser window.

2476

Loading MIBs in the MIB Database

When you install NNM, the standard SNMP version 1 and 2 MIBs are automatically loaded and configured for your convenience. Often devices on your network have their own custom vendor-specific MIBs that allow for monitoring specific aspects of that vendor's devices, and allow you to customize NNM to proactively manage the devices. If you are running extensible SNMP agents on your devices, the agents may be using custom MIB files. Before you can take advantage of these custom MIB capabilities, the MIB definition loaded into NNM's MIB database must match the version of the MIB in use on the device itself.

Figure 12-1 Configuring Custom MIB File Definitions



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0960
3740
Doc:

NOTE To obtain the most recent version of a MIB file, check NNM's installation CD, contact the vendor who wrote the MIB file, or search the WWW (`ftp://ftp.isi.edu/mib/`) for quick access to the MIB file. Make sure the MIB definition loaded into NNM's MIB database matches the version of the MIB in use on the device itself.

The NNM installation CD includes hundreds of vendor-specific MIBs for your convenience. Simply load the MIBs that are relevant and useful for your specific network configuration. When you load a MIB into NNM's MIB database, that MIB's trap definitions are automatically added to the Event Configuration application so that you can customize NNM's use of each one. Use NNM's Event Configuration to identify which traps are forwarded to NNM's Alarm Browser. (See the "Event Configuration Overview" on page 422 for more information.)

Once a MIB is loaded, you can use NNM's Data Collection & Thresholds application to configure threshold monitoring and set scheduled collection intervals for the MIB objects of your choice.

Prerequisites

Before loading a MIB for a device, ensure that these prerequisites are met:

- The new device must be installed on the network according to the installation instructions provided by the vendor. The SNMP agent running on the device must be configured to forward traps to the NNM management station.
- You must obtain a copy of the current MIB definition file from the vendor or NNM's installation CD.
- Locate the MIB file (on NNM's installation CD, all MIB definitions are stored in the `snmp_mibs` subdirectory). To keep the MIB files sorted logically, the best practice is to create a subdirectory on the management station labeled with the vendor's name. Then copy the MIB file to that subdirectory on the management station before loading it. For example:
  - *Windows:* `install_dir\snmp_mibs\vendor\MIB`
  - *UNIX:* `$OV_SNMP_MIBS/vendor/MIB`

- The MIB must conform to *RFC 1155*, *RFC 1212*, *RFC 1902*, *RFC 1903*, or *RFC 1904*.
- If you have unloaded all the MIBs from the management station, it is recommended that you load MIB-II before you load an enterprise-specific MIB.

Procedure Tips

TIP

Close NNM's `Event Configuration` window prior to loading any MIB file. NNM automatically establishes a preliminary event configuration for you of each trap in the new MIB (provided the `Event Configuration` window is closed).

To load a MIB:

1. Place the NNM installation CD into the management station's CD drive. By default, NNM assumes you want a MIB from the installation CD. If the enterprise-specific MIB that you want to load is located elsewhere, you can enter the full path name to the file after opening the `Load/Unload MIB` window (in the field labeled `MIB File to Load`).
2. From any submap, select `Options:Load/Unload MIB:SNMP`. See NNM's online help from within the `Load/Unload MIB:SNMP` window for more information.
3. If the MIB file contains trap definitions, a dialog box appears asking if you would like to establish generic configurations for each trap in NNM's Event Configuration.

You can use the `Tools:SNMP MIB Browser` operation to view the new MIB objects. See "SNMP MIB Browser" on page 412.

If a MIB does not load properly, you will receive an error message. The problem could be:

- A syntax error in the MIB.

  The Load/Unload MIB program's error message identifies the MIB object where the error is occurring.
- Mismatched versions of the vendor's MIB.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0961
3740
Doc:

For example, the vendor's MIB on the NNM installation CD might not match the installed MIB version on the vendor's device on your network. In this case, obtain the MIB version that matches the MIB currently on the device.

In either case, contact the vendor to resolve the problem.

24-32

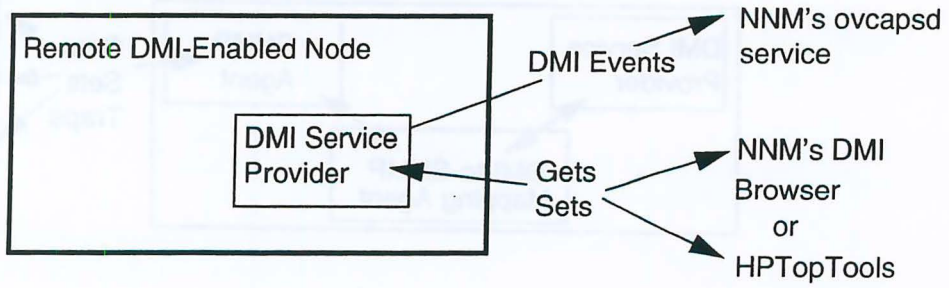
DMI Browser

The DMI Browser is available on NNM management stations running a Windows operating system. From any submap under `Tools:DMI Browser`. The DMI Browser allows you to view real-time MIF values for the DMI-enabled device currently selected on your submap.

Creating DMI Queries

In addition to DMI events, DMI also supplies GET and SET capabilities for some attributes.

Figure 12-2 **Queries to a DMI Service Provider**



- *DMI version 2:*

  To run DMI queries of devices running any DMI 2.0 service provider, use NNM's DMI Browser application. See the online help from within the DMI Browser for more information.

- *DMI version 1.1:*

  To run DMI queries of devices running the HP-RDMI service provider, use the HPTopTools application provided in the contributor's subdirectory on the NNM installation CD. See the `readme` file in the contributor's directory (see page 74).

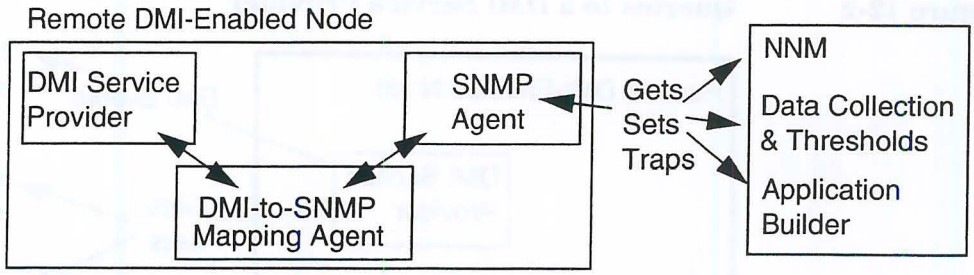
NOTE As an alternative, rather than communicating directly with the DMI service provider on your device, you can communicate with the DMI service provider indirectly through an SNMP agent installed on the

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0962
3740
Doc:

device along with a DMI-to-SNMP mapping agent. (Intel provides a mapping agent in their DMI 2.0 Service Provider Software Development Kit.) See the following figure.

The SNMP agent then handles all communications. Therefore, NNM tools such as the MIB Browser, MIB Application Builder, Data Collection & Thresholds application, and SNMP Grapher can be used to query DMI data via the DMI-to-SNMP mapping agent. NNM no longer subscribes to the DMI service provider to receive DMI events from devices running a DMI-to-SNMP mapping agent.

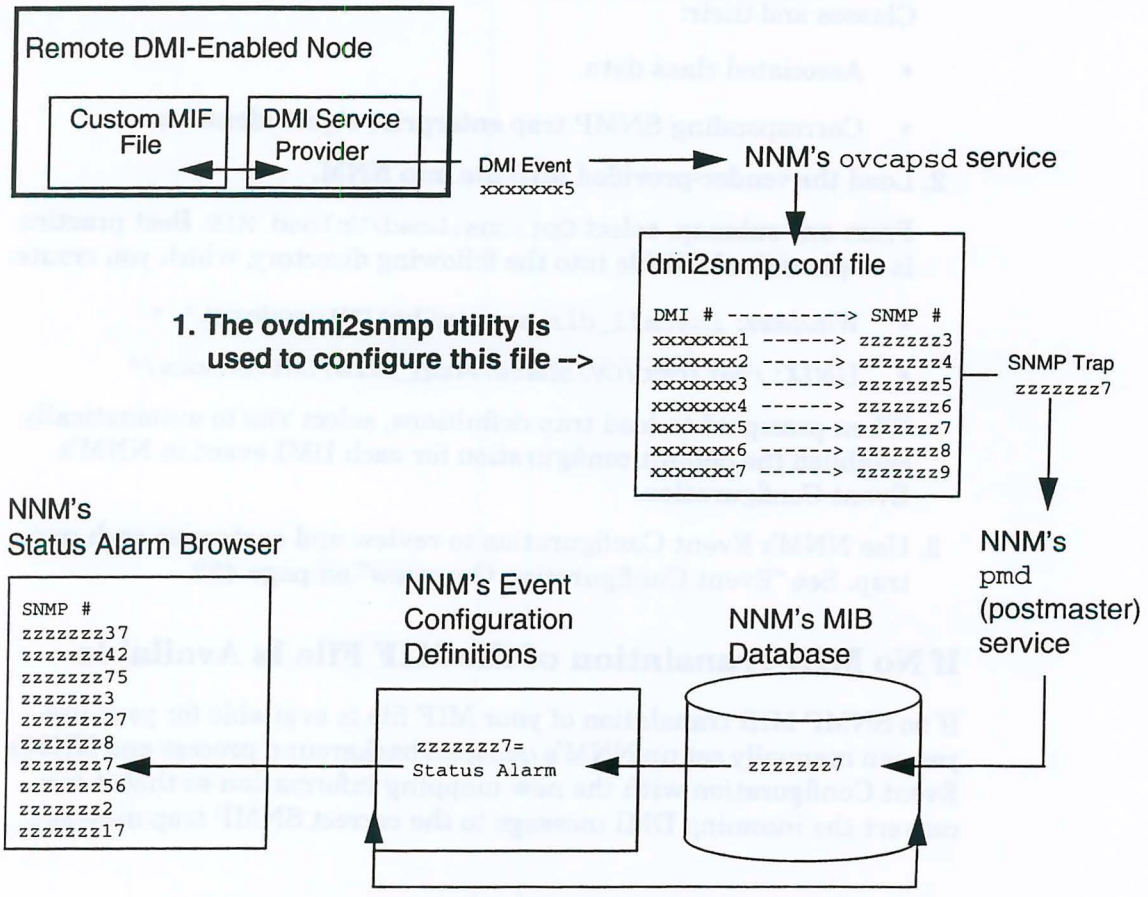
Figure 12-3 Bypassing a DMI Service Provider with an SNMP Agent



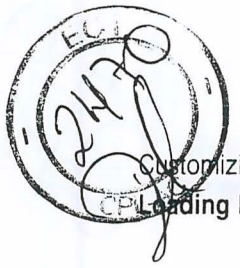
Loading DMI-to-SNMP Event Mappings

If your DMI service provider software is using a vendor-specific MIF instead of or in addition to the DMTF's standard MIF, you must configure NNM to understand the custom MIF events. Otherwise, a generic DMI event message (based upon the `dmiEventIndication` definition) is posted to the Alarm Browser each time the vendor-specific DMI event is received. To customize NNM's treatment of these events, you need to complete several steps, as shown in the following figure.

Figure 12-4 Configuring Custom MIF File Definitions



ECT nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0963
3740
Doc:



If a MIB Translation of the MIF File Is Available

The vendor of the DMI MIF may provide an SNMP MIB translation for your use. This allows you to load the MIB file and work with the event configurations in the same manner as you work with any SNMP MIB. However, an additional step is required. You must also provide the `ovcapsd` service with the new mapping information so that it can convert the incoming DMI event message to the correct SNMP trap message.

1. Update `ovcapsd`'s mapping file.

   A tool is provided to assist with this task. See the *ovdmi2snmp* reference page in NNM's online help for information about how to do this step. You will need to know each of the MIF's Event Generation Classes and their:

   - Associated class data.
   - Corresponding SNMP trap enterprise object identifier.

2. Load the vendor-provided MIB file into NNM.

   From any submap, select `Options:Load/Unload MIB`. Best practice is to place the MIB file into the following directory, which you create:

   - *Windows:* `install_dir\snmp_mibs\DMIvendors\*.*`
   - *UNIX:* `/var/opt/OV/share/snmp_mibs/DMIvendors/*`

   When prompted to load trap definitions, select `YES` to automatically establish the default configuration for each DMI event in NNM's Event Configuration.

3. Use NNM's Event Configuration to review and customize each new trap. See "Event Configuration Overview" on page 422.

If No MIB Translation of the MIF File Is Available

If no SNMP MIB translation of your MIF file is available for your use, you can manually set up NNM's `ovcapsd` background process and NNM's Event Configuration with the new mapping information so that it can convert the incoming DMI message to the correct SNMP trap message.

TIP MIF-to-MIB translation tools that convert any MIF file to a MIB file are available. Intel provides one in their DMI 2.0 Service Provider Software Development Kit.

1. Update ovcapsd's mapping file.

   A tool is provided to assist with this task. See the *ovdmi2snmp* reference page in NNM's online help for information about how to do this step. You will need to know each of the MIF's Event Generation Classes and their:

   - Associated class data.
   - Unique SNMP trap enterprise object identifier for the DMI Event Generation Class, which you choose.
   - SNMP trap ID, which is equal to the DMI Event ID.

   If your company has a registered "enterprise branch" assigned through the Internet Assigned Numbers Authority (IANA), use one of those available numbers. Otherwise, you may create a new OID that is unique to your installation under the `hpOVUserDefnEvents` branch (`1.3.6.1.4.11.2.17.9.xxxxx`).

2. Use NNM's Event Configuration to create a new trap configuration manually for each DMI event in your MIF file. Be sure to use the same corresponding SNMP trap enterprise object identifier and event/trap ID that you used in step 1 for each event. See "Event Configuration Overview" on page 422.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0964
Doc. 3740

Event Configuration Overview

SNMP events are the building blocks of network management. Alarms are generated when NNM receives certain events. Thoughtful planning and use of event configuration will allow NNM to monitor your network effectively, taking the pressure off of you and your team. The Event Configuration application enables you to control and enhance the way in which NNM handles events. This section describes the following few suggestions among numerous possibilities:

- Control alarm message posting and text.
  - — Control which alarms are posted into NNM's Alarm Browser and which alarms are ignored.
  - — Assign an Alarm Browser category for the event's alarm.
  - — Customize alarm messages to make them more meaningful or to provide specific troubleshooting information to your team.
- Establish automatic actions for NNM to perform whenever a specific event is received (such as dialing a pager).
- Place access to a commonly used batch file command or any executable (such as launching commonly used troubleshooting tools) on NNM menus for your team's convenience.

For more ideas about customizing NNM's event system, review the choices in the `Event Configuration` window and refer to NNM's online help available from within the `Event Configuration` window.

Prerequisites

- The MIB for which you want to configure events must be loaded into NNM's MIB database. From any submap, select `Options:Load/Unload MIBs:SNMP` to display the list of all MIBs currently in NNM's MIB database. If the MIB you wish to use is not loaded, see "Loading MIBs in the MIB Database" on page 413.
  - — A generic configuration for each trap from the MIB is automatically set up in NNM's event configuration feature when you load the MIB.

ECS Correlations

NNM's Built-In Correlations

NNM includes a set of event correlations (the Bundled Edition correlations):

- Connector Down Correlation System (page 361)
  This feature encompasses more than event correlation. NNM's map processes and alarm monitoring processes have been enhanced to help you speed up the task of identifying the source of a problem on your network as it occurs.
- Frame Relay Correlation (page 365)
  This correlation detects and reports specific problems with virtual connections. It distinguishes between failures within the provider network and failures within the local network.
- ManageX Server Down Correlation (page 369)
  When certain ManageX services become unavailable, this correlation combines HP OpenView ManageX events with NNM's topology events, creates new high level ManageX messages, and forwards them to the ManageX message reader. These messages explain why ManageX services are unavailable. Events sent to NNM by ManageX appear in the NNM Alarm Browser. Enable this correlation only if ManageX and NNM will be used together.
- Pair Wise Correlation (page 371)
  This correlation matches a *parent* event to one or more previously occurring *child* events; for example, an Interface Down alarm (OV_IF_Down) followed by an Interface Up alarm (OV_IF_Up) within a designated time frame. You can configure the behavior of alarms passing through this correlation.
- Repeated Event Correlation (page 375)
  This correlation identifies multiple duplicate alarms which are associated with a single physical event and bundles them together under a single alarm.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0965
Doc: 3740

- Scheduled Maintenance Correlation (page 379)
  When conducting planned network maintenance that requires multiple devices to be off-line for a certain amount of time, this correlation allows you to exclude events generated because of the maintenance activity.

Connector Down Correlation

Use of this correlation can prevent event storms when a router (or other connector device) goes down. In the event of a network failure, NNM automatically determines:

- Which device is malfunctioning.
- Which other network devices are impacted by this failure. That is, which functional network devices are now *inaccessible to the management station* over the network because of the failing device. These inaccessible devices are referred to as *secondary failures*.
- Which *inaccessible* network devices are *important* to the productivity of the organization and thus should be given high priority.

Behavior NNM automatically determines the route to a node that is down and checks each connector device along the path to that node to determine the primary malfunction.

Only the alarm about the primary device is logged to the Alarm Browser, making it easy for you to determine the root cause of the problem. To view the error messages regarding devices considered secondary failures:

- From the Alarm Browser, select the correlated alarm's message and select `Actions:Show Correlated Events` or double-click on the correlated column.
- From the web-based Alarm Browser, select the correlated alarm's message and select `Actions:Alarm Details` and select the `Correlations` tab.

NNM slows down polling traffic to all affected devices (i.e. devices considered secondary failures other than the primary malfunction) until the primary device is recovered. The map automatically updates to indicate the primary failure and the affected secondary failures below the primary failure.

You can establish a list of mission-critical devices (Important Node filter) that are never considered secondary failures.

Setting Parameters There are several configuration parameters for the `ConnectorDown` correlation contained within the correlation, itself. However, the `ConnectorDown` correlation is mainly controlled by NNM rather than the Event Correlation Service. It is recommended that you do not modify the correlation itself.

To set parameters for the `ConnectorDown` correlation, from any NNM submap, select `Options:Network Polling Configuration`. (See "Secondary Failure Polling" on page 192 for instructions.)

Make sure that the `Secondary Failures Polling Options` field is enabled because this field determines whether the `ConnectorDown` correlation is being used. The settings in the other fields are up to you (see the following examples for information about the behavior of different choices).

- Important Node Filter
  Designate the name of the filter you created which lists all nodes that are mission-critical and should, therefore, never be placed in secondary-failure status. In the case of a failure resulting in devices contained in the list becoming inaccessible, alarm messages pertaining to these devices would continue to appear in the Alarm Browser window. (See "Router/Switch Health" on page 390 for information about the correlation of alarms from nodes listed in the Important Nodes filter.)

  This filter resides in the same file that contains any discovery filters, DHCP filters, etc.:

  — *Windows:* `install_dir\conf\C\filters`

  — *UNIX:* `$OV_CONF/C/filters`

  See the *OVfilterIntro* reference page (or the UNIX manpage) in NNM's online help for more information about defining filters. See also *A Guide to Scalability and Distribution* for information about creating filters.

- Important Node Behavior
  Designate which status change you prefer to receive for the devices listed in the important-node filter: Down (red on map) or Unknown (blue on map).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0966
3740
Doc:

- Secondary Node Polling Multiplier
  To prevent the generation of unnecessary polling traffic, specify a multiplier by which any scheduled polling should be extended during the failure for devices designated as secondary devices.
- Secondary Node Behavior
  Designate which status change you prefer to receive for devices determined to be secondary failures: Down (red on the map), Unknown (blue on the map), or Unchanged (no change reflected on the map).
- Secondary Failure Alarm Suppression
  Designate whether or not you want to prevent alarm messages about secondary failures from being posted to the Alarm Browser's main categories. If this function is selected, the secondary devices' alarm messages are displayed by selecting the primary alarm message in the Alarm Browser window and selecting the `Actions:Show Correlated Events` menu item.

NOTE See *A Guide to Scalability and Distribution* for information about configuring this feature on collection stations and their corresponding management station.

The following examples illustrate how these settings affect the behavior of NNM.

Example 11-1 Example 1 Default Settings without Using a Filter

```
Important Node Filter File: None
Important Node's Failure Status: Down (irrelevant because no devices are
identified in the filter)
Secondary Node Failure Status: Unknown (blue on the map)
Suppress Alarms for Secondary Failures: True
Secondary Node Polling Multiplier: 2
```

During a network failure:

- The node determined to be the primary cause of the failure appears as a red (critical) symbol on the map, an alarm message is posted in the Alarm Browser, and polling intervals remain constant.
- Since no filter has been specified, no secondary nodes are considered important.

- All secondary-failure nodes are displayed as blue symbols (unknown) on the map. The alarm messages for all secondary devices do not appear in the Alarm Browser list. To view secondary alarm messages, select the corresponding primary alarm and select the `Actions:Show Correlated Events` menu item. Once a node is identified as a secondary failure, its polling intervals are doubled.

Example 11-2 Example 2 Default Settings with a Filter

```
Important Node Filter File: YourFilterName
Important Node's Failure Status: Down (red on the map)
Secondary Node Failure Status: Unknown (blue on the map)
Suppress Alarms for Secondary Failures: True
Secondary Node Polling Multiplier: 2
```

During a network failure:

- The device determined to be the primary cause of the failure appears as a red (critical) symbol on the map, an alarm message is posted in the Alarm Browser, and polling intervals remain constant.
- Any affected device that is specified as an important device in your filter file appears as a red symbol (critical) on the map, polling intervals remain constant, and alarm messages are posted in the Alarm Browser window.
- All secondary-failure interfaces on all nodes are displayed as blue symbols (unknown) on the map. The alarm messages for all secondary devices do not appear in the Alarm Browser list. To view secondary alarm messages, select the corresponding primary alarm and select the `Actions:Show Correlated Events` menu item. Once a node is identified as a secondary failure, it's polling intervals are doubled.

Example 11-3 Example 3 Minimum Network Traffic During Event Correlation

```
Important Node Filter File: YourFilterName
Important Node Behavior: Unknown (blue on the map)
Secondary Node Behavior: Ignore (no change on the map)
Secondary Failure Alarm Suppression: True
Secondary Node Polling Multiplier: 10
```

During a network failure:

- The device determined to be the primary cause of the failure appears as a red (critical) symbols on the map, an alarm message is posted in the Alarm Browser, and polling intervals remain constant.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0967
3740
Doc:

- Any affected device that is specified as an important device in your filter file appears as a blue symbol (unknown) on the map, polling intervals remain constant, and alarm messages are posted in the Alarm Browser window.
- All secondary-failure interfaces on all nodes are ignored, no change is reflected on the map. No alarm messages are generated for secondary devices. Once a node is identified as a secondary failure, its polling intervals are multiplied by 10.

Example 11-4 Example 4 Behavior Like Previous Releases of NNM

To disable the *secondary device* strategy and configure NNM to consider all devices as primary, deselect the `Secondary Failures Polling Options` field to disable the Connector Down correlation. This will have the following effect.

```
Important Node Filter File: None
Important Node Behavior: (irrelevant because no devices identified in the filter)
Secondary Node Behavior: Down (red on the map)
Secondary Failure Alarm Suppression: False (all alarms posted)
Secondary Node Polling Multiplier: 1 (no change)
```

During a network failure:

- The device determined to be the primary cause of the failure appears as a red (critical) symbol on the map, an alarm message is posted in the Alarm Browser, and polling intervals remain constant.
- Since no filter has been specified, no secondary nodes are singled out as important nodes.
- All secondary-failure interfaces on all nodes are displayed as red symbols (critical) on the map. The alarm messages for all secondary devices are sent directly to the Alarm Browser list. No polling intervals are changed.

Frame Relay Correlation

The `FrameRelay` correlation detects and reports problems with frame relay virtual connections. This correlation narrows the troubleshooting area for frame relay problems and reduces the number of events in the Alarm Browser by reporting only one alarm that represents all affected virtual connections.



Behavior

NOTE The FrameRelay correlation detects and analyzes frDLCIStatusChange traps from devices that support the circuit state changes described in RFC2115.

This correlation begins when a frame relay device generates several frDLCIStatusChange traps as shown in Example 11-5 on page 366. Notice that each frDLCIStatusChange trap contains an SNMP variable-binding named state that is set to active, inactive, or invalid. The FrameRelay correlation counts each time a frDLCIStatusChange trap's state value changes from invalid/inactive to active.

The FrameRelay correlation counts two state transitions for the traps shown in Example 11-5: the first at 10:10:10 and the second at 10:10:30. Two minutes after the first state change, the FrameRelay correlation generates an OV_FrameRelayReset event. Two minutes is the default Window setting and can be modified. See "Setting Parameters" on page 368 for more information.

Example 11-5 The frDLCIStatusChange Trap

```
01/01 10:10:00 frDLCIStatusChange: ifIndex=1, DLCI=401, state=inactive
01/01 10:10:10 frDLCIStatusChange: ifIndex=1, DLCI=401, state=active
01/01 10:10:20 frDLCIStatusChange: ifIndex=1, DLCI=401, state=invalid
01/01 10:10:30 frDLCIStatusChange: ifIndex=1, DLCI=401, state=active
```

The frDLCIStatusChange trap indicates a problem with the PVC or the local equipment. NNM further analyzes this trap and reports whether the problem's root cause is located within the local network or the provider network.

To use the FrameRelay correlation you must enable SNMP trap forwarding on the frame relay routers and enable the FrameRelay correlation as shown in "Setting Parameters" on page 368. The router must support RFC2115.

Below are three examples of how to use the FrameRelay correlation to help you diagnose problems.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 0968
3740
Doc.

Figure 11-2 The Frame Relay Network



Example 11-6 NNM Reports a Problem with an Abnormal State Change Frequency

Refer to Figure 11-2 for this example. The following steps illustrate when NNM would generate an `OV_FrameRelayReset` event:

1. Router A generates a large number of `frDLCIStatusChange` traps within a configurable period of time.
2. The `FrameRelay` correlation counts several state transitions after analyzing the `frDLCIStatusChange` traps.
3. NNM generates an `OV_FrameRelayReset` event, indicating that there is a problem with either the frame relay network or the local router serial interface.

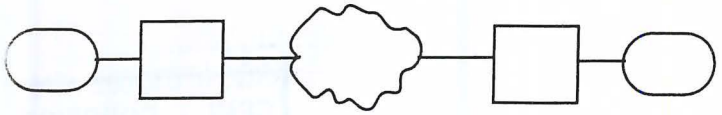
   The `OV_FrameRelayReset` event indicates that a problem exists due to a number of state transitions occurring within a certain time period as reported by Router A.

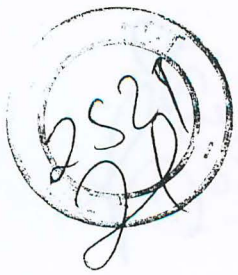
   You need to do some manual troubleshooting to diagnose this problem.

The `OV_FrameRelayReset` alarm contains an interface index on which the virtual connections are layered. This alarm reports the interface index along with the affected DLCIs and the number of times a reset occurs within the time period. For example, if an `OV_FrameRelayReset` alarm message contains `[(401, 2), (402, 1)]`, this indicates there were two resets for DLCI 401 and one reset for DLCI 402.

Example 11-7 NNM Reports a Problem with a Local Router Interface

Refer to Figure 11-2 on page 367 for this example. The following steps illustrate when NNM would generate an `OV_FrameRelayLocalCircuitProblem` event:





1. Router A generates a large number of `frDLCIStatusChange` traps within a configurable period of time. The status is currently `inactive`, and is toggling between `active` and `inactive`.
2. Either before or after the `frDLCIStatusChange` traps occur, router A sends a `link_Down` trap with the *`ifLocalReason`* variable-binding set to `LMI failed`. That indicates a possible LMI failure on Router A.
3. NNM generates an `OV_FrameRelayLocalCircuitProblem` event, indicating that there is a router serial interface failure on Router A.

   You need to troubleshoot the serial interface on Router A.

Example 11-8 **NNM Reports a Problem with the Frame Relay Network**

Refer to Figure 11-2 on page 367 for this example. The following steps illustrate when NNM would generate an `OV_FrameRelayCarrierProblem` event:

1. Local Router A generates a large number of `frDLCIStatusChange` traps within a configurable period of time.
2. The `frCircuitState` variable-binding within the `DLCIStatusChange` trap is invalid for the DLCIs generating the `DLCIStatusChange` events.
3. NNM generates an `OV_FrameRelayCarrierProblem` event, indicating that there is a problem with the frame relay network.

   You need to call your service provider.

Setting Parameters Complete the following steps if you want to view more information about or modify the `FrameRelay` correlation.

TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.

CPMI - CORREIOS
Fls. Nº 0969
3740

3. If you want to enable or disable the `FrameRelay` correlation: from the `ECS Configuration` window, highlight the `FrameRelay` correlation, then select either `Enable` or `Disable`.
4. From the `ECS Configuration` window, highlight the `FrameRelay` correlation and select `Describe` to review the correlation description.
5. From the `ECS Configuration` window, highlight the `FrameRelay` correlation and select `Modify` to bring up the `FrameRelay-Modify` screen.

   The `Window` parameter, used as a time window for counting status transitions from the `frDLCIStatusChange` trap, is the only configurable parameter for the `FrameRelay` correlation.
6. To view the parameter description or modify the configurable parameter, select the parameter, then select `View/Modify`.

NOTE If you modify the `Windows` parameter, set the parameter to a value between two and five minutes. As you set the value higher, the `FrameRelay` correlation consumes more memory resources.

ManageX Server Down Correlation

The `MgXServerDown` correlation analyzes the network health, generates new high level ManageX messages, and delivers these messages to the ManageX message reader. The resulting messages explain why certain ManageX services are unavailable. ManageX messages also appear in the NNM Alarm Browser once this correlation is configured and enabled.

The message information is of value to the ManageX system administrator as it explains what portions of the network are interfering with ManageX operation. This information eliminates the need for the ManageX administrator to contact the network administrator and improves the efficiency of both the network administrator and the system administrator.

Behavior ManageX console events are picked up by the *NNM Lights Out policy* (nnmIntegration.mxc) and converted to an SNMP trap which is sent to NNM. These events route through the ECS `MgXServerDown` correlation for evaluation by NNM.

2519

If NNM discovers that a ManageX device is down, the ECS `MgXServerDown` correlation will determine if the interface-down event is due to a problem on a connector device (router interface, switch, etc.). The result of the analysis is encapsulated in an event that NNM converts into an SNMP trap and sends to the ManageX NNM WMI policy (nnmWmiEventPolicy.mxw) where it is converted into a ManageX console message for display in the ManageX message reader.

Setting Parameters There are numerous configurable parameters contained in the `MgXServerDown` correlation. Complete the following steps if you want to review parameter definitions or modify parameters contained within the `MgXServerDown` correlation.

TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

`Options:Event Configuration`. This launches the `Event Configuration` window.

2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.
3. From the `ECS Configuration` window, highlight the `MgXServerDown` correlation and select `Describe` to review the correlation description.
4. From the `ECS Configuration` window, highlight the `MgXServerDown` correlation and select `Modify` to bring up the `MgXServerDown-Modify` screen.
5. To view parameter descriptions or modify any of the configurable parameters, select the parameter, then select `View/Modify`.

TIP From the `View/Modify` window, select `Help` for general information on making correlation modifications.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0970
3740
Doc:

Pair Wise Correlation

This correlation matches a *parent* event to one or more previously occurring *child* events. You can configure child events to:

- Display in the Alarm Browser while awaiting arrival of a parent event, or
- Only display in the Alarm Browser if the specified time window is exceeded without the arrival of a matching parent event,
- Upon arrival of a parent event, be removed from the Alarm Browser and nested beneath the parent event, or set to Acknowledged.

For example, consider several repeated OV_IF_Down events followed by an OV_IF_Up event within a designated time frame. This correlation could be configured to either remove or acknowledge the OV_IF_Down events upon arrival of the OV_IF_Up event. The OV_IF_Down events are nested under the OV_IF_Up alarm message in the Alarm Browser.

You can add SNMP traps and events to the `PairWise` correlation, provided that you know how the source that is sending the trap is identified. The SNMP MIB Object ID (OID) works in combination with one of the following to specify the source. The combination being used is determined by the developer of the underlying MIB. You must know the appropriate combination in order to configure additional events into this correlation:

- `agent-addr` attribute
- Any source wildcard (your choice)
- SNMP variable-binding name
- SNMP variable-binding position

Behavior You control the behavior of this correlation. The following three examples explain some of your choices. Remember that in order for an event to be displayed within the Alarm Browser, the event's configuration must *not* be set to:

- Don't log or display
- Log only

See "Event Configuration Overview" on page 422 for information about setting an event's configuration.

Example 11-9 Don't Display the Child Events or the Parent Event

```
ChildEventImmediateOutput = False
InhibitParentOfInhibitedChild = True
```

The correlation monitors the defined event parent/child relationships in the background. You never see the parent or any child events in the Alarm Browser unless the time of the defined window period is exceeded and no parent event arrives. If no parent is received, the child events are displayed in the Alarm Browser.

Example 11-10 Display the Parent Event, Nest Child Events Beneath Parent

```
ChildEventImmediateOutput = False
InhibitParentOfInhibitedChild = False
```

The correlation monitors the defined event parent/child relationships in the background. When the parent event is received, the parent event is displayed in the Alarm Browser with the child events nested beneath. If no parent is received within the defined window period, the child events are displayed in the Alarm Browser.

Example 11-11 Display Both the Parent and Child Events in the Alarm Browser

```
ChildEventImmediateOutput = True
InhibitParentOfInhibitedChild = ignored (True or False)
```

Child events are displayed in the Alarm Browser upon arrival. The correlation monitors the defined event parent/child relationships, and when the parent event is received, the parent event is displayed in the Alarm Browser with the child events nested beneath. You choose whether the child events are removed from the Alarm Browser list or set to Acknowledged upon arrival of the parent event.

To view nested child alarms:

- From the Alarm Browser, select the parent alarm message and select `Actions:Show Correlated Events` or double-click on the correlated column.
- From the web-based Alarm Browser, select the parent alarm message and select `Actions:Alarm Details` then select the `Correlations` tab. You can also select the parent alarm message, click on the view button and then select the `Correlations` tab.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0971
3740
Doc:

Setting Parameters Complete the following steps if you want to review parameter definitions or modify parameters contained within the `PairWise` correlation.

TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

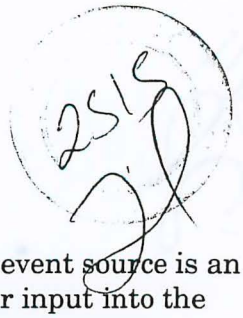
1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.
3. From the `ECS Configuration` window, highlight the `PairWise` correlation and select `Describe` to review the correlation description.
4. From the `ECS Configuration` window, highlight the `PairWise` correlation and select `Modify` to bring up the `PairWise-Modify` screen.
5. To view parameter descriptions or modify any of the configurable parameters, select the parameter, then select `View/Modify`.

TIP From the `View/Modify` window, select `Help` for general information on making correlation modifications.

This correlation allows configuration of the following parameters.

These two tables define which events are being monitored by the correlation and define the parent/child relationships:

- The `InputEventTypeListStringSources` table is used when the event source is a simple string which is not an IP address. This table is used to set event types for input into the correlation and determine the parent and child event sources.



- The `InputEventTypeList` table is used when the event source is an IP address. This table is used to set event types for input into the correlation and determine the parent and child event sources.

The following two parameters control when alarms appear in the Alarm Browser:

- The `ChildEventImmediateOutput` parameter determines whether the `PairWise` correlation outputs child events immediately or if it holds onto child events for further processing and possible cancellation by a parent event.

  `False` = The `PairWise` correlation holds onto child events for the duration of the `PairedTimeWindow`. If the `PairWise` correlation receives a matching parent event from the same source, within the appropriate amount of time, the child event is nested beneath the parent event in the Alarm Browser. If the `PairWise` correlation does not receive a matching parent event within the `PairedTimeWindow`, the child event is displayed in the Alarm Browser.

  `True` = Child events are displayed in the Alarm Browser upon arrival. Child events may be deleted or acknowledged in the Alarm Browser at a later time if a matching parent event arrives.

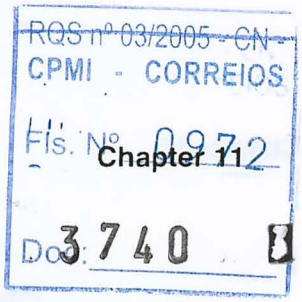
- The `InhibitParentOfInhibitedChild` parameter determines whether parent events are displayed in the Alarm Browser.

  `ateOutput` is true, the `PairWise` correlation ignores the `InhibitParentOfInhibitedChild` parameter and sends parent events to the Alarms Browser immediately.

  `True` = The correlation monitors the defined event parent/child relationships in the background. You never see either parent or child alarms in the Alarm Browser unless the time of the defined window period is exceeded and no parent event arrives. If no parent is received, the child events are displayed in the Alarm Browser.

  `False` = The parent event is displayed in the Alarm Browser upon arrival, with all child events nested beneath.

The following parameters fine tune the correlation:



- The `DeleteOrAcknowledge` parameter determines whether a child event is deleted or acknowledged from the Alarm Browser once it is matched to a parent event (assuming that `ChildEventImmediateOutput = True`).
- The `PairedTimeWindow` is the maximum time that the child event waits for a parent event. However, the `PairWise` correlation has a built in *pattern delete* feature. If a parent event arrives outside of the defined window, the Alarm Browser is scanned for any defined child events from the same source as the parent event.
- The `IgnoreSecondaryFailureEvents` parameter determines whether this correlation monitors events from devices identified as secondary failures. When set to `True`, secondary failures are monitored by the `ConnectorDown` correlation (page 361), and not by the `PairWise` correlation.

Repeated Event Correlation

This correlation allows multiple alarms which are associated with a single physical event to be bundled together and replaced by a single alarm in NNM's Alarm Browser.

For example, the OpenView `OV_PhysAddr_Mismatch` alarm is one of several alarms that are configured and active by default. When the physical address of a device changes, NNM generates multiple events as neighboring systems discover the change and NNM reads this conflicting information. The `RepeatedEvent` correlation suppresses the multiple instances of the physical address change alarms and correlates them into one alarm for any particular node. You specify the time interval; for example, after receipt of the first of many repeated alarms, suppress duplicates for 2 hours. Then generate another alarm and resume suppression of duplicate alarms for two more hours.

You can add other SNMP traps to the `RepeatedEvent` correlation for suppression of duplicate alarms, provided that you know the following information. Event Identifiers (MIB OIDs) work in combination with one of the following to specify how to obtain the source of the incoming trap:

- `agent-addr` attribute
- Any source wildcard (your choice)
- SNMP variable-binding name
- SNMP variable-binding position

2513

The combination being used is determined by the developer of the underlying MIB. You must know the appropriate combination in order to configure additional events into this correlation.

Behavior In NNM's Alarm Browser, all traps with the same key identifier [OID +source specifier] are nested under the first trap received for the specified time period. Only the first alarm in the series is posted into the Alarm Browser's main list. To view the rest of the alarms:

- From the Alarm Browser, select the primary message and select `Actions: Show Correlated Events` or double-click on the correlated column.
- From the web-based Alarm Browser, select the primary message and select `Actions:Alarm Details`, then select the `Correlations` tab. You can also select the primary message, click on the view button and then select the `Correlations` tab.

Setting Parameters Complete the following steps if you want to review parameter definitions or modify parameters contained within the `RepeatedEvent` correlation.

TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit: Event Correlation`. This brings up the `ECS Configuration` window.
3. From the `ECS Configuration` window, highlight the `RepeatedEvent` correlation and select `Describe` to review the correlation description.
4. From the `ECS Configuration` window, highlight the `RepeatedEvent` correlation and select `Modify` to bring up the `RepeatedEvent-Modify` screen.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0973
3740
Doc:



5. To view parameter descriptions or modify any of the configurable parameters, select the parameter, then select `View/Modify`.

TIP From the `View/Modify` window, select `Help` for general information on making correlation modifications.

The `RepeatedEvent` correlation contains the following parameters:

- The *`HoldFirstEventTime`* parameter sets an overall maximum time that initial events are held for later correlation with future events.
- The *`MaxHoldFirstEvents`* parameter sets an overall maximum number of first events to hold for later correlation with future events.
- The `InputEventTypeList` is a table that specifies the event types and event source identifiers that are input to this correlation. The following `Generic Trap Strings` and `Input Event OID` descriptions are included as event types in the `InputEventTypeList` table.

  `Generic Trap String`: The following generic trap names are contained within the correlation. Valid generic trap names are:

  coldStart

  warmStart

  linkDown

  linkUp

  authenticationFailure

  egpNeighborLoss

  By default, all of the generic traps are set to false (event not enabled) and are not evaluated by the `RepeatedEvent` correlation.

  `Input Event OID`: The Specific Event Types (Input Event `OID`) specify the trap `OID`. Two Input Event `OID`s are set to true (by default):

  `OV_PhysAddr_Mismatch (1.3.6.1.4.1.11.2.17.1.0.58982401)`

  `OV_Node_Added (.1.3.6.1.4.1.11.2.17.1.0.58785794)`

Enabling a particular row in the `InputEventTypeList-Modify` screen allows the event to be used as an input event into the correlation.

TIP Make sure that the Event Configuration settings for the trap you are enabling is *not* set to either of the following. If it is, your correlated alarm will never show up in the NNM Alarm Browser:

— Don't log or display

— Log only

See "Event Configuration Overview" on page 422.

- The `RepeatedTimeWindow` parameter sets an overall maximum time to correlate duplicate events. This value is used for both fixed (`RollingWindow=false`) and rolling (`RollingWindow=true`) time windows.

- The `CreateUpdateEvent` parameter allows you to specify whether or not to delete the original alarm from the Alarm Browser and create a new summary event when the time limit for this correlation is exceeded. If `CreateUpdateEvent` is true, the `RepeatedEvent` correlation creates a new, identical summary event that contains a count of the correlated events. If `CreateUpdateEvent` is false, the original alarm is not deleted from the Alarm Browser and no update event is created.

- Setting the `RollingWindow` parameter to true means that the time window is not fixed to a set time duration. The rolling time window resets each time the correlation receives another duplicate event.

  For example, the `RepeatedTimeWindow` parameter is set to 10 minutes with the `RollingWindow` parameter set to true. An event reports a conflicting MAC layer address. A second identical event arrives (repeats) within 10 minutes of the initial event. The time window for the correlation extends for another 10 minutes and the event is nested beneath the initial event in the Alarm Browser.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. 0974
Doc. 3740

Scheduled Maintenance Correlation

Computer nodes and network segments are occasionally scheduled for maintenance. Such an occurrence typically results in a number of SNMP traps or HP OpenView events being generated. The `ScheduledMaintenance` correlation prevents unnecessary alarms during maintenance.

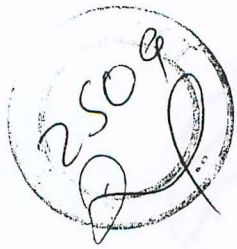
Behavior When the `ScheduledMaintenance` correlation detects the first event from a specified node or network segment within the specified time range, an event is generated and posted in the NNM Alarm Browser with the message: `Scheduled Maintenance`. The triggering event and all subsequent matching events are nested beneath the Scheduled Maintenance alarm. To view the nested alarms:

- From the Alarm Browser, select the primary message and select `Actions:Show Correlated Events` or double-click on the correlated column.
- From the web-based Alarm Browser, select the primary message and select `Actions:Alarm Details` and select the *Correlations tab.*

Setting Parameters Complete the following steps if you want to configure and enable the `ScheduledMaintenance` Correlation.

TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the [?] tab. Click Tasks, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.
3. If you want to enable or disable the `ScheduledMaintenance` correlation: from the `ECS Configuration` window, highlight the `ScheduledMaintenance` correlation. Then select either `Enable` or `Disable`.



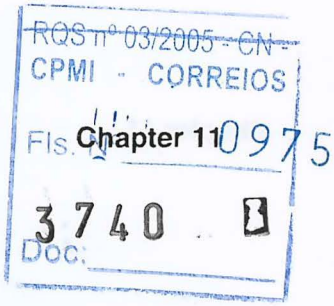
4. From the `ECS Configuration` window, highlight the `ScheduledMaintenance` correlation and select `Describe` to review the correlation description.
5. From the `ECS Configuration` window, highlight the `ScheduledMaintenance` correlation and select `Modify` to bring up the `ScheduledMaintenance-Modify` screen.
6. To view or modify the affected network devices, or set the name of the planned outage, or activate/deactivate a planned outage: select `MaintenanceList` from the `ScheduledMaintenance-Modify` window and click on `View/Modify`.
7. To view or modify the date, time, and duration of a planned outage: Select `OutageTimeSpecification` from the `ScheduledMaintenance-Modify` window and click on `View/Modify` to make changes. It's important to note that a time window name is specified and configured in the `OutageTimeSpecification-Modify` window. This time window name is then referenced in the `MaintenanceList` definition.
8. To view any other parameter descriptions or modify any of the other configurable parameters, select the parameter, then select `View/Modify`.

TIP From the `View/Modify` window, select `Help` for general information on making correlation modifications.

Command Line Control

You can enable, disable, and control correlations from the `Options:Event Configuration` or `Edit:Event Correlation` menu item. However, if you need to debug a test correlation or enable tracing or logging for support purposes, use the `ecsmgr` command line utility. Possible tasks include:

- Starting or stopping event logging.
- Configuring error logging and trace logging.
- Creating a new stream.



See the *ecsmgr* reference page in NNM's online help (or the UNIX manpage) for more information.

Correlation File Structure

Each correlation is comprised of four files. Correlations are stored in the following directory:

- *Windows:* `install_dir\conf\ecs\circuits\*.*`
- *UNIX:* `$OV_CONF/ecs/circuits/*.*`

Do not edit these files directly. Only the `*.ds` file can be altered by using the `Options:Event Configuration`, or `Edit:Event Correlation` menu items.

Table 11-1 Correlation File Structure

correlation`.eco`	Compiled correlation file (not editable).
correlation`.ds`	Data Store file containing externally configurable parameter values (text).
correlation`.fs`	Optional Fact Store file containing topological or other information describing relationships (text).
`C/`*correlation*`.param` or `$LANG/`*correlation*`.param`	Parameter file that describes the parameters configurable by the ECS Event Configuration window (text).

Troubleshooting

Correlation Not Displayed

If the correlation you want is not displayed:

- In the ECS Event Configuration window, click `[Update View]` to refresh the list display. Updates made by other users and updates made from the command line are not reflected in the list of correlations until you click `[Update View]`.
- The correlation may not have been loaded (installed).



Correlation Status Incorrect

If the Status of the correlation appears to be incorrect:

- In the ECS Event Configuration window, select the appropriate stream. Correlations are enabled in the selected stream only and the correlation status reflects the status for the selected stream only. A correlation may be enabled in one stream and disabled in others.
- Click `[Update View]` to refresh the list display.

ECS Event Configuration Window Hangs

If the ECS Event Configuration window appear to hang when you click `[Verify Table]` or `[OK]` after modifying a parameter value:

- Wait until the server responds. Verification is performed on the server and can take some time if the server is very busy.
- Check that the connection with the server has not been severed.

Too Many Alarms Are Showing Up

Did you change the NNM Event Configuration default settings for any events from "log-only" to display in the NNM Alarm Browser? Consider changing some of them back to "log-only" For example, you do not need to display the Link Down events received from your Cisco router because NNM is already monitoring status. The NNM `OV_IF_Down` event is the same as the hardware's Link Down trap.

Expand the configuration of de-duplication to include any repetitive events (see "De-Duplication of Alarms" on page 358).

Obtaining Additional Event Correlations

NNM includes several **Bundled Edition** correlations. No additional license or software is required to use these correlations. HP tests and supports these correlations.

There are three additional sources for correlations that can run in NNM:

- **Contributed Edition** correlations are provided by HP OpenView Partners. Check the HP OpenView web page for links (also check OpenView partners' web sites for access to these correlations). No

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº: 0976
3740
Doc:

additional license or software is required. HP does not test or support the Contributed Edition correlations. They are tested and supported by the partner.

- **Extended Edition** correlations can be obtained from system integrators, such as HP Consulting Service (see "HP Consulting Service" on page 76) and others. They are tested and supported by the supplier.
- **Designer Edition** correlations are written by you. You must purchase and use the HP OpenView ECS Designer product. HP does not test or support the Designer Edition correlations. They must be tested and supported by you.

If you add correlations to NNM, they must be installed and their initial parameter values configured. When a correlation is enabled, its memory tables must fill with events before correlation becomes effective. Like the correlations supplied with NNM, you can then make further modifications to the parameter values while the correlation is enabled.

So You Want To Develop Your Own Correlation?

Developing your own event correlations is a powerful option but a non-trivial task. You should consider carefully whether this is something you want to do or whether it might be quicker, simpler, and cheaper to contract with a specialist to supply the correlation or correlations you need.

If you need only one or two special correlations, then it is probably not worthwhile developing them yourself. Instead, you should consider contracting a specialist to develop them for you. Contact HP Consulting Service (see "HP Consulting Service" on page 76) or other system integrators for assistance.

To develop a correlation you need to:

- Purchase the HP OpenView ECS Designer product, a separately licensed component.
- Learn to develop correlations (ECS Designer training, and/or documentation).
- Design and debug the correlation, data store file, and parameter file.
- If required, develop processes to use the ECS Annotation and/or Event I/O APIs, as described in the *HP OpenView ECS Developer's Guide*.

- Deploy the correlation to each management station and collection station, as described in the documentation that you received when you purchased ECS Designer.

When to Design Your Own Event Correlations There are several key factors which indicate that a new correlation is required, or that an existing correlation needs to be reconstructed:

- No existing correlation provides the correlation you need.
- Parameters of an existing correlation need to be set to values that are outside the minimum and maximum allowed in the ECS Event Configuration window.
- The correlation requires access to external data (for example, to look up an inventory database) and therefore needs to use ECS annotation.
- Special event I/O requirements exist.

What is Involved

NOTE All de-duplication configurations, correlators defined within Correlation Composer, and all correlations defined within ECS must *work well* ement station. Before you begin, it is critical that you print out and read the following white paper:

`Developing_NNM_Event_Reduction.pdf`

- *Windows:* `NNM_install_dir\Doc\WhitePapers\`
- *UNIX:* `$OV_DOC/WhitePapers/`

This information explains how to ensure that you do not break existing implementations.

You *might* need to install the white papers on Windows-based NNM management stations. See "White Papers" on page 75.

To design an effective correlation, you must:

- Understand typical network event patterns and what they mean.
- Know the architecture of your network management system.
- Identify external data access (ECS Annotation) requirements.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0977
3740
Doc:

- Define the problem concisely in terms of filtering and time-related if-then statements.
- Determine if all data is available from the events themselves. If not determine if:
  - The external data is subject to change or is relatively stable.
  - The required data is small enough to store in memory.
  - The access speed and reliability is sufficient when extracting from your database (particularly if the database is remote).

Then, to develop the correlations, in addition to purchasing the HP OpenView ECS Designer product, you need to:

- Set up a test platform.
- Obtain or develop sample logs of events (perhaps use NNM backup files).
- If Event I/O or Annotation is required, refer to the *HP OpenView ECS Developer's Guide* (provided and obtain an ANSI C/C++ compiler.
- If ASCII events must be correlated, use the ASCII Module of the HP OpenView ECS Designer product.

2503

Correlation Composer Correlators

NNM's Built-In Correlators

NNM includes a set of correlators:

- "Cisco Chassis Failure" on page 387.
  Monitors Cisco traps for three error conditions: temperature, fan failure, and power supply fault. Generates a new alarm if the condition persists for the specified time period.
- "Router/Switch Intermittent Status Changes" on page 393.
  Listens for `OV_IF_Down` alarms from routers and switches, and creates a new alarm when more than *N* interface-down events are received within *M* minutes from a specific interface (defaults N=5, M=30min). Only the new `OV_Intermittent` alarm appears in the NNM Alarm Browser.
- "Router/Switch Health" on page 390.
  (actually a group of three correlators) Correlates Interface status alarms with their related router or switch Node status alarm. `OV_IF_Unknown` and `OV_IF_Down` status alarms from interfaces within routers or switches are suppressed and nested beneath the Node-status alarm.
- "Multiple Reboots on Routers/Switches" on page 388.
  Listens for `coldStart` and `warmStart` traps and creates a new alarm when more than *N* `coldStart/warmStart` traps are received within *M* minutes from a specific SNMP-agent/IP-address pair (defaults N=4, M=5min).
- "HSRP Group Health" on page 394.
  (actually a group of 6 correlators on UNIX only) If you purchased the NNM Extended Topology product, this group of six correlators analyzes an HSRP group status change and notifies you of the results by generating an `OV_HSRP_x` status alarm, with related alarms nested beneath.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0978
3740
Doc:

Cisco Chassis Failure

Correlates events forwarded from switches supporting the `CISCO-STACK-MIB.my` MIB.

Behavior Certain Cisco and HP routers and switches that support the CISCO-STACK MIB can be configured to send traps that report chassis error conditions to the NNM management station. This correlator monitors the SNMP variable-binding data within the Cisco traps that provides information about the reasons for a failure.

If a *temperature*, *fan failure*, or *power supply* fault condition persists for a period longer than the configured time interval, one of the following events is generated and sent to the NNM Alarm Browser:

- `OV_Chassis_Temperature` (.1.3.6.1.4.1.11.2.17.1.0.58982424)
- `OV_Chassis_FanFailure` (.1.3.6.1.4.1.11.2.17.1.0.58982425)
- `OV_Chassis_PowerSupply` (.1.3.6.1.4.1.11.2.17.1.0.58982426)

Conditions that persist for a time less than the specified Window Period are discarded.

Setting Parameters Complete the following steps if you want to review parameter definitions or modify parameters contained within the `OV_Chassis_Cisco` correlator.

TIP

There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.
3. From the `ECS Configuration` window, select the `'default'` stream. Then, highlight `Composer` in the correlation table and select `Modify`. The `Correlation Composer` window appears in your web browser.

4. In the `Correlation Composer` window, right-click the `OV_Chassis_Cisco` correlator and select `Modify` to display the `Description` tab.
5. Carefully read the information in the `Description` tab. Do not change any parameters other than the one specifically listed:
   - Window Period
6. Click the `Definition` tab to access the parameter settings. Click `[Help]` for information about each field.
7. After making the desired changes, close the correlator configuration window and return to the `Correlation Composer` main window.
8. Exit the `Correlation Composer` main window.
9. Save your changes when prompted to do so. This updates the NNM correlator fact store file.

Multiple Reboots on Routers/Switches

The Multiple Reboots correlator detects and reports problems with routers and switches that reboot multiple times within a specified time window.

Behavior The ECS `PairWise` correlation (page 371) suppresses `OV_Node_Down` alarms when the corresponding `OV_Node_Up` alarm arrives. Therefore, you may never see these events in the NNM Alarm Browser. This `OV_MultipleReboots` correlator detects a repetitive down/up situation within routers and switches and generates an `OV_Multiple_Reboots` alarm to warn you of a potential problem.

If a `coldStart` or `warmStart` trap arrives and no such traps have previously been seen for this SNMP-agent/IP-address pair, a new interval is started. If `coldStart` or `warmStart` traps already exist for this system, a counter is updated and checked to see if the number of counts exceeds the configured threshold. If the count exceeds the threshold and the trap is still within the current interval for this system, an `OV_Multiple_Reboot` alarm is posted in the NNM Alarm Browser. All further `coldStart` or `warmStart` traps within the specified time interval are nested under the `OV_Multiple_Reboot` alarm.

Once the interval expires, the sequence begins again.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0979
Doc: 3740

Setting Parameters Complete the following steps if you want to review parameter definitions or modify parameters contained within the `OV_MultipleReboots` correlator.

TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.
3. From the `ECS Configuration` window, select the `'default'` stream. Then, highlight `Composer` in the correlation table and select `Modify`. The `Correlation Composer` window appears in your web browser.
4. In the `Correlation Composer` window, right-click the `OV_MultipleReboots` correlator and select `Modify` to display the `Description` tab.
5. Carefully read the information in the `Description` tab. Do not change any parameters other than those specifically listed:
   - Count
   - Window Period
6. Click the `Definition` tab to access the parameter settings. Click `[Help]` for information about each field.
7. After making the desired changes, close the correlator configuration window and return to the `Correlation Composer` main window.
8. Exit the `Correlation Composer` main window.
9. Save your changes when prompted to do so. This updates the NNM correlator fact store file.

2499

Router/Switch Health

Suppresses interface status alarms from devices other than routers or switches so that these alarms never appear in the NNM Alarm Browser. The assumption is that you do not wish to see end-node interface status alarms.

Displays, in the NNM Alarm Browser, the important interface status alarms from your routers and switches. Suppresses the unimportant interface status alarms from those same routers and switches.

Router/switch health is actually determined by a group of three correlators:

- OV_NodeIf_NodeDown
- OV_NodeIf_NodeNotConnector
- OV_NodeIF_PrimaryIFUnknown

Behavior Suppresses interface status alarms from devices other than routers or switches.

Suppresses interface status alarms from unused (unconnected) ports within routers or switches.

Addresses the following failure scenarios that the ECS `ConnectorDown` correlation (page 361) doesn't detect:

- If fewer than *all* the interfaces on a router or switch fail, the interface status alarms display in your Alarm Browser. Intermediate node status alarms (`OV_Node_Warning`, `OV_Node_Marginal`, or `OV_Node_Major`) are configured as *log-only*, so they never appear in your Alarm Browser.
- If *all* the interfaces on a router or switch fail, `OV_Node_Down` alarm displays in your Alarm Browser with the interface alarms nested underneath.
- If a router or switch failure is a secondary failure (for example a Switch B is inaccessible due to a Switch A failure), then the ECS `ConnectorDown` correlation suppresses all of the events associated with Switch B. The suppressedInterface alarms are nested under the primary Switch A `OV_Node_Down` alarm.

  However, if the Secondary Failure Polling configuration identifies Switch B as an **Important Node** (listed in your Important Node filter, see page 361 and page 192) the Switch B secondary failure

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0980
3740
Doc:

events are not suppressed by the ECS ConnectorDown correlation. In this case, the Switch B OV_Node_Unknown alarm is displayed in the NNM Alarm Browser. The OV_NodeIf group of correlators nest the associated Interface status alarms beneath the parent node alarm. The Switch B OV_Node_Unknown alarm is not nested under the Switch A alarm.

Setting Parameters Complete the following steps if you want to review parameter definitions or modify parameters contained within the OV_IF_NodeDown correlator.

TIP There are several ways to access the event correlation features. For more information, from any submap, select Tools:HP OpenView Launcher. Select the [?] tab. Click Tasks, Event Correlation Management. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select Options:Event Configuration. This launches the Event Configuration window.
2. From NNM's Event Configuration window, select Edit:Event Correlation. This brings up the ECS Configuration window.
3. From the ECS Configuration window, select the 'default' stream. Then, highlight Composer in the correlation table and select Modify. The Correlation Composer window appears in your web browser.
4. In the Correlation Composer window, right-click the OV_IF_NodeDown correlator and select Modify to display the Description tab.
5. Carefully read the information in the Description tab. Do not change any parameters other than the one specifically listed:
   - Window Period
6. Click the Definition tab to access the parameter settings. Click [Help] for information about each field.
7. After making the desired changes, close the correlator configuration window and return to the Correlation Composer main window.
8. Exit the Correlation Composer main window.



9. Save your changes when prompted to do so. This updates the NNM correlator fact store file.

Disabling the OV_NodeIF Correlator Group In releases prior to NNM 6.31, *node-status-events* were displayed in the Alarm Browser, and *interface-status-events* were configured as log-only so that they never displayed in the Alarm Browser. In this release of NNM, interface status events are usually displayed unless a catastrophic failure is detected (all interfaces within a node are down). If a catastrophic event is detected, the node alarm is displayed with the interface alarms nested beneath.

This procedure explains how to return to the old NNM behavior, if desired:

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. Select `OpenView`.
3. Sort the events using the `View:Sort->Sort by Event Name` command.
4. Edit the `OV_IF_Unknown` and `OV_IF_Down` events and change the `Category` field to `Log only`.
5. Edit the following events and change the `Category` field to `Status Alarms` instead of `Log only`:
   - OV_Network_Major
   - OV_Network_Critical
   - OV_Segment_Major
   - OV_Segment_Critical
   - OV_Node_Warning
   - OV_Node_Marginal
   - OV_Node_Major
   - OV_Remote_Mgr_Up
6. Select `[OK]`.
7. Save your changes using the `File:Save` command.
8. Exit using the `File:Exit` command.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0981
3740
Doc:

Once you have the events reconfigured, complete the following to disable the group of three OV_NodeIF correlators:

1. From any NNM submap, select Tools:HP OpenView Launcher. Select the [?] tab. Click:
   - Tasks
   - Event Correlation Management
   - Correlation Composer
   - Read the information in the *Disabling a Correlator* topic.
2. Access the Correlator Composer main window and disable the following three correlators. You must disable *all* of them:
   - OV_NodeIf_NodeDown
   - OV_NodeIf_NodeNotConnector
   - OV_NodeIF_PrimaryIFUnknown

Router/Switch Intermittent Status Changes

Identifies routers or switches that are reporting intermittent up/down status.

Behavior If an interface is continuously going down and then coming up, the ECS PairWise correlation (page 371) cancels the OV_IF_Down event when the OV_IF_Up event arrives. Therefore, you would never see these events in the NNM Alarm Browser.

This correlator (OV_Connector_IntermittentStatus) detects a repetitive interface down/up situation within a router or switch and generates an OV_Intermittent alarm if the OV_IF_Down event occurs the specified number of times (Count) during the specified time (Window Period).

Setting Parameters Complete the following steps if you want to review parameter definitions or modify parameters contained within the OV_Connector_IntermittentStatus correlator.



TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.
3. From the `ECS Configuration` window, select the `'default'` stream. Then, highlight `Composer` in the correlation table and select `Modify`. The `Correlation Composer` window appears in your web browser.
4. In the `Correlation Composer` window, right-click the `OV_Connector_IntermittentStatus` correlator and select `Modify` to display the `Description` tab.
5. Carefully read the information in the `Description` tab. Do not change any parameters other than those specifically listed:
   - Count
   - Window Period
6. Click the `Definition` tab to access the parameter settings. Click `[Help]` for information about each field.
7. After making the desired changes, close the correlator configuration window and return to the `Correlation Composer` main window.
8. Exit the `Correlation Composer` main window.
9. Save your changes when prompted to do so. This updates the NNM correlator fact store file.

HSRP Group Health

If you purchased the NNM Extended Topology product, six correlators work together to monitor HSRP group status within your networking environment. These six HSRP correlators are only provided with NNM management stations installed on a UNIX operating system. All six are required to calculate HSRP group health:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 0982
3740
Doc:

- OV_HSRP_StatusChange
- OV_HSRP_If
- OV_HSRP_NewNNMEtTopo
- OV_HSRP_ProcessIfEvent
- OV_HSRP_ProcessTrap
- OV_HSRP_Trap_DrillDown

Behavior The following sequence is followed:

1. Listens for any *interface-status-change* alarms from an interface that is assigned to an HSRP group. If detected, initiates an `OV_Force_If_Group_Status_Polling` event for the identified HSRP group.

   Also, listens for any HSRP *trap*. If detected, initiates an `OV_Force_If_Group_Status_Polling` event for the identified HSRP group.

2. Runs the correlator logic to calculate the health of the HSRP group being monitored by using the results of the `OV_Force_If_Group_Status_Polling`. Posts one of the following alarms in the NNM Alarm Browser reporting the results:

   - `OV_HSRP_Up`
     An HSRP group is completely normal, and providing routing functionality.
   - `OV_HSRP_State_Transition`
     An HSRP group has changed either its active router or standby router or both.
   - `OV_HSRP_Marginal`
     An HSRP group has all interfaces in either Unknown or Normal status only, with at least one in each status.
   - `OV_HSRP_Warning`
     An HSRP group has all interfaces with Unknown status, except for one with Normal status.
   - `OV_HSRP_Unknown`
     An HSRP group has all interfaces in Unknown IP status. Network problems exist between the management station and all the interfaces. This HSRP group is providing routing only if an



interface with an Unknown IP status is actually functioning, but due to other network problems, cannot be reached from the NNM management station.

- `OV_HSRP_Major`
  An HSRP group has one or more interfaces with Critical IP status, and one or more interfaces with Unknown IP status. There are no interfaces with a Normal IP status. This HSRP group is providing routing functionality only if an interface with an Unknown IP status is actually functioning, but due to other network problems, cannot be reached from the NNM management station.

- `OV_HSRP_Down`
  An HSRP group is completely down. No active or standby interfaces in this HSRP group could be identified.

3. Nests all related *interface-status-change* alarms, from members of an HSRP group, under the relevant `OV_HSRP_x` status alarm.

   Also, nests all related HSRP *traps* under the relevant `OV_HSRP_x` status alarm.

4. Restarts the HSRP analysis process if any change is detected within the NNM Extended Topology database during the time that the
   ated.

Setting Parameters Complete the following steps if you want to review parameter definitions or modify parameters contained within the
lator. This is the *only* correlator within the HSRP group of correlators that can be modified.

TIP There are several ways to access the event correlation features. For more information, from any submap, select `Tools:HP OpenView Launcher`. Select the `[?]` tab. Click `Tasks`, `Event Correlation Management`. Read the information under *Accessing the Event Correlation Configuration Windows*.

1. From any submap, select `Options:Event Configuration`. This launches the `Event Configuration` window.
2. From NNM's `Event Configuration` window, select `Edit:Event Correlation`. This brings up the `ECS Configuration` window.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0983
3740
Doc:

3. From the ECS Configuration window, select the 'default' stream. Then, highlight Composer in the correlation table and select Modify. The Correlation Composer window appears in your web browser.
4. In the Correlation Composer window, right-click the OV_HSRP_StatusChange correlator and select Modify to display the Description tab.
5. Carefully read the information in the Description tab. Do not change any parameters other than the one specifically listed:
   - NetmonGroupPollWaitTime (in seconds)
6. Click the Definition tab to access the parameter settings. Click [Help] for information about each field.
7. After making the desired changes, close the correlator configuration window and return to the Correlation Composer main window.
8. Exit the Correlation Composer main window.
9. Save your changes when prompted to do so. This updates the NNM correlator fact store file.

Correlator Fact Store File

The correlators, themselves, are all stored within one file. You should never edit this file directly; only make changes through the Correlator Composer window. The file is automatically included when ovbackup and ovrestore are run (see "Backup/Restore to Protect Your Investment of Time" on page 165). If you are planning to make experimental changes to the correlator parameter settings, you may wish to make a backup of this file before proceeding.

All correlator configurations are stored within one NNM fact store file. No other correlator fact store files are allowed within NNM:

Windows: `\NNM_install_dir\conf\ecs\circuits\Composer.fs`

UNIX: `$OV_CONF/ecs/circuits/Composer.fs`

Troubleshooting

For troubleshooting information about the Correlation Composer, see the following references:

- Access the following pdf format manual from the NNM main window, select `Help:Documentation:`

  — *HP OpenView Correlation Composer's Guide*

- Access the following pdf-format white paper file: `Developing_NNM_Event_Reduction.pdf`

  — *Windows:* `NNM_install_dir\Doc\WhitePapers\`

  — *UNIX:* `$OV_DOC/WhitePapers/`

  This information explains how to ensure that you do not break existing event reduction implementations. It also explains the process required for carefully merging your new correlators into the NNM correlator fact store file.

  You *might* need to install the white papers on Windows-based NNM management stations. See "White Papers" on page 75.

- The `TroubleshootingEventReduction.txt` file explains how to create event logs and play them back into the NNM event correlation system for testing purposes:

  — *Windows:* `NNM_install_dir\contrib\ecs\`

  — *UNIX:* `$OV_CONTRIB/ecs/`

  You *might* need to install the contib files on Windows-based NNM management stations. See "The contrib Directory" on page 74.

Creating Additional Correlators

NOTE

All de-duplication configurations, correlators defined within Correlation Composer, and all correlations defined within ECS must *work well together* on your NNM management station. Before you begin, it is critical that you print out and read the following white paper:

`Developing_NNM_Event_Reduction.pdf`

- *Windows:* `NNM_install_dir\Doc\WhitePapers\`
- *UNIX:* `$OV_DOC/WhitePapers/`

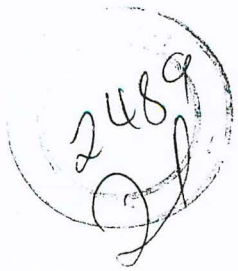
This information explains how to ensure that you do not break existing implementations.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0984
3740
Doc:

You *might* need to install the white papers on Windows-based NNM management stations. See "White Papers" on page 75.

Correlation Composer provides templates for the most commonly used correlation logic. These templates make it easy for you to develop your own:

- **Enhanced**
  Used to trigger the creation of one or more new alarms or to augment the information content of an alarm.
- **MultiSource**
  Used to define a relationship between an arbitrary number of alarms, potentially from different sources, that together form a logical set that identifies a problem. The set of alarms must all arrive within a defined time period. Upon completion of the set, the alarms can be discarded, modified, or a new more meaningful alarm can be generated.
- **Rate**
  Used to measure the number of incoming events within a defined time period. When a specified number is received, you can choose to discard the alarms and generate a new more meaningful alarm.
- **Repeated**
  Used to either discard duplicate alarms within a defined time period, or generate a new alarm each time an additional alarm is received so that the current number of alarms received can be specified in the alarm message text.
- **Suppress**
  Used when a specific category of alarms needs to be discarded, so that they never appear in the NNM Alarm Browser.
- **Transient**
  Used to detect a defined number of paired event occurrences within a defined time period, such as node up/node down. The paired events can be discarded, and a new more meaningful alarm can be generated.



NOTE Support for the correlator template named **User Defined** is not included. If you wish to use the Correlation Composer **User Defined** template, contact HP to purchase a Partner Care Extended support contract before beginning.

Correlators can be chained together to accomplish complex tasks (see "Router/Switch Health" on page 390 and "HSRP Group Health" on page 394 for examples of correlator groups).

If you wish to use external calls, contact HP to purchase a Partner Care Extended support contract before beginning.

Print out and read the following reference materials:

- Access the following pdf format manual from the NNM main window, select `Help:Documentation:`
  - — *HP OpenView Correlation Composer's Guide*
- Find the *csmerge* reference page in NNM's online help (or the UNIX manpage) for information about Correlation Composer's tool for merging new correlators (that are developed and tested in an isolated environment) back into the NNM correlator fact store file on your production NNM management station.
- Access the following pdf-format white paper file: `Developing_NNM_Event_Reduction.pdf`
  - — *Windows:* `NNM_install_dir\Doc\WhitePapers\`
  - — *UNIX:* `$OV_DOC/WhitePapers/`

  This information explains how to ensure that you do not break existing event reduction implementations. It also explains the process required for carefully merging your new correlators into the NNM correlator fact store file.
- The `TroubleshootingEventReduction.txt` file explains how to create event logs and play them back into the NNM event correlation system for testing purposes:
  - — *Windows:* `NNM_install_dir\contrib\ecs\`
  - — *UNIX:* `$OV_CONTRIB/ecs/`

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0985
3740
Doc:

Developing your own event correlators is a powerful option, but a non-trivial task. You should consider carefully whether this is something you want to do or whether it might be quicker, simpler, and cheaper to contract with a specialist to supply the correlator or correlators you need. Contact HP Consulting Service (see "HP Consulting Service" on page 76) or other system integrators for assistance.

To develop a correlator you need to:

- Learn to develop correlators through Correlation Composer training and/or documentation.
- Design and debug the correlator on an isolated test machine.
- Deploy the correlator to each NNM management station and collection station, as described in the `Developing_NNM_Event_Reduction.pdf` white paper.

When to Design Your Own Event Correlators

There are several key factors which indicate that a new correlator is required, or that an existing correlator needs to be reconstructed:

- No existing correlator provides the correlation you need.
- Parameters of an existing correlator need to be set to values that are outside the minimum and maximum allowed.
- The correlator requires access to external data (for example, to look up an inventory database) and therefore needs to use ECS annotation.
- Special event I/O requirements exist.

What is Involved

To design an effective correlator, you must:

- Understand typical network event patterns and what they mean.
- Know the architecture of your network management system.
- Identify external data access (ECS Annotation) requirements.
- Define the problem concisely in terms of filtering and time-related if-then statements.
- Determine if all data is available from the event's variable-bindings. If not determine if:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0986
3740
Doc:

— The external data is subject to change or is relatively stable.

— The required data is small enough to store in memory.

— The access speed and reliability is sufficient when extracting from your database (particularly if the database is remote).

Then, to develop the correlators, you need to:

- Set up a test platform.
- Develop sample logs of events. See the following file for information about how to create log files of events, and how to feed them into the NNM event correlation system in your test environment:

  — *Windows:*

  NNM_install_dir\contrib\ecs\TroubleshootingEventReduction.txt

  — *UNIX:*

  $OV_CONTRIB/ecs/TroubleshootingEventReduction.txt

- Your NNM support contract includes coverage for the use of the following Correlation Composer templates (provided that you do not invoke calls to APIs, libraries, scripts, or programs that are not included as part of the Correlation Composer product embedded within NNM):

  — Enhanced

  — MultiSource

  — Rate

  — Repeated

  — Suppress

  — Transient

  If you wish to use external calls, contact HP to purchase a Partner Care Extended support contract before beginning.

NOTE Support for the correlator template named **User Defined** is not included. If you wish to use the Correlation Composer **User Defined** template, contact HP to purchase a Partner Care Extended support contract before beginning.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0987
3740
Doc:

What is an SNMP Variable-Binding and How Do I Identify One?

When an SNMP event or trap is generated, a group of *variables* are included in the data. These variables are defined within the MIB file from which the event or trap originates. These variables are often referred to as *var-binds* because they are bound to a particular instance of the SNMP event or trap. The *SNMP variable-binding list* associated with a particular trap or event can provide a wealth of valuable information for you to use when creating your own event reduction strategies using NNM de-duplication, ECS correlation, or Correlation Composer correlator. This section explains a couple of ways to determine the available SNMP variable-bindings:

- "Look within the MIB File" on page 404.
- "Check the Alarm Message Text in the Alarm Browser" on page 405.

This section also explains the SNMP variable-bindings contained within the NNM *interface-status* and *node-status* alarms on page 405, because they can be very useful when defining event reduction implementations.

Look within the MIB File

The most direct way to determine the available SNMP variable-bindings is to locate the MIB file, open the MIB file with an ASCII editor, and look up the variable list for that particular trap or event. Check the documentation that came with your router or switch to locate the MIBs currently in use. If you do not have a copy of the MIB file, try using the MIB Depot web site. It may be a good resource for obtaining MIBs:

`http://www.mibdepot.com`

Otherwise, contact the vendor who created that particular MIB to obtain a copy.

See also "Exchanging Management Information" on page 27 for more information about MIB files.

Check the Alarm Message Text in the Alarm Browser

The alarm messages that display within the NNM Alarm Browser are controlled by the NNM Event Configuration settings. Usually the alarm message text includes a specified subset of available SNMP variable-binding values, as defined through the NNM `Event Configuration` window.

NOTE

For more information about NNM's Event Configuration feature and the choices for controlling alarm message text, see "Event Configuration Overview" on page 422. The event configuration settings are stored in the `trapd.conf` file.

You can easily modify the alarm message configuration settings. See "Variables and Special Characters Allowed" on page 436 for information about alarm message configuration choices. Some very useful alarm message variables are:

$# = prints out the total number of SNMP variable-bindings defined within the originating MIB of the incoming trap

$* = prints out the value passed with each of the defined SNMP variable-bindings

You can use the alarm message information as a starting point for your event reduction strategy, even if you do not have a copy of the MIB.

Any incoming traps whose MIBs have not been loaded into NNM (see "Loading MIBs in the MIB Database" on page 413) are displayed as generic traps called `EnterpriseDefault` (.1.3.6.1.4.1.*). The alarm message for the "generic" trap is defined as follows:

```
no format in trapd.conf. $# args: $*
```

Special SNMP Variable-Bindings within NNM Interface and Node Status Alarms

The OpenView interface and node status events include a wealth of information transported in SNMP variable-bindings. They are of particular interest when developing new de-duplication configurations, correlations, and correlators.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0988
3740
Doc:

NOTE The first variable in the SNMP variable-binding list is traditionally considered to be var-bind "1" (one). If you are developing a Correlation Composer correlator, the first variable in the SNMP variable-binding list is var-bind "0" (zero).

OpenView Interface Status Variable Bindings

- **Var-Bind 1:** The ID of application sending the event.
- **Var-Bind 2:** The hostname of the node that caused the event.
- **Var-Bind 3:** The HP OpenView object identifier of the node that caused the event.
- **Var-Bind 4:** The database name, if applicable.
- **Var-Bind 5:** A time stamp for when the event occurred.
- **Var-Bind 6:** The HP OpenView object identifier of the interface that caused the event.
- **Var-Bind 7:** The name or label for the interface that caused the event.
- **Var-Bind 8:** The IP address for the interface that caused the event, or "0" if unavailable.
- **Var-Bind 9:** The NNM management station ID.
- **Var-Bind 10:** Event correlation event UUID which identifies the primary failure.
- **Var-Bind 11:** Number of bits in the subnet mask of interface.
- **Var-Bind 12:** Locale neutral description of the interface (typically `ifAlias`). Note that the regular label for the interface is transmitted in var-bind 7 and so the presence of this new variable-binding allows the interface name (for example, lan0) and the interface `ifAlias` to be displayed simultaneously.
- **Var-Bind 13:** Locale neutral comma separated list of capabilities of the interface. For example, `isSwitch,isIPRouter`. Not all capabilities are included that may be available in NNM. The primary purpose of this interface is to identify connector devices within event reduction implementations.

2487

- **Var-Bind 14:** Name of the primary failure host if available.
- **Var-Bind 15:** Name of the primary failure entity if available.
- **Var-Bind 16:** The HP OpenView object identifier of primary failure entity if available.
- **Var-Bind 17:** Locale neutral description of the primary failure entity if available.
- **Var-Bind 18:** Locale neutral comma separated list of capabilities of the primary failure entity if available.

Variable-binding 14 through 18 describe the primary failure. For example, node C may be inaccessible due to a failure on router R. Node R would be the primary failure and node C would be the secondary failure. If node R is a primary failure then variable-binding 12 through 15 will describe node R and all the other variable-binding describe node C. If node C is a primary failure then all the SNMP variable-bindings describe node C. See "Connector Down Correlation" on page 361 and "Secondary Failure Polling" on page 192 for more information about designating primary and secondary failures.

OpenView Node Status Variable Bindings

- **Var-Bind 8:** Locale neutral comma separated list of capabilities of the entity. For example, `isSwitch`, `isIPRouter`.
- **Var-Bind 9:** Name of the primary failure host if available.
- **Var-Bind 10:** Name of the primary failure entity if available.
- **Var-Bind 11:** The HP OpenView object identifier of primary failure entity if available.
- **Var-Bind 12:** Locale neutral description of the primary failure entity if available.
- **Var-Bind 13:** Locale neutral comma separated list of capabilities of the primary failure entity if available.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0989
3740
Doc:

What is an SNMP Variable-Binding and How Do I Identify One?

12 Customizing Events: Doing It Your Way

RQS nº 03/2005 - CN -
CPMI - CORREIOS
0990
Fls. Nº
3740
Doc:

NNM allows you to take control of the event system through the use of several built-in applications. This chapter explains the purpose and use of each of these standard NNM applications:

- *SNMP MIB Browser* (page 412) and *Load/Unload MIBs* (page 413). Allows you to load and explore the functionality of the MIBs of your choosing. Once the MIB is loaded, you can query to determine the remote device's status, configuration, and available resources. You can also *set* MIB object values, provided you configured your network's community names into NNM.
- *DMI Browser* (page 417) and mapping MIFs (page 419). *NNM for the Windows operating system only:* Allows you to explore and access the functionality of a network device's Desktop Management Interface (DMI) service provider to which NNM subscribes. You can query to determine the remote device's status, configuration, and available resources.
- *Event Configuration* (page 422). Allows you to customize events, such as changing standard wording of MIB-generated error messages to more meaningful messages for your organization. You can control which Alarm Browser category the event is assigned to and also configure:
  - — Automatic Actions, such as dialing a pager, that execute whenever NNM receives a specific event. An Automatic Action command is tied to a particular event and can be limited to a specified list of IP hostnames and/or IPX addresses.
  - — Additional Actions that provide access to batch files or executables that your team uses occasionally. You configure the additional actions to show up in NNM's menu bar. Additional Actions can be applied to any alarm or specified groups of alarms.
- Information gathering applications:
  - — *MIB Application Builder* (page 443). Allows you to set up new menu items within NNM that provide access to your choice of useful MIB objects on an as-needed basis.

2474

— *Data Collection & Thresholds* (page 447).
Allows you to configure NNM to gather your choice of SNMP-MIB objects automatically (scheduling specific collections, establishing threshold monitoring of devices, and controlling what shows up in the Alarm Browser as a result).

— *MIB Expressions* (page 460).
You can create MIB expressions (mathematical formulas using MIB objects for analysis) to be used by Data Collection & Thresholds.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 0991
3740

SNMP MIB Browser

The SNMP MIB Browser is available from any submap under `Tools:SNMP MIB Browser`. The SNMP MIB Browser is useful for:

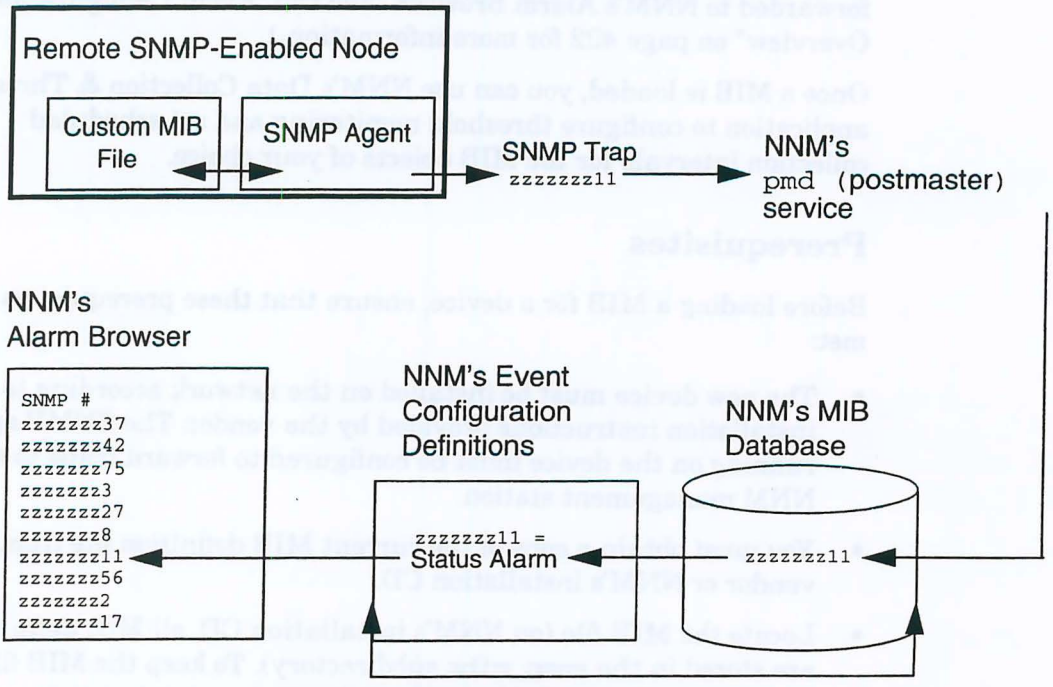
- Exploring your MIBs and their objects to become familiar with the network management capabilities that they provide. It serves as a useful reference tool. Type in any MIB number and view the description of what it is intended to do. Click on any leaf in any loaded MIB tree to view the MIB object's description.
- Querying MIB objects and viewing the returned instances for a network device that you selected on the submap or specified by typing in the IP address. You can view real-time MIB values for a selected node. You can also collect multiple instances by specifying a time interval for queries and display a graph of the results. The node for which you want to view MIB objects must support SNMPv1 or SNMPv2C.
- Setting MIB values on a network device. Prerequisites are:
  - The selected node on which you want to set MIB objects must support SNMPv1 or SNMPv2C.
  - The SNMP agent on the selected node must be configured to respond to SNMP SetRequests.
  - You must know the agent's SET-community name.

For more information about what you can do with NNM's SNMP MIB Browser, see the online help available within the SNMP MIB Browser window.

Loading MIBs in the MIB Database

When you install NNM, the standard SNMP version 1 and 2 MIBs are automatically loaded and configured for your convenience. Often devices on your network have their own custom vendor-specific MIBs that allow for monitoring specific aspects of that vendor's devices, and allow you to customize NNM to proactively manage the devices. If you are running extensible SNMP agents on your devices, the agents may be using custom MIB files. Before you can take advantage of these custom MIB capabilities, the MIB definition loaded into NNM's MIB database must match the version of the MIB in use on the device itself.

Figure 12-1 Configuring Custom MIB File Definitions



Either load the MIB file or manually define each event in Event Configuration

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 0992
3740
Doc:

NOTE To obtain the most recent version of a MIB file, check NNM's installation CD, contact the vendor who wrote the MIB file, or search the WWW (`ftp://ftp.isi.edu/mib/`) for quick access to the MIB file. Make sure the MIB definition loaded into NNM's MIB database matches the version of the MIB in use on the device itself.

The NNM installation CD includes hundreds of vendor-specific MIBs for your convenience. Simply load the MIBs that are relevant and useful for your specific network configuration. When you load a MIB into NNM's MIB database, that MIB's trap definitions are automatically added to the Event Configuration application so that you can customize NNM's use of each one. Use NNM's Event Configuration to identify which traps are forwarded to NNM's Alarm Browser. (See the "Event Configuration Overview" on page 422 for more information.)

Once a MIB is loaded, you can use NNM's Data Collection & Thresholds application to configure threshold monitoring and set scheduled collection intervals for the MIB objects of your choice.

Prerequisites

Before loading a MIB for a device, ensure that these prerequisites are met:

- The new device must be installed on the network according to the installation instructions provided by the vendor. The SNMP agent running on the device must be configured to forward traps to the NNM management station.
- You must obtain a copy of the current MIB definition file from the vendor or NNM's installation CD.
- Locate the MIB file (on NNM's installation CD, all MIB definitions are stored in the `snmp_mibs` subdirectory). To keep the MIB files sorted logically, the best practice is to create a subdirectory on the management station labeled with the vendor's name. Then copy the MIB file to that subdirectory on the management station before loading it. For example:
  - *Windows:* `install_dir\snmp_mibs\vendor\MIB`
  - *UNIX:* `$OV_SNMP_MIBS/vendor/MIB`

- The MIB must conform to *RFC 1155*, *RFC 1212*, *RFC 1902*, *RFC 1903*, or *RFC 1904*.
- If you have unloaded all the MIBs from the management station, it is recommended that you load MIB-II before you load an enterprise-specific MIB.

Procedure Tips

TIP

Close NNM's `Event Configuration` window prior to loading any MIB file. NNM automatically establishes a preliminary event configuration for you of each trap in the new MIB (provided the `Event Configuration` window is closed).

To load a MIB:

1. Place the NNM installation CD into the management station's CD drive. By default, NNM assumes you want a MIB from the installation CD. If the enterprise-specific MIB that you want to load is located elsewhere, you can enter the full path name to the file after opening the `Load/Unload MIB` window (in the field labeled `MIB File to Load`).
2. From any submap, select `Options:Load/Unload MIB:SNMP`. See NNM's online help from within the `Load/Unload MIB:SNMP` window for more information.
3. If the MIB file contains trap definitions, a dialog box appears asking if you would like to establish generic configurations for each trap in NNM's Event Configuration.

You can use the `Tools:SNMP MIB Browser` operation to view the new MIB objects. See "SNMP MIB Browser" on page 412.

If a MIB does not load properly, you will receive an error message. The problem could be:

- A syntax error in the MIB.

  The Load/Unload MIB program's error message identifies the MIB object where the error is occurring.
- Mismatched versions of the vendor's MIB.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0993
3740
Doc:

For example, the vendor's MIB on the NNM installation CD might not match the installed MIB version on the vendor's device on your network. In this case, obtain the MIB version that matches the MIB currently on the device.

In either case, contact the vendor to resolve the problem.

24-72

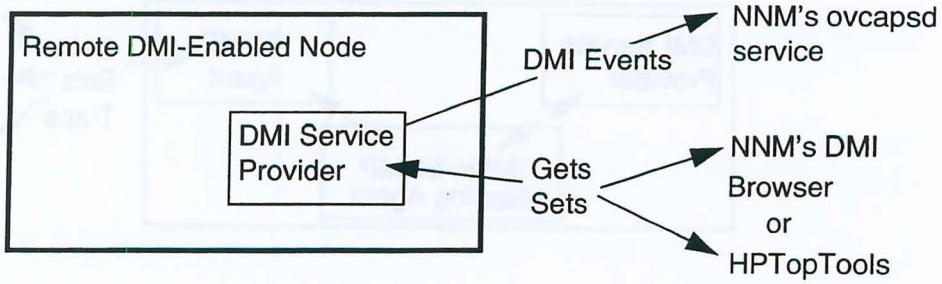
DMI Browser

The DMI Browser is available on NNM management stations running a Windows operating system. From any submap under `Tools:DMI Browser`. The DMI Browser allows you to view real-time MIF values for the DMI-enabled device currently selected on your submap.

Creating DMI Queries

In addition to DMI events, DMI also supplies GET and SET capabilities for some attributes.

Figure 12-2 Queries to a DMI Service Provider



- *DMI version 2:*

  To run DMI queries of devices running any DMI 2.0 service provider, use NNM's DMI Browser application. See the online help from within the DMI Browser for more information.

- *DMI version 1.1:*

  To run DMI queries of devices running the HP-RDMI service provider, use the HPTopTools application provided in the contributor's subdirectory on the NNM installation CD. See the `readme` file in the contributor's directory (see page 74).

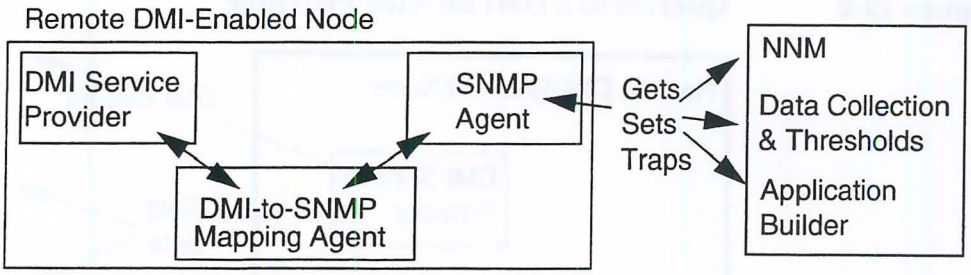
NOTE As an alternative, rather than communicating directly with the DMI service provider on your device, you can communicate with the DMI service provider indirectly through an SNMP agent installed on the

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0994
Doc: 3740

device along with a DMI-to-SNMP mapping agent. (Intel provides a mapping agent in their DMI 2.0 Service Provider Software Development Kit.) See the following figure.

The SNMP agent then handles all communications. Therefore, NNM tools such as the MIB Browser, MIB Application Builder, Data Collection & Thresholds application, and SNMP Grapher can be used to query DMI data via the DMI-to-SNMP mapping agent. NNM no longer subscribes to the DMI service provider to receive DMI events from devices running a DMI-to-SNMP mapping agent.

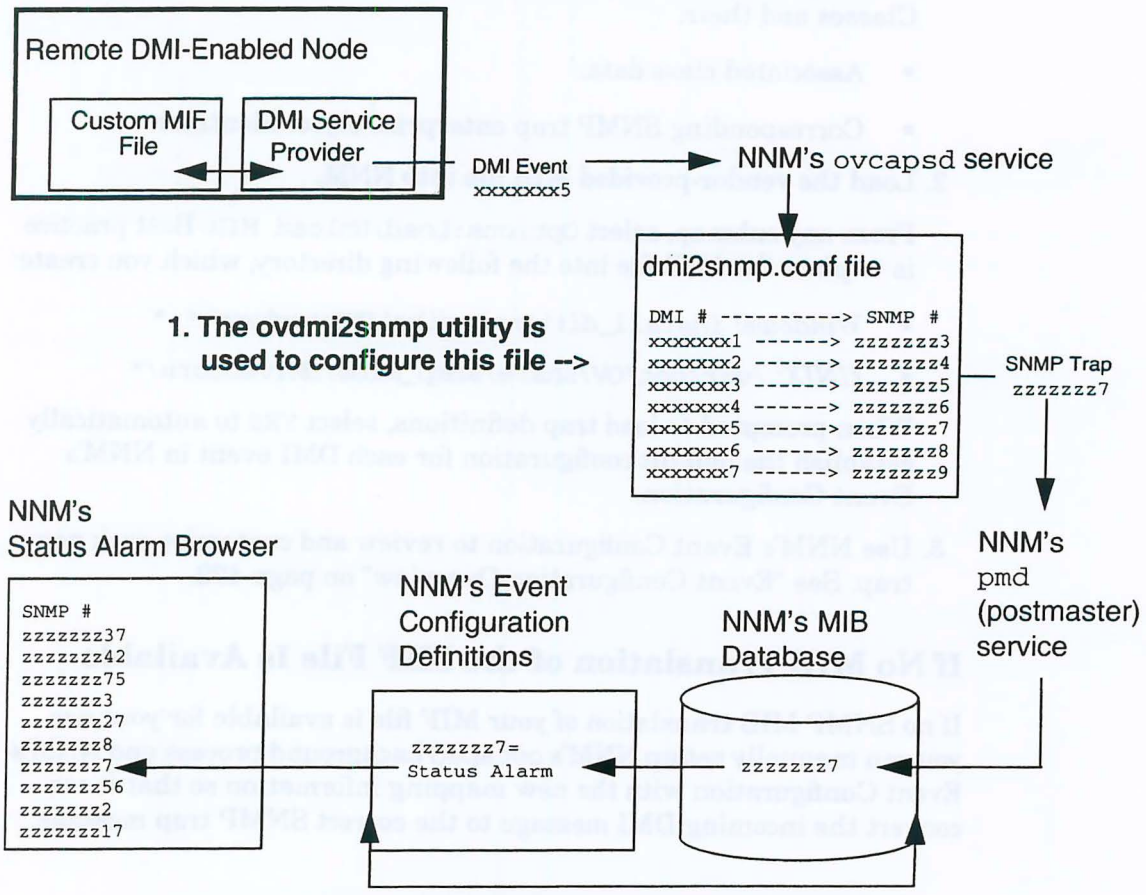
Figure 12-3 Bypassing a DMI Service Provider with an SNMP Agent



Loading DMI-to-SNMP Event Mappings

If your DMI service provider software is using a vendor-specific MIF instead of or in addition to the DMTF's standard MIF, you must configure NNM to understand the custom MIF events. Otherwise, a generic DMI event message (based upon the `dmiEventIndication` definition) is posted to the Alarm Browser each time the vendor-specific DMI event is received. To customize NNM's treatment of these events, you need to complete several steps, as shown in the following figure.

Figure 12-4 Configuring Custom MIF File Definitions



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0995
3740
Doc:

If a MIB Translation of the MIF File Is Available

The vendor of the DMI MIF may provide an SNMP MIB translation for your use. This allows you to load the MIB file and work with the event configurations in the same manner as you work with any SNMP MIB. However, an additional step is required. You must also provide the `ovcapsd` service with the new mapping information so that it can convert the incoming DMI event message to the correct SNMP trap message.

1. Update `ovcapsd`'s mapping file.

   A tool is provided to assist with this task. See the *ovdmi2snmp* reference page in NNM's online help for information about how to do this step. You will need to know each of the MIF's Event Generation Classes and their:

   - Associated class data.
   - Corresponding SNMP trap enterprise object identifier.

2. Load the vendor-provided MIB file into NNM.

   From any submap, select `Options:Load/Unload MIB`. Best practice is to place the MIB file into the following directory, which you create:

   - *Windows:* `install_dir\snmp_mibs\DMIvendors\*.*`
   - *UNIX:* `/var/opt/OV/share/snmp_mibs/DMIvendors/*`

   When prompted to load trap definitions, select `YES` to automatically establish the default configuration for each DMI event in NNM's Event Configuration.

3. Use NNM's Event Configuration to review and customize each new trap. See "Event Configuration Overview" on page 422.

If No MIB Translation of the MIF File Is Available

If no SNMP MIB translation of your MIF file is available for your use, you can manually set up NNM's `ovcapsd` background process and NNM's Event Configuration with the new mapping information so that it can convert the incoming DMI message to the correct SNMP trap message.

TIP MIF-to-MIB translation tools that convert any MIF file to a MIB file are available. Intel provides one in their DMI 2.0 Service Provider Software Development Kit.

1. Update ovcapsd's mapping file.

   A tool is provided to assist with this task. See the *ovdmi2snmp* reference page in NNM's online help for information about how to do this step. You will need to know each of the MIF's Event Generation Classes and their:

   - Associated class data.
   - Unique SNMP trap enterprise object identifier for the DMI Event Generation Class, which you choose.
   - SNMP trap ID, which is equal to the DMI Event ID.

   If your company has a registered "enterprise branch" assigned through the Internet Assigned Numbers Authority (IANA), use one of those available numbers. Otherwise, you may create a new OID that is unique to your installation under the `hpOVUserDefnEvents` branch (`1.3.6.1.4.11.2.17.9.xxxxx`).

2. Use NNM's Event Configuration to create a new trap configuration manually for each DMI event in your MIF file. Be sure to use the same corresponding SNMP trap enterprise object identifier and event/trap ID that you used in step 1 for each event. See "Event Configuration Overview" on page 422.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0996
3740
Doc:

Event Configuration Overview

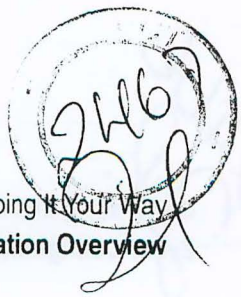
SNMP events are the building blocks of network management. Alarms are generated when NNM receives certain events. Thoughtful planning and use of event configuration will allow NNM to monitor your network effectively, taking the pressure off of you and your team. The Event Configuration application enables you to control and enhance the way in which NNM handles events. This section describes the following few suggestions among numerous possibilities:

- Control alarm message posting and text.
  - — Control which alarms are posted into NNM's Alarm Browser and which alarms are ignored.
  - — Assign an Alarm Browser category for the event's alarm.
  - — Customize alarm messages to make them more meaningful or to provide specific troubleshooting information to your team.
- Establish automatic actions for NNM to perform whenever a specific event is received (such as dialing a pager).
- Place access to a commonly used batch file command or any executable (such as launching commonly used troubleshooting tools) on NNM menus for your team's convenience.

For more ideas about customizing NNM's event system, review the choices in the `Event Configuration` window and refer to NNM's online help available from within the `Event Configuration` window.

Prerequisites

- The MIB for which you want to configure events must be loaded into NNM's MIB database. From any submap, select `Options:Load/Unload MIBs:SNMP` to display the list of all MIBs currently in NNM's MIB database. If the MIB you wish to use is not loaded, see "Loading MIBs in the MIB Database" on page 413.
  - — A generic configuration for each trap from the MIB is automatically set up in NNM's event configuration feature when you load the MIB.



— MIB objects that are not *traps* can be manually set up in NNM's Event Configuration program. You can then generate GET, SET, or data collection events based upon the new event configuration.

- Make sure that you understand the enterprise-specific MIB. To configure events, you need to understand the trap definitions for the device and what they do. Most device vendors include documentation about their enterprise-specific traps with their product. This documentation typically describes the trap and when the trap is generated. In addition, some vendors include overview information describing strategies for how to manage their specific device. The vendor documentation can give you the conceptual understanding that you need to configure effective event formats and actions.

Event Configuration Window

TIP You cannot configure events from the NNM's web interface. However, the web-based Alarm Browser displays the alarms resulting from your event configurations.

To display the `Event Configuration` window:

- From any Alarm Browser window, select `Actions:Configure Event`.
- From any submap, select `Options:Event Configuration`.

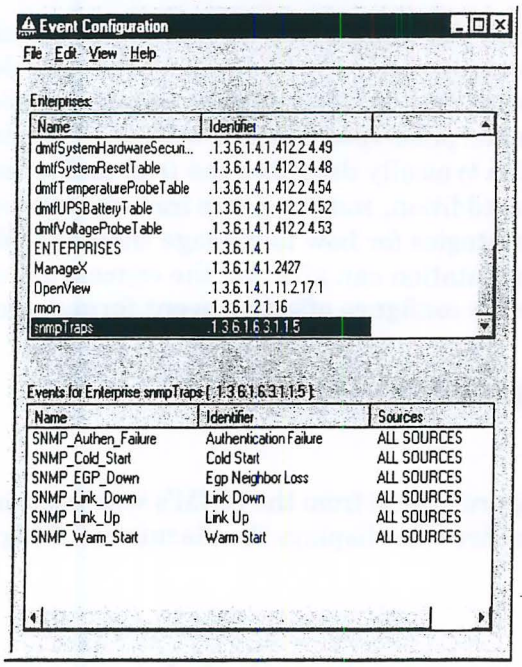
The `Event Configuration` window contains an `Enterprise Identification` section, an `Event Identification` section, and a menu bar.

To close the `Event Configuration` window, select `File:Close`. Be sure to save your changes as you exit. Event configurations are stored in the `trapd.conf` file.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0997
3740
Doc:

Figure 12-5 shows the `Event Configuration` window.

Figure 12-5 Event Configuration Window



Enterprise Identification List

The MIB files that define specific events are supplied by a number of vendors (enterprises). The list in the top half of the `Event Configuration` window identifies the enterprise that supplied the MIB whose event you wish to configure. For example, if you are configuring NNM to communicate with a Cisco Router's SNMP agent, then the event configuration should be defined under the corresponding Cisco enterprise identification (`.1.3.6.1.4.1.9.`).

Events generated by NNM processes (such as `netmon` or `snmpCollect`) will use the HP OpenView enterprise identifier.

NOTE If you are configuring a threshold event created by the HP OpenView SNMP Data Collector, you should configure it under the `OpenView` enterprise name (`.1.3.6.1.4.1.11.2.17.1`), regardless of which node the Data Collector is polling. Even if the event is for a Cisco device

exceeding a threshold, the enterprise ID of the event will be `OpenView`, not Cisco, since the event is coming from the HP OpenView SNMP Data Collector.

Select the enterprise associated with the events you want to configure. Each item in the list contains:

`Enterprise Name`

A convenient and meaningful representation of the Enterprise ID used by the Event Configuration application. This label usually corresponds to the enterprise name as defined by the enterprise-specific MIB.

`Enterprise ID`

The system object ID in dotted notation. The ID corresponds to the value supplied with the trap. If no traps are defined for an enterprise, the application will generate a generic message using the `ENTERPRISES` enterprise. `ENTERPRISES` acts as a default.

You can add or delete enterprises using:

- *Windows:* The `Edit:Events` menu item.
- *UNIX:* The `Edit:Configure` menu item.

Event Identification

The list in the bottom half of the `Event Configuration` window identifies events associated with the enterprise selected in the top half. By default, NNM configures all standard SNMP trap definitions and automatically supplies a generic configuration of all traps present in any MIB that you load into the MIB database. You may configure any event (trap, GET, SET, or custom data collection event). If no enterprise is selected, the list will be blank.

`Event Name`

The name used to reference the event (can be anything meaningful to you).

`Event Identifier`

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0998
3740
Doc:

The event identifiers may be shown as generic and specific traps or as object identifiers, depending on how you have the `View:Event Identifiers` menu set up.

If the menu is set up to display the events as SNMP traps, then the generic traps 0 through 5 are defined by SNMP and assume a specific trap of 0. The generic trap 6 is the enterprise-specific trap. `EnterpriseDefault` provides default trap handling for all traps for an enterprise. The specific traps are defined for this enterprise. The vendor defines what the specific trap numbers mean.

The object identifier for an event is in dotted decimal format. For enterprise-specific events, this identifier is the concatenation of an enterprise object ID, 0, and the specific number (for example, `1.3.6.1.4.1.11.2.17.1.0.58916872`). For SNMP generic traps (0-5), this identifier is the concatenation of the `snmpTraps` enterprise object ID and the generic trap number incremented by one (for example, `1.3.6.1.6.3.1.1.5.5` for the `SNMP_Authen_Failure` generic trap).

The default is to view the events as object identifiers.

`Sources`

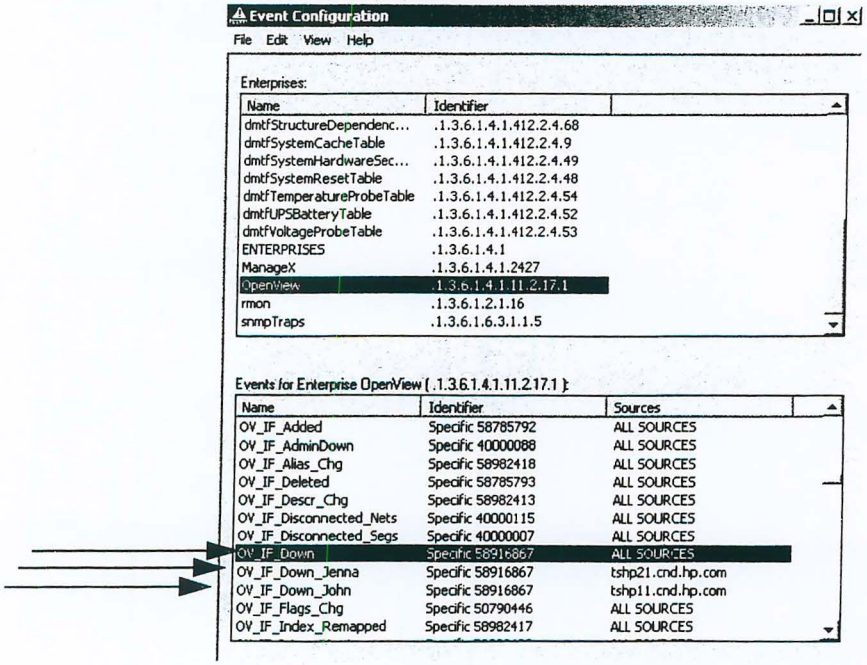
The potential sources for the event (such as nodes), or `ALL SOURCES` if this event is to be used regardless of the source of the event.

NNM allows you to configure events in a number of ways and even add new events. The preconfigured event definitions provide a starting point for your use.

For example, you can use the `OV_IF_Down` MIB object to monitor your most critical routers. For this example, assume that John is in charge of the routers at site A, and Jenna is in charge of the routers at site B. You can copy the preconfigured `OV_IF_Down` and rename it to `OV_IF_Down_John`; change the source field to indicate router interfaces for which John is responsible; then configure NNM to page John whenever a router for which he is responsible goes down. Now repeat the procedure and create another event configuration that you name

OV_IF_Down_Jenna; change the source field to indicate router interfaces for which Jenna is responsible; then configure NNM to page Jenna whenever a router for which she is responsible goes down.

Figure 12-6 Copying Preconfigured Events to Create New Ones



Vendors provide MIB objects that allow you to take this concept a step further and proactively monitor performance on your critical devices. You can configure events to alert you to potential trouble, rather than waiting for a device to fail and send a trap to the management station.

You can add, modify, copy, or delete events using:

- *Windows:* Select the event, then select the `Edit:Events` menu item.
- *UNIX:* Select the event, then use the `Edit` menu.

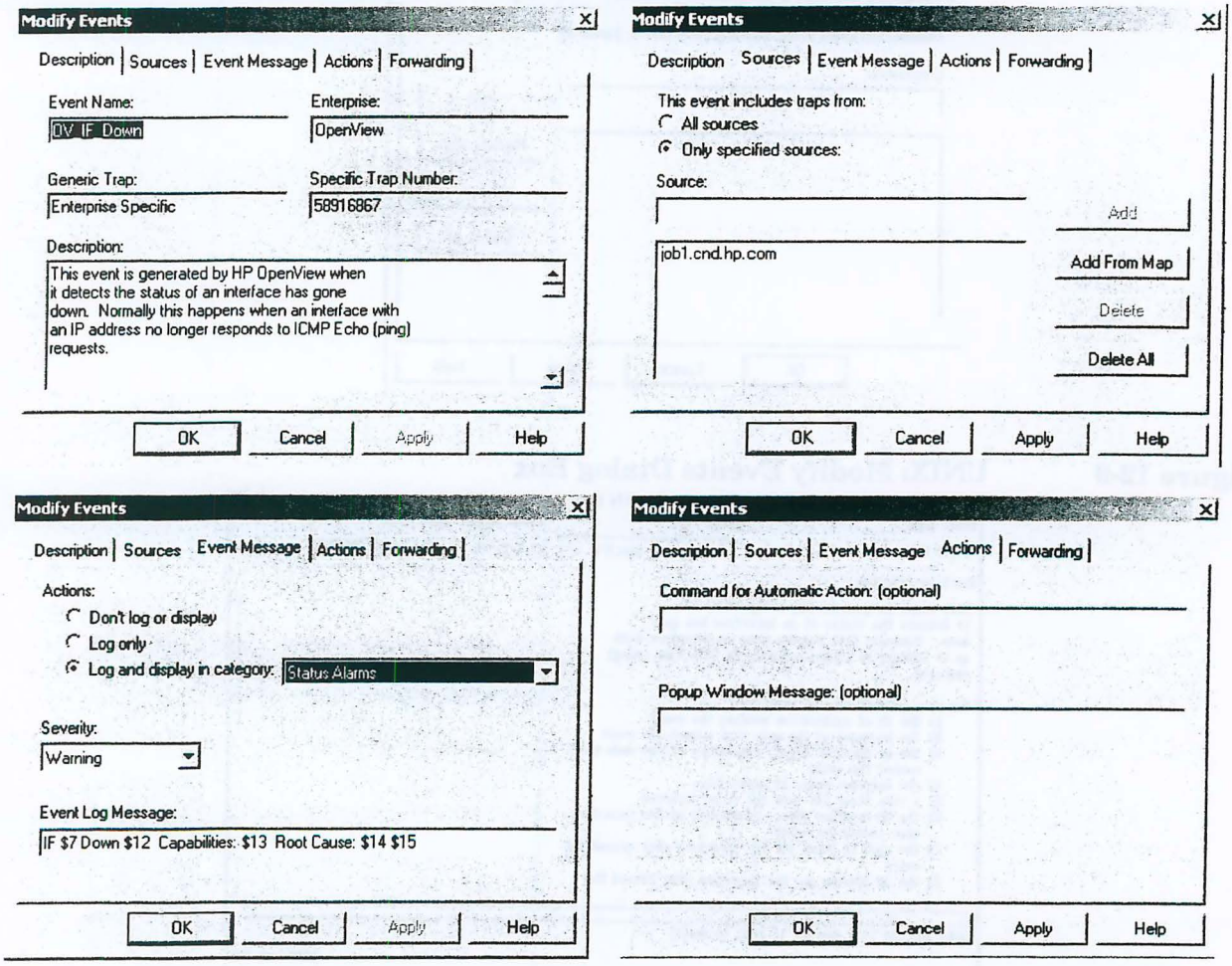
Events can be customized in a wide variety of ways to meet your team's needs. Review the choices in the `Event Configuration` window and refer to NNM's online help available from within this window for more information and ideas.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 0999
3740

The customizations that you make to event configurations are written to the `trapd.conf` file. Refer to the *trapd.conf* reference page in NNM's online help (or the UNIX manpage) for more information.

This section covers *only a few* of the possibilities for configuring events.

Figure 12-7 Windows: Modify Events Property Sheet (5 tabs)



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1000
3740
Doc.

Figure 12-8 **Windows: Modify Events Property Sheet, continued**

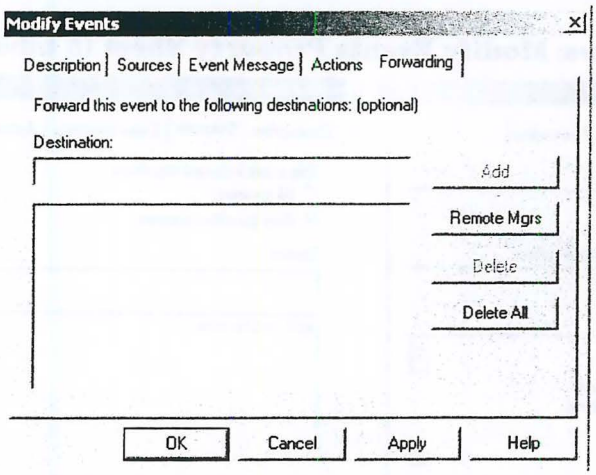
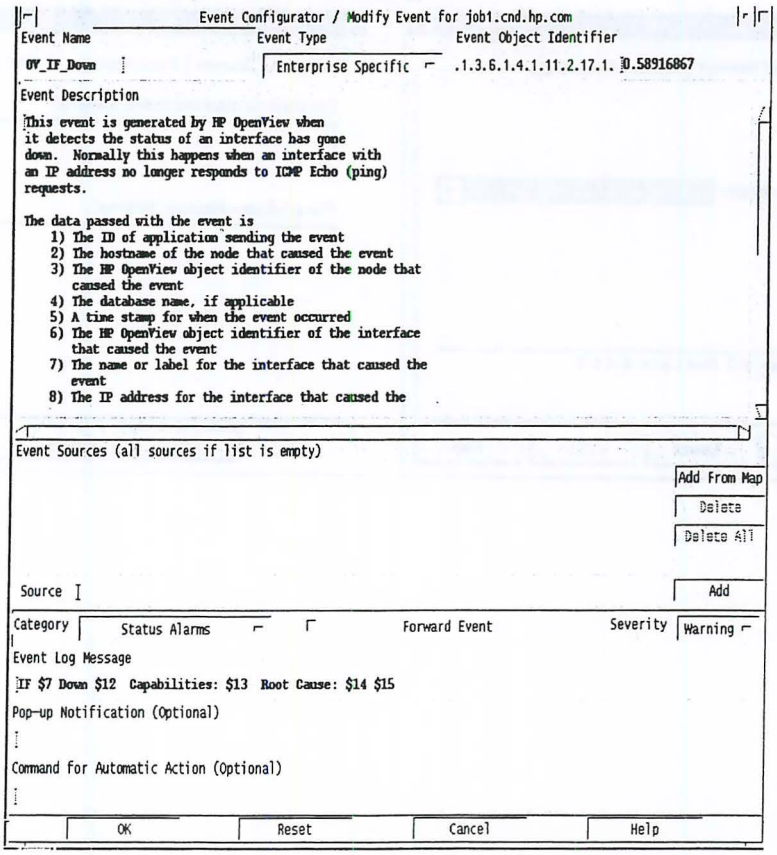


Figure 12-9 **UNIX: Modify Events Dialog Box**



Controlling Alarm Message Posting and Text

You can control how NNM handles specific alarms, such as:

- Control which alarms are posted into NNM's Alarm Browser and which alarms are ignored.
- Assign an Alarm Browser category for the event's alarm.
- Customize alarm messages to make them more meaningful or to provide specific troubleshooting information to your team.

Selecting Events to Post in the Alarm Browser

1. Ensure that the prerequisites have been met (see "Prerequisites" on page 422). Then, open the `Event Configuration` window:
   - From any Alarm Browser window, select `Actions:Configure Event`.
   - From any submap, select `Options:Event Configuration`.
2. In the top half of the window, select the enterprise that supplied the MIB file that defines the SNMP event that you wish to configure. In the bottom half of the window, select the specific SNMP event:
   - *Windows:* Select `Edit:Events->Modify`, then select the `Event Message` tab.
   - *UNIX:* Select `Edit:Modify Event`.
3. To ensure that NNM posts the alarm in the Alarm Browser, make a selection in the `Category` field. Also make a selection in the `Severity` field to control the severity rating that NNM assigns to this alarm.

TIP See "Creating a New Alarm Category" on page 349 for information about creating your own custom categories.

Changing Event Configurations

1. Ensure that the prerequisites have been met (see "Prerequisites" on page 422). Then open the `Event Configuration` window:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1001
Doc 3740

- From any Alarm Browser window, select `Actions:Configure Event`.
- From any submap, select `Options:Event Configuration`.

2. In the top half of the window, select the enterprise that supplied the MIB file that defines the SNMP event that you wish to configure. In the bottom half of the window, select the specific SNMP event:
   - *Windows:* Select `Edit:Events->Copy`, then select the `Event Message` tab.
   - *UNIX:* Select `Edit:Copy Event`.
3. Type in a name for the new configuration that is meaningful to you.

TIP Copy the original name and add a meaningful extension so that both events remain together in the event list.

4. Change the source so that your customization only applies to specific host names or IP addresses.
5. To ensure that NNM posts the alarm in the Alarm Browser, make a selection in the `Category` field. Also make a selection in the `Severity` field to control the severity rating that NNM assigns to this alarm.

TIP See "Creating a New Alarm Category" on page 349 for information about creating your own custom categories.

6. To enhance the text of the alarm message so that it is more meaningful to your team, in the `Event Log Message` field, type in the new information. Follow the guidelines in "Variables and Special Characters Allowed" on page 436.

   For more information, see NNM's online help from within the `Event Configuration` window.

The customizations that you make to event configurations are written to the `trapd.conf` file. Refer to the *trapd.conf* reference page in NNM's online help (or the UNIX manpage) for more information.

Example Custom Alarm Message To configure an event to post the following entry in the Alarm Browser:

```
Inconsistent subnet mask 255.0.0.0 on interface lan0,should
be 255.255.248.0
```

The entry in the `Event Log Message` field would be:

```
Inconsistent subnet mask $9 on interface $7,should be $10
```

Defining Automatic Actions for Events

You can define actions for NNM to perform automatically whenever a specific trap (event) is received. Follow the directions in NNM's online help available from within the `Event Configuration` window.

NOTE

By default, NNM only performs commands that are trusted commands. If the command you specify is not in the `trustedCmds.conf` directory, then NNM generates an event and the action is not executed. See the *ovactiond* reference page (or the UNIX manpage) for more information. Trusted commands are listed in the following directory.

- *Windows:* *install_dir*`\conf\trustedCmds.conf`
- *UNIX:* `$OV_CONF/trustedCmds.conf`

1. Ensure that the prerequisites have been met (see "Prerequisites" on page 422). Then open the `Event Configuration` window:
   - From any Alarm Browser window, select `Actions:Configure Event`.
   - From any submap, select `Options:Event Configuration`.
2. In the top half of the window, select the enterprise that supplied the MIB file that establishes the SNMP trap that you wish to configure. In the bottom half of the window, select the specific SNMP trap:
   - *Windows:* Select `Edit:Events->Copy` (or `Modify`), then select the `Additional Actions` tab.
   - *UNIX:* Select `Edit:Copy Event` (or `Modify Event`).
3. Type in a name for the new configuration that is meaningful to you.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1002
3740
Doc:

TIP Copy the original name and add a meaningful extension so that both events remain together in the event list.

4. Change the source so that your customization only applies to specific host names or IP addresses.
5. To configure NNM to take action automatically whenever this event is received by the Alarm Browser, in the `Command for Automatic Action` field, type in your instructions using "Variables and Special Characters Allowed" on page 436.

   For more information, see NNM's online help from within the Event Configuration windows.

The customizations that you make to event configurations are written to the `trapd.conf` file. Refer to the *trapd.conf* reference page in NNM's online help (or the UNIX manpage) for more information.

Example Commands for Automatic Action

Any program invoked from the Automatic Actions field must run to completion with no user input.

NOTE By default, the following examples are not in the `trustedCmds.conf` directory. As root or administrator, you must add to the `trustedCmds.conf` directory any commands that you want to execute as automatic actions. You cannot use special characters such as & and | in your automatic action commands. See the *ovactiond* reference page (or the UNIX manpage) for more information. Trusted commands are listed in the following directory.

- *Windows:* *`install_dir`*`\conf\trustedCmds.conf`
- *UNIX:* `$OV_CONF/trustedCmds.conf`

Example 1: Send a message to a pager You can specify a paging command as an automatic action. Refer to the "Configuration: Recommended Paging Software" section of the NNM Release Notes for specific information about HP's recommended paging software.

The following is general information about scripting an automatic action to launch pager software.

1. Install and test the pager software.
2. Create a batch file that invokes the pager software and place it in the following directory. The program invoked by the batch file must run to completion with no user input:

   Windows: `install_dir\bin`

   UNIX: `$OV_BIN/`
3. Identify the event that should initiate a pager action, as follows: Select `Options:Event Configuration`. The `Event Configuration` dialog box appears. Select `Edit:Events->New` to define a new event for the selected node.
4. In the `Command for Automatic Actions (optional)` field, enter the name of the batch file.

NOTE

Windows only: If you need to use the backslash character (for example in the batch file's path), use "\\" (double backslash).

5. You can generate a test event using `SNMPNOTIFY` on another system to trigger this event and verify that the pager message was successfully sent.

Example 2: Pop-up Window Message This example pops up a message on the management station's monitor.

Specify the following in the `Popup Window Message` field:

```
An authentication failure at IPaddress:$3, community:$4
```

The output will be:

```
Authentication failure at IPaddress:15.2.77.99,
community:admin
```

Example 3: Set an Object's Status Color This example assumes that you have installed the `contrib` files (see "The contrib Directory" on page 74). Type the following command, all on one line, in the `Command for Automatic Action` field. This event status color change will be overwritten by the `ipmap` process if the object is managed by HP

2455
PROC nº 03/2005 - CN
CPMI - CORREIOS
FLS. Nº 1003
3740
DOC.

OpenView. It is suggested that a symbol in the object's submap be modified instead. See the *trapd.conf* reference page (or the UNIX manpage) for a discussion of the parameters used in an `snmptrap` command to change the status color of an object on the map.

Windows: If you need to use the backslash character (for example in the batch file's path), use "`\\`" (double backslash). Note the path statement is case-sensitive.

```
\\install_dir\\contrib\\NNM\\setStatus\\setStatus $A Testing
```

UNIX:

```
/usr/OV/contrib/NNM/setStatus/setStatus $A Testing
```

Example 4: Send an Audible Alert This example assumes that you have installed the `contrib` files (see "The contrib Directory" on page 74). Type the following command, all on one line, in the `Command for Automatic Action` field. This event will only be heard if an `xnmevents` process is running. See the *trapd.conf* reference page (or the UNIX manpage) for more information.

Windows: If you need to use the backslash character (for example in the batch file's path), use "`\\`" (double backslash).

```
\\install_dir\\contrib\\NNM\\ringBell\\ringBell $A "User
Alert"
```

UNIX:

```
/usr/OV/contrib/NNM/ringBell/ringBell $A "User Alert"
```

Variables and Special Characters Allowed

When customizing event configuration's `Event Log Message`, Popup Window Message (in UNIX called Pop-up Notification), and `Command for Automatic Action` fields, use special "$ variables" to present data that was received with the event. You may enter several special characters to give you control of the formatted output. The format can include the following standard C `printf` formats, which will be converted to their ASCII equivalent. (See also NNM's online help available from the `Event Configuration` window for more information.)

Note that nonprintable characters are converted to their `\ooo` equivalent for display in the event browser or when passed to the operator-initiated (manual) actions. The two exceptions are that a tab is displayed as `\t` in the event browser and as spaces in pop-up messages. A newline is

displayed as \n in the event browser and as a new line in pop-up messages. All nonprintable characters are passed unconverted to automatic actions executed by ovactiond.

Special Characters

\a	Alert (bell) character
\b	Backspace
\f	Formfeed
\n	Newline
\r	Carriage return
\t	Horizontal tab
\v	Vertical tab
\\	Backslash
ooo	Octal number, first character must be 0 or 1 and second and third numbers must be 0-7
\x*hh*	Hex number, both *hh* characters must be [0-9][a-f][A-F]

You can also include information from the incoming event by using the $[*arg*] format specification.

Special Information Variables

You can also include information from the incoming event by using the $[*arg*] format specification. The following $ variables are valid regardless of the type of event (SNMPv1, SNMPv2C, CMIP, GENERIC):

$[*arg*]

$x	Print the date the event was received using the local date representation (*UNIX only:* see the %x option in the *strftime* manpage).
$X	Print the time the event was received using the local time representation (*UNIX only:* see the %X option in *strftime* manpage).
$@	Print the time the event was received as a number of seconds since the Epoch (Jan 1, 1970) using the time_t representation.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1004
3740
Doc:

`$O`	Print the name (object identifier) of the received event.
`$o`	Print the name (object identifier) of the received event as a string of numbers.
`$V`	Print the event type, based on the transport the event was received. Currently supported types are `SNMPv1`, `SNMPv2C`, `CMIP`, and `GENERIC`.
`$r`	Print the implied source of the event in textual form. This may not be the true source of the event if the true source is proxying for another source, such as when a monitoring application running locally is reporting information about a remote node.
`$ar`	Same as `$r` except print the IP address instead of the name.
`$R`	Print the true source of the event in textual form. This value is inferred via the transport mechanism which delivered the event. If the event was forwarded, this will display the address of the remote event framework (that is, remote `pmd`'s system).
`$aR`	Same as `$R` except print the IP address instead of the name.
`$c`	Print the category in which the event belongs.
`$s`	Print the severity of the event.
`$N`	Print the name (textual alias) of the event format specification used to format the event, as defined in `trapd.conf`.
`$F`	Print the textual name of the remote event framework's system (that is, remote `pmd`'s system) if this event was forwarded; otherwise, print the local system's name.
`$U`	Universally Unique Identifier (UUID) of the current event in the form of a long string of alphanumeric characters.
`$$`	Print the `$` character.

Sequential Attribute Variables

The following $ variables are used to access the sequential attributes that were received with the event. Each event has attributes associated with it (possibly none). They are accessed using the $*n* notation, where *n* is the positional attribute, with 1 being the first possible attribute. The printing format is based on the ASN.1 type of the attribute. These attributes are equivalent to the variable bindings in an SNMP trap.

$[*arg*]

$#
: Print the number of attributes in the event.

$*
: Print all the attributes as [*seq*] *name* (*type*): *value* strings, where *seq* is the attribute sequence number.

$*n*
: Print the *n*th attribute as a *value* string.

$-*n*
: Print the *n*th attribute as a *name* (*type*): *value* string.

$+*n*
: Print the *n*th attribute as a *name*:*value* string.

$>*n*
: Print all attributes greater than *n* as *value* strings; useful for printing a variable number of arguments. $>0 is equivalent to $* without sequence numbers, names, or types.

$>-*n*
: Print all attributes greater than *n* as [*seq*] *name* (*type*): *value* strings.

$>+*n*
: Print all variables greater than *n* as *name*: *value* strings.

SNMP-Specific Variables for Traps

The following variables are valid only for events created from SNMPv1 or SNMPv2 traps:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1005
3740
Doc:

`$[arg]`	
`$C`	Print the trap community string.
`$E`	Print the trap enterprise as a text string, if possible; otherwise, as in the `$e` arg below.
`$e`	Print the trap enterprise as an object ID string of numbers.
`$A`	Print the trap agent address as defined in the trap protocol data unit (PDU). Note that this may be different from the agent that actually sent the event. If the name server knows about this node, the node name will be printed; otherwise, the IP address will be printed.
`$aA`	Same as $a except print the IP address instead of the name.
`$G`	Print the trap's generic-trap number.
`$S`	Print the trap's specific-trap number.
`$T`	Print the trap's `sysUpTime` time-stamp. This is the remote machine's time in hundredths of a second between the last reinitialization of the device and the generation of the trap; it is *not* the time the event was received.

Obsoleted/Reserved Variables

The following variables are reserved or obsoleted. Their use may cause unpredictable results, and should not be used:

`$[arg]`	
`$L`	Obsolete, do not use.
`$i`	Do not use.
`$I`	Do not use.
`$t`	Do not use.
`$=`	Do not use.

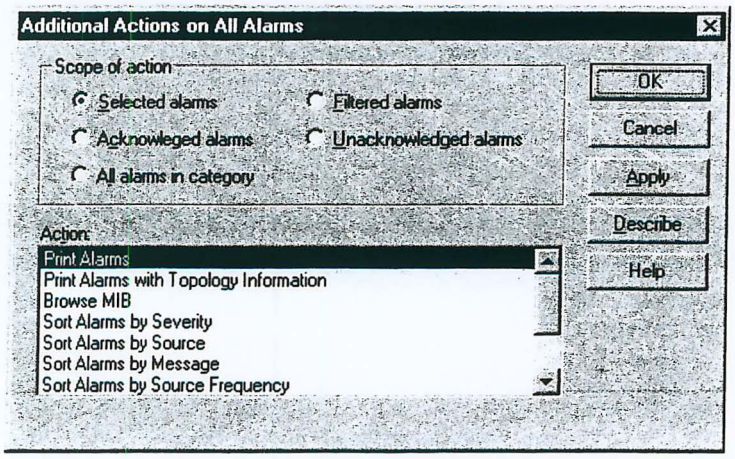
Defining Additional Actions

NOTE This feature is not available through NNM's web interface. It is available on the management station and from remote consoles.

You can configure NNM to provide easy access to batch files or executable files that your team commonly uses. An example might be to forward the event to a trouble ticket system, to send email regarding the event, or to archive the event. You provide the programs for the additional action.

The `Additional Actions` window is accessed from any Alarm Browser window under `Actions:Additional Actions`.

Figure 12-10 Additional Actions



Additional Actions are not the same as *Automatic Actions* for events. The difference between an Additional Action and an Automatic Action is that the Automatic Action automatically runs when the event is received; whereas the Additional Action is run only at the operator's choosing. The Automatic Action is tied to a particular event, whereas an Additional Action can be run on any event.

Although the additional actions list is accessed through any Alarm Browser window, you modify the list of possible additional actions through the `Event Configuration` window.

To display the `Event Configuration` window:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1006
3740
Doc:

- From any Alarm Browser window, select `Actions:Configure Event`.
- From any submap, select `Options:Event Configuration`.

To configure an additional action:

- *Windows:* Select `Edit:Additional Actions`.
- *UNIX:* Select `Edit:Configure->Additional Actions`.

See NNM's online help available within the `Additional Actions` dialog box for more information. For an explanation of how to write an additional action, see the *trapd.conf* reference page in NNM's online help (or the UNIX manpage).

2427

Using the MIB Application Builder

The MIB Application Builder application of Network Node Manager enables you to set up easy access to MIB objects that your team commonly uses. The application that you create displays real-time gathered MIB instances. You select the manner in which the information should be presented: form, table, or graph. You set up access to your application through NNM's map menu structure.

For examples of what is possible, see the standard applications provided in the map menu structure under:

- `Configuration:System Information`

  This example shows real-time instances of six MIB objects in *form* format.

- `Fault:Test IP/TCP/SNMP`

  This example shows real-time instances of four MIB objects in *table* format.

- `Performance:Network Polling Statistics`

  This example shows real-time instances of six MIB objects in *graph* format. You specify the interval between polling instances.

The MIB Application Builder is helpful when you want to monitor specific MIB objects on an as-needed basis. By integrating your MIB application in the menu bar, you have a convenient way to monitor multivendor network devices. For example, you could create multiple MIB applications under NNM's Performance menu that access the vendor-specific MIBs supplied by each router vendor:

```
Performance:Routers->HP
Performance:Routers->Cisco
Performance:Routers->Wellfleet
Performance:Routers->Proteon
```

TIP Use NNM's Data Collection & Thresholds application (see page 447) if you want to automate the collection, rather than use it on an as-needed basis.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1007
3740
Doc:

Prerequisites

- Make sure the enterprise-specific MIB you will use to build your MIB application is loaded in the MIB database on the management station and the same version is on the device itself. (The `Options:Load/Unload MIBs:SNMP` dialog box lists all MIB modules currently loaded in the MIB database.) If the enterprise-specific MIB is not loaded, see "Loading MIBs in the MIB Database" earlier in this chapter.
- Make sure you understand the enterprise-specific MIB. To build useful applications, you need to understand the definitions of the MIB objects and what they do.

  Most device vendors include documentation about their enterprise-specific MIB with their product. This documentation typically describes the MIB objects and what the objects do. In addition, some vendors include overview information describing strategies for managing their specific devices. The vendor documentation can give you the conceptual understanding that you need to build an effective application.

  Note that enterprise-specific MIBs are device-specific. For example, if you build an application for a Cisco router using a Cisco MIB, you probably cannot use that application on a Wellfleet router.

NOTE Familiarize yourself with the MIBs by using the `Tools:SNMP MIB Browser` operation.

- Design your application. Consider the following:
  - — Which objects do you want to include in your application?
  - — Which objects make sense to group?
- Should you graph this information or put it in a table or form? You can choose from one of three presentation styles -- Form, Table, or Graph.
  - — `Form`. Use this option to display MIB information that is not part of a table and does not change very often (for example, system description).

The information associated with each MIB object is displayed one MIB object per line with the MIB value to the right of the MIB label. Any type of MIB object is allowed.

— `Table`. Use this option to display MIB information that constructs a logical table in the MIB (for example, a routing table).

The MIB objects are laid out horizontally, making up the columns of the table. Each entry in the MIB table makes up the rows of the application table. Any type of MIB object is allowed.

NOTE You cannot create table applications which consist of MIB fields from multiple MIB tables.

— `Graph`. Use this option to display numeric MIB information that fluctuates over time (for example, interface statistics). Only numeric MIB values are allowed.

- Plan the menu structure. For example, if you have multiple devices from different vendors, you may want to organize the menu structure such that you have all MIB applications for routers grouped under one menu.

Procedure Tips

Refer to NNM's online help available within the `MIB Application Builder` window for information about how to add, modify, or delete applications.

When you build your applications, keep the following in mind:

- You must provide a unique name for the MIB application.
- You can perform MIB operations on one or more MIB objects at a time.
- Menu path. Decide which NNM menu your application belongs under, such as Performance, Fault, Configuration, or Tools. Use the character sequence -> to separate menu items in the menu path field.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1008
3740
Doc:

If the menu path field is blank, the application is created and automatically registered; however, the application will not appear in the menu bar. This is useful for creating applications to be used as the action for an executable symbol.

- You can specify selection rules for your application. Selection rules determine when a menu item is unavailable and when it is available. They are based upon defined capabilities of the nodes for which this application is compatible. If the application is registered in the menu bar, the menu item for this application is only accessible if the capabilities of the selected nodes match those defined in this selection rule; for example, `isSNMPSupported`. See NNM's online help within the `MIB Application Builder` window for more information.
- You can enter help text for your application. For example, you may want to give a general description of the MIB operation and how to interpret the information that is obtained. When you create the MIB operation menu item, the program automatically adds an entry under:
  - — *Windows:* `Help:On Application`.
  - — *UNIX:* `Help:Misc->Function` and in the dialog box help.

Data Collection & Thresholds

This section describes how to use NNM's Data Collections & Thresholds application to do the following:

- Collect MIB data from network nodes automatically at regularly scheduled intervals.
- Store the collected MIB data in a file.
- Set threshold monitoring on critical devices.

See page 469 for information about viewing the data after it is collected.

TIP You cannot configure Data Collections & Thresholds from NNM's web interface. However, the web-based Alarm Browser displays the alarms resulting from your configurations.

Prerequisites

- The node for which you want to collect data must support SNMP version 1 or version 2c.
- Make sure the correct version of the enterprise-specific MIB that you want to use to collect data is loaded into the MIB database on the management station. (The `Options:Load/Unload MIBs:SNMP` menu item lists all MIB modules currently in the MIB description file.) If the enterprise-specific MIB is not loaded, see "Loading MIBs in the MIB Database" on page 413.
- You can collect data or monitor thresholds on numeric MIB objects; that is, the MIB objects defined as `Counter`, `Gauge`, `INTEGER`, `IpAddress`, `Counter64`, or `TimeTicks`.
- You can collect data on MIB objects with a `String` data type; that is, monitor MIB objects such as `sysContact`.
- To configure your system to collect MIB data, you need to understand the definitions of the MIB objects and what they do.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1009
3740
Doc:



Most device vendors include documentation about their enterprise-specific MIB with their product. This documentation typically describes the MIB object and what the object means. In addition, some vendors include overview information describing strategies for how to manage their specific device. The vendor documentation can give you the conceptual understanding you need to configure your system to collect MIB data.

- Decide if it would be useful to collect the results of a MIB expression (MIB objects combined into a mathematical formula) rather than individual MIB objects. If you want to use a MIB expression, see "Creating and Using MIB Expressions" on page 460 for information about writing and using MIB expressions.
- Identify the nodes on which you will collect data. For example, for a network segment, you may want to collect data on the router, the hubs, and the key file server.
- Identify how often you want to collect data.
- Ensure the management station has enough room to store the data. NNM automatically collects data by default (select `Options: Data Collection and Thresholds` to see the list of current data collections). The amount of disk space required depends upon how much data you collect. For an example, say that you want to collect data for 10 MIB objects on 50 nodes, each with an average of 8 instances of these objects. If you choose a collection interval of half an hour, the collection rate will be 10x50x8x2 = 8000 values/hour. Since each value collected consumes 24 bytes of disk space, the disk consumption rate is 8000x24 = 192,000 bytes/hour.

  Windows: Data is stored in the *`install_dir`*`\databases\snmpCollect` directory.

  UNIX: Data is stored in the `$OV_DB/snmpCollect` directory. If you need more disk space, symbolically link to another file system.

TIP

For HP-UX systems only: You can expand the file system with Logical Volume Manager. Extend the logical volume, then use `extendfs` (hfs) or `fsadm` (vxfs).

244

Procedure Tips

To access NNM's Data Collection & Thresholds application, from any submap, select `Options:Data Collection & Thresholds:SNMP`. Refer to NNM's online help available from the Data Collection & Thresholds window for directions and additional information.

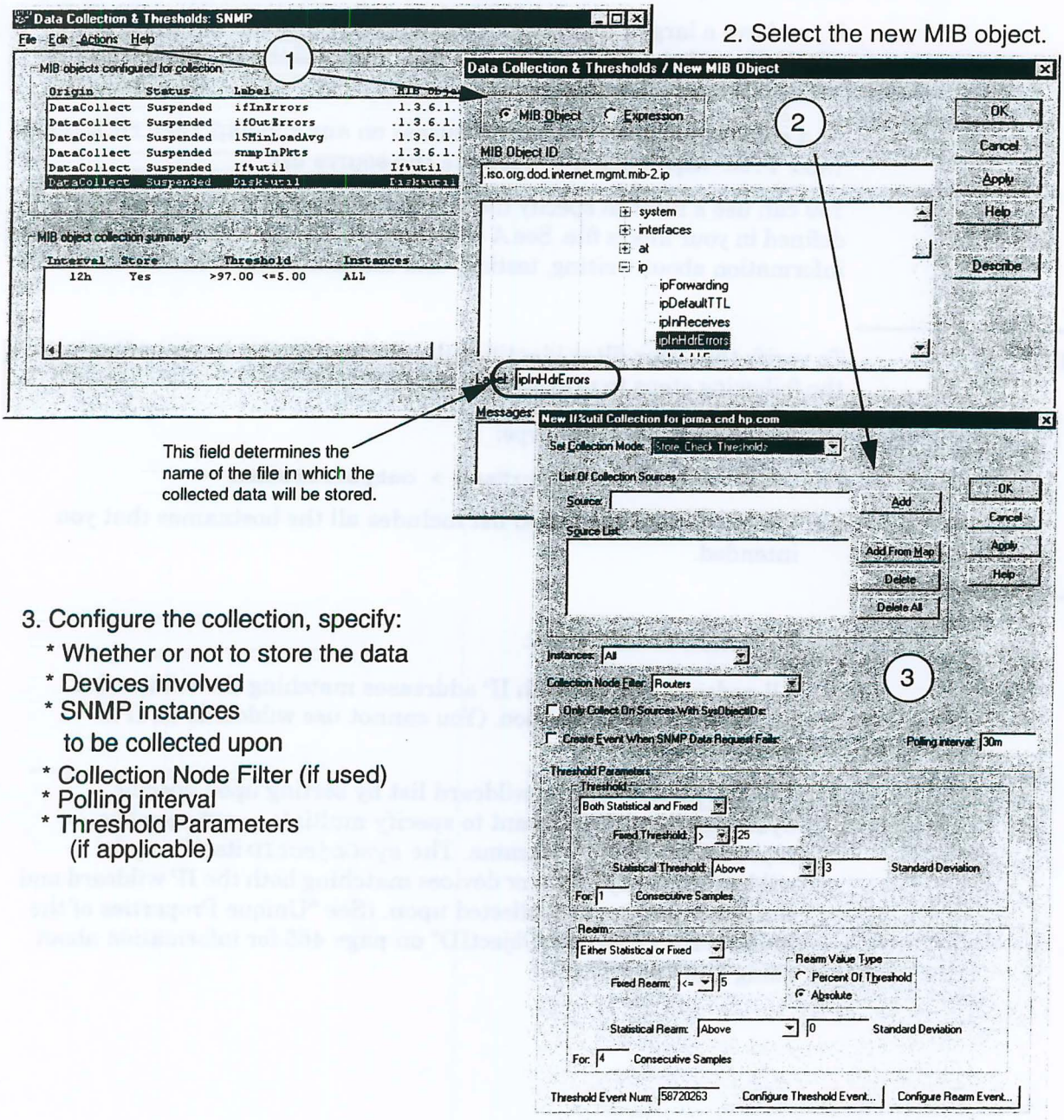
Select the MIB object or expression to be used for data collection. The `Label` field (circled in the following figure) in the MIB selection window determines the file name where the collected data will be stored. (Make

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1010
3740
Doc:

sure the label conforms with file naming conventions for your operating system.) The label defaults to the last component of the MIB mnemonic name.

Figure 12-11 Data Collection Configuration

1. Use Edit:Modify to reconfigure an existing MIB Object or MIB expression for collection.
   or use Edit:New to specify a New MIB Object or expression to collect upon (GET).



3. Configure the collection, specify:
   * Whether or not to store the data
   * Devices involved
   * SNMP instances
     to be collected upon
   * Collection Node Filter (if used)
   * Polling interval
   * Threshold Parameters
     (if applicable)

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1011
3740
Doc:

Then, configure the collection and designate the devices to be monitored.

You specify the devices to be monitored by IP host name, `sysObjectID`, IP address, IP address wildcard (such as `15.21.*.*`), and/or (*NNM for Windows only*) IPX address.

If you have a large number of nodes to specify, you can list them in an ASCII file and simply place the full path name to the file in the `List of Collection Sources` field.

As a convenience, you can select sources on any submap, then click the `[Add From Map]` button to populate the source list.

You can use a filter to specify the list of objects. You may use any filter defined in your filters file. See *A Guide to Scalability and Distribution* for information about writing, testing, and implementing a filter.

TIP

To verify that your filter identifies the sources you wish to monitor, use the following steps to preview the list:

1. At the command line, type:

   ```
   ovfiltertest -f filterName > outputFileName
   ```

2. Verify that the generated list includes all the hostnames that you intended.

With wildcard IP addresses:

- All nodes or devices with IP addresses matching the wildcarded address are collected upon. (You cannot use wildcards on IPX addresses.)
- You can further limit a wildcard list by sorting upon specific `sysObjectIDs`. If you want to specify multiple `sysObjectIDs`, separate them with a comma. The `sysObjectID` itself may be wildcarded. Only nodes or devices matching both the IP wildcard and the `sysObjectID` are collected upon. (See "Unique Properties of the SNMP MIB Object sysObjectID" on page 465 for information about using sysObjectID.)

NOTE

You *must* save *any* changes for the new configuration to take effect. For example, if you suspend collection on a MIB object by selecting `Actions:Suspend Collection`, the `Status` column in the selection list indicates `Suspended`. However, even though the `Status` column displays a `Suspended` status, this change does not take effect until you select `File:Save`.

The data collection configuration is reanalyzed by `snmpCollect` each time you select `File:Save`. If you used IP wildcards, and you have a large number of managed nodes, there may be a significant delay before collections resume.

Counters are computed by calculating the change per second in the sampled values. Gauges and integers store the actual sampled value.

To view the collected data, open the Data Collection & Thresholds window, highlight the specific collection configuration in the list, and then select `Actions:Show Data`.

TIP

SNMP polling requests using the `Options:Data Collection & Thresholds:SNMP` menu item increase the amount of network traffic. If this becomes a problem:

- Change the status for particular collections to `Suspended` from within the Data Collection & Thresholds dialog box.
- Modify the details of your custom data collection by either deleting nodes, deleting instances, excluding nodes, or changing polling intervals.

Defining Thresholds for Monitored MIB Objects

Thresholds let you take a proactive approach to network management. You can manually define thresholds for specific MIB objects that you are monitoring, or have NNM calculate statistical thresholds for you. You can configure events to be posted in the Alarm Browser and/or automatic actions to be taken when the specified thresholds are exceeded. Once you have established a threshold and configured a threshold event, you can

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1012
3740
Doc:

use the web Reporting interface to create threshold violation reports. See NNM's online help for more information about the web Reporting interface.

If setting fixed thresholds, first determine what would constitute reasonable thresholds. To decide on a threshold value, you need to know what is normal and what is out of range. Only you can decide what is normal behavior for a device on your network. Generally, HP recommends that you collect information about a device throughout one complete business cycle before determining the normal high/low range. Consider collecting values such as error rates, retry limits, collisions, throughput, relation rates, and many more. Explore the MIB being used to determine which information to collect.

As soon as you install NNM, data collections on certain MIB objects are started. (You can see which objects are being collected from which devices by selecting `Options:Data Collection and Thresholds`.) This data is available for automatically setting thresholds based upon deviation from normal values. NNM uses the following process to establish statistical thresholds based upon the data being collected:

1. NNM gathers data as configured in Data Collection & Thresholds (the `snmpCollect` background process collects, compares, and stores requested SNMP MIB values).
2. NNM exports the collected *trend* data to the data warehouse every hour. See the *request_list* reference page in NNM's online help (or the UNIX manpage) for information about when NNM runs export tasks.
3. The data warehouse computes, for each instance of each configured collection:
   - The number of data points gathered in the past four days
   - The data summary
   - The sum of the squares for each collection

   This information, from the previous four days, is written to the `snmpColStats.txt` file. This file is recreated each time data is exported to the data warehouse. A notification event is sent to `snmpCollect`.

   These data points are sorted into three time periods, 8 p.m.-5 p.m., 5 p.m.-8 a.m., and weekends. See the *statTimeRanges.conf* reference page in NNM's online help (or the UNIX manpage) for information about controlling the definitions of the time periods.

4. When using automatic statistical threshold generation for a data collection configuration, `snmpCollect` reads `snmpColStats.txt` and calculates, one threshold standard deviation for each time period (bucket) for each data collection instance. Every time the `snmpColStats.txt` file is read, NNM compares the standard deviation calculations to the standard deviation that you specified. An alarm is generated if the current standard deviation exceeds the threshold standard deviation. See the *snmpCollect* reference page in NNM's online help (or the UNIX manpage) for more information.

   Multiple thresholds are allowed per node, one for each instance; for example, one threshold set for a primary hard drive, and a different threshold set for the secondary hard drive.

CAUTION If you are using `ovdwtrend -trim` or `-delete` options to manage the volume of your collected data, ensure that your schedule allows sufficient data history for the statistical threshold feature. See the *ovdwtrend* reference page in NNM's online help (or the UNIX manpage) for information.

Prerequisites

- Configure the data collection to which the threshold applies (see "Data Collection & Thresholds" on page 447).
- You can monitor thresholds on numeric MIB objects; that is, the MIB objects defined as `Counter`, `Gauge`, `INTEGER`, `IpAddress`, `Counter64`, or `TimeTicks`. You can also set thresholds on MIB expressions (see "Creating and Using MIB Expressions" on page 460).

Procedure Tips

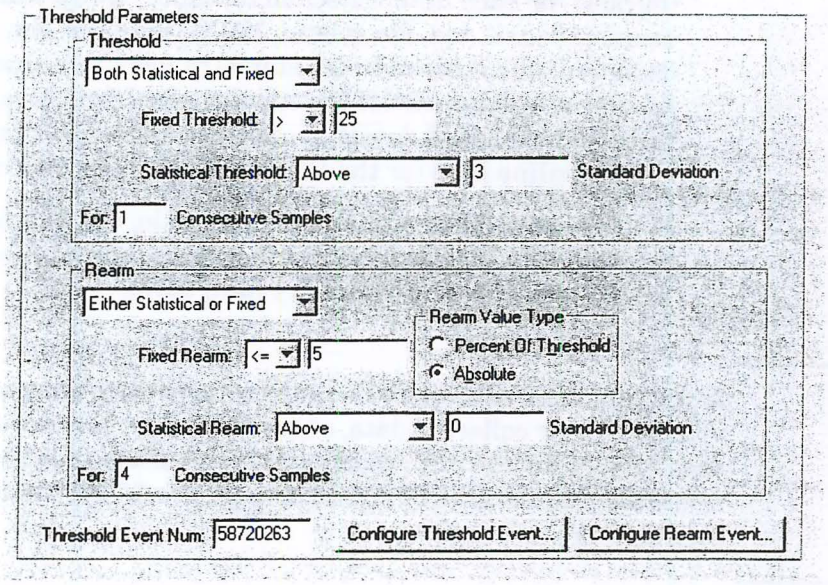
Access the collection configuration dialog box of the configured Data Collection you have been using to establish the normal operating range of your device. Select *one* of the following menu items from the `Option` menu next to the `Collection Mode` label:

- `Don't Store, Check Thresholds`
- `Store, Check Thresholds`
  (required if you want to use the statistical threshold feature)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1013
3740
Doc:

The `Threshold` and `Rearm` fields are now available.

Figure 12-12 Threshold Area of Data Collection Window



To set up fixed-value threshold monitoring, select "Fixed" or "Both Statistical and Fixed" mode, specify a threshold value, and specify the number of consecutive samples required to violate the threshold. To set up fixed-value rearm monitoring, specify a fixed rearm value or percent, and the number of consecutive samples required to rearm the threshold.

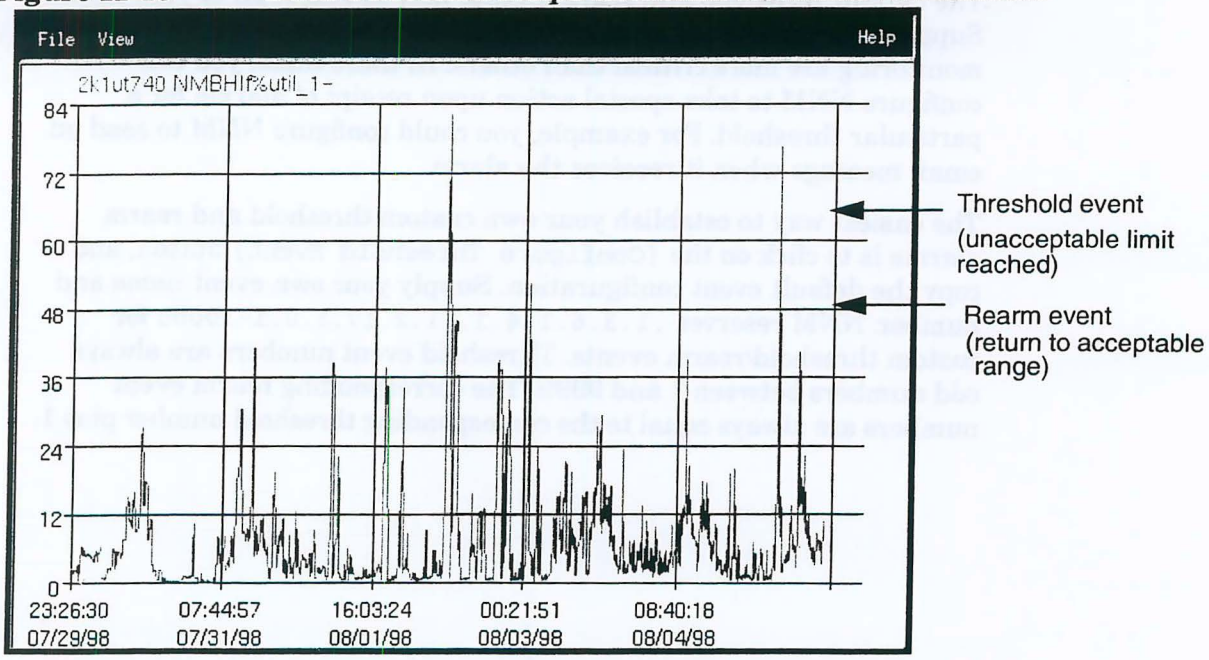
To set up automatic statistical threshold monitoring, select "Statistical" or "Both Statistical and Fixed" mode, specify the standard deviation, and specify the number of consecutive samples required to violate the threshold. To set up automatic statistical rearm monitoring, select "Both Statistical and Fixed" or "Either Statistical and Fixed" mode, specify standard deviation, and specify the number of consecutive samples required to violate the threshold. NNM automatically calculates the standard deviation according to the data warehouse's schedule for exporting trend data.

When the threshold setting is exceeded, a threshold-exceeded alarm is posted in the Alarm Browser, and any automatic actions (such as dialing a pager) that you specify in the Event Configuration are executed.

The *rearm value* controls how frequently a threshold event is generated. The *rearm* indicates that the device has returned to a non-critical state. A *rearm alarm* is posted in the Alarm Browser and any automatic

actions that you specified in the Event Configuration are executed. Another threshold event is not generated until the rearm event occurs and the collected value again reaches the threshold setting.

Figure 12-13 Data Collection Helps Establish Realistic Thresholds



For example, suppose you want to monitor interface percent-utilization. You can set a `Threshold` of 70% and a `Rearm` value of 50%. When the data collector detects a value above 70%, a threshold alarm is generated. Another threshold alarm will be generated only if the reading drops below 50% (sending a rearm alarm) and then goes above 70% again. Note that you can also specify absolute values rather than percentages.

Optionally, specify a value for the `Consecutive Samples` field. This value specifies the number of consecutive times the `Threshold` or `Rearm` expression must be satisfied before a corresponding alarm is generated. This field lets you distinguish sustained abnormality from a brief spike in behavior.

NNM uses two preconfigured events under the `OpenView` enterprise name (`.1.3.6.1.4.1.11.2.17.1.0.`) as the default events for thresholds and rearms:

```
OV_DataCollectThres (58720263)
```


ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1014
3740



`OV_DataCollect_Rearm (58720264)`

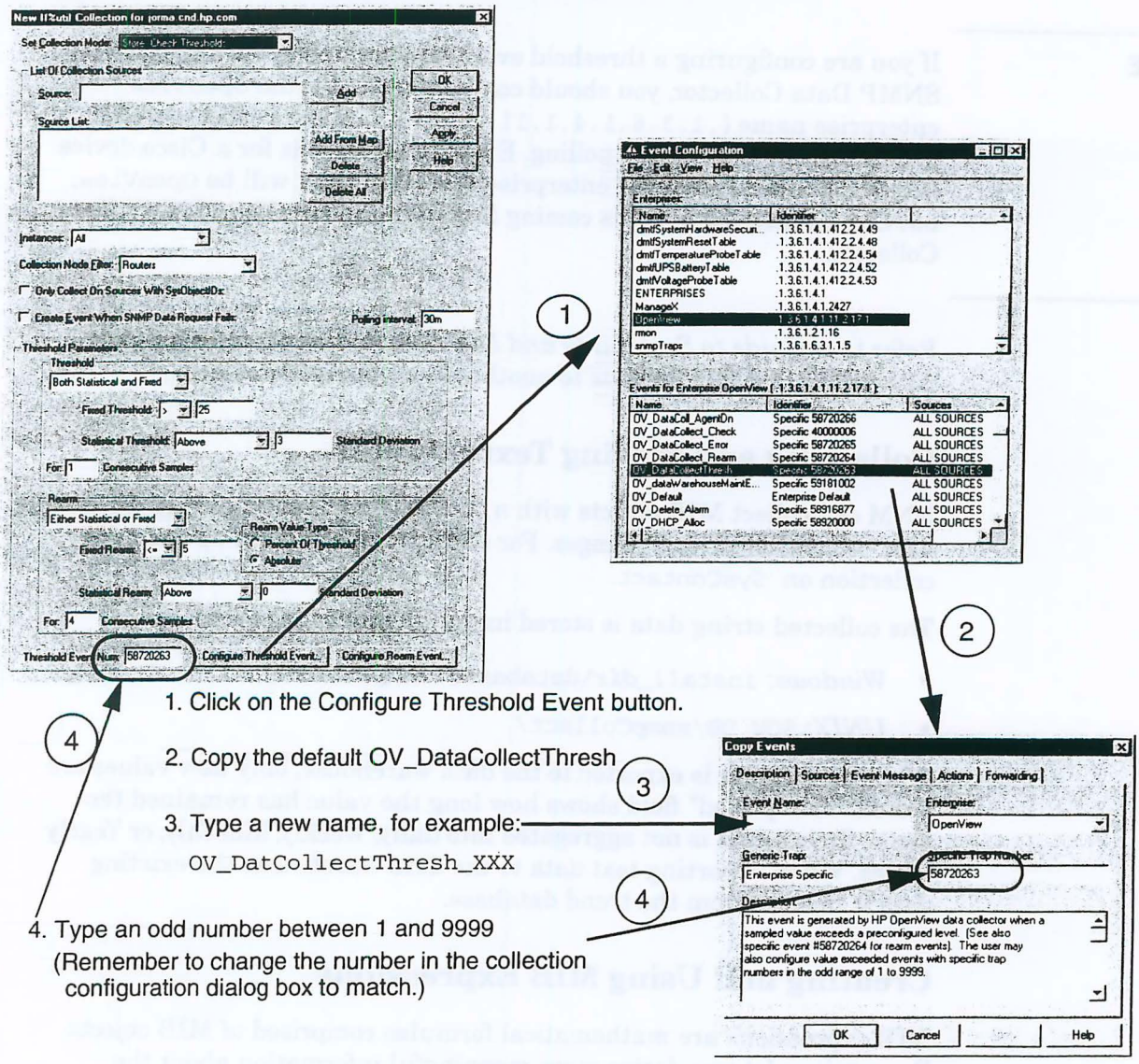
The default alarm is posted in the Alarm Browser's Threshold Alarms category.

The default threshold and rearm events may not meet all of your needs. Suppose, for example, that some of the threshold values you are monitoring are more critical than others. In these cases, you can configure NNM to take special action upon receipt of alarms for a particular threshold. For example, you could configure NNM to send an email message when it receives the alarm.

The easiest way to establish your own custom threshold and rearm alarms is to click on the `[Configure Threshold Event]` button, and copy the default event configuration. Supply your own event name and number. NNM reserves `.1.3.6.1.4.1.11.2.17.1.0.1-10000` for custom threshold/rearm events. Threshold event numbers are always odd numbers between 1 and 9999. The corresponding rearm event numbers are always equal to the corresponding threshold number plus 1.

NOTE If you create a custom threshold event, you must also create a matching rearm event.

Figure 12-14 Customizing the Threshold Event



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1015
3740
Doc:

For example, the threshold event ID 1005 will have a rearm event ID of 1006. These rearm event IDs are automatically assigned but *not* automatically configured in NNM. If you use one of the optional threshold event numbers, you must configure events for both the threshold and rearm event IDs (use the `[Configure Threshold Event]` and `[Configure Rearm Event]` buttons).

NOTE

If you are configuring a threshold event created by the HP OpenView SNMP Data Collector, you should configure it under the `OpenView` enterprise name (`.1.3.6.1.4.1.11.2.17.1.0.`), regardless of which node the Data Collector is polling. Even if the event is for a Cisco device exceeding a threshold, the enterprise ID of the event will be `OpenView`, not Cisco, since the event is coming from the HP OpenView SNMP Data Collector.

Refer to *A Guide to Scalability and Distribution* for information about forwarding threshold events to another management station.

Collecting and Storing Textual Data

NNM can collect MIB objects with a `String` data type. This data can be used to monitor device changes. For example, you can set up data collection on `SysContact`.

The collected string data is stored in the following locations.

- *Windows:* `install_dir\databases\snmpCollect\`
- *UNIX:* `$OV_DB/snmpCollect/`

When string data is exported to the data warehouse, only new values are stored. The "period" field shows how long the value has remained the same. String data is not aggregated into daily, Weekly, Monthly, or Yearly tables. When exporting text data to the data warehouse, the existing data is deleted from the trend database.

Creating and Using MIB Expressions

MIB expressions are mathematical formulas comprised of MIB objects. Expressions let you derive more meaningful information about the health of your network than you could gather using individual MIB objects. MIB expressions are used by several NNM components, and are

available for your use through the Data Collection & Thresholds window. You can also create your own and add them to the list by making additions to the `mibExpr.conf` file and the `mibExpr.conf` file.

Default MIB Expressions

NNM includes many default MIB expressions for your convenience. To explore the default MIB expressions, from any submap, select `Options:Data collection & Thresholds`, then select the following menu item:

Windows: `Edit:MIB Object->New`

UNIX: `Edit:Add->MIB Objects...`

Select the `Expressions` radio button. The list of predefined MIB expressions is displayed for your use. The following are a small sampling of the MIB expressions provided:

RQS nº 03/2005
CPMI - CORR
Fls. Nº 1016
3740
Doc:

Equation 12-1 **If%deferred (MIB II)**
The percent of packets on an interface which were deferred:

$$(\text{packets deferred rate} \div \text{packets transmitted rate}) \times 100$$

Equation 12-2 **If%collision (MIB II)**
Percent of packets on an interface which collided:

$$(\text{collision rate} \div \text{packets transmitted rate}) \times 100$$

Equation 12-3 **If%inErrors (MIB II)**
Percent of input packets on an interface which had an error:

$$\left(\frac{\text{input error rate}}{\text{received unicast packet rate} + \text{received non-unicast packet rate}}\right) \times 100$$

Equation 12-4 **If%outErrors (MIB II)**
Percent of output packets on an interface which had an error:

$$\left(\frac{\text{output error rate}}{\text{transmitted unicast packet rate} + \text{transmitted non-unicast packet rate}}\right) \times 100$$

Equation 12-5 **If%util (MIB II)**
Percent of available bandwidth utilized on an interface:

$$\left(\frac{(\text{received byte rate} + \text{transmitted byte rate}) \times 8}{\text{interface link speed}}\right) \times 100$$

Equation 12-6 **IfInOutOctets (MIB II)**
Total absolute traffic on an interface or the summation of octets (bytes) sent and received on an interface:

$$\text{received byte rate} + \text{transmitted byte rate}$$

Equation 12-7 **IfInOutPackets (MIB II)**
Total absolute traffic on an interface or summation of packets sent and received on an interface:

$$\left(\frac{\text{received unicast packet rate}}{\text{received non-unicast packet rate}} + \frac{\text{transmitted unicast packet rate}}{\text{transmitted non-unicast packet rate}}\right)$$

Equation 12-8 **Disk%util (HP-UX MIB)**
Percentage of disk utilization:

$$\left(\frac{\text{blocks} - \text{free blocks}}{\text{blocks} - \text{free blocks} + \text{available blocks}}\right) \times 100$$

Simply select one from the list and configure it for data collection and/or threshold monitoring on your network's devices.

TIP

There are seven additional MIB expressions defined specifically for use with the HP-extensible agent. They are located in:

- *Windows:* `install_dir\conf\extExpr.conf`
- *UNIX:* `$OV_CONF/extExpr.conf`

Open the file to read about them.

The mibExpr.conf File

The expressions are stored in an ASCII file:

- *Windows:* `install_dir\conf\mibExpr.conf`
- *UNIX:* `$OV_CONF/mibExpr.conf`

You can modify this file or create your own expressions using the `xnmcollect -loadExpr` utility. Best practice is to create a separate file with your new or revised MIB expressions, and then merge the expressions into the `mibExpr.conf file` using the following utility from the command prompt:

```
xnmcollect -loadExpr filename
```

The `-loadExpr` checks syntax, removes duplicate expressions, and rewrites the file.

See the *mibExpr.conf* reference page in NNM's online help (or the UNIX manpage) for information about writing your own MIB expressions; and see the *xnmcollect* reference page in NNM's online help (or the UNIX manpage) for information about updating the `mibExpr.conf` file.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1017
3740
Doc:

The mib.coerce File

The `mibExpr.conf` file works in partnership with the `mib.coerce` file. Entries in the `mib.coerce` file instruct NNM to convert (coerce) a received MIB value from one data type to another (for example, from a gauge or counter to an integer) for use in the mathematical formula defined in the `mibExpr.conf` file. The `mib.coerce` file is an editable ASCII file:

- *Windows:* `install_dir\conf\mib.coerce`
- *UNIX:* `$OV_CONF/mib.coerce`

After making changes to the `mib.coerce` file, you must force NNM to acknowledge the changes; from the command line, type:

```
xnmloadmib -event
```

See the *mib.coerce* reference page in NNM's online help (or the UNIX manpage) for more information about converting MIB values from one data type to another for use in your MIB expression.

Unique Properties of the SNMP MIB Object sysObjectID

The sysObjectID is an important SNMP MIB object to NNM operations. This section describes:

- What the sysObjectID is
- How network management operations use the sysObjectID

The sysObjectID is registered in the Internet-standard MIB-II module as iso.org.dod.internet.mgmt.mib-2.system.sysObjectID (1.3.6.1.2.1.1.2). The sysObjectID is used for administrative purposes to uniquely identify the type of SNMP agent software that is running on a given vendor's hardware. This object is different from most other MIB objects; when you query it, you get back an object identifier that describes the product. For example, when you query the iso.org.dod.internet.mgmt.mib-2.system.sysObjectID using the MIB Browser on an HP OpenView SNMP Agent that is running on an HP 9000 Series 700 or Sun SPARCstation, SNMP returns one of the following object identifiers:

```
iso.org.dod.internet.private.enterprises.hp.nm.system.hpsun.sparc.sun4
iso.org.dod.internet.private.enterprises.hp.nm.system.hpsun.sparc.sun5
iso.org.dod.internet.private.enterprises.hp.nm.system.hpux.hp9000s700
```

This result tells you how the HP 9000 Series 700 or Solaris agent is registered in the MIB. The numeric identifier for Solaris is 1.3.6.1.4.1.11.2.3.10.1.2

Note that there is no value associated with the object ID returned in sysObjectID. It is a unique identifier.

The sysObjectID includes both hardware and software information, and varies depending on the type of hardware and agent software. Some vendors have a different sysObjectID for every version of their agents. For example, Hewlett-Packard sells several SNMP agents, each uniquely identified. To distinguish the HP 9000 Series 800 agent from the HP 9000 Series 700 or Solaris agent, HP registered the HP 9000 Series 800 agent as:

```
iso.org.dod.internet.private.enterprises.hp.nm.system.hpux.hp9000s800
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1018
3740
Doc:

netmon, a service (background process) that automatically discovers the nodes on your network, obtains the sysObjectID when it queries SNMP nodes. NNM operations take advantage of this special object in the following ways:

- To identify the vendor; that is, the manufacturer of the hardware.
- To identify the source of the SNMP agent, which is the type of agent software running on the hardware. For example, if you do a GetRequest to a Sun SPARCstation, the vendor is Sun, but the SNMP agent may be
  - An HP OpenView SNMP Agent for SunOS
  - An SCO UNIX for SunOS agent
  - Other SNMP agent software
- To determine IP topology behavior. An agent's sysObjectID provides hints about what type of node the agent is; for example, a gateway, a bridge, or a host.
- To determine symbol type when putting symbols for newly discovered nodes on the map; for example, a bridge, a gateway, or a hub.
- To identify the source of an event. A sysObjectID is sent in every event. You can use the sysObjectID when you configure events and data collections. The reference in the Event Configuration dialog box to enterprise ID is generally synonymous with the sysObjectID of the agent that generated the event.

Like NNM, you can take advantage of the sysObjectID in many ways, such as:

- From any submap, select Find:Object By Attribute to locate quickly all of a certain manufacturer's model-X when they require a software upgrade.
- If you are writing a rules-based application or script, use the sysObjectID as a rule index.
- On any submap, select a node and use Edit:Object Properties to quickly determine which SNMP agent is running on that node.
- Use the sysObjectID in your filter definitions: discovery, topology, map, etc.

- Use the `sysObjectID` when using the `ovtopodump` command to generate useful lists.
- Customize NNM to display a symbol that you created for a specific type of object (see Appendix D, "Changing All the Symbols for a Particular Device," on page 661).
- If NNM displays an object on the map with a generic symbol (just the outside shape, no vendor-specific icon within the shape), you can specify the icon of your choice to be mapped to that device's `sysObjectID` (see Appendix D, "Changing All the Symbols for a Particular Device," on page 661).
- Specify nodes for which data should be collected, as described in the previous section.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1019
3740
Doc:

13 Using Event Data

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1020
3740
Doc:



NNM provides several features that can assist you in analyzing the network data that has been collected:

- *Graph SNMP Data* (page 471)

  Display collected SNMP data in graphs. This can be SNMP data that has been collected over time and stored in a file, or real-time values that are graphed as they are collected, or both at the same time.

- *Data Warehouse* (page 476)

  Allows you to export collected historical data for use with other statistical analysis tools. Command line functions allow you to maintain the data warehouse database.

- *Web Reporting Interface*

  Allows you to use data from the data warehouse to create reports using a set of predefined templates. See the *Reporting and Data Analysis* online manual and the online help for more information.

NOTE For information about how to merge data from multiple NNM collection stations into a single database, see *A Guide to Scalability and Distribution*.

Ideas for utilizing your collected data:

- Anticipate the need for more network and computer resources, such as gateways and disk space.
- Detect deviations in normal activity.
- Isolate network faults and performance problems.
- Generate inventory reports.

Graphing SNMP Data

The NNM Grapher tool allows you to graph collected MIB data from within the SNMP MIB Browser. Once the Grapher window is displayed, you can set time intervals to continue the collection and even automatically establish a configuration for continuous monitoring by selecting `File:Configure in Data Collector`.

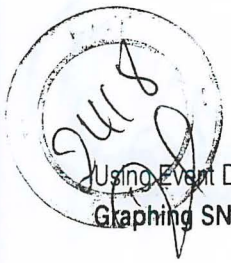
The NNM Grapher tool also enables you to organize MIB data that was collected by the Data Collections & Thresholds feature and view it in graph form. You can graph combinations of data values in the same graph. The data values can be different instances of MIB variables or different variables for different nodes. For example, you can graph instance 1 and instance 3 of a MIB variable for one system, or you could graph instance 3 of a MIB variable for one system, and a completely different variable for another system. You can also normalize the data over configurable time periods to identify trends in the historical data.

This section describes the following:

- Graphing collected data, which includes graphing all data or graphing selected data only, and updating data that has been graphed.
- Graphing historical and real-time data in the same graph.
- Zooming in and out of a specific period of time to view the data in greater or less detail.
- Modifying line attributes in a graph.
- Printing a graph.

NOTE The Grapher tool is available in NNM on a Windows or UNIX operating system. If you are using NNM on the Web, there is a Grapher tool available in the `contrib` directory. (See page 74 for information about using programs from the `contrib` directory.)

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1021
3740
Doc:



Graphing Collected Data

You can graph the data collected in the Data Collector's database by using the `Performance:Graph SNMP Data->All` and `Performance:Graph SNMP Data->Selected Nodes` menu items. You can also access the Grapher tool from within the SNMP MIB Browser or by using the `xnmgraph` command. Refer to the *xnmgraph* reference page in NNM's online help (or the UNIX manpage) for more information.

Behavior

The Graph Selected Nodes dialog box consists of a line graph. The legend across the top of the graph identifies the currently graphed data. Time is shown on the X-axis.

The menu bar has functions that enable you to manipulate the data. The menu bar also has help entries explaining how to use the different menu options to manipulate the data.

The Graph SNMP Data operation does not update the graph with new information as the data is collected. To update the graph with the most current MIB data, select `File:Update Data` from the Grapher menu bar.

Refer to the online help within the graph window for additional information.

Graphing All Data

The `Performance:Graph SNMP Data->All` operation enables you to view collected data in graph form without first having to build an application. This is useful when you want to browse all the data in the Data Collector's database:

- *Windows:* Data is stored in the *`install_dir`*`\databases\snmpCollect` directory.
- *UNIX:* Data is stored in the `$OV_DB/snmpCollect` directory. (If you need more disk space, symbolically link to another file system.)

TIP

For HP-UX systems only: You can expand the file system with Logical Volume Manager. Extend the logical volume, then use `extendfs` (hfs) or `fsadm` (vxfs).

Use this operation when you want to graph some data points just once, or when you want to compare different variables across different systems. For example, let's say you want to compare the load averages to the number of packets, but had not used the Application Builder (see page 443) to set up your own application for this purpose. You can easily use the Graph All operation to graph these two variables together.

CAUTION

This operation reads in *all* the collected data from the Data Collector database into its memory. Depending on the amount of data stored in the database, displaying the Graph All dialog box may take a long time.

Graphing Data on Selected Nodes

The `Performance:Graph SNMP Data->Selected Nodes` operation enables you to view collected data on the nodes that are currently selected on the map, without having to use the Application Builder (see page 443) to set up your own application for this purpose. This is useful when you want to browse the collected data for these nodes. Use this operation when you want to graph some data points just once, or when you want to compare different variables across different systems.

For example, let's say you want to compare the load averages to the number of packets on the selected systems, but had not used the Application Builder (see page 443) to set up your own application for this purpose. You can use the Graph Selected Nodes operation to easily graph these variables together.

Graphing Historical and Real-Time Data in the Same Graph

When you use the Grapher tool via an NNM-provided menu item, the Grapher displays both the collected data and real-time data in the same graph (for example, `Performance:Network Activity`).

When Grapher starts up, it does the following:

1. Reads in the data from the Data Collector's database.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1022
Doc:

When the Grapher tool first comes up, it loads all the collected data from the Data Collector database and seeds its memory with the information in the database. The resolution of the collected data is determined by what the Data Collector was configured to collect.

Once the Grapher tool is running, the tool does not interact with the data in the Data Collector database again (unless you select `File:Update Data`). The Data Collector operates in the background and continues to collect data. This data is available for you to use in future operations.

2. Starts to graph the real-time data.

   The real-time data displayed is independent of the Data Collector. The Grapher tool processes SNMP requests based on the interval specified under `View:Time Intervals` and displays the data in the graph. Unless you save the graphed data to a file using the `File:Save As` menu item, the real-time data is lost as soon as you exit the Grapher.

Stopping Real-Time Data Graphing

To stop real-time data graphing, from the Graph window:

- *Windows:*

  Select `Options:Time Intervals->SNMP Polling Off`.

- *UNIX:*

  Select `View:Time Intervals->SNMP Polling Off`.

Grapher Operations

This section describes some common operations for manipulating a graph.

Selecting Time Intervals

To select time intervals, using the left mouse button:

- Click on the left edge of the graph to page back one screen.
- Click on the right edge of the graph to page forward one screen.
- Click within the graph to center the graph around the selected point in time. Holding the mouse button down and dragging enables you to fine tune the point that you want centered.

Zooming In and Out of a Graph

The Grapher allows you to zoom in and out of a specific period of time in order to view data in greater or lesser detail. To do so, using the right mouse button, click anywhere within the graph. An option menu appears. You can zoom in and out to different amounts of detail. You can also use the menu to page forward, page backward, or show different data points.

Modifying a Line Attribute

To access the `Line Configuration` dialog box, from the Graph window:

- *Windows:* Select `Options:Line Configuration`.

  Option buttons are arranged in rows and columns. Each item in the list controls the attributes for a particular line on the graph.

- *UNIX:* Select `View:Line Configuration`.

  Option buttons are arranged in rows and columns. Each row in the list controls the attributes for a particular line on the graph.

Printing a Graph

To Print a graph, from the Graph window:

- *Windows:* Select `File:Print`. The standard `Print` dialog box appears. Make your selections and click `[OK]`.
- *UNIX:* An `xwd`-compatible file is produced by the Grapher. The default `Print` command is configured in the Grapher print resource. The commands shown in the Print Command window are used to print that file. If the default command does not meet your needs, you can change it. Before you configure the default `Print` command, determine which command options will give you the best printouts. See NNM's online help for more information.

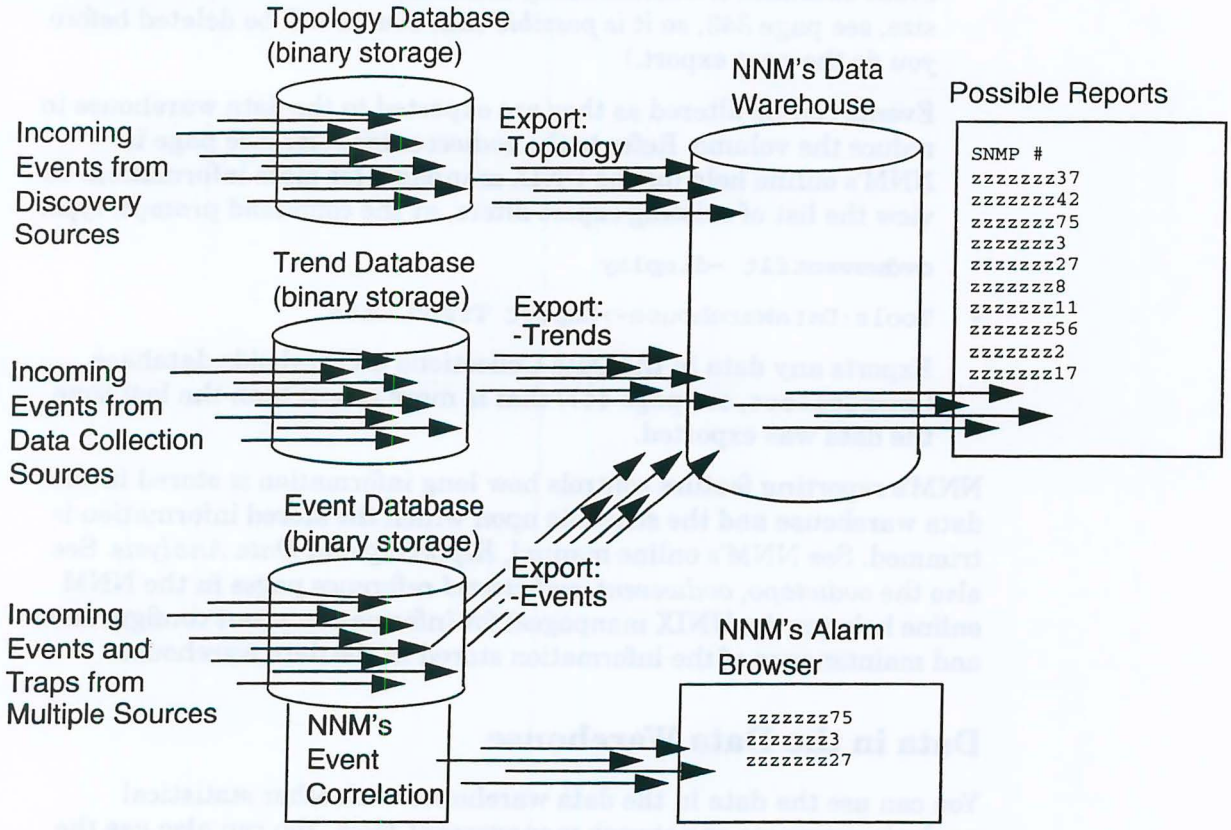
RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1023
Doc. 3740

Data Warehouse

The NNM data warehouse is a relational database (RDBMS) provided with NNM. NNM stores a *copy* of the information from the NNM operational databases into the data warehouse so you can gain an historical perspective of your network information. The data warehouse information is accessible with standard SQL statements using ODBC tools. You can also create reports from the data using the NNM web Reporting interface.

By contrast, the information in the NNM *event database* is discarded when a certain volume is reached (see page 343). Information copied to the *data warehouse* is retained for as long as you need it. You can derive reports from hourly, daily, weekly, monthly, or even yearly information. The limit to the size of the data warehouse is up to you and the allotted hard drive space for the data warehouse.

Figure 13-1 NNM's Event Flow



NNM periodically populates the data warehouse according to a schedule. See the *ovrequestd* and *request_list* reference page in NNM's online help (or the UNIX manpage) for more information. To view the current schedule, at the command prompt, type:

```
request_list schedule
```

You can also manually populate the data warehouse using the following pull-down menu items:

- `Tools:DataWarehouse->Export Topology`

  Exports the current network topology information, replacing any topology information previously sent to the data warehouse.

- `Tools:DataWarehouse->Export Events`

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1024
3740
Doc:

Exports any event database information that is more current than the last time the events database was exported. (Remember: NNM's event database is automatically trimmed when it reaches maximum size, see page 343, so it *is possible* that events will be deleted before you do the next export.)

Events can be filtered as they are exported to the data warehouse to reduce the volume. Refer to the *ovdweventflt* reference page in NNM's online help (or the UNIX manpage) for more information. To view the list of existing export filters, at the command prompt, type:

```
ovdweventflt -display
```

- `Tools:DataWarehouse->Export Trend Data`

  Exports any data in the Data Collections &Thresholds database (`snmpCollect`, see page 447) that is more recent than the last time the data was exported.

NNM's reporting feature controls how long information is stored in the data warehouse and the schedule upon which the stored information is trimmed. See NNM's online manual, *Reporting and Data Analysis.* See also the *ovdwtopo*, *ovdwevent*, *ovdwtrend* reference pages in the NNM online help (or the UNIX manpages) for information about configuration and maintenance of the information stored in the data warehouse.

Data in the Data Warehouse

You can use the data in the data warehouse with other statistical analysis programs or network management tools. You can also use the data to create reports with NNM's web Reporting interface.

See the NNM online manual, *Reporting and Data Analysis.* See also the NNM online help.

Reporting

Reporting is enabled by default when NNM is installed. Once the report data is collected, daily and month-to-date reports for general availability, threshold violation exceptions, and network performance are available from the `Tools:Report Presenter` command or from the HP OpenView Launcher. Daily Inventory reports are available as soon as the report data is collected. For more information about reporting see page 45 in this manual.

For more information about the Reporting feature, see the section labeled "Reporting Interface" on page 516 in this manual.

For more information about the NNM databases and the data warehouse, consult the online manual *Reporting and Data Analysis*.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1025
3740
Doc:

14 NNM on the Web

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls, Nº 1026
3740



NNM on the Web

This chapter describes HP OpenView's Java™-based web interface, and tells you how to set up, configure, and administer NNM's web applications.

This chapter will not attempt to teach you how to use all the features of HP OpenView's web interface. You should consult the NNM online help within the web interface for usage instructions. For an introduction, explore the *Get Acquainted with HP OpenView Network Node Manager: Training for NNM Operators* CD provided with NNM.

This chapter refers to HP OpenView Application Registration Files (ARF) in several places. If you are not familiar with that file, review its functionality in the online manual *Creating and Using Registration Files*.

TIP

If you make changes or additions to the web registration files ensure that your new files are properly backed up. They are *not* included in NNM's backup scripts. See "Backup/Restore to Protect Your Investment of Time" on page 165 for more information.

This chapter includes:

- An overview of the HP OpenView web applications, including setting up the web applications and security for the web applications (page 484).
- A description of the HP OpenView Launcher, the UI integration point for the web applications, including configuration details (page 492).
- A description of the Network Presenter, the web application that displays maps and map data (page 501).
- A description of the SNMP Data Presenter, which displays the results of operations that gather data from managed SNMP nodes (page 509).
- A description of the web-based Alarm Browser, a graphical interface that presents network alarm data, including a comparison of the web-based Alarm Browser and the Alarm Browser running on the management station (page 512).
- A description of Event Correlation Services, NNM's multi-protocol event correlator (page 515).

- A description of the Reporting interface, the web application that allows you to configure and view reports (page 516).
- A description of several supplemental views of discovered nodes (page 518).

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1027
3740
Doc:

Overview

HP OpenView's Java-based web interface further expands NNM's network management capabilities. A part of NNM's base product, the web interface and its applications present the same information about your network that is available from the NNM management station. This information is now presented in a familiar, operator-friendly format that you can access from a remote workstation running a web browser. From your web browser on any PC or UNIX operating system workstation, you can log onto the web and access NNM on the management station to display maps and alarm information. You can easily monitor the status of your network from any place at any time, a real advantage when your pager goes off in the middle of the night!

The HP OpenView Web lets you:

- Inquire about the status of your network and troubleshoot problems from anywhere via the World Wide Web.
- Obtain dynamic updates on map information.
- Share management data with others.
- Present both a graphical and tabular view of the network.
- Access and configure security for web applications.
- Launch NNM and other web-based applications.
- Interact with a familiar web interface.
- Configure and view reports.

The HP OpenView Web includes the following applications:

- HP OpenView Launcher
- HP OpenView Network Presenter
- HP OpenView SNMP Data Presenter
- HP OpenView Alarm Browser
- HP OpenView ECS Configuration
- HP OpenView Correlation Composer
- HP OpenView Reporting interface

An overview and the administration of each of these applications is discussed in the following sections of this chapter.

Setting Up the HP OpenView Web

When you install NNM on the management station the files and applications necessary to run the web interface are also installed. The management station must also have a web server running.

When you install NNM on a management station running Windows, a web server is not installed, since the Windows operating system comes with its own web server. The web server on the Windows operating system is automatically configured for NNM's use during the NNM installation.

When you install NNM on a management station with a UNIX operating system, a web server *is* installed. This server is fully configured to access scripting aliases and documentation aliases used by NNM. The web server uses port 3443 for communication.

If you want to set up your own web server, configure the port number and set up the aliases `OvCgi`, `OvDocs`, and `OvBackgrounds`, see NNM's release notes for additional information about installing a web server.

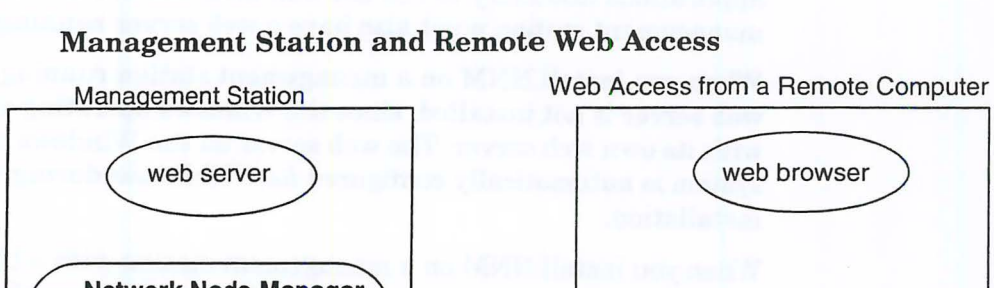
The client station only needs to have a web browser running. Supported web browsers are:

- Netscape
- Microsoft Internet Explorer

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1028
3740
Doc:

NOTE Refer to the "Supported Configurations: Supported Web Browsers" section of the NNM Release Notes for specific information about supported web browsers.

Figure 14-1 Management Station and Remote Web Access



See Figure A-4, "Services and Files for the Web Components," on page 551 for more detailed information about the files and services (processes) on the management station and remote computer at installation time.

On the management station, there must be a non-web based version of NNM running for each map that will be accessible through remote web access. For example, if you want your team to be able to access the Home Office map and the map showing your operations in Germany, you must start NNM on the management station with your Home Office map displayed and start another instance of NNM on the management station with the Germany map displayed. See page 508 for more information.

From remote sites you can now use your web browser and NNM's Network Presenter to display the Home Office map or the Germany map.

Role Configuration Files for the HP OpenView Web

Since the HP OpenView Web can be accessed from virtually any system, security measures are in place to ensure that only authorized users log in to your NNM management station. The way the HP OpenView Launcher and the web applications use these mechanisms varies. The security mechanisms are:

- User authentication (password) file.
- User authorization (roles) file.
- Session configuration file.
- Audit log files.
- `ovw.auth` and `ovwdb.auth` files (used by the Network Presenter and discussed in the section "Configuring Security for the Network Presenter" on page 506).

Since the Launcher is the access point for all other web applications, it provides the first level of security. When security is enabled via the session configuration file, the user password file and user roles file are read to ensure that the user is authorized to access NNM on the management station. The user roles file ensures that only those applications approved for that user role are made available via the Launcher.

User Authentication (Password) File

User authentication is accomplished through a user name and user password. Users should not use the same password as their operating system password. Since the passwords are passed in cleartext format at the beginning of a session, it is possible that they may be intercepted. The Launcher uses the user password file when the user attempts to log on.

The user password file is located on the management station at:

Windows: *`install_dir`*`\www\etc\htpasswd`

UNIX: `/etc/opt/OV/share/www/etc/htpasswd`

Entries in the file appear as:

```
john: FXSD198sdfADS
sue: PO12ADFpoiuS
```

The file is installed with administrator-only (Windows operating system) or root-only (UNIX operating system) permission.

Set passwords as follows:

`ovhtpasswd` *`username`*

The command prompts you for the password for that user.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1029
3740
Doc:

See the *ovhtpasswd* reference page in NNM's online help (or UNIX manpage) for more information about this command.

User Authorization File

Users may be assigned to any number of groups for authorization purposes. These user groups are called user roles in NNM. A **user role** is a designation given to individuals who perform specific tasks with NNM. Users are assigned roles, and then those roles are given access to specific URLs. The Launcher uses the user roles file to define what list items are visible from the Launcher window. When a user logs in, his or her role is verified, and then he or she can access the URLs assigned to that specific role. User roles are valid only when a user accesses NNM via the web interface; they are not valid when a user accesses NNM directly on a management station.

Predefined user roles and their functions are listed below. You can change these roles, or add new roles.

- NetworkAdmin

  The role of NetworkAdmin is intended for individuals who have a higher level of knowledge of networks. Capabilities for configuration of the network and connecting devices, and advanced troubleshooting should be associated with this user role.

- NetworkOper

  The role of NetworkOper is intended for individuals who do routine troubleshooting and maintenance tasks associated with the network. Capabilities for monitoring the network, and routine troubleshooting and maintenance of the network and network devices should be associated with this user role.

- NTAdmin

  The role of NTAdmin is intended for individuals who have a higher level of knowledge of the Windows operating system. Capabilities for configuration of the Windows operating system and advanced troubleshooting should be associated with this role.

- NTOper

The role of NTOper is intended for individuals who do routine troubleshooting and maintenance tasks associated with Windows operating system. Capabilities for monitoring the system, and routine troubleshooting and maintenance of the Windows operating system should be associated with this user role.

- UNIXAdmin

  The role of UNIXAdmin is intended for individuals who have a higher level of knowledge of UNIX operating systems. Capabilities for configuration of UNIX operating systems and advanced troubleshooting should be associated with this user role.

- UNIXOper

  The role of UNIXOper is intended for individuals who do routine troubleshooting and maintenance tasks associated with UNIX operating systems. Capabilities for monitoring the system, and routine troubleshooting and maintenance of UNIX operating system should be associated with this user role.

- OVAdmin

  The role of OVAdmin is intended for individuals who do configuration and customization of the HP OpenView environment and management applications. Capabilities for configuring and customizing management applications should be associated with this role.

The user roles file is located on the management station at:

Windows: `install_dir\www\etc\htgroup`

UNIX: `/etc/opt/OV/share/www/etc/htgroup`

The format of the user roles file is:

```
NetworkAdmin: user1 user2

NetworkOper: user4 user5

NTAdmin:user1 user3

UNIXOper: user6
```

You can also use a plus sign (+) instead of specific user names. This allows any user access to the capabilities of that user role.

User roles work in conjunction with the `Access` specification in the Launcher Registration Files (WLRF). See "Action Block" on page 496.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1030
3740
Doc:

Session Configuration File

The session configuration file is used by the Launcher. A **session** is a group of applications associated with a particular user on a particular display. When a user logs in, all the applications started (directly or indirectly) from the Launcher are part of that session. The applications that are part of a session can share information, such as locale.

A session is terminated when the user exits the web browser, when the session has been inactive for some configurable period of time (the default is 9 hours), or when the management station is shut down.

The session configuration file allows you to enable or disable security for NNM's web applications (default is disabled). If you specify `Off` in the `UserLogin` field of this file, NNM's web applications open directly. If you specify `On` in the `UserLogin` field of this file, NNM's web applications display a login dialog box upon opening.

WARNING **The default is for the session configuration file to disable security. If the security mechanisms are disabled in this file, users will not be presented with a login screen, and will have access to all registered actions.**

The session configuration file is located on the management station at:

Windows: *`install_dir`*`\www\conf\session.conf`

UNIX: `/etc/opt/OV/share/www/conf/session.conf`

The session configuration file has the following format:

```
UserLogin: on|off
LoginLogging: on|off
AccessLogging: on|off
SessionTimeout: hours
```

The default values are `off` for the first three items, and 9 hours for the session timeout. Time should be specified in integer values. Open the editable ASCII `session.conf` file for more information.

If you modify this file while you have the Launcher running, you need to exit the web browser and restart the Launcher for the new information to take effect.

Audit Log Files

There are two audit log files — one for logging logins and one for logging URL access from the Launcher. These are useful for security auditing purposes, as you can check on which users are accessing the Launcher by monitoring these files.

There is no log file management; the files continue to grow. You should periodically check these files and when they get large, you should save them or trim them.

The files are located on the management station at:

Windows: *install_dir*\www\logs\login_log (login log)

install_dir\www\logs\access_log (access log)

UNIX: /var/opt/OV/www/logs/launch/login_log (login log)

/var/opt/OV/www/logs/launcher/access_log (access log)

Each log entry is a single line of text. If the session configuration file is set to LoginLogging:on, the following information is recorded:

- Host
- User name
- Date
- Session number
- Access permitted; either Allowed or DENIED
- URL accessed (for the access_log file only)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1031
3740
Doc:

The HP OpenView Launcher

The HP OpenView Launcher is the user interface integration point for the HP OpenView web applications. Just as with management station-based NNM, developers can tie their applications into NNM's web interface. Then users access those applications through the Launcher interface.

You can also create your own application that you access from the Launcher. If you create your own application, you can integrate it with the Launcher by creating a registration file for that application.

The Launcher provides functionality in three areas:

- Launching of management functionality and applications via a URL or via the web interface.
- User login and user roles.
- Maintenance of session information shared by all web interfaces.

Launcher User Interface

The Launcher interface is started from a web browser. The URL for the Launcher is:

`http://hostname:[port]/OvCgi/ovlaunch.exe`

For example, if the host system is a management station named `UX-manage1` running a UNIX operating system, you would enter:

`http://ux-manage1:3443/OvCgi/ovlaunch.exe`

A web server is automatically installed on UNIX management stations and configured to use port number 3443 for communication.

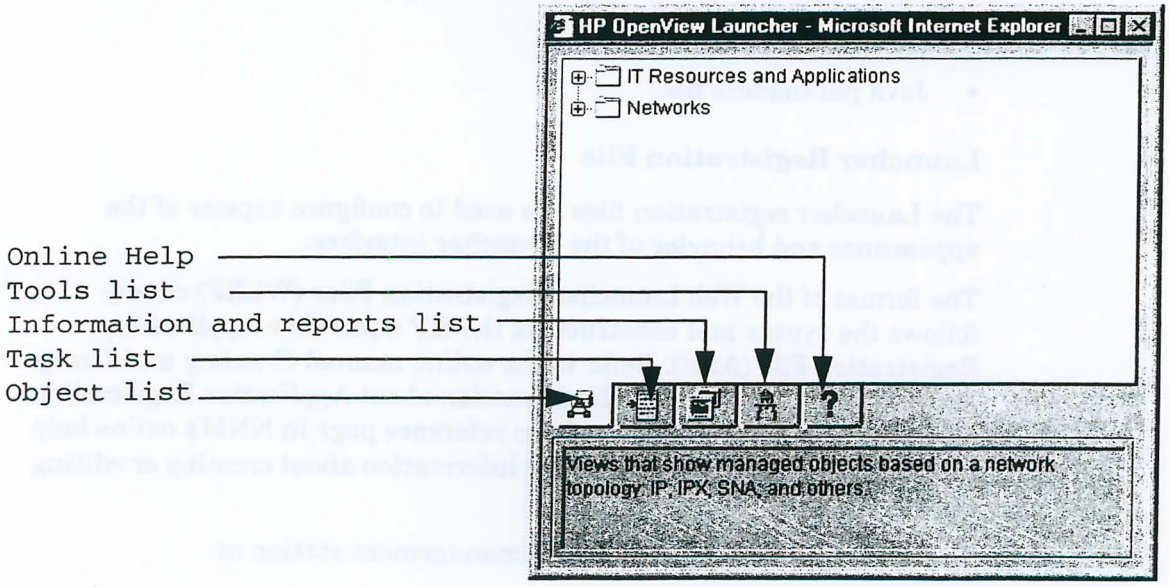
If the host system is a workstation named `nt-mgmt` running Windows, you would enter:

`http://nt-mgmt/OvCgi/ovlaunch.exe`

No port number is required for management stations running a Windows operating system.

If the management station has been configured for security, a login screen appears where the user enters his or her name and password. If no security has been configured, the Launcher window comes up without asking for login and password.

Figure 14-2 The Launcher Window



The Launcher window displays a tabular view of the capabilities available through the Launcher. The bottom tabs of the Launcher window contain the Task, Tool, Object Views, Management Areas, and Help categories. These categories correspond to the basic functionality of NNM on a management station. These are also the categories where other HP OpenView web applications will be linked.

Click on a category to expand it, or click on the expanded category to contract it. You can also click on the +/- indicator.

If you double-click on a list item, you execute the URL associated with that item.

The categories that are displayed in the tabular section of the Launcher window are determined by the user roles file and the Launcher Registration Files (WLRF), described next.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1032
3740
Doc:

Configuring the Launcher

There are several files you can use to customize the Launcher.

- Launcher registration files.
- Error log file.
- Installed locale file.
- Java parameters file.

Launcher Registration File

The Launcher registration files are used to configure aspects of the appearance and behavior of the Launcher interface.

The format of the Web Launcher Registration Files (WLRF) closely follows the syntax and constructs of the HP OpenView Application Registration File (ARF). Refer to the online manual *Creating and Using Registration Files* for general information about Application Registration files. Refer to the *LauncherRegIntro* reference page in NNM's online help (or the UNIX manpage) for specific information about creating or editing the WLRF files.

The WLRF files are located on the management station at:

Windows*: install_dir*\www\registration\launcher\C*.*

UNIX: /etc/opt/OV/share/www/registration/launcher/$LANG

The bitmaps referenced in the WLRF are located in:

Windows*: install_dir*\www\htdocs\C\images*.*

UNIX: /opt/OV/share/www/htdocs/$LANG/bitmaps

Components of the WLRF There are several sections of a WRLF that you might need to modify. Only those sections will be discussed here.

Once you have modified a WLRF file, you can check it for errors with the command `regverify`. See the *regverify* reference page in NNM's online help (or the UNIX manpage) for more information.This command is located on the management station at:

Windows*: install_dir*\bin\regverify

UNIX: /opt/OV/bin/regverify

Tab Block

The Launcher has several tabs at the bottom of its window. The tab block indicates under which of the tabs an application will appear.

The tab block allows an optional icon file name to display on the tab. If one is not specified, a default will be used. The icon appears in front of the name of the application in the Launcher content area. The format for icons is 16x16 GIF. The file name is relative to:

Windows: *install_dir*\www\htdocs\bitmaps

UNIX: $OV_WWW/htdocs/bitmaps

The tab block also contains optional active help text. This active help is presented when the mouse pointer is over the tab.

The tab block contains List Item entries instead of Menu Items (for the menu bar). Following is a sample of the tab block.

```
Tab <60> "Tools" Icon "launcher/toolsfold.20.gif"
        ActiveHelp { "tools" }
{
        <70> "Session"
                Icon "launcher/toolsfold.16.gif"
                ActiveHelp {"Session Info" }
                f.list "SESSION";
}
```

List Block

The list block of the WLRF corresponds to the menu block in the ARF.

The following statements are allowed in the list block:

- Precedence value

  This has the same definition as in the ARF.

- List Item Label

  This is the label that is displayed for the entry.

- Icon

  This is a locale-dependent icon that is displayed for the list item. The format for icons is 16x16 GIF.

- ActiveHelp

  This is the active help text that is displayed when the mouse pointer is placed over the entry.

- Functions

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1033
3740
Doc:

Two functions are supported:

— `f.action`

This indicates a terminal list item. It points to an Action block that has the action definition.

— `f.list`

This indicates a component list item. It points to a list block to allow the definition of a hierarchical tree list.

Following is a sample of the list block.

```
List "SESSION"{
     <80> "Session Info Viewer"
               Icon "launcher/tools.16.gif"
               ActiveHelp { "Session Info Viewer" }
               f.action "printsession";
}
```

Action Block

The action block of the WLRF serves the same function as in the ARF. The following statements are allowed in the action block:

- URL

  This is the URL to launch for the action. The URL may contain the special variable `$OVwWebServer`. This variable will be substituted with the name of the system from which the Launcher was loaded.

- Access

  This is a list of user roles that have access to this action. If a user does not belong to a group that has access, the user will not see the list item that invokes this action in their Launcher window. If the access statement is not present, all valid users can access this action. The user roles values correspond to entries in the user roles file. For example, `NetworkAdmin`. See "User Authorization File" on page 488.

- Window

  The Window statement specifies the characteristics of the window into which the URL will be loaded. If the WebWindow statement is not present, the URL will be loaded into an unnamed full web browser window.

  The Window definition has the following components:

2393

— Window name

This is a name for the window to allow window reuse by targeting a named window. The window name is a string of alphanumeric characters and underscores; it may not include blanks. If a new window is desired every time the URL is loaded, a blank window name (" ") may be given.

— Type (full, intermediate, or limited)

Type specifies the type of the window and determines which features it supports. If no type field is present in a window block, `full` is assumed. The values are:

— `full`, all window elements present and user configurable.

— `intermediate`, directories and menubar off, all other window elements present and user configurable.

— `limited`, all window elements off but user configurable.

— Toolbar (on or off)

— Location (on or off)

— Status (on or off)

— Scrollbars (on or off)

— Resizable (on or off)

— Width (integer value)

— Height (integer value)

Following is a sample of the action block.

```
Action printsession
{
    URL "/OvCgi/printsession.exe";
    WebWindow "OvPrintSession" {
        Type full;
        Toolbar off;
        Status off;
    }
}
```

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1034
3740
Doc:

Error Log File

The Launcher error log records internal errors from the Launcher. You can use the output from this file when discussing a problem with the HP Response Center or HP support personnel.

The Launcher error log file is located in:

Windows: *install_dir*\www\logs\launcher\error_log

UNIX: $OV_WWW/launcher/error_log

The error log contains the following information:

- Date
- Host
- User
- Session
- Reason or error

The error log file continues to grow without bounds. You need to watch the size of this file and truncate it as needed.

If the error log file does not give you sufficient information for troubleshooting, you can set a parameter in the URL for **ovlaunch.exe** that will enable more in-depth error logging on a session level. See "Troubleshooting Web Components" on page 613 for more information. The parameter is:

http://sysname:3443/OvCgi/ovlaunch.exe?Debug=/tmp/file

Language Selection

The Launcher and the Web applications started from the Launcher execute under a particular language, such as English or Japanese. The language used by the Launcher and the Web applications is based on the following:

- The language specified by the user when the security is enabled.
- The language specified by the user through the URL.
- The language specified by the browser.

Once a session is started, the language selection cannot be changed without restarting the browser with a different language.

Language Selection When Security is Enabled Security is enabled via the session configuration file. When security is enabled, the user is presented with a login page listing the languages available for the session under the `[Options]` button. This list represents the languages supported by the Launcher and other installed products that integrate into the Launcher. The languages presented in `[Options]` is based on the contents of the `locales.installed` file. This file is located in:

Windows: *`install_dir`*`\www\conf\locales.installed`

UNIX: `/etc/opt/OV/share/www/conf/locales.installed`

This file contains a list of locales for which the Web applications have been localized. For instance, if the Japanese NNM has been installed, this file will contain an entry for English and for Japanese, for example:

```
en
ja
```

This file can be modified by a developer or administrator. When an HP OpenView web application has been localized to a language not listed in this file, a locale entry should be added to this file. Refer to the *HP OpenView Windows Developer's Guide* for details on syntax.

Language Specified Through the URL The language for a session can be specified when the `ovlaunch.exe` URL is specified. This is done through the CGI parameter `AcceptLang`. This language specification will take precedence over the browser language specification, but can be overridden if security is on and the user chooses a different language on the login page. If security is not on, the login page will come up in the language specified by the `AcceptLang` parameter. For example:

`http://`*`mysystem`*`:3443/OvCgi/ovlaunch.exe?AcceptLang=ja`

Language Specified Through the Browser When security is not enabled, the Launcher uses language specified through the browser. For instance, if the browser has been configured to run in English, the Launcher will execute in English.

Java Parameters File

There are some Java parameters that you can modify to control Launcher appearance. You change these parameters by modifying the APPLET block in the following file, located on the management station at:

RQS nº 03/2005 - CN - CPMI - CORREIOS
1035
Fls. Nº
3740
Doc:

Windows: *install_dir*\www\htdocs\C\nnm\launcher\browser.html

UNIX: $OV_WWW/htdocs/$LANG/nnm/launcher/browser.html

The Java parameters that you can modify are:

- background
- foreground
- activeTabColor
- inactiveTabColor
- treeBackground
- treeForeground
- treeConnectingLineColor
- displayActiveHelp
- activeHelpLines
- fontName
- fontStyle
- fontSize
- displayInFrame

HP OpenView Network Presenter

The HP OpenView Network Presenter is a Java-based applet that connects to NNM for the purpose of displaying maps. It provides multiple views of map data on a management station from any system with a web browser that supports Internet Explorer or Netscape Navigator.

NOTE Refer to the "Supported Configurations: Supported Web Browsers" section of the NNM Release Notes for specific information about supported web browsers.

The Network Presenter communicates with the management station to get registration information, map data, and map object data. It provides read-only access to the map data and has dynamic updates to reflect the changes that occur on the management station. You can navigate through the map views, select and obtain status on symbols, and launch other web applications on the selected objects via the Network Presenter.

Starting the Network Presenter

You must start an NNM session on the management station for each map that you want available through the web, as described on page 485.

You can invoke the Network Presenter through the Launcher using either of the following tabs:

`Objects` tab, then choose `Networks:IP Network`

`Tools` tab, then choose `NNM:Network Presenter`

Alternatively, you can enter the URL for the Network Presenter:

`http://`*`hostname`*`[:`*`port`*`]/OvCgi/jovw.exe?[MapName=`*`mapname`*`&ObjectName=`*`selectionname`*`]`

On UNIX operating systems, you must specify port number `3443`. Ona Windows operating system, no port number is required. The `MapName` and `ObjectName` fields are optional.

The `MapName` field specifies which map to open. The `ObjectName` field specifies what object to show initially. Refer to the *OvWebURLIntro* reference page in NNM's online help (or UNIX manpage) for more information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1036
3740
Doc:

NOTE When starting the Network Presenter directly from the URL, you lose the session information that the Network Presenter would have if it were started from the Launcher, including language information.

If a *mapname* is not specified in the URL used to start the Launcher, Network Presenter attempts to connect to an NNM session running with the default map. If there is no NNM session running with the default map, the Network Presenter displays an error message that says the map was not found.

If a *mapname* is specified in the URL, the Network Presenter attempts to connect to an NNM session on the management station with an open map called *mapname*. If there is no NNM session running on the management station with this map open, the Network Presenter displays an error message that says the map was not found.

If you close the NNM session or open a new map, the Network Presenter session attached to that NNM session is ended. The Network Presenter displays a dialog box informing the users that NNM is closing its map.

By default, the Launcher will start the Network Presenter with the `default` map displayed. To make a map other than `default` available to the Network Presenter, modify the `jovw` Web Launcher Registration File (WLRF) that specifies in the URL portion which map to open. See "Listing Multiple Maps in the Launcher" on page 508 and "Launcher Registration File" on page 494 for information.

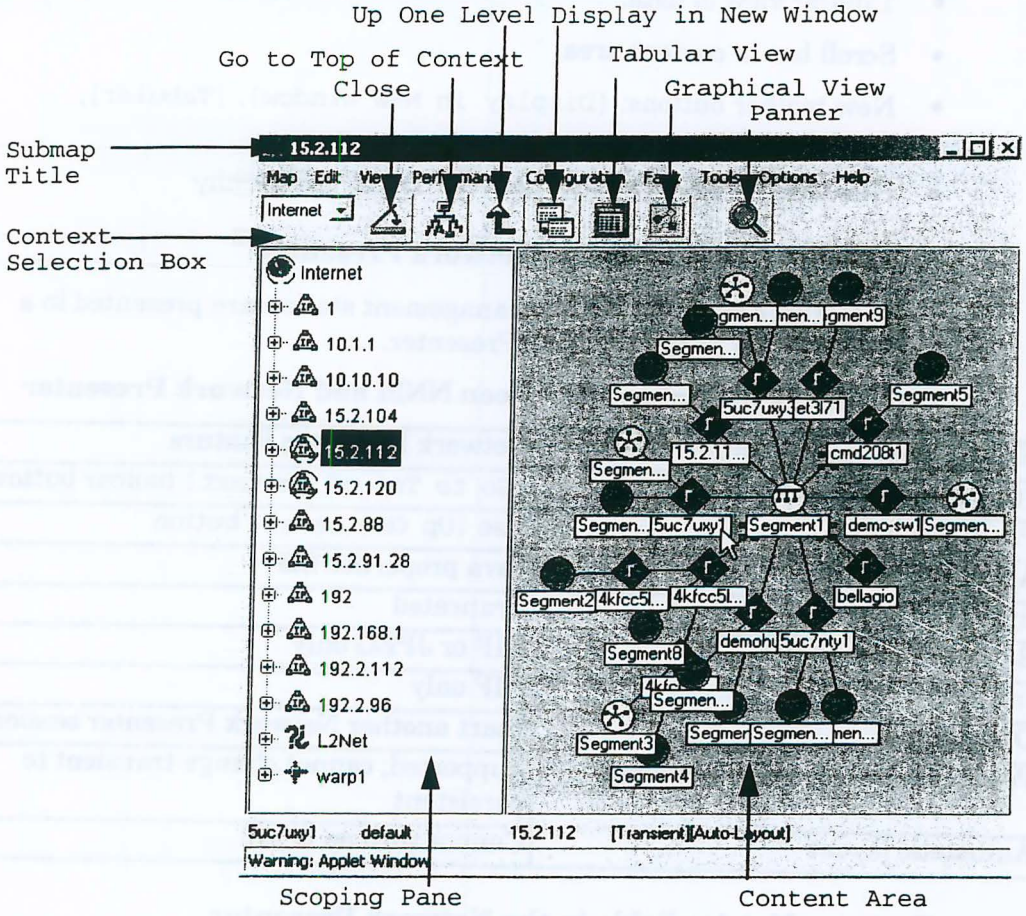
The Network Presenter Window

The Network Presenter window has the following components:

- Submap title
- Menu bar
- Context selection box
- Toolbar
- Content area
- Scoping pane

- Status bar

Figure 14-3 **Network Presenter Window**



Network Presenter versus NNM on a Management Station

There are some differences in the functionality and presentation of information between the Network Presenter and NNM on a management station.

Features in the Network Presenter

Following are features in the Network Presenter that are not available in NNM on a management station.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1037
3740
Doc:

- Context selection box to choose among the highest-level views.
- Scoping pane.
- Tabular view of data.
- Scroll bar in content area.
- New toolbar buttons: `[Display in New Window]`, `[Tabular]`, `[Graphical]`
- New menu items: `Up One Level`, `Top of Hierarchy`

Features That Differ in the Network Presenter

Some features from NNM on a management station are presented in a different format in the Network Presenter.

Table 14-1 Differences in Features Between NNM and Network Presenter

NNM Management Station Feature	Network Presenter Feature
`[Go to Root]` toolbar button	`[Go to Top of Context]` toolbar button
Parent toolbar	Use `[Up One Level]` button
App-defaults file	Java properties file
Symbol labels	Truncated
Background graphics	GIF or JPEG only
Inner shapes	GIF only
Open map	Start another Network Presenter session
Persistent and transient submaps	Supported; cannot change transient to persistent
Automatic layout	Cannot turn on or off

Features Not Available in the Network Presenter

The following features in NNM on a management station that are not available in the Network Presenter.

- `Map Description` dialog box.
- `Submap Properties` dialog box.
- `Locate Submap` dialog box.
- Home submap.
- `Symbol Properties` dialog box.
- Snapshots.

- Symbol enhancements (flashing, transparent, alerts, etc.).
- Menu collapsing.
- Symbol, submap editing.
- Invoking executable symbols.

Interaction Between NNM on the Management Station and the Network Presenter

Since the Network Presenter cannot do editing, the Network Presenter does not influence what happens to NNM on the management station; however, changes in the current session on the management station are dynamically reflected in the content area and scoping pane of the Network Presenter as appropriate. You will see changes in the content area if the submap that is displayed on the management station changes. You will see changes in the scoping pane if that level of hierarchy is displayed. Changes are not dynamically reflected in open dialog boxes.

Configuring the Network Presenter

You can modify the Network Presenter Registration Files (NPRF) to configure certain aspects of the Network Presenter.

The NPRFs are located on the management station at:

Windows: *install_dir*\www\registration\jovw\c*.*

UNIX: /etc/opt/OV/share/www/registration/jovw/$LANG

The format of the Network Presenter Registration Files (NPRF) closely follows the syntax and constructs of the HP OpenView Application Registration File (ARF). Refer to the online manual *Creating and Using Registration Files* for general information about Application Registration files. Refer to the *NetworkPresenterRegIntro* reference page in NNM's online help (or the UNIX manpage) for specific information about creating or editing the NPRF files.

You can add entries to the Action block to specify your own applications to be called when the Network Presenter is launched. You can also change the WebWindow properties in the Action block to control some aspects of the appearance of the Network Presenter (see "Components of the WLRF" on page 494 for sample contents of a registration file). You can add pull-down menus, toolbar buttons, and popup menus that operate on selected objects.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1038
3740
Doc:

Configuring Security for the Network Presenter

There are two levels of security for the Network Presenter.

- The `session.conf` file, described earlier in this chapter.
- The `ovw.auth` and `ovwdb.auth` files, described next.

The Network Presenter allows role-based, restricted access to menu items that have action blocks that contain access statements. See the *Action Block* description on page 496 for more information.

Authorization Files The `ovw.auth` and `ovwdb.auth` files specify which users are allowed access to which management stations. These files are located on the management station at:

Windows: *`install_dir`*`\conf\ovw.auth`

`install_dir``\conf\ovwdb.auth`

UNIX: `$OV_CONF/ovw.auth`

`$OV_CONF/ovwdb.auth`

Each of these files contain instructions for their use.

Using Symbol Registration Files and Bitmaps

Symbol registration files used by the Network Presenter are the same as those used by NNM on a management station. Therefore, if a symbol definition is added for NNM on a management station, it also appears in the Network Presenter. Symbol registration files are located in:

Windows: *`install_dir`*`\symbols\%LANG%`

UNIX: `$OV_SYMBOLS/$LANG`

See the *OVwRegIntro* reference page in NNM's online help (or the UNIX manpage) for more information about creating or editing symbol registration files.

The graphic files for the symbols, themselves, are stored in two places. One directory used by NNM on the management station (see page 664), and one directory used by NNM's web-based interface. The web-based interface requires GIF files. Other additional graphic file formats are supported on the management station. If you create your own GIF files, place a copy in each location.

The Network Presenter loads its bitmaps in GIF format from the directory:

Windows: *install_dir*\www\htdocs\bitmaps

UNIX: $OV_WWW/bitmaps

TIP

If you can see a symbol on the management station, but cannot see it over the web interface, check the Contrib directory (see page 74) for the convertBitmaps.ovpl script which walks through each graphic in the management station's symbol graphic directory and ensures that a corresponding GIF file exists or is created in the web interfaces's symbol directory.

Symbols in the web-based interface have the same appearance as in NNM on a management station; however, the symbol labels do not scale based upon the size of the label. Instead, a long label is truncated to fit the space available.

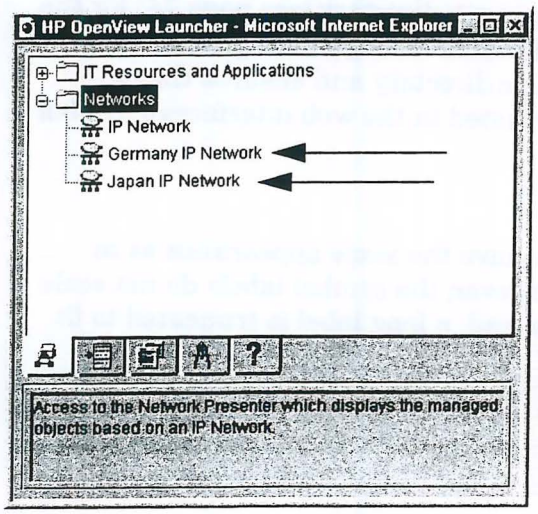
RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1039
3740
Doc:

Listing Multiple Maps in the Launcher

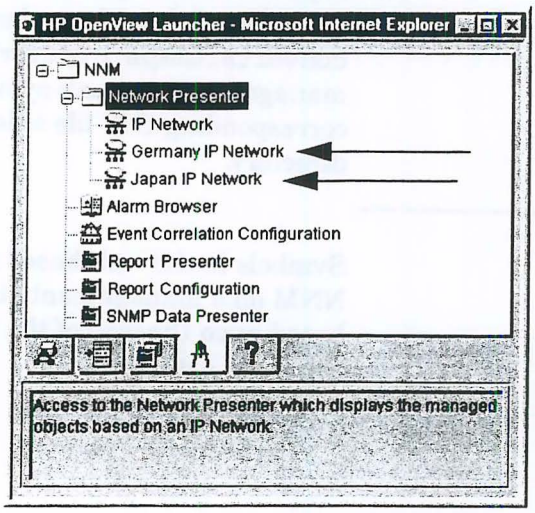
You can modify the Launcher registration file for the Network Presenter so that each of your custom maps is listed.

Figure 14-4 Listing Multiple Maps in the Launcher Window

Custom Maps Added to Object View Tab



Custom Maps Added to Tools Tab



For each map, you must make additions to the `List` and `Action` blocks of the following file:

- Windows: *`install_dir`*`\www\registration\launcher\C\jovw`
- *UNIX:* `$OV_WWW_REG/launcher/$LANG/jovw`

Open this file and read the instructions provided for more information. See also the *LauncherRegIntro* reference page in NNM's online help (or the UNIX manpage) for specific information about creating or editing the WLRF files.

On the management station, there must be a non-web based version of NNM running for each map that will be accessible from the Network Presenter. For example, if you want your team to be able to access the Germany map and the map showing your operations in Japan, you must start NNM on the management station with your Germany map displayed and start another instance of NNM on the management station with the Japan map displayed.

SNMP Data Presenter

The SNMP Data Presenter displays results of operations that present tabular or textual data for managed SNMP nodes selected from the map.

You can use the SNMP Data Presenter even if there is no NNM session running on the management station. The SNMP Data Presenter accesses NNM's Application Registration Files (ARFs) to retrieve information about menu structure and actions, executes the command on the management station, and displays the results in the web browser.

The SNMP Data Presenter displays configuration, performance and fault information. Here are a few examples:

- Interface status.
- SNMP authentication failures.
- TCP connections.
- IP Network addresses.
- IP Routing tables.
- IP ARP cache table.
- System information.
- SNMP trap recipients.

To start the SNMP Data Presenter, select the target node in the content area of Network Presenter and then select one of the following:

- `Performance:SNMP Data Presenter`
- `Configuration:SNMP Data Presenter`
- `Fault:SNMP Data Presenter`

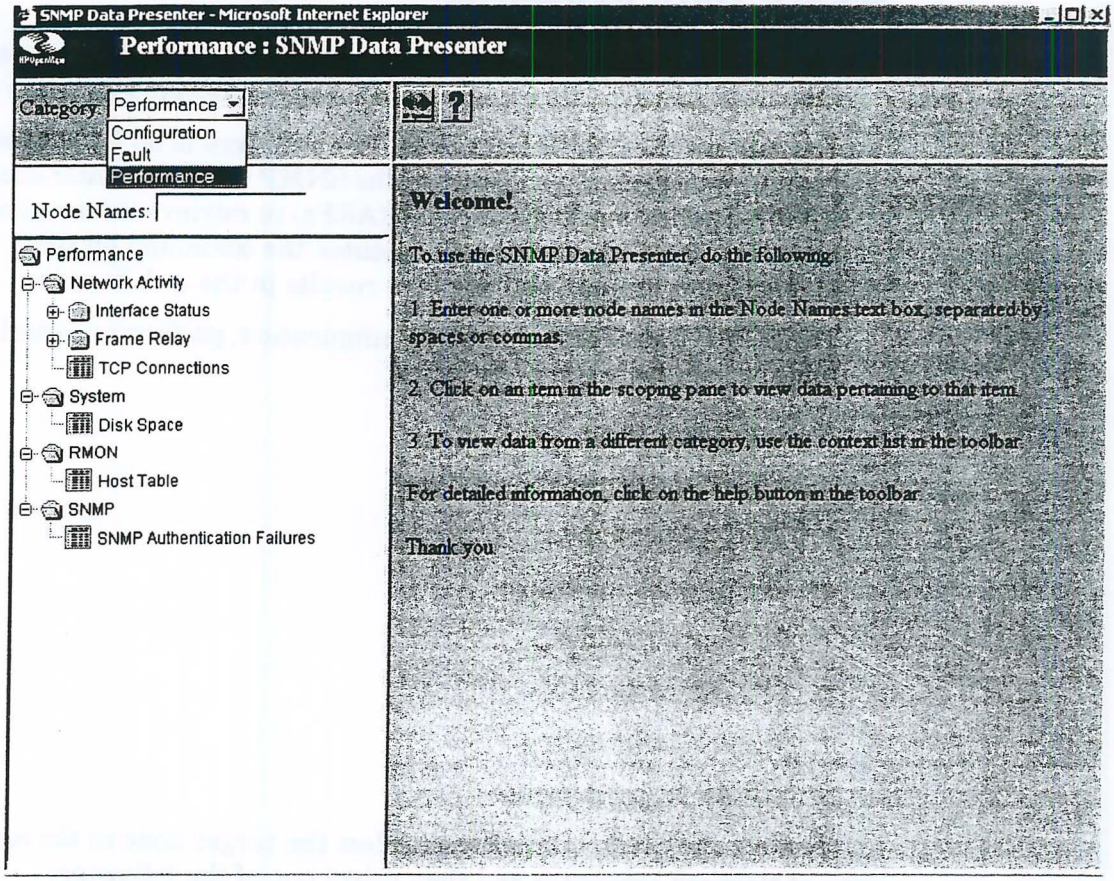
To start the SNMP Data Presenter from the Launcher, select:

- `Tools` tab, then `NNM:SNMP Data Presenter`

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1040
3740
Doc:

The SNMP Data Presenter window is shown in Figure 14-5.

Figure 14-5 SNMP Data Presenter Window



Scoping Pane Content Pane

When accessed from the `Tools` tab, the scoping pane contains categories and actions in a tree format. You can click on the category items to expand them and then click on an action to execute that action. You can also use the Category pull-down.

The results of an action are shown in the content area. A link at the bottom of this area allows you to display a new web browser window with the currently displayed information. This allows for easy comparing of data.

Configuring the SNMP Data Presenter

The SNMP Data Presenter uses NNM's Application Registration Files (ARFs) and the Application Builder. Because of this, you can execute the same SNMP monitoring operations as you do in NNM, and add new operation commands to the menu structure with Application Builder.

See NNM's online manual, *Creating and Using Registration Files,* for details about editing application registration files (ARFs). See "Using the MIB Application Builder" on page 443 for more information about the Application Builder feature.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1041
3740
Doc:

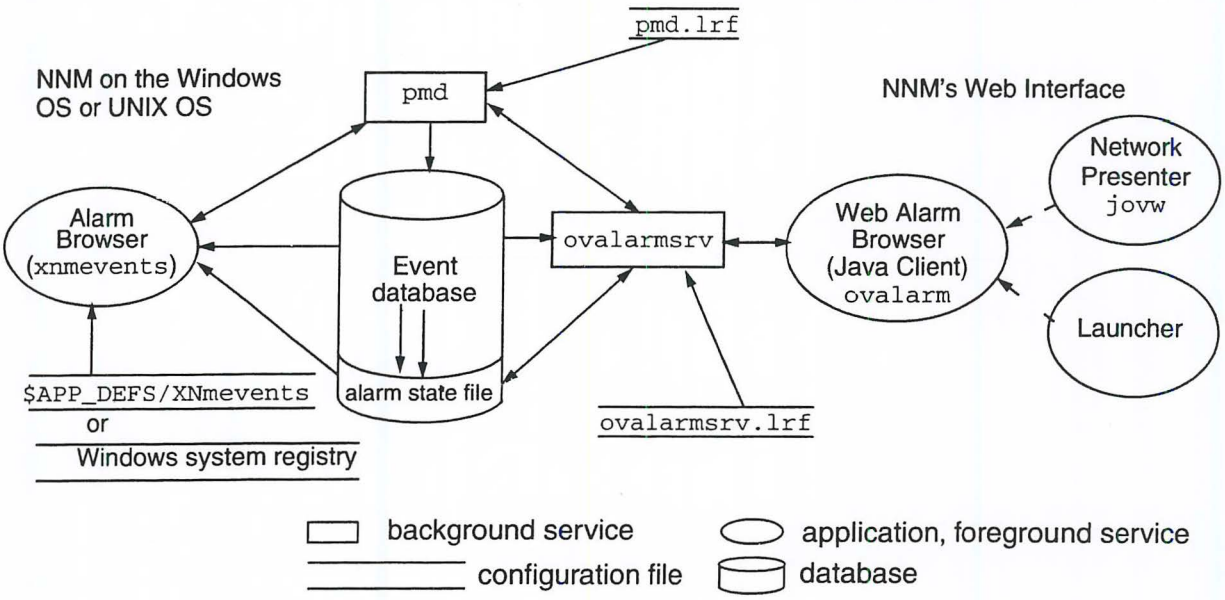
Alarm Browser

The Alarm Browser presents alarm data via the web interface. Through the Alarm Browser, you can filter alarms and take actions on specific alarms. All alarms are global to all web users, as are the acknowledge, delete, change category, and change severity functions.

The web-based Alarm Browser service, `ovalarmsrv`, is started by `ovstart` when you start an NNM session on the management station.

Figure 14-6 illustrates the relationship and data flow between the Alarm Browser application on a management station and the web-based Alarm Browser.

Figure 14-6 Relationship Between the Two Alarm Browsers

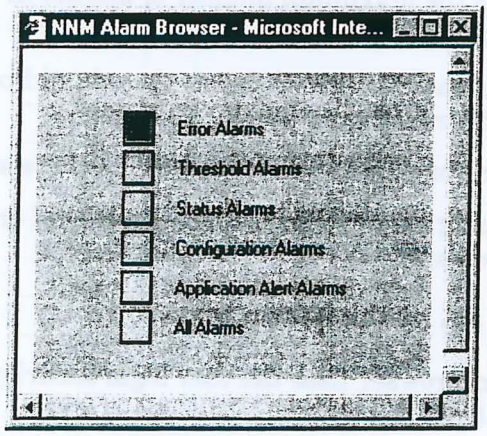


You access the Alarm Browser using one of the following methods:

- In the Launcher, select the `Tools` tab, then select `NNM:Alarm Browser`

- In Network Presenter, select the `Fault` menu, then select `Alarm Browser`.

Figure 14-7 Web-Based Alarm Browser's Category Window



Using and Configuring the Alarm Browser

You can use the Alarm Browser to perform the following:

- Acknowledge/Unacknowledge alarms.
- Move alarms to a different category.
- Assign alarm severities.
- Filter alarms.
- Delete alarms.
- Examine alarm details to find correlated events.

To move an existing alarm message to a different category. Select the alarm that you want to recategorize. Then select `Actions:Change Category` from the menu bar. Refer to the online help if you need more information.

This change affects only the selected alarms. Future alarms of the same type will continue to be posted in the old category's list.

You can configure an alarm to activate your web browser to a specific URL. See "Launching Specific Views or URLs from Alarms" on page 340 for more information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1042
3740
Doc:

See Chapter 12, Customizing Events: Doing It Your Way, for configuration options:

- Setting the maximum size of the event database (default 16 MB).
- Setting the maximum number of alarms in the Alarm Browser's state file (default 3500).
- Setting the number of alarms that should be deleted each time the state file reaches maximum capacity.
- Copying or restoring the Alarm Browser's state file.
- Assigning alarms to other categories and creating new alarm categories.

Security for the Alarm Browser

The Alarm Browser uses the user login security mechanisms, described earlier in this chapter.

Event Reduction

Event reduction is the process by which the relationship between events is identified. Once identified, a smaller number of new events providing higher information content can be generated. This simplifies the task of diagnosing network faults. There are three event reduction strategies that are configured and working within NNM. You can access the configuration windows for two of them over the web:

- "ECS Correlations" on page 360
- "Correlation Composer Correlators" on page 386

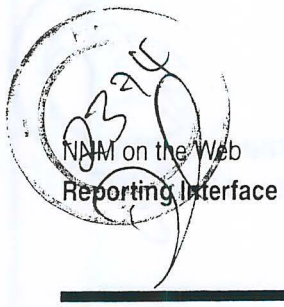
There are several ways to access these event correlation features. For more information, from any submap:

- Select `Toos:HP OpenView Launcher`.
- Select the `[?]` tab.
- Click `Tasks, Event Correlation Management`.

  Read the information under *Accessing the Event Correlation Configuration Windows*

For information about the NNM event reduction strategies, see Chapter 11, "Event Reduction Capabilities: Getting to the Root Cause," on page 351.

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1043
3740
Doc:



Reporting Interface

The web Reporting interface is a graphical user interface that is available through a web browser. The Reporting interface consists of:

- Report Configuration-- create, modify, and view report schedules.
- Report Presenter-- view reports.

You can access the Report Configuration in one of the following ways:

- From NNM on a management station, select the `Options:Report Configuration` menu item.
- From Network Presenter, select the `Options:Report Configuration` menu item.
- From the Launcher, select the `Tools` tab, and expand the NNM category. Double-click on `Report Configuration`.
- From your browser, specify the following URL:

  `http://`*`hostname`* `[:`*`port`*`]/OvCgi/RptConfig.exe`

  You need to specify a port if you are running NNM on a UNIX machine.

You can access the Report Presenter in one of the following ways:

- From NNM on a management station, select the `Tools:Report Presenter` menu item.
- From Network Presenter, select the `Tools:Report Presenter` menu item.
- From the Launcher, select the `Tools` tab, and expand the NNM category. Double-click on `Report Presenter`.
- From your browser, specify the following URL:

  `http://`*`hostname`* `[:`*`port`*`]/OvCgi/RptPresenter.exe`

  You need to specify a port if you are running NNM on a UNIX machine.

The NNM Analysis and Reporting interface will be displayed in your browser window.

Refer to the online manual *Reporting and Data Analysis with HP OpenView NNM* and the web online help for more information.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1044
3740
Doc.

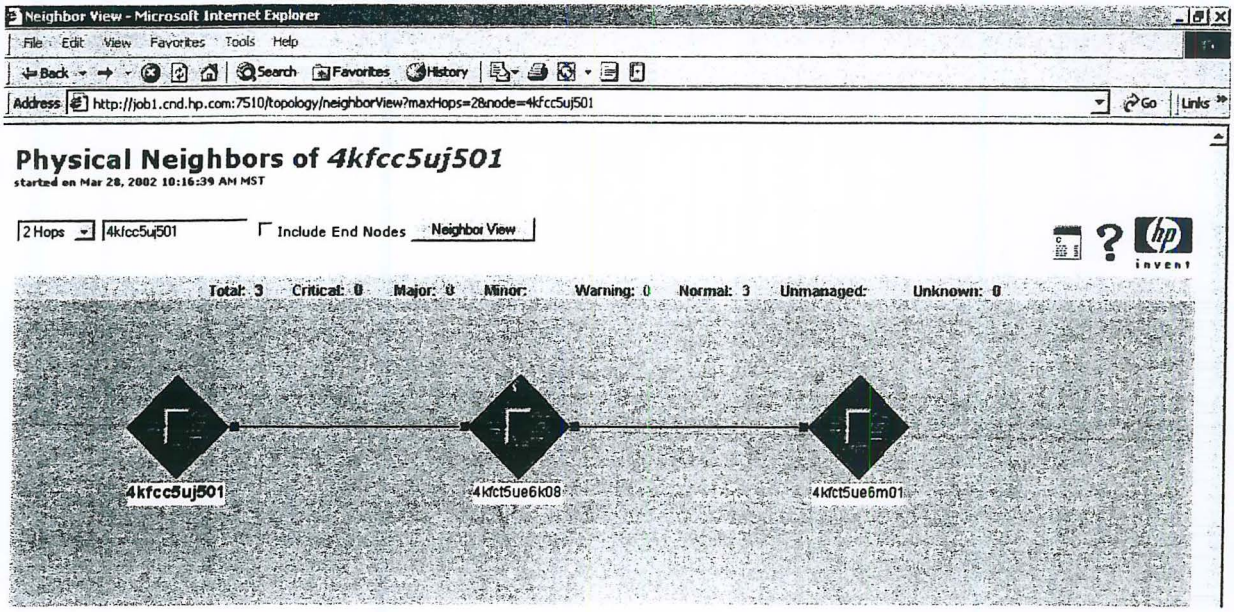
Additional Views

NNM presents several different views of discovered nodes. NNM's Neighbor view, Path view, Node view, Cisco Discovery Protocol view (CDP view), Station view, Internet view, and Port-Address Mapping capabilities show topology views that supplement NNM's map views.

Neighbor View

The Neighbor view shows you a graphical representation of the selected device and the connector devices related to it, within a specified number of hops of the selected device.

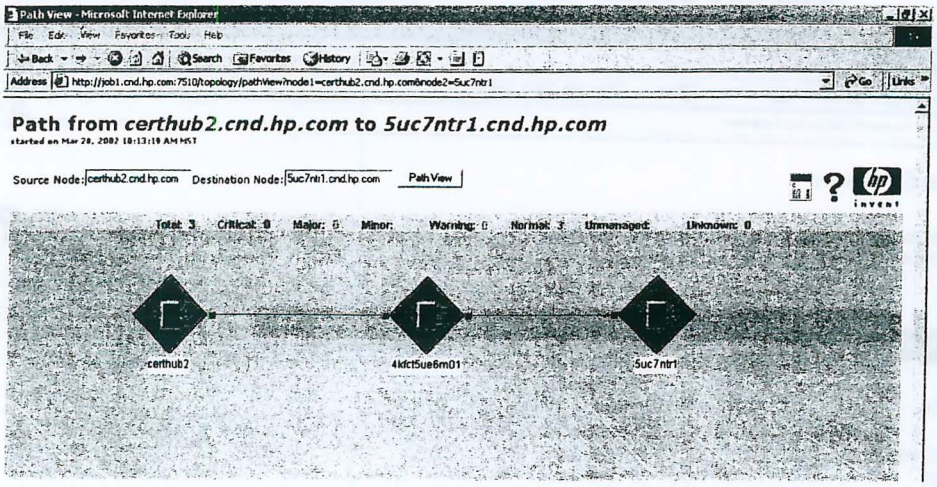
Figure 14-8 Neighbor View Example



Path View

The Path view shows you a graphical representation of the path between two nodes. NNM calculates the shortest path between the source and destination nodes from information contained in the topology database.

Figure 14-9 Path View Example

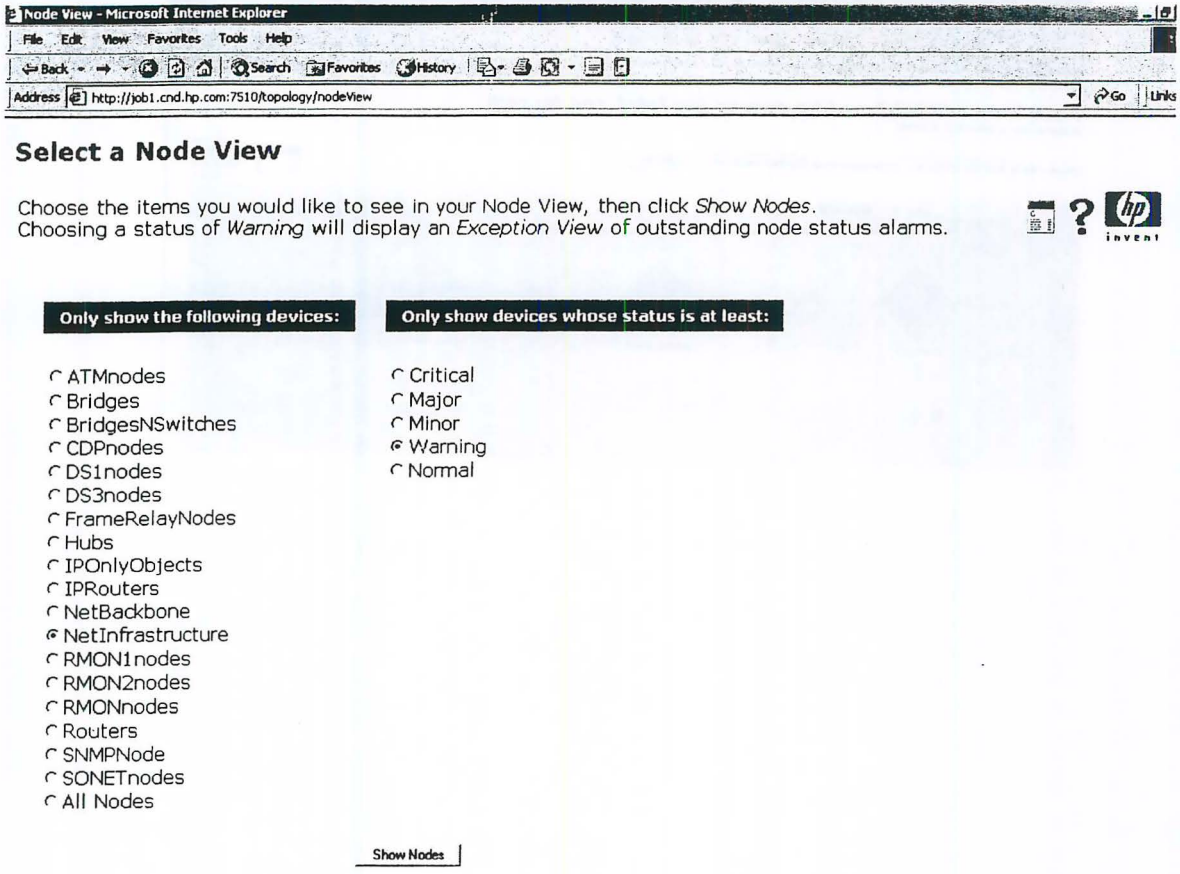


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 519
Doc. 3740

Node View

The Node view creates a visualization of a set of nodes and shows how they are connected. To create a visualization, use the NNM `Tools:Views->Node` menu item. The `Node View` interface contains device types and device status selections as shown in Figure 14-10.

Figure 14-10 Selecting a Node View

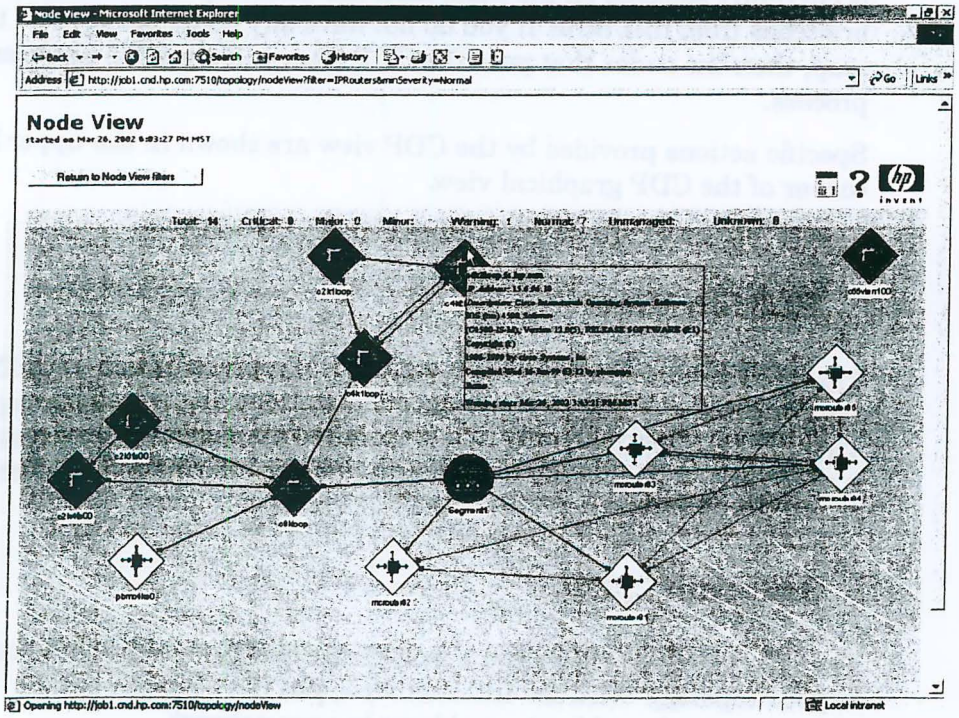


Device selection relies on filters contained within the `filters` file. This is the same file that contains filters such as discovery filters and DHCP filters. The filters file is found in the following locations:

- Windows: *`install_dir`*`\conf\C\filters`
- *UNIX:* `$OV_CONF/C/filters`

For detailed information about how to develop a filter, refer to *A Guide to Scalability and Distribution*.

Figure 14-11 Node View Example



When working with Node view, placing your mouse over a node displays additional information about the node, such as the hostname, IP address, model number and version, system location, and system contact, subject to availability. Single-clicking allows you to zoom in and zoom out on the display. Double-clicking a node shows the node's attributes from the `ovtopodump` command.

CDP View

Cisco Discovery Protocol (CDP) is a Cisco-proprietary protocol that enables the gathering of information about the types of devices in the network, the links between those devices, and the number of interfaces within each device. It runs on Cisco-manufactured devices, including routers, bridges, access servers, and switches.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1046
3740
Doc:

You can view the CDP connectivity of your network by selecting `Tools:Views->CDP` from NNM, the HP OpenView Launcher, or from the Network Presenter. The `Tools:Views->CDP` menu item presents a graphical view of all the CDP nodes in the NNM topology. If a CDP node is currently selected on the map, then the discovery of CDP nodes branches from this node. If you do not have any nodes selected on the map, then the nodes that pass the CDP filter will start the discovery process.

Specific actions provided by the CDP view are shown in the upper left corner of the CDP graphical view.

See *CDP View* in NNM's online help for information.

Station View

The Station view shows you a graphical representation of the NNM collection stations and management stations discovered in your topology. This view is useful only in a distributed management environment. See *A Guide to Scalability and Distribution* for information about distributed environments.

Internet View

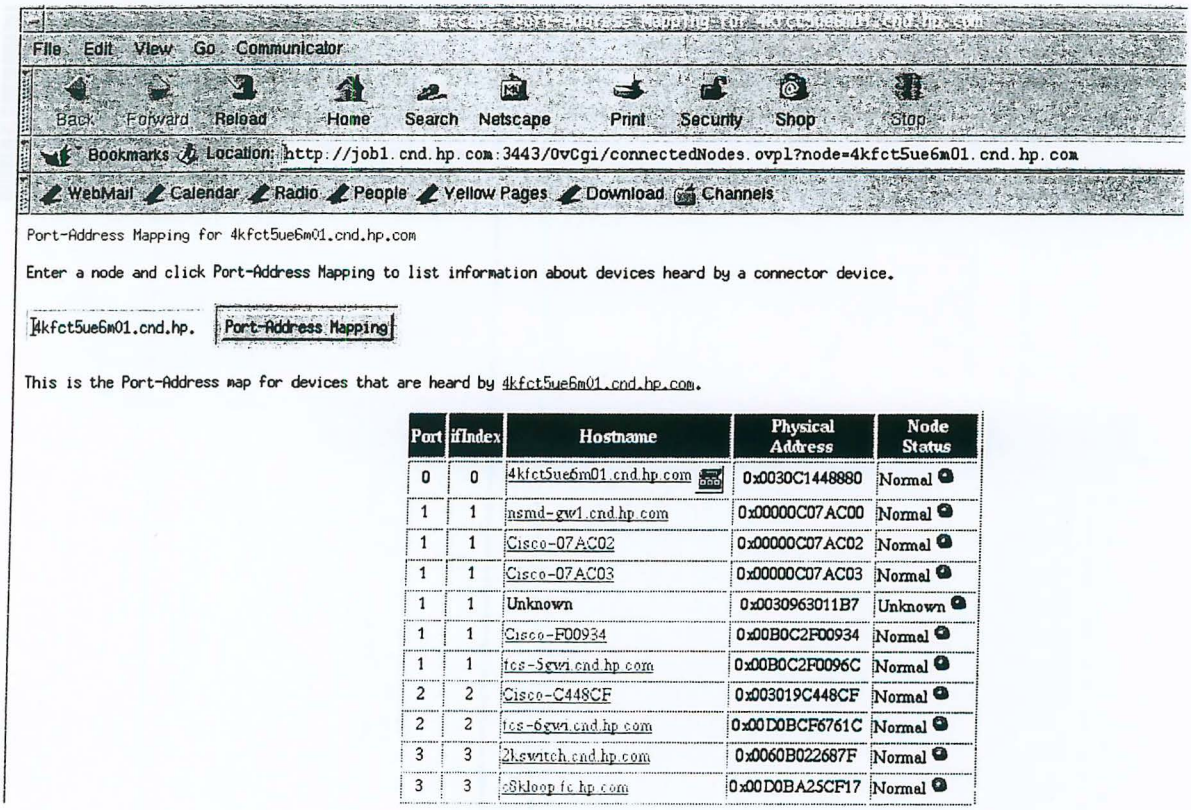
The Internet view shows you a graphical representation of the networks in your topology. With the Internet view, you can view the general status of your network and locate problems in your network.

Port-Address Mapping

By selecting a node and using the `Tools:Port-Address Mapping` menu item you'll see a table of all devices connected to the selected node. The menu item works for most devices that support the *Transparent Forwarding Database MIB* or the *Bridge MIB*.

In Figure 14-12 the user selected device `4kfct5ue6m01` from the NNM map, then used the `Tools:Port-Address Mapping` command to display a table of all of the devices connected to the selected node along with information associated with these connected devices.

Figure 14-12 Example of Port-Address Mapping Table



Port	ifIndex	Hostname	Physical Address	Node Status
0	0	4kfct5ue6m01.cnd.hp.com	0x0030C1448880	Normal
1	1	nsmd-gw1.cnd.hp.com	0x00000C07AC00	Normal
1	1	Cisco-07AC02	0x00000C07AC02	Normal
1	1	Cisco-07AC03	0x00000C07AC03	Normal
1	1	Unknown	0x0030963011B7	Unknown
1	1	Cisco-F00934	0x00B0C2F00934	Normal
1	1	fcs-5gw1.cnd.hp.com	0x00B0C2F0096C	Normal
2	2	Cisco-C448CF	0x003019C448CF	Normal
2	2	fcs-6gw1.cnd.hp.com	0x00D0BCF6761C	Normal
3	3	2l.switch.cnd.hp.com	0x0060B022687F	Normal
3	3	c8kloop.fc.hp.com	0x00D0BA25CF17	Normal

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1047
3740
Doc:

The information associated with each MIB object is displayed one MIB object per line with the MIB value to the right of the MIB label. Any type of MIB object is allowed.

— `Table`. Use this option to display MIB information that constructs a logical table in the MIB (for example, a routing table).

The MIB objects are laid out horizontally, making up the columns of the table. Each entry in the MIB table makes up the rows of the application table. Any type of MIB object is allowed.

NOTE You cannot create table applications which consist of MIB fields from multiple MIB tables.

— `Graph`. Use this option to display numeric MIB information that fluctuates over time (for example, interface statistics). Only numeric MIB values are allowed.

- Plan the menu structure. For example, if you have multiple devices from different vendors, you may want to organize the menu structure such that you have all MIB applications for routers grouped under one menu.

Procedure Tips

Refer to NNM's online help available within the `MIB Application Builder` window for information about how to add, modify, or delete applications.

When you build your applications, keep the following in mind:

- You must provide a unique name for the MIB application.
- You can perform MIB operations on one or more MIB objects at a time.
- Menu path. Decide which NNM menu your application belongs under, such as Performance, Fault, Configuration, or Tools. Use the character sequence -> to separate menu items in the menu path field.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1048
3740
Doc:

If the menu path field is blank, the application is created and automatically registered; however, the application will not appear in the menu bar. This is useful for creating applications to be used as the action for an executable symbol.

- You can specify selection rules for your application. Selection rules determine when a menu item is unavailable and when it is available. They are based upon defined capabilities of the nodes for which this application is compatible. If the application is registered in the menu bar, the menu item for this application is only accessible if the capabilities of the selected nodes match those defined in this selection rule; for example, `isSNMPSupported`. See NNM's online help within the `MIB Application Builder` window for more information.
- You can enter help text for your application. For example, you may want to give a general description of the MIB operation and how to interpret the information that is obtained. When you create the MIB operation menu item, the program automatically adds an entry under:
  - — *Windows:* `Help:On Application`.
  - — *UNIX:* `Help:Misc->Function` and in the dialog box help.

Data Collection & Thresholds

This section describes how to use NNM's Data Collections & Thresholds application to do the following:

- Collect MIB data from network nodes automatically at regularly scheduled intervals.
- Store the collected MIB data in a file.
- Set threshold monitoring on critical devices.

See page 469 for information about viewing the data after it is collected.

TIP You cannot configure Data Collections & Thresholds from NNM's web interface. However, the web-based Alarm Browser displays the alarms resulting from your configurations.

Prerequisites

- The node for which you want to collect data must support SNMP version 1 or version 2c.
- Make sure the correct version of the enterprise-specific MIB that you want to use to collect data is loaded into the MIB database on the management station. (The `Options:Load/Unload MIBs:SNMP` menu item lists all MIB modules currently in the MIB description file.) If the enterprise-specific MIB is not loaded, see "Loading MIBs in the MIB Database" on page 413.
- You can collect data or monitor thresholds on numeric MIB objects; that is, the MIB objects defined as `Counter`, `Gauge`, `INTEGER`, `IpAddress`, `Counter64`, or `TimeTicks`.
- You can collect data on MIB objects with a `String` data type; that is, monitor MIB objects such as `sysContact`.
- To configure your system to collect MIB data, you need to understand the definitions of the MIB objects and what they do.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1049
3740
Doc:



Most device vendors include documentation about their enterprise-specific MIB with their product. This documentation typically describes the MIB object and what the object means. In addition, some vendors include overview information describing strategies for how to manage their specific device. The vendor documentation can give you the conceptual understanding you need to configure your system to collect MIB data.

- Decide if it would be useful to collect the results of a MIB expression (MIB objects combined into a mathematical formula) rather than individual MIB objects. If you want to use a MIB expression, see "Creating and Using MIB Expressions" on page 460 for information about writing and using MIB expressions.
- Identify the nodes on which you will collect data. For example, for a network segment, you may want to collect data on the router, the hubs, and the key file server.
- Identify how often you want to collect data.
- Ensure the management station has enough room to store the data. NNM automatically collects data by default (select `Options: Data Collection and Thresholds` to see the list of current data collections). The amount of disk space required depends upon how much data you collect. For an example, say that you want to collect data for 10 MIB objects on 50 nodes, each with an average of 8 instances of these objects. If you choose a collection interval of half an hour, the collection rate will be 10x50x8x2 = 8000 values/hour. Since each value collected consumes 24 bytes of disk space, the disk consumption rate is 8000x24 = 192,000 bytes/hour.

  Windows: Data is stored in the *`install_dir`*`\databases\snmpCollect` directory.

  UNIX: Data is stored in the `$OV_DB/snmpCollect` directory. If you need more disk space, symbolically link to another file system.

TIP

For HP-UX systems only: You can expand the file system with Logical Volume Manager. Extend the logical volume, then use `extendfs` (hfs) or `fsadm` (vxfs).

Procedure Tips

To access NNM's Data Collection & Thresholds application, from any submap, select `Options:Data Collection & Thresholds:SNMP`. Refer to NNM's online help available from the Data Collection & Thresholds window for directions and additional information.

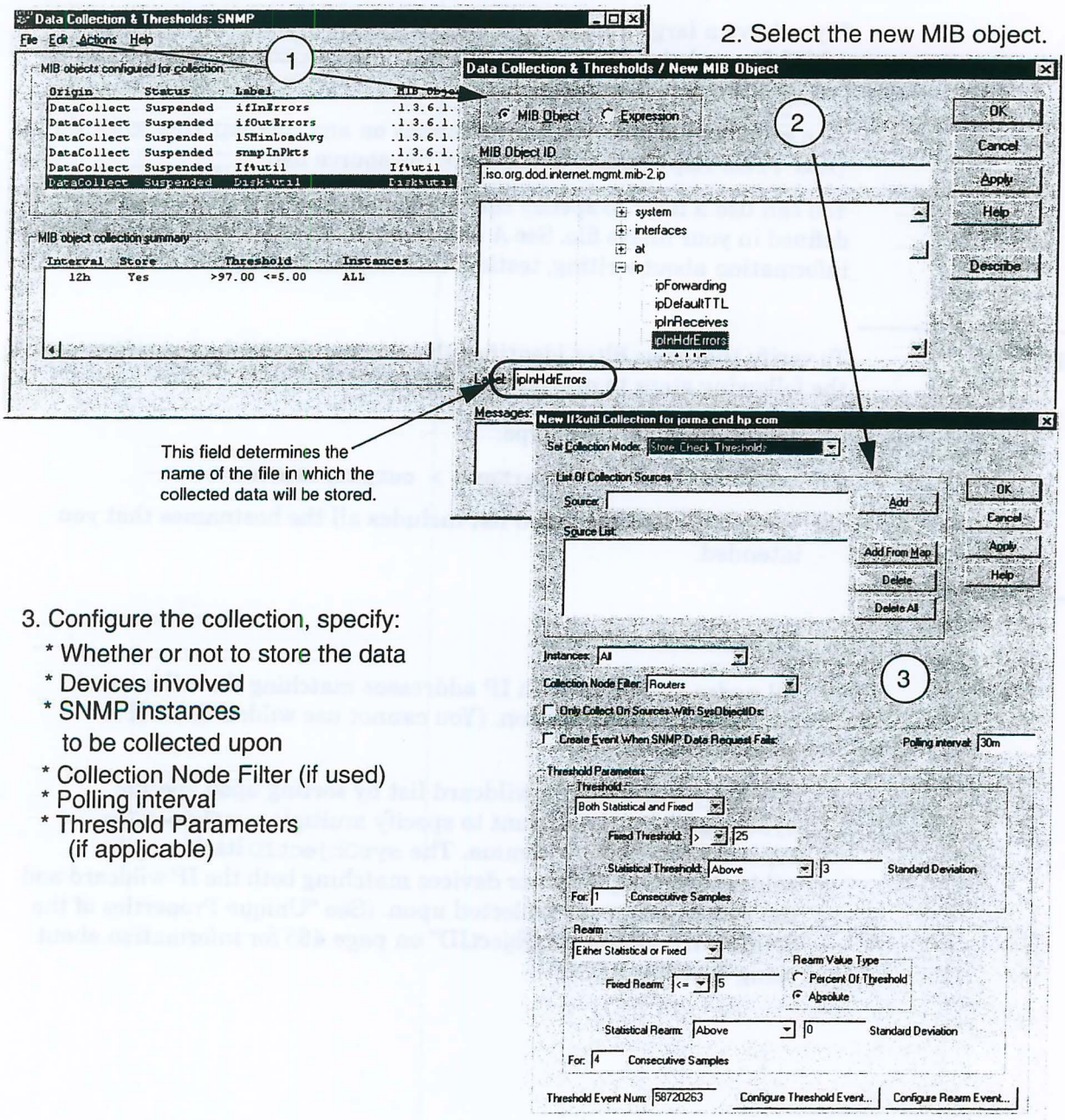
Select the MIB object or expression to be used for data collection. The `Label` field (circled in the following figure) in the MIB selection window determines the file name where the collected data will be stored. (Make

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1050
3740
Doc:

sure the label conforms with file naming conventions for your operating system.) The label defaults to the last component of the MIB mnemonic name.

Figure 12-11 Data Collection Configuration

1. Use Edit:Modify to reconfigure an existing MIB Object or MIB expression for collection.
   or use Edit:New to specify a New MIB Object or expression to collect upon (GET).



3. Configure the collection, specify:
   * Whether or not to store the data
   * Devices involved
   * SNMP instances
     to be collected upon
   * Collection Node Filter (if used)
   * Polling interval
   * Threshold Parameters
     (if applicable)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1051
3740
Doc:

Then, configure the collection and designate the devices to be monitored.

You specify the devices to be monitored by IP host name, `sysObjectID`, IP address, IP address wildcard (such as `15.21.*.*`), and/or (*NNM for Windows only*) IPX address.

If you have a large number of nodes to specify, you can list them in an ASCII file and simply place the full path name to the file in the `List of Collection Sources` field.

As a convenience, you can select sources on any submap, then click the `[Add From Map]` button to populate the source list.

You can use a filter to specify the list of objects. You may use any filter defined in your filters file. See *A Guide to Scalability and Distribution* for information about writing, testing, and implementing a filter.

TIP

To verify that your filter identifies the sources you wish to monitor, use the following steps to preview the list:

1. At the command line, type:

   ```
   ovfiltertest -f filterName > outputFileName
   ```

2. Verify that the generated list includes all the hostnames that you intended.

With wildcard IP addresses:

- All nodes or devices with IP addresses matching the wildcarded address are collected upon. (You cannot use wildcards on IPX addresses.)
- You can further limit a wildcard list by sorting upon specific `sysObjectIDs`. If you want to specify multiple `sysObjectIDs`, separate them with a comma. The `sysObjectID` itself may be wildcarded. Only nodes or devices matching both the IP wildcard and the `sysObjectID` are collected upon. (See "Unique Properties of the SNMP MIB Object sysObjectID" on page 465 for information about using sysObjectID.)

NOTE You *must* save *any* changes for the new configuration to take effect. For example, if you suspend collection on a MIB object by selecting `Actions:Suspend Collection`, the `Status` column in the selection list indicates `Suspended`. However, even though the `Status` column displays a `Suspended` status, this change does not take effect until you select `File:Save`.

The data collection configuration is reanalyzed by `snmpCollect` each time you select `File:Save`. If you used IP wildcards, and you have a large number of managed nodes, there may be a significant delay before collections resume.

Counters are computed by calculating the change per second in the sampled values. Gauges and integers store the actual sampled value.

To view the collected data, open the Data Collection & Thresholds window, highlight the specific collection configuration in the list, and then select `Actions:Show Data`.

TIP SNMP polling requests using the `Options:Data Collection & Thresholds:SNMP` menu item increase the amount of network traffic. If this becomes a problem:

- Change the status for particular collections to `Suspended` from within the Data Collection & Thresholds dialog box.
- Modify the details of your custom data collection by either deleting nodes, deleting instances, excluding nodes, or changing polling intervals.

Defining Thresholds for Monitored MIB Objects

Thresholds let you take a proactive approach to network management. You can manually define thresholds for specific MIB objects that you are monitoring, or have NNM calculate statistical thresholds for you. You can configure events to be posted in the Alarm Browser and/or automatic actions to be taken when the specified thresholds are exceeded. Once you have established a threshold and configured a threshold event, you can

ROS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 1052
3740

use the web Reporting interface to create threshold violation reports. See NNM's online help for more information about the web Reporting interface.

If setting fixed thresholds, first determine what would constitute reasonable thresholds. To decide on a threshold value, you need to know what is normal and what is out of range. Only you can decide what is normal behavior for a device on your network. Generally, HP recommends that you collect information about a device throughout one complete business cycle before determining the normal high/low range. Consider collecting values such as error rates, retry limits, collisions, throughput, relation rates, and many more. Explore the MIB being used to determine which information to collect.

As soon as you install NNM, data collections on certain MIB objects are started. (You can see which objects are being collected from which devices by selecting `Options:Data Collection and Thresholds`.) This data is available for automatically setting thresholds based upon deviation from normal values. NNM uses the following process to establish statistical thresholds based upon the data being collected:

1. NNM gathers data as configured in Data Collection & Thresholds (the `snmpCollect` background process collects, compares, and stores requested SNMP MIB values).
2. NNM exports the collected *trend* data to the data warehouse every hour. See the *request_list* reference page in NNM's online help (or the UNIX manpage) for information about when NNM runs export tasks.
3. The data warehouse computes, for each instance of each configured collection:
   - The number of data points gathered in the past four days
   - The data summary
   - The sum of the squares for each collection

   This information, from the previous four days, is written to the `snmpColStats.txt` file. This file is recreated each time data is exported to the data warehouse. A notification event is sent to `snmpCollect`.

   These data points are sorted into three time periods, 8 p.m.-5 p.m., 5 p.m.-8 a.m., and weekends. See the *statTimeRanges.conf* reference page in NNM's online help (or the UNIX manpage) for information about controlling the definitions of the time periods.

4. When using automatic statistical threshold generation for a data collection configuration, `snmpCollect` reads `snmpColStats.txt` and calculates, one threshold standard deviation for each time period (bucket) for each data collection instance. Every time the `snmpColStats.txt` file is read, NNM compares the standard deviation calculations to the standard deviation that you specified. An alarm is generated if the current standard deviation exceeds the threshold standard deviation. See the *snmpCollect* reference page in NNM's online help (or the UNIX manpage) for more information.

   Multiple thresholds are allowed per node, one for each instance; for example, one threshold set for a primary hard drive, and a different threshold set for the secondary hard drive.

CAUTION If you are using `ovdwtrend -trim` or `-delete` options to manage the volume of your collected data, ensure that your schedule allows sufficient data history for the statistical threshold feature. See the *ovdwtrend* reference page in NNM's online help (or the UNIX manpage) for information.

Prerequisites

- Configure the data collection to which the threshold applies (see "Data Collection & Thresholds" on page 447).
- You can monitor thresholds on numeric MIB objects; that is, the MIB objects defined as `Counter`, `Gauge`, `INTEGER`, `IpAddress`, `Counter64`, or `TimeTicks`. You can also set thresholds on MIB expressions (see "Creating and Using MIB Expressions" on page 460).

Procedure Tips

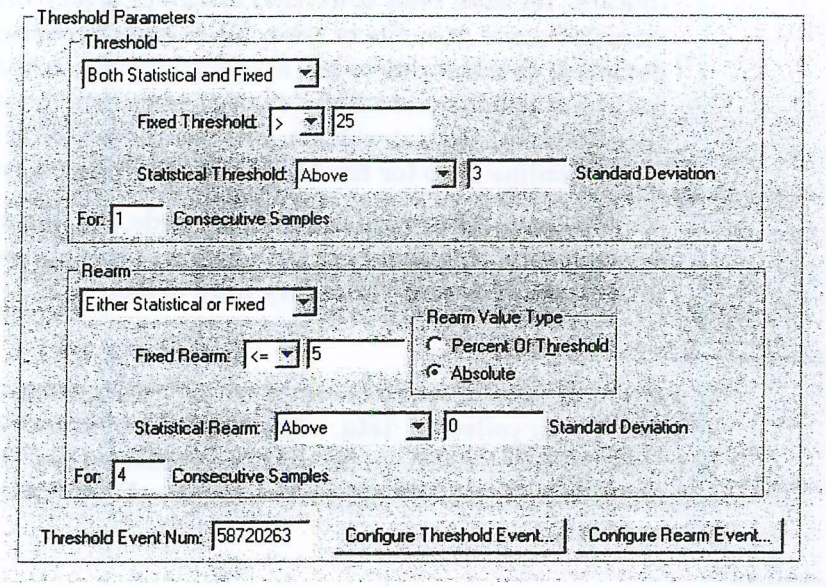
Access the collection configuration dialog box of the configured Data Collection you have been using to establish the normal operating range of your device. Select *one* of the following menu items from the `Option` menu next to the `Collection Mode` label:

- `Don't Store, Check Thresholds`
- `Store, Check Thresholds`
  (required if you want to use the statistical threshold feature)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1053
3740

The Threshold and Rearm fields are now available.

Figure 12-12 Threshold Area of Data Collection Window



To set up fixed-value threshold monitoring, select "Fixed" or "Both Statistical and Fixed" mode, specify a threshold value, and specify the number of consecutive samples required to violate the threshold. To set up fixed-value rearm monitoring, specify a fixed rearm value or percent, and the number of consecutive samples required to rearm the threshold.

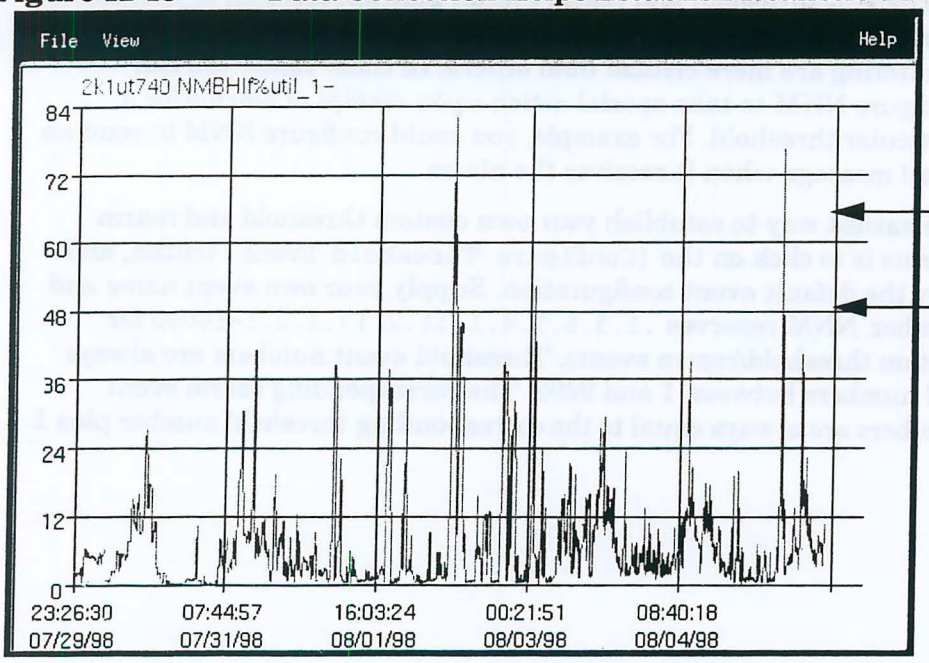
To set up automatic statistical threshold monitoring, select "Statistical" or "Both Statistical and Fixed" mode, specify the standard deviation, and specify the number of consecutive samples required to violate the threshold. To set up automatic statistical rearm monitoring, select "Both Statistical and Fixed" or "Either Statistical and Fixed" mode, specify standard deviation, and specify the number of consecutive samples required to violate the threshold. NNM automatically calculates the standard deviation according to the data warehouse's schedule for exporting trend data.

When the threshold setting is exceeded, a threshold-exceeded alarm is posted in the Alarm Browser, and any automatic actions (such as dialing a pager) that you specify in the Event Configuration are executed.

The *rearm value* controls how frequently a threshold event is generated. The *rearm* indicates that the device has returned to a non-critical state. A *rearm alarm* is posted in the Alarm Browser and any automatic

actions that you specified in the Event Configuration are executed. Another threshold event is not generated until the rearm event occurs and the collected value again reaches the threshold setting.

Figure 12-13 Data Collection Helps Establish Realistic Thresholds



For example, suppose you want to monitor interface percent-utilization. You can set a `Threshold` of 70% and a `Rearm` value of 50%. When the data collector detects a value above 70%, a threshold alarm is generated. Another threshold alarm will be generated only if the reading drops below 50% (sending a rearm alarm) and then goes above 70% again. Note that you can also specify absolute values rather than percentages.

Optionally, specify a value for the `Consecutive Samples` field. This value specifies the number of consecutive times the `Threshold` or `Rearm` expression must be satisfied before a corresponding alarm is generated. This field lets you distinguish sustained abnormality from a brief spike in behavior.

NNM uses two preconfigured events under the `OpenView` enterprise name (`.1.3.6.1.4.1.11.2.17.1.0.`) as the default events for thresholds and rearms:

```
OV_DataCollectThres (58720263)
```


ROS nº 03/2005 - CN - CPMI - CORREIOS Fls.,Nº 1054 3740 Doc:



`OV_DataCollect_Rearm (58720264)`

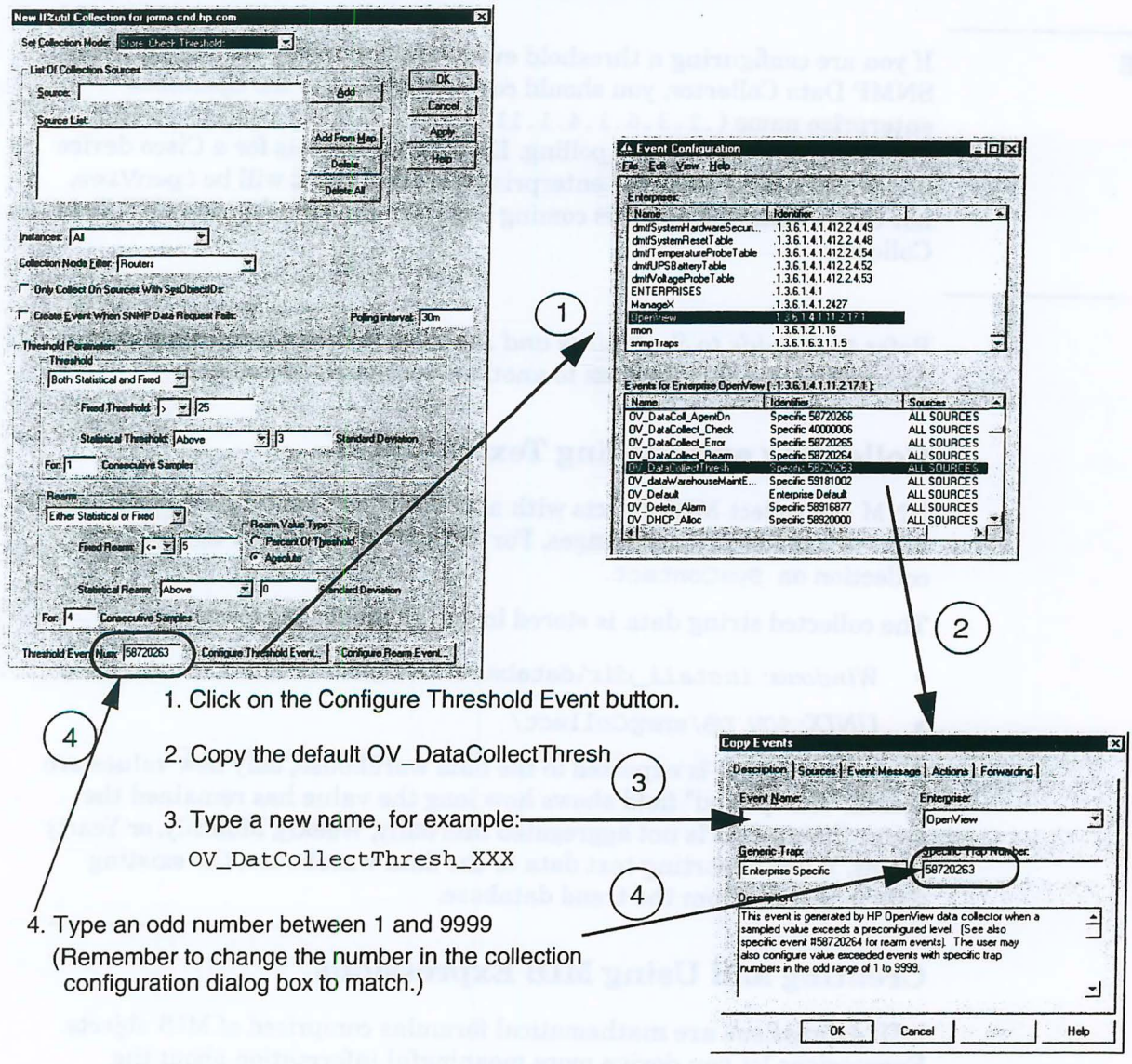
The default alarm is posted in the Alarm Browser's Threshold Alarms category.

The default threshold and rearm events may not meet all of your needs. Suppose, for example, that some of the threshold values you are monitoring are more critical than others. In these cases, you can configure NNM to take special action upon receipt of alarms for a particular threshold. For example, you could configure NNM to send an email message when it receives the alarm.

The easiest way to establish your own custom threshold and rearm alarms is to click on the `[Configure Threshold Event]` button, and copy the default event configuration. Supply your own event name and number. NNM reserves `.1.3.6.1.4.1.11.2.17.1.0.1-10000` for custom threshold/rearm events. Threshold event numbers are always odd numbers between 1 and 9999. The corresponding rearm event numbers are always equal to the corresponding threshold number plus 1.

NOTE If you create a custom threshold event, you must also create a matching rearm event.

Figure 12-14 Customizing the Threshold Event



RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls., Nº 1055
3740
Doc:

For example, the threshold event ID 1005 will have a rearm event ID of 1006. These rearm event IDs are automatically assigned but *not* automatically configured in NNM. If you use one of the optional threshold event numbers, you must configure events for both the threshold and rearm event IDs (use the `[Configure Threshold Event]` and `[Configure Rearm Event]` buttons).

NOTE

If you are configuring a threshold event created by the HP OpenView SNMP Data Collector, you should configure it under the `OpenView` enterprise name (`.1.3.6.1.4.1.11.2.17.1.0.`), regardless of which node the Data Collector is polling. Even if the event is for a Cisco device exceeding a threshold, the enterprise ID of the event will be `OpenView`, not Cisco, since the event is coming from the HP OpenView SNMP Data Collector.

Refer to *A Guide to Scalability and Distribution* for information about forwarding threshold events to another management station.

Collecting and Storing Textual Data

NNM can collect MIB objects with a `String` data type. This data can be used to monitor device changes. For example, you can set up data collection on `SysContact`.

The collected string data is stored in the following locations.

- *Windows:* *`install_dir`*`\databases\snmpCollect\`
- *UNIX:* `$OV_DB/snmpCollect/`

When string data is exported to the data warehouse, only new values are stored. The "period" field shows how long the value has remained the same. String data is not aggregated into daily, Weekly, Monthly, or Yearly tables. When exporting text data to the data warehouse, the existing data is deleted from the trend database.

Creating and Using MIB Expressions

MIB expressions are mathematical formulas comprised of MIB objects. Expressions let you derive more meaningful information about the health of your network than you could gather using individual MIB objects. MIB expressions are used by several NNM components, and are

available for your use through the Data Collection & Thresholds window. You can also create your own and add them to the list by making additions to the `mibExpr.conf` file and the `mibExpr.conf` file.

Default MIB Expressions

NNM includes many default MIB expressions for your convenience. To explore the default MIB expressions, from any submap, select `Options:Data collection & Thresholds`, then select the following menu item:

Windows: `Edit:MIB Object->New`

UNIX: `Edit:Add->MIB Objects...`

Select the `Expressions` radio button. The list of predefined MIB expressions is displayed for your use. The following are a small sampling of the MIB expressions provided:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1056
3740
Doc:

Equation 12-1 **If%deferred (MIB II)**
The percent of packets on an interface which were deferred:

$$(\text{packets deferred rate} \div \text{packets transmitted rate}) \times 100$$

Equation 12-2 **If%collision (MIB II)**
Percent of packets on an interface which collided:

$$(\text{collision rate} \div \text{packets transmitted rate}) \times 100$$

Equation 12-3 **If%inErrors (MIB II)**
Percent of input packets on an interface which had an error:

$$\left(\frac{\text{input error rate}}{\text{received unicast packet rate} + \text{received non-unicast packet rate}}\right) \times 100$$

Equation 12-4 **If%outErrors (MIB II)**
Percent of output packets on an interface which had an error:

$$\left(\frac{\text{output error rate}}{\text{transmitted unicast packet rate} + \text{transmitted non-unicast packet rate}}\right) \times 100$$

Equation 12-5 **If%util (MIB II)**
Percent of available bandwidth utilized on an interface:

$$\left(\frac{(\text{received byte rate} + \text{transmitted byte rate}) \times 8}{\text{interface link speed}}\right) \times 100$$

Equation 12-6 **IfInOutOctets (MIB II)**
Total absolute traffic on an interface or the summation of octets (bytes) sent and received on an interface:

$$\text{received byte rate} + \text{transmitted byte rate}$$

Equation 12-7 **IfInOutPackets (MIB II)**
Total absolute traffic on an interface or summation of packets sent and received on an interface:

$$\left(\frac{\text{received unicast packet rate}}{\text{received non-unicast packet rate}} + \frac{\text{transmitted unicast packet rate}}{\text{transmitted non-unicast packet rate}}\right)$$

Equation 12-8 **Disk%util (HP-UX MIB)**
Percentage of disk utilization:

$$\left(\frac{\text{blocks} - \text{free blocks}}{\text{blocks} - \text{free blocks} + \text{available blocks}}\right) \times 100$$

Simply select one from the list and configure it for data collection and/or threshold monitoring on your network's devices.

TIP

There are seven additional MIB expressions defined specifically for use with the HP-extensible agent. They are located in:

- *Windows:* `install_dir\conf\extExpr.conf`
- *UNIX:* `$OV_CONF/extExpr.conf`

Open the file to read about them.

The mibExpr.conf File

The expressions are stored in an ASCII file:

- *Windows:* `install_dir\conf\mibExpr.conf`
- *UNIX:* `$OV_CONF/mibExpr.conf`

You can modify this file or create your own expressions using the `xnmcollect -loadExpr` utility. Best practice is to create a separate file with your new or revised MIB expressions, and then merge the expressions into the `mibExpr.conf file` using the following utility from the command prompt:

```
xnmcollect -loadExpr filename
```

The `-loadExpr` checks syntax, removes duplicate expressions, and rewrites the file.

See the *mibExpr.conf* reference page in NNM's online help (or the UNIX manpage) for information about writing your own MIB expressions; and see the *xnmcollect* reference page in NNM's online help (or the UNIX manpage) for information about updating the `mibExpr.conf` file.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1057
3740
Doc:

The mib.coerce File

The `mibExpr.conf` file works in partnership with the `mib.coerce` file. Entries in the `mib.coerce` file instruct NNM to convert (coerce) a received MIB value from one data type to another (for example, from a gauge or counter to an integer) for use in the mathematical formula defined in the `mibExpr.conf` file. The `mib.coerce` file is an editable ASCII file:

- *Windows:* `install_dir\conf\mib.coerce`
- *UNIX:* `$OV_CONF/mib.coerce`

After making changes to the `mib.coerce` file, you must force NNM to acknowledge the changes; from the command line, type:

```
xnmloadmib -event
```

See the *mib.coerce* reference page in NNM's online help (or the UNIX manpage) for more information about converting MIB values from one data type to another for use in your MIB expression.

Unique Properties of the SNMP MIB Object sysObjectID

The `sysObjectID` is an important SNMP MIB object to NNM operations. This section describes:

- What the `sysObjectID` is
- How network management operations use the `sysObjectID`

The `sysObjectID` is registered in the Internet-standard MIB-II module as `iso.org.dod.internet.mgmt.mib-2.system.sysObjectID` (`1.3.6.1.2.1.1.2`). The `sysObjectID` is used for administrative purposes to uniquely identify the type of SNMP agent software that is running on a given vendor's hardware. This object is different from most other MIB objects; when you query it, you get back an object identifier that describes the product. For example, when you query the `iso.org.dod.internet.mgmt.mib-2.system.sysObjectID` using the MIB Browser on an HP OpenView SNMP Agent that is running on an HP 9000 Series 700 or Sun SPARCstation, SNMP returns one of the following object identifiers:

```
iso.org.dod.internet.private.enterprises.hp.nm.system.hpsun.sparc.sun4
iso.org.dod.internet.private.enterprises.hp.nm.system.hpsun.sparc.sun5
iso.org.dod.internet.private.enterprises.hp.nm.system.hpux.hp9000s700
```

This result tells you how the HP 9000 Series 700 or Solaris agent is registered in the MIB. The numeric identifier for Solaris is `1.3.6.1.4.1.11.2.3.10.1.2`

Note that there is no value associated with the object ID returned in `sysObjectID`. It is a unique identifier.

The `sysObjectID` includes both hardware and software information, and varies depending on the type of hardware and agent software. Some vendors have a different `sysObjectID` for every version of their agents. For example, Hewlett-Packard sells several SNMP agents, each uniquely identified. To distinguish the HP 9000 Series 800 agent from the HP 9000 Series 700 or Solaris agent, HP registered the HP 9000 Series 800 agent as:

```
iso.org.dod.internet.private.enterprises.hp.nm.system.hpux.hp9000s800
```


ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1058
3740
Doc:

netmon, a service (background process) that automatically discovers the nodes on your network, obtains the sysObjectID when it queries SNMP nodes. NNM operations take advantage of this special object in the following ways:

- To identify the vendor; that is, the manufacturer of the hardware.
- To identify the source of the SNMP agent, which is the type of agent software running on the hardware. For example, if you do a GetRequest to a Sun SPARCstation, the vendor is Sun, but the SNMP agent may be
  - — An HP OpenView SNMP Agent for SunOS
  - — An SCO UNIX for SunOS agent
  - — Other SNMP agent software
- To determine IP topology behavior. An agent's sysObjectID provides hints about what type of node the agent is; for example, a gateway, a bridge, or a host.
- To determine symbol type when putting symbols for newly discovered nodes on the map; for example, a bridge, a gateway, or a hub.
- To identify the source of an event. A sysObjectID is sent in every event. You can use the sysObjectID when you configure events and data collections. The reference in the Event Configuration dialog box to enterprise ID is generally synonymous with the sysObjectID of the agent that generated the event.

Like NNM, you can take advantage of the sysObjectID in many ways, such as:

- From any submap, select Find:Object By Attribute to locate quickly all of a certain manufacturer's model-X when they require a software upgrade.
- If you are writing a rules-based application or script, use the sysObjectID as a rule index.
- On any submap, select a node and use Edit:Object Properties to quickly determine which SNMP agent is running on that node.
- Use the sysObjectID in your filter definitions: discovery, topology, map, etc.

- Use the `sysObjectID` when using the `ovtopodump` command to generate useful lists.
- Customize NNM to display a symbol that you created for a specific type of object (see Appendix D, "Changing All the Symbols for a Particular Device," on page 661).
- If NNM displays an object on the map with a generic symbol (just the outside shape, no vendor-specific icon within the shape), you can specify the icon of your choice to be mapped to that device's `sysObjectID` (see Appendix D, "Changing All the Symbols for a Particular Device," on page 661).
- Specify nodes for which data should be collected, as described in the previous section.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1059
Doc. 3740

13 Using Event Data

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1060
3740
Doc:



NNM provides several features that can assist you in analyzing the network data that has been collected:

- *Graph SNMP Data* (page 471)

  Display collected SNMP data in graphs. This can be SNMP data that has been collected over time and stored in a file, or real-time values that are graphed as they are collected, or both at the same time.

- *Data Warehouse* (page 476)

  Allows you to export collected historical data for use with other statistical analysis tools. Command line functions allow you to maintain the data warehouse database.

- *Web Reporting Interface*

  Allows you to use data from the data warehouse to create reports using a set of predefined templates. See the *Reporting and Data Analysis* online manual and the online help for more information.

NOTE

For information about how to merge data from multiple NNM collection stations into a single database, see *A Guide to Scalability and Distribution.*

Ideas for utilizing your collected data:

- Anticipate the need for more network and computer resources, such as gateways and disk space.
- Detect deviations in normal activity.
- Isolate network faults and performance problems.
- Generate inventory reports.

Graphing SNMP Data

The NNM Grapher tool allows you to graph collected MIB data from within the SNMP MIB Browser. Once the Grapher window is displayed, you can set time intervals to continue the collection and even automatically establish a configuration for continuous monitoring by selecting `File:Configure in Data Collector`.

The NNM Grapher tool also enables you to organize MIB data that was collected by the Data Collections & Thresholds feature and view it in graph form. You can graph combinations of data values in the same graph. The data values can be different instances of MIB variables or different variables for different nodes. For example, you can graph instance 1 and instance 3 of a MIB variable for one system, or you could graph instance 3 of a MIB variable for one system, and a completely different variable for another system. You can also normalize the data over configurable time periods to identify trends in the historical data.

This section describes the following:

- Graphing collected data, which includes graphing all data or graphing selected data only, and updating data that has been graphed.
- Graphing historical and real-time data in the same graph.
- Zooming in and out of a specific period of time to view the data in greater or less detail.
- Modifying line attributes in a graph.
- Printing a graph.

NOTE The Grapher tool is available in NNM on a Windows or UNIX operating system. If you are using NNM on the Web, there is a Grapher tool available in the `contrib` directory. (See page 74 for information about using programs from the `contrib` directory.)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1061
3740
Doc:

Graphing Collected Data

You can graph the data collected in the Data Collector's database by using the `Performance:Graph SNMP Data->All` and `Performance:Graph SNMP Data->Selected Nodes` menu items. You can also access the Grapher tool from within the SNMP MIB Browser or by using the `xnmgraph` command. Refer to the *xnmgraph* reference page in NNM's online help (or the UNIX manpage) for more information.

Behavior

The Graph Selected Nodes dialog box consists of a line graph. The legend across the top of the graph identifies the currently graphed data. Time is shown on the X-axis.

The menu bar has functions that enable you to manipulate the data. The menu bar also has help entries explaining how to use the different menu options to manipulate the data.

The Graph SNMP Data operation does not update the graph with new information as the data is collected. To update the graph with the most current MIB data, select `File:Update Data` from the Grapher menu bar.

Refer to the online help within the graph window for additional information.

Graphing All Data

The `Performance:Graph SNMP Data->All` operation enables you to view collected data in graph form without first having to build an application. This is useful when you want to browse all the data in the Data Collector's database:

- *Windows:* Data is stored in the *`install_dir`*`\databases\snmpCollect` directory.
- *UNIX:* Data is stored in the `$OV_DB/snmpCollect` directory. (If you need more disk space, symbolically link to another file system.)

TIP

For HP-UX systems only: You can expand the file system with Logical Volume Manager. Extend the logical volume, then use `extendfs` (hfs) or `fsadm` (vxfs).

Use this operation when you want to graph some data points just once, or when you want to compare different variables across different systems. For example, let's say you want to compare the load averages to the number of packets, but had not used the Application Builder (see page 443) to set up your own application for this purpose. You can easily use the Graph All operation to graph these two variables together.

CAUTION This operation reads in *all* the collected data from the Data Collector database into its memory. Depending on the amount of data stored in the database, displaying the Graph All dialog box may take a long time.

Graphing Data on Selected Nodes

The `Performance:Graph SNMP Data->Selected Nodes` operation enables you to view collected data on the nodes that are currently selected on the map, without having to use the Application Builder (see page 443) to set up your own application for this purpose. This is useful when you want to browse the collected data for these nodes. Use this operation when you want to graph some data points just once, or when you want to compare different variables across different systems.

For example, let's say you want to compare the load averages to the number of packets on the selected systems, but had not used the Application Builder (see page 443) to set up your own application for this purpose. You can use the Graph Selected Nodes operation to easily graph these variables together.

Graphing Historical and Real-Time Data in the Same Graph

When you use the Grapher tool via an NNM-provided menu item, the Grapher displays both the collected data and real-time data in the same graph (for example, `Performance:Network Activity`).

When Grapher starts up, it does the following:

1. Reads in the data from the Data Collector's database.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1062
3740
Doc:

When the Grapher tool first comes up, it loads all the collected data from the Data Collector database and seeds its memory with the information in the database. The resolution of the collected data is determined by what the Data Collector was configured to collect.

Once the Grapher tool is running, the tool does not interact with the data in the Data Collector database again (unless you select `File:Update Data`). The Data Collector operates in the background and continues to collect data. This data is available for you to use in future operations.

2. Starts to graph the real-time data.

   The real-time data displayed is independent of the Data Collector. The Grapher tool processes SNMP requests based on the interval specified under `View:Time Intervals` and displays the data in the graph. Unless you save the graphed data to a file using the `File:Save As` menu item, the real-time data is lost as soon as you exit the Grapher.

Stopping Real-Time Data Graphing

To stop real-time data graphing, from the Graph window:

- *Windows:*

  Select `Options:Time Intervals->SNMP Polling Off`.

- *UNIX:*

  Select `View:Time Intervals->SNMP Polling Off`.

Grapher Operations

This section describes some common operations for manipulating a graph.

Selecting Time Intervals

To select time intervals, using the left mouse button:

- Click on the left edge of the graph to page back one screen.
- Click on the right edge of the graph to page forward one screen.
- Click within the graph to center the graph around the selected point in time. Holding the mouse button down and dragging enables you to fine tune the point that you want centered.

Zooming In and Out of a Graph

The Grapher allows you to zoom in and out of a specific period of time in order to view data in greater or lesser detail. To do so, using the right mouse button, click anywhere within the graph. An option menu appears. You can zoom in and out to different amounts of detail. You can also use the menu to page forward, page backward, or show different data points.

Modifying a Line Attribute

To access the `Line Configuration` dialog box, from the Graph window:

- *Windows:* Select `Options:Line Configuration`.

  Option buttons are arranged in rows and columns. Each item in the list controls the attributes for a particular line on the graph.
- *UNIX:* Select `View:Line Configuration`.

  Option buttons are arranged in rows and columns. Each row in the list controls the attributes for a particular line on the graph.

Printing a Graph

To Print a graph, from the Graph window:

- *Windows:* Select `File:Print`. The standard `Print` dialog box appears. Make your selections and click `[OK]`.
- *UNIX:* An `xwd`-compatible file is produced by the Grapher. The default `Print` command is configured in the Grapher print resource. The commands shown in the Print Command window are used to print that file. If the default command does not meet your needs, you can change it. Before you configure the default `Print` command, determine which command options will give you the best printouts. See NNM's online help for more information.

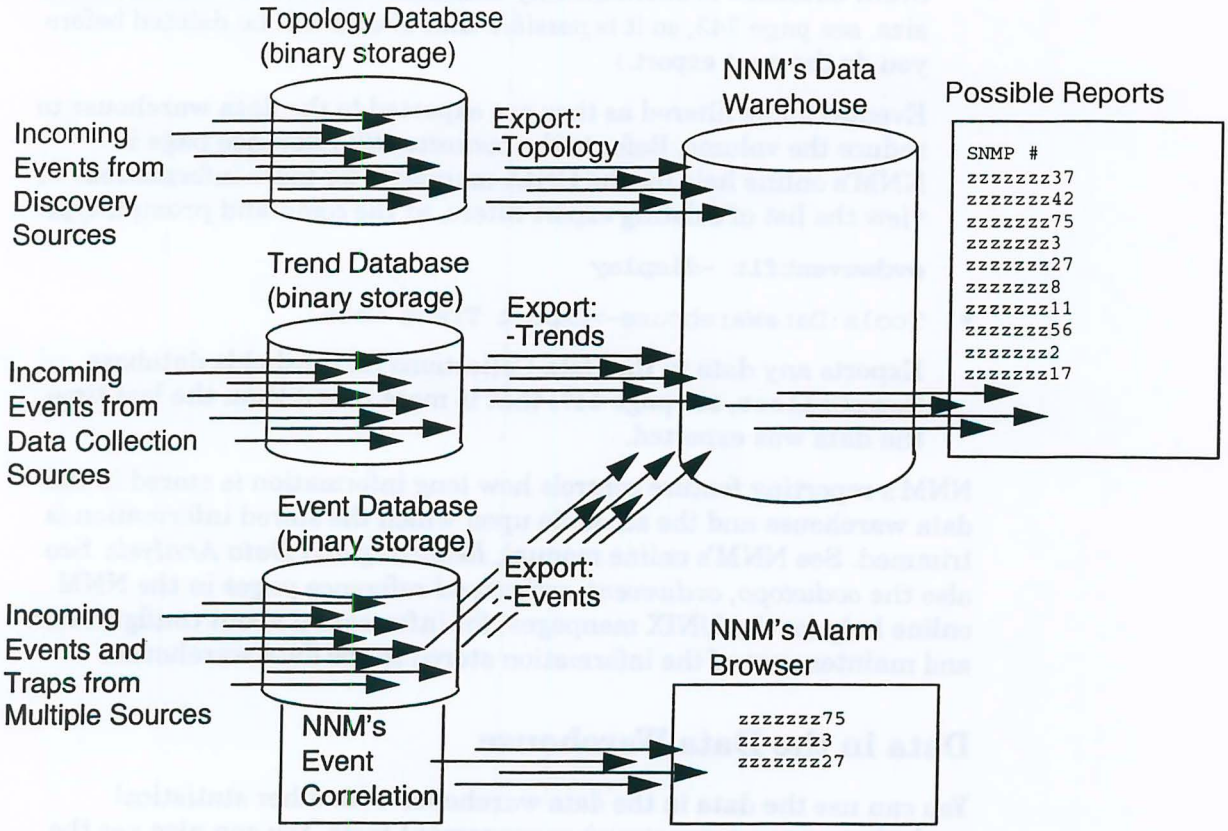
ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1063
3740
Doc:

Data Warehouse

The NNM data warehouse is a relational database (RDBMS) provided with NNM. NNM stores a *copy* of the information from the NNM operational databases into the data warehouse so you can gain an historical perspective of your network information. The data warehouse information is accessible with standard SQL statements using ODBC tools. You can also create reports from the data using the NNM web Reporting interface.

By contrast, the information in the NNM *event database* is discarded when a certain volume is reached (see page 343). Information copied to the *data warehouse* is retained for as long as you need it. You can derive reports from hourly, daily, weekly, monthly, or even yearly information. The limit to the size of the data warehouse is up to you and the allotted hard drive space for the data warehouse.

Figure 13-1 NNM's Event Flow



NNM periodically populates the data warehouse according to a schedule. See the *ovrequestd* and *request_list* reference page in NNM's online help (or the UNIX manpage) for more information. To view the current schedule, at the command prompt, type:

```
request_list schedule
```

You can also manually populate the data warehouse using the following pull-down menu items:

- `Tools:DataWarehouse->Export Topology`

  Exports the current network topology information, replacing any topology information previously sent to the data warehouse.

- `Tools:DataWarehouse->Export Events`

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls: Nº 1477
3740
Doc:

Exports any event database information that is more current than the last time the events database was exported. (Remember: NNM's event database is automatically trimmed when it reaches maximum size, see page 343, so it *is possible* that events will be deleted before you do the next export.)

Events can be filtered as they are exported to the data warehouse to reduce the volume. Refer to the *ovdweventflt* reference page in NNM's online help (or the UNIX manpage) for more information. To view the list of existing export filters, at the command prompt, type:

```
ovdweventflt -display
```

- `Tools:DataWarehouse->Export Trend Data`

  Exports any data in the Data Collections &Thresholds database (`snmpCollect`, see page 447) that is more recent than the last time the data was exported.

NNM's reporting feature controls how long information is stored in the data warehouse and the schedule upon which the stored information is trimmed. See NNM's online manual, *Reporting and Data Analysis.* See also the *ovdwtopo*, *ovdwevent*, *ovdwtrend* reference pages in the NNM online help (or the UNIX manpages) for information about configuration and maintenance of the information stored in the data warehouse.

Data in the Data Warehouse

You can use the data in the data warehouse with other statistical analysis programs or network management tools. You can also use the data to create reports with NNM's web Reporting interface.

See the NNM online manual, *Reporting and Data Analysis.* See also the NNM online help.

Reporting

Reporting is enabled by default when NNM is installed. Once the report data is collected, daily and month-to-date reports for general availability, threshold violation exceptions, and network performance are available from the `Tools:Report Presenter` command or from the HP OpenView Launcher. Daily Inventory reports are available as soon as the report data is collected. For more information about reporting see page 45 in this manual.

For more information about the Reporting feature, see the section labeled "Reporting Interface" on page 516 in this manual.

For more information about the NNM databases and the data warehouse, consult the online manual *Reporting and Data Analysis*.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1065
3740
Doc:

14 NNM on the Web

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls! Nº 1066
3740
Doc:



NNM on the Web

This chapter describes HP OpenView's Java™-based web interface, and tells you how to set up, configure, and administer NNM's web applications.

This chapter will not attempt to teach you how to use all the features of HP OpenView's web interface. You should consult the NNM online help within the web interface for usage instructions. For an introduction, explore the *Get Acquainted with HP OpenView Network Node Manager: Training for NNM Operators* CD provided with NNM.

This chapter refers to HP OpenView Application Registration Files (ARF) in several places. If you are not familiar with that file, review its functionality in the online manual *Creating and Using Registration Files*.

TIP

If you make changes or additions to the web registration files ensure that your new files are properly backed up. They are *not* included in NNM's backup scripts. See "Backup/Restore to Protect Your Investment of Time" on page 165 for more information.

This chapter includes:

- An overview of the HP OpenView web applications, including setting up the web applications and security for the web applications (page 484).
- A description of the HP OpenView Launcher, the UI integration point for the web applications, including configuration details (page 492).
- A description of the Network Presenter, the web application that displays maps and map data (page 501).
- A description of the SNMP Data Presenter, which displays the results of operations that gather data from managed SNMP nodes (page 509).
- A description of the web-based Alarm Browser, a graphical interface that presents network alarm data, including a comparison of the web-based Alarm Browser and the Alarm Browser running on the management station (page 512).
- A description of Event Correlation Services, NNM's multi-protocol event correlator (page 515).

- A description of the Reporting interface, the web application that allows you to configure and view reports (page 516).
- A description of several supplemental views of discovered nodes (page 518).

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1067
3740
Doc:

Overview

HP OpenView's Java-based web interface further expands NNM's network management capabilities. A part of NNM's base product, the web interface and its applications present the same information about your network that is available from the NNM management station. This information is now presented in a familiar, operator-friendly format that you can access from a remote workstation running a web browser. From your web browser on any PC or UNIX operating system workstation, you can log onto the web and access NNM on the management station to display maps and alarm information. You can easily monitor the status of your network from any place at any time, a real advantage when your pager goes off in the middle of the night!

The HP OpenView Web lets you:

- Inquire about the status of your network and troubleshoot problems from anywhere via the World Wide Web.
- Obtain dynamic updates on map information.
- Share management data with others.
- Present both a graphical and tabular view of the network.
- Access and configure security for web applications.
- Launch NNM and other web-based applications.
- Interact with a familiar web interface.
- Configure and view reports.

The HP OpenView Web includes the following applications:

- HP OpenView Launcher
- HP OpenView Network Presenter
- HP OpenView SNMP Data Presenter
- HP OpenView Alarm Browser
- HP OpenView ECS Configuration
- HP OpenView Correlation Composer
- HP OpenView Reporting interface

An overview and the administration of each of these applications is discussed in the following sections of this chapter.

Setting Up the HP OpenView Web

When you install NNM on the management station the files and applications necessary to run the web interface are also installed. The management station must also have a web server running.

When you install NNM on a management station running Windows, a web server is not installed, since the Windows operating system comes with its own web server. The web server on the Windows operating system is automatically configured for NNM's use during the NNM installation.

When you install NNM on a management station with a UNIX operating system, a web server *is* installed. This server is fully configured to access scripting aliases and documentation aliases used by NNM. The web server uses port 3443 for communication.

If you want to set up your own web server, configure the port number and set up the aliases `OvCgi`, `OvDocs`, and `OvBackgrounds`, see NNM's release notes for additional information about installing a web server.

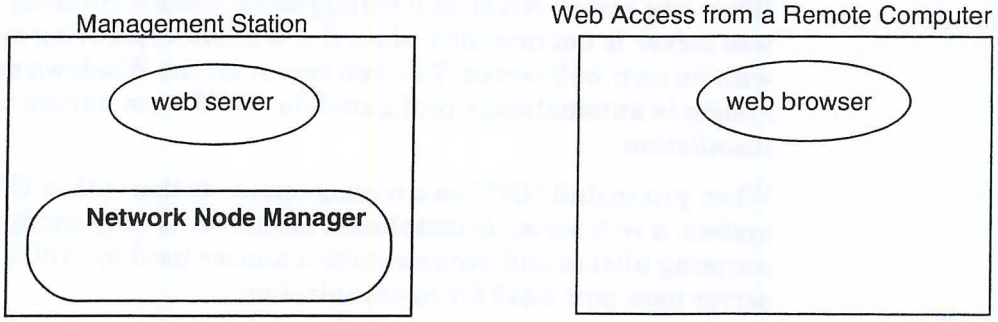
The client station only needs to have a web browser running. Supported web browsers are:

- Netscape
- Microsoft Internet Explorer

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1068
3740
Doc:

NOTE Refer to the "Supported Configurations: Supported Web Browsers" section of the NNM Release Notes for specific information about supported web browsers.

Figure 14-1 Management Station and Remote Web Access



See Figure A-4, "Services and Files for the Web Components," on page 551 for more detailed information about the files and services (processes) on the management station and remote computer at installation time.

On the management station, there must be a non-web based version of NNM running for each map that will be accessible through remote web access. For example, if you want your team to be able to access the Home Office map and the map showing your operations in Germany, you must start NNM on the management station with your Home Office map displayed and start another instance of NNM on the management station with the Germany map displayed. See page 508 for more information.

From remote sites you can now use your web browser and NNM's Network Presenter to display the Home Office map or the Germany map.

Role Configuration Files for the HP OpenView Web

Since the HP OpenView Web can be accessed from virtually any system, security measures are in place to ensure that only authorized users log in to your NNM management station. The way the HP OpenView Launcher and the web applications use these mechanisms varies. The security mechanisms are:

- User authentication (password) file.
- User authorization (roles) file.
- Session configuration file.
- Audit log files.
- `ovw.auth` and `ovwdb.auth` files (used by the Network Presenter and discussed in the section "Configuring Security for the Network Presenter" on page 506).

Since the Launcher is the access point for all other web applications, it provides the first level of security. When security is enabled via the session configuration file, the user password file and user roles file are read to ensure that the user is authorized to access NNM on the management station. The user roles file ensures that only those applications approved for that user role are made available via the Launcher.

User Authentication (Password) File

User authentication is accomplished through a user name and user password. Users should not use the same password as their operating system password. Since the passwords are passed in cleartext format at the beginning of a session, it is possible that they may be intercepted. The Launcher uses the user password file when the user attempts to log on.

The user password file is located on the management station at:

Windows: *`install_dir`*`\www\etc\htpasswd`

UNIX: `/etc/opt/OV/share/www/etc/htpasswd`

Entries in the file appear as:

```
john: FXSD198sdfADS
sue: PO12ADFpoiuS
```

The file is installed with administrator-only (Windows operating system) or root-only (UNIX operating system) permission.

Set passwords as follows:

`ovhtpasswd` *`username`*

The command prompts you for the password for that user.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1069
3740
Doc:

See the *ovhtpasswd* reference page in NNM's online help (or UNIX manpage) for more information about this command.

User Authorization File

Users may be assigned to any number of groups for authorization purposes. These user groups are called user roles in NNM. A **user role** is a designation given to individuals who perform specific tasks with NNM. Users are assigned roles, and then those roles are given access to specific URLs. The Launcher uses the user roles file to define what list items are visible from the Launcher window. When a user logs in, his or her role is verified, and then he or she can access the URLs assigned to that specific role. User roles are valid only when a user accesses NNM via the web interface; they are not valid when a user accesses NNM directly on a management station.

Predefined user roles and their functions are listed below. You can change these roles, or add new roles.

- NetworkAdmin

  The role of NetworkAdmin is intended for individuals who have a higher level of knowledge of networks. Capabilities for configuration of the network and connecting devices, and advanced troubleshooting should be associated with this user role.

- NetworkOper

  The role of NetworkOper is intended for individuals who do routine troubleshooting and maintenance tasks associated with the network. Capabilities for monitoring the network, and routine troubleshooting and maintenance of the network and network devices should be associated with this user role.

- NTAdmin

  The role of NTAdmin is intended for individuals who have a higher level of knowledge of the Windows operating system. Capabilities for configuration of the Windows operating system and advanced troubleshooting should be associated with this role.

- NTOper

The role of NTOper is intended for individuals who do routine troubleshooting and maintenance tasks associated with Windows operating system. Capabilities for monitoring the system, and routine troubleshooting and maintenance of the Windows operating system should be associated with this user role.

- UNIXAdmin

  The role of UNIXAdmin is intended for individuals who have a higher level of knowledge of UNIX operating systems. Capabilities for configuration of UNIX operating systems and advanced troubleshooting should be associated with this user role.

- UNIXOper

  The role of UNIXOper is intended for individuals who do routine troubleshooting and maintenance tasks associated with UNIX operating systems. Capabilities for monitoring the system, and routine troubleshooting and maintenance of UNIX operating system should be associated with this user role.

- OVAdmin

  The role of OVAdmin is intended for individuals who do configuration and customization of the HP OpenView environment and management applications. Capabilities for configuring and customizing management applications should be associated with this role.

The user roles file is located on the management station at:

Windows: *install_dir*\www\etc\htgroup

UNIX: /etc/opt/OV/share/www/etc/htgroup

The format of the user roles file is:

```
NetworkAdmin: user1 user2

NetworkOper: user4 user5

NTAdmin:user1 user3

UNIXOper: user6
```

You can also use a plus sign (+) instead of specific user names. This allows any user access to the capabilities of that user role.

User roles work in conjunction with the Access specification in the Launcher Registration Files (WLRF). See "Action Block" on page 496.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1070
3740
Doc:

Session Configuration File

The session configuration file is used by the Launcher. A **session** is a group of applications associated with a particular user on a particular display. When a user logs in, all the applications started (directly or indirectly) from the Launcher are part of that session. The applications that are part of a session can share information, such as locale.

A session is terminated when the user exits the web browser, when the session has been inactive for some configurable period of time (the default is 9 hours), or when the management station is shut down.

The session configuration file allows you to enable or disable security for NNM's web applications (default is disabled). If you specify `Off` in the `UserLogin` field of this file, NNM's web applications open directly. If you specify `On` in the `UserLogin` field of this file, NNM's web applications display a login dialog box upon opening.

WARNING **The default is for the session configuration file to disable security. If the security mechanisms are disabled in this file, users will not be presented with a login screen, and will have access to all registered actions.**

The session configuration file is located on the management station at:

Windows: *`install_dir`*`\www\conf\session.conf`

UNIX: `/etc/opt/OV/share/www/conf/session.conf`

The session configuration file has the following format:

```
UserLogin: on|off
LoginLogging: on|off
AccessLogging: on|off
SessionTimeout: hours
```

The default values are `off` for the first three items, and 9 hours for the session timeout. Time should be specified in integer values. Open the editable ASCII `session.conf` file for more information.

If you modify this file while you have the Launcher running, you need to exit the web browser and restart the Launcher for the new information to take effect.

Audit Log Files

There are two audit log files — one for logging logins and one for logging URL access from the Launcher. These are useful for security auditing purposes, as you can check on which users are accessing the Launcher by monitoring these files.

There is no log file management; the files continue to grow. You should periodically check these files and when they get large, you should save them or trim them.

The files are located on the management station at:

Windows: `install_dir\www\logs\login_log` (login log)

`install_dir\www\logs\access_log` (access log)

UNIX: `/var/opt/OV/www/logs/launch/login_log` (login log)

`/var/opt/OV/www/logs/launcher/access_log` (access log)

Each log entry is a single line of text. If the session configuration file is set to `LoginLogging:on`, the following information is recorded:

- Host
- User name
- Date
- Session number
- Access permitted; either `Allowed` or `DENIED`
- URL accessed (for the `access_log` file only)

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1071
3740
Doc:

The HP OpenView Launcher

The HP OpenView Launcher is the user interface integration point for the HP OpenView web applications. Just as with management station-based NNM, developers can tie their applications into NNM's web interface. Then users access those applications through the Launcher interface.

You can also create your own application that you access from the Launcher. If you create your own application, you can integrate it with the Launcher by creating a registration file for that application.

The Launcher provides functionality in three areas:

- Launching of management functionality and applications via a URL or via the web interface.
- User login and user roles.
- Maintenance of session information shared by all web interfaces.

Launcher User Interface

The Launcher interface is started from a web browser. The URL for the Launcher is:

`http://hostname:[port]/OvCgi/ovlaunch.exe`

For example, if the host system is a management station named `UX-manage1` running a UNIX operating system, you would enter:

`http://ux-manage1:3443/OvCgi/ovlaunch.exe`

A web server is automatically installed on UNIX management stations and configured to use port number 3443 for communication.

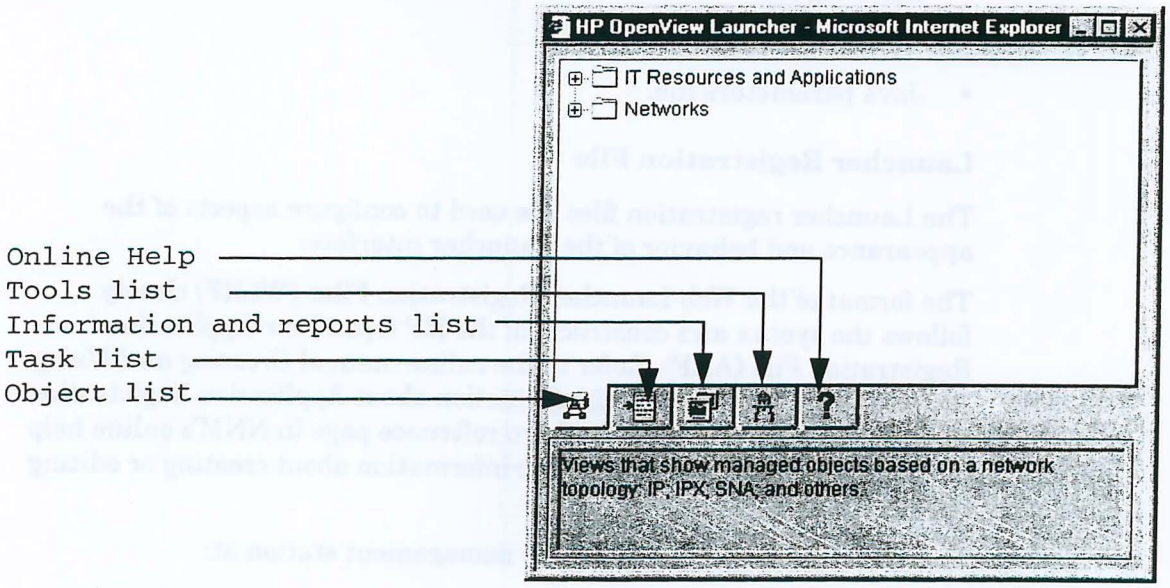
If the host system is a workstation named `nt-mgmt` running Windows, you would enter:

`http://nt-mgmt/OvCgi/ovlaunch.exe`

No port number is required for management stations running a Windows operating system.

If the management station has been configured for security, a login screen appears where the user enters his or her name and password. If no security has been configured, the Launcher window comes up without asking for login and password.

Figure 14-2 The Launcher Window



The Launcher window displays a tabular view of the capabilities available through the Launcher. The bottom tabs of the Launcher window contain the Task, Tool, Object Views, Management Areas, and Help categories. These categories correspond to the basic functionality of NNM on a management station. These are also the categories where other HP OpenView web applications will be linked.

Click on a category to expand it, or click on the expanded category to contract it. You can also click on the +/- indicator.

If you double-click on a list item, you execute the URL associated with that item.

The categories that are displayed in the tabular section of the Launcher window are determined by the user roles file and the Launcher Registration Files (WLRF), described next.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1072
3740
Doc:

Configuring the Launcher

There are several files you can use to customize the Launcher.

- Launcher registration files.
- Error log file.
- Installed locale file.
- Java parameters file.

Launcher Registration File

The Launcher registration files are used to configure aspects of the appearance and behavior of the Launcher interface.

The format of the Web Launcher Registration Files (WLRF) closely follows the syntax and constructs of the HP OpenView Application Registration File (ARF). Refer to the online manual *Creating and Using Registration Files* for general information about Application Registration files. Refer to the *LauncherRegIntro* reference page in NNM's online help (or the UNIX manpage) for specific information about creating or editing the WLRF files.

The WLRF files are located on the management station at:

Windows: *install_dir*\www\registration\launcher\C*.*

UNIX: /etc/opt/OV/share/www/registration/launcher/$LANG

The bitmaps referenced in the WLRF are located in:

Windows: *install_dir*\www\htdocs\C\images*.*

UNIX: /opt/OV/share/www/htdocs/$LANG/bitmaps

Components of the WLRF There are several sections of a WRLF that you might need to modify. Only those sections will be discussed here.

Once you have modified a WLRF file, you can check it for errors with the command `regverify`. See the *regverify* reference page in NNM's online help (or the UNIX manpage) for more information.This command is located on the management station at:

Windows: *install_dir*\bin\regverify

UNIX: /opt/OV/bin/regverify

Tab Block

The Launcher has several tabs at the bottom of its window. The tab block indicates under which of the tabs an application will appear.

The tab block allows an optional icon file name to display on the tab. If one is not specified, a default will be used. The icon appears in front of the name of the application in the Launcher content area. The format for icons is 16x16 GIF. The file name is relative to:

Windows: *install_dir*\www\htdocs\bitmaps

UNIX: $OV_WWW/htdocs/bitmaps

The tab block also contains optional active help text. This active help is presented when the mouse pointer is over the tab.

The tab block contains List Item entries instead of Menu Items (for the menu bar). Following is a sample of the tab block.

```
Tab <60> "Tools" Icon "launcher/toolsfold.20.gif"
        ActiveHelp { "tools" }
{
        <70> "Session"
                Icon "launcher/toolsfold.16.gif"
                ActiveHelp {"Session Info" }
                f.list "SESSION";
}
```

List Block

The list block of the WLRF corresponds to the menu block in the ARF.

The following statements are allowed in the list block:

- Precedence value

  This has the same definition as in the ARF.

- List Item Label

  This is the label that is displayed for the entry.

- Icon

  This is a locale-dependent icon that is displayed for the list item. The format for icons is 16x16 GIF.

- ActiveHelp

  This is the active help text that is displayed when the mouse pointer is placed over the entry.

- Functions

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1073
3740
Doc:

Two functions are supported:

— `f.action`

This indicates a terminal list item. It points to an Action block that has the action definition.

— `f.list`

This indicates a component list item. It points to a list block to allow the definition of a hierarchical tree list.

Following is a sample of the list block.

```
List "SESSION"{
     <80> "Session Info Viewer"
                Icon "launcher/tools.16.gif"
                ActiveHelp { "Session Info Viewer" }
                f.action "printsession";
}
```

Action Block

The action block of the WLRF serves the same function as in the ARF. The following statements are allowed in the action block:

- URL

  This is the URL to launch for the action. The URL may contain the special variable `$OVwWebServer`. This variable will be substituted with the name of the system from which the Launcher was loaded.

- Access

  This is a list of user roles that have access to this action. If a user does not belong to a group that has access, the user will not see the list item that invokes this action in their Launcher window. If the access statement is not present, all valid users can access this action. The user roles values correspond to entries in the user roles file. For example, `NetworkAdmin`. See "User Authorization File" on page 488.

- Window

  The Window statement specifies the characteristics of the window into which the URL will be loaded. If the WebWindow statement is not present, the URL will be loaded into an unnamed full web browser window.

  The Window definition has the following components:

2393

— Window name

This is a name for the window to allow window reuse by targeting a named window. The window name is a string of alphanumeric characters and underscores; it may not include blanks. If a new window is desired every time the URL is loaded, a blank window name (" ") may be given.

— Type (full, intermediate, or limited)

Type specifies the type of the window and determines which features it supports. If no type field is present in a window block, `full` is assumed. The values are:

— `full`, all window elements present and user configurable.

— `intermediate`, directories and menubar off, all other window elements present and user configurable.

— `limited`, all window elements off but user configurable.

— Toolbar (on or off)

— Location (on or off)

— Status (on or off)

— Scrollbars (on or off)

— Resizable (on or off)

— Width (integer value)

— Height (integer value)

Following is a sample of the action block.

```
Action printsession
{
    URL "/OvCgi/printsession.exe";
    WebWindow "OvPrintSession" {
        Type full;
        Toolbar off;
        Status off;
    }
}
```

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1074
3740
Doc:

Error Log File

The Launcher error log records internal errors from the Launcher. You can use the output from this file when discussing a problem with the HP Response Center or HP support personnel.

The Launcher error log file is located in:

Windows: *install_dir*\www\logs\launcher\error_log

UNIX: $OV_WWW/launcher/error_log

The error log contains the following information:

- Date
- Host
- User
- Session
- Reason or error

The error log file continues to grow without bounds. You need to watch the size of this file and truncate it as needed.

If the error log file does not give you sufficient information for troubleshooting, you can set a parameter in the URL for **ovlaunch.exe** that will enable more in-depth error logging on a session level. See "Troubleshooting Web Components" on page 613 for more information. The parameter is:

```
http://sysname:3443/OvCgi/ovlaunch.exe?Debug=/tmp/file
```

Language Selection

The Launcher and the Web applications started from the Launcher execute under a particular language, such as English or Japanese. The language used by the Launcher and the Web applications is based on the following:

- The language specified by the user when the security is enabled.
- The language specified by the user through the URL.
- The language specified by the browser.

Once a session is started, the language selection cannot be changed without restarting the browser with a different language.

Language Selection When Security is Enabled Security is enabled via the session configuration file. When security is enabled, the user is presented with a login page listing the languages available for the session under the `[Options]` button. This list represents the languages supported by the Launcher and other installed products that integrate into the Launcher. The languages presented in `[Options]` is based on the contents of the `locales.installed` file. This file is located in:

Windows: *`install_dir`*`\www\conf\locales.installed`

UNIX: `/etc/opt/OV/share/www/conf/locales.installed`

This file contains a list of locales for which the Web applications have been localized. For instance, if the Japanese NNM has been installed, this file will contain an entry for English and for Japanese, for example:

```
en
ja
```

This file can be modified by a developer or administrator. When an HP OpenView web application has been localized to a language not listed in this file, a locale entry should be added to this file. Refer to the *HP OpenView Windows Developer's Guide* for details on syntax.

Language Specified Through the URL The language for a session can be specified when the `ovlaunch.exe` URL is specified. This is done through the CGI parameter `AcceptLang`. This language specification will take precedence over the browser language specification, but can be overridden if security is on and the user chooses a different language on the login page. If security is not on, the login page will come up in the language specified by the `AcceptLang` parameter. For example:

```
http://mysystem:3443/OvCgi/ovlaunch.exe?AcceptLang=ja
```

Language Specified Through the Browser When security is not enabled, the Launcher uses language specified through the browser. For instance, if the browser has been configured to run in English, the Launcher will execute in English.

Java Parameters File

There are some Java parameters that you can modify to control Launcher appearance. You change these parameters by modifying the APPLET block in the following file, located on the management station at:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1075
3740
Doc:

Windows: *install_dir*\www\htdocs\C\nnm\launcher\browser.html

UNIX: $OV_WWW/htdocs/$LANG/nnm/launcher/browser.html

The Java parameters that you can modify are:

- background
- foreground
- activeTabColor
- inactiveTabColor
- treeBackground
- treeForeground
- treeConnectingLineColor
- displayActiveHelp
- activeHelpLines
- fontName
- fontStyle
- fontSize
- displayInFrame

HP OpenView Network Presenter

The HP OpenView Network Presenter is a Java-based applet that connects to NNM for the purpose of displaying maps. It provides multiple views of map data on a management station from any system with a web browser that supports Internet Explorer or Netscape Navigator.

NOTE Refer to the "Supported Configurations: Supported Web Browsers" section of the NNM Release Notes for specific information about supported web browsers.

The Network Presenter communicates with the management station to get registration information, map data, and map object data. It provides read-only access to the map data and has dynamic updates to reflect the changes that occur on the management station. You can navigate through the map views, select and obtain status on symbols, and launch other web applications on the selected objects via the Network Presenter.

Starting the Network Presenter

You must start an NNM session on the management station for each map that you want available through the web, as described on page 485.

You can invoke the Network Presenter through the Launcher using either of the following tabs:

`Objects` tab, then choose `Networks:IP Network`

`Tools` tab, then choose `NNM:Network Presenter`

Alternatively, you can enter the URL for the Network Presenter:

`http://`*`hostname`*`[:`*`port`*`]/OvCgi/jovw.exe?[MapName=`*`mapname`*`&ObjectName=`*`selectionname`*`]`

On UNIX operating systems, you must specify port number `3443`. Ona Windows operating system, no port number is required. The `MapName` and `ObjectName` fields are optional.

The `MapName` field specifies which map to open. The `ObjectName` field specifies what object to show initially. Refer to the *OvWebURLIntro* reference page in NNM's online help (or UNIX manpage) for more information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1076
3740
Doc:

NOTE When starting the Network Presenter directly from the URL, you lose the session information that the Network Presenter would have if it were started from the Launcher, including language information.

If a *mapname* is not specified in the URL used to start the Launcher, Network Presenter attempts to connect to an NNM session running with the default map. If there is no NNM session running with the default map, the Network Presenter displays an error message that says the map was not found.

If a *mapname* is specified in the URL, the Network Presenter attempts to connect to an NNM session on the management station with an open map called *mapname*. If there is no NNM session running on the management station with this map open, the Network Presenter displays an error message that says the map was not found.

If you close the NNM session or open a new map, the Network Presenter session attached to that NNM session is ended. The Network Presenter displays a dialog box informing the users that NNM is closing its map.

By default, the Launcher will start the Network Presenter with the `default` map displayed. To make a map other than `default` available to the Network Presenter, modify the `jovw` Web Launcher Registration File (WLRF) that specifies in the URL portion which map to open. See "Listing Multiple Maps in the Launcher" on page 508 and "Launcher Registration File" on page 494 for information.

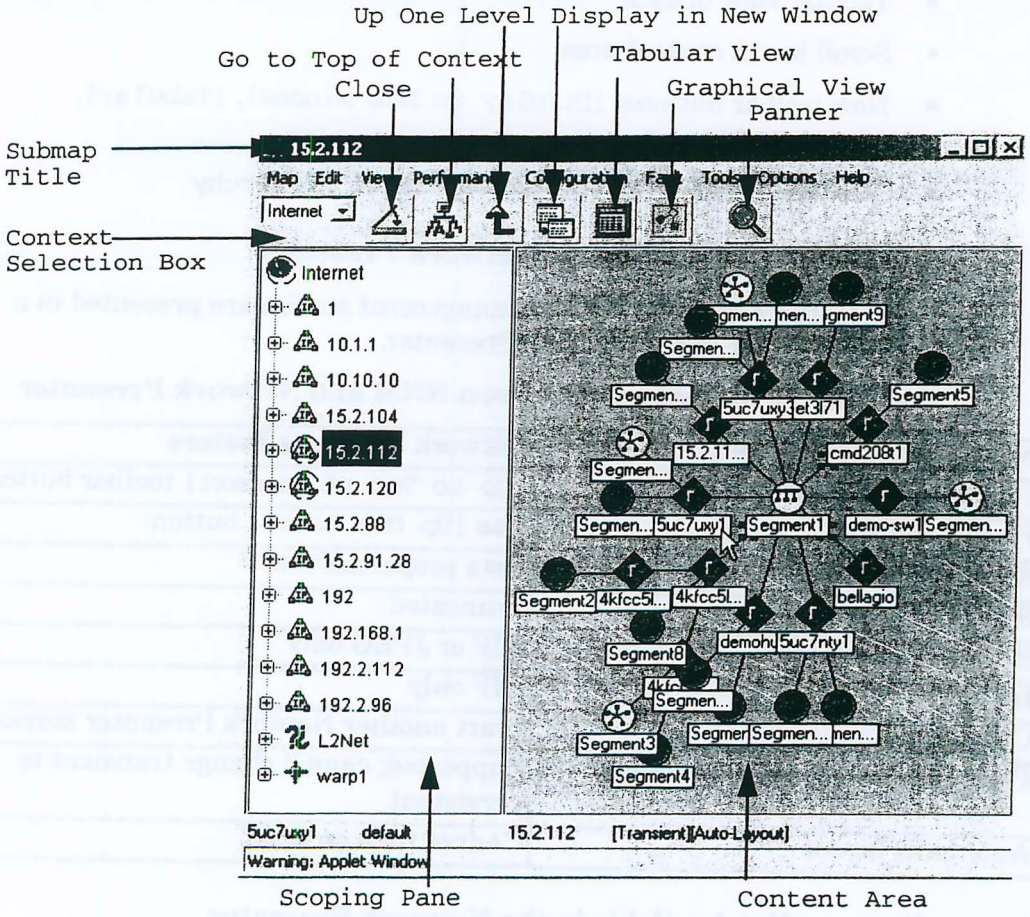
The Network Presenter Window

The Network Presenter window has the following components:

- Submap title
- Menu bar
- Context selection box
- Toolbar
- Content area
- Scoping pane

- Status bar

Figure 14-3 **Network Presenter Window**



Network Presenter versus NNM on a Management Station

There are some differences in the functionality and presentation of information between the Network Presenter and NNM on a management station.

Features in the Network Presenter

Following are features in the Network Presenter that are not available in NNM on a management station.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1077
3740
Doc:

- Context selection box to choose among the highest-level views.
- Scoping pane.
- Tabular view of data.
- Scroll bar in content area.
- New toolbar buttons: `[Display in New Window]`, `[Tabular]`, `[Graphical]`
- New menu items: `Up One Level`, `Top of Hierarchy`

Features That Differ in the Network Presenter

Some features from NNM on a management station are presented in a different format in the Network Presenter.

Table 14-1 Differences in Features Between NNM and Network Presenter

NNM Management Station Feature	Network Presenter Feature
`[Go to Root]` toolbar button	`[Go to Top of Context]` toolbar button
Parent toolbar	Use `[Up One Level]` button
App-defaults file	Java properties file
Symbol labels	Truncated
Background graphics	GIF or JPEG only
Inner shapes	GIF only
Open map	Start another Network Presenter session
Persistent and transient submaps	Supported; cannot change transient to persistent
Automatic layout	Cannot turn on or off

Features Not Available in the Network Presenter

The following features in NNM on a management station that are not available in the Network Presenter.

- `Map Description` dialog box.
- `Submap Properties` dialog box.
- `Locate Submap` dialog box.
- Home submap.
- `Symbol Properties` dialog box.
- Snapshots.

- Symbol enhancements (flashing, transparent, alerts, etc.).
- Menu collapsing.
- Symbol, submap editing.
- Invoking executable symbols.

Interaction Between NNM on the Management Station and the Network Presenter

Since the Network Presenter cannot do editing, the Network Presenter does not influence what happens to NNM on the management station; however, changes in the current session on the management station are dynamically reflected in the content area and scoping pane of the Network Presenter as appropriate. You will see changes in the content area if the submap that is displayed on the management station changes. You will see changes in the scoping pane if that level of hierarchy is displayed. Changes are not dynamically reflected in open dialog boxes.

Configuring the Network Presenter

You can modify the Network Presenter Registration Files (NPRF) to configure certain aspects of the Network Presenter.

The NPRFs are located on the management station at:

Windows: `install_dir\www\registration\jovw\c\*.*`

UNIX: `/etc/opt/OV/share/www/registration/jovw/$LANG`

The format of the Network Presenter Registration Files (NPRF) closely follows the syntax and constructs of the HP OpenView Application Registration File (ARF). Refer to the online manual *Creating and Using Registration Files* for general information about Application Registration files. Refer to the *NetworkPresenterRegIntro* reference page in NNM's online help (or the UNIX manpage) for specific information about creating or editing the NPRF files.

You can add entries to the Action block to specify your own applications to be called when the Network Presenter is launched. You can also change the WebWindow properties in the Action block to control some aspects of the appearance of the Network Presenter (see "Components of the WLRF" on page 494 for sample contents of a registration file). You can add pull-down menus, toolbar buttons, and popup menus that operate on selected objects.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1078
3740
Doc:

Configuring Security for the Network Presenter

There are two levels of security for the Network Presenter.

- The `session.conf` file, described earlier in this chapter.
- The `ovw.auth` and `ovwdb.auth` files, described next.

The Network Presenter allows role-based, restricted access to menu items that have action blocks that contain access statements. See the *Action Block* description on page 496 for more information.

Authorization Files The `ovw.auth` and `ovwdb.auth` files specify which users are allowed access to which management stations. These files are located on the management station at:

Windows: *`install_dir`*`\conf\ovw.auth`

`install_dir``\conf\ovwdb.auth`

UNIX: `$OV_CONF/ovw.auth`

`$OV_CONF/ovwdb.auth`

Each of these files contain instructions for their use.

Using Symbol Registration Files and Bitmaps

Symbol registration files used by the Network Presenter are the same as those used by NNM on a management station. Therefore, if a symbol definition is added for NNM on a management station, it also appears in the Network Presenter. Symbol registration files are located in:

Windows: *`install_dir`*`\symbols\%LANG%`

UNIX: `$OV_SYMBOLS/$LANG`

See the *OVwRegIntro* reference page in NNM's online help (or the UNIX manpage) for more information about creating or editing symbol registration files.

The graphic files for the symbols, themselves, are stored in two places. One directory used by NNM on the management station (see page 664), and one directory used by NNM's web-based interface. The web-based interface requires GIF files. Other additional graphic file formats are supported on the management station. If you create your own GIF files, place a copy in each location.

The Network Presenter loads its bitmaps in GIF format from the directory:

Windows: *install_dir*\www\htdocs\bitmaps

UNIX: $OV_WWW/bitmaps

TIP

If you can see a symbol on the management station, but cannot see it over the web interface, check the Contrib directory (see page 74) for the convertBitmaps.ovpl script which walks through each graphic in the management station's symbol graphic directory and ensures that a corresponding GIF file exists or is created in the web interfaces's symbol directory.

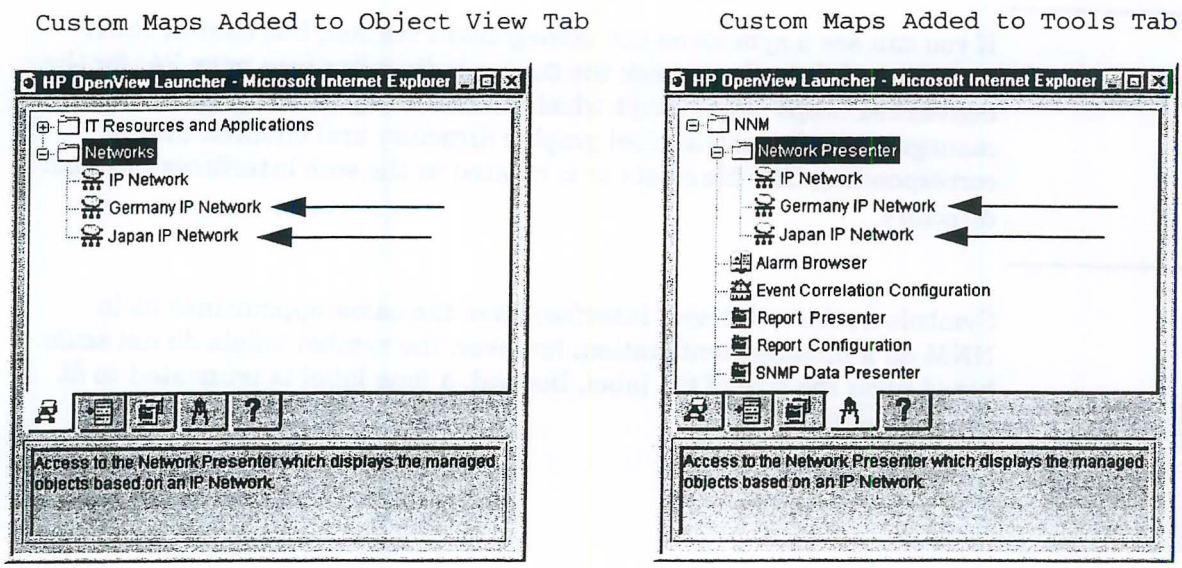
Symbols in the web-based interface have the same appearance as in NNM on a management station; however, the symbol labels do not scale based upon the size of the label. Instead, a long label is truncated to fit the space available.

RQS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 1079
3740
Doc:

Listing Multiple Maps in the Launcher

You can modify the Launcher registration file for the Network Presenter so that each of your custom maps is listed.

Figure 14-4 Listing Multiple Maps in the Launcher Window



For each map, you must make additions to the `List` and `Action` blocks of the following file:

- Windows: *`install_dir`*`\www\registration\launcher\C\jovw`
- *UNIX:* `$OV_WWW_REG/launcher/$LANG/jovw`

Open this file and read the instructions provided for more information. See also the *LauncherRegIntro* reference page in NNM's online help (or the UNIX manpage) for specific information about creating or editing the WLRF files.

On the management station, there must be a non-web based version of NNM running for each map that will be accessible from the Network Presenter. For example, if you want your team to be able to access the Germany map and the map showing your operations in Japan, you must start NNM on the management station with your Germany map displayed and start another instance of NNM on the management station with the Japan map displayed.

SNMP Data Presenter

The SNMP Data Presenter displays results of operations that present tabular or textual data for managed SNMP nodes selected from the map.

You can use the SNMP Data Presenter even if there is no NNM session running on the management station. The SNMP Data Presenter accesses NNM's Application Registration Files (ARFs) to retrieve information about menu structure and actions, executes the command on the management station, and displays the results in the web browser.

The SNMP Data Presenter displays configuration, performance and fault information. Here are a few examples:

- Interface status.
- SNMP authentication failures.
- TCP connections.
- IP Network addresses.
- IP Routing tables.
- IP ARP cache table.
- System information.
- SNMP trap recipients.

To start the SNMP Data Presenter, select the target node in the content area of Network Presenter and then select one of the following:

- `Performance:SNMP Data Presenter`
- `Configuration:SNMP Data Presenter`
- `Fault:SNMP Data Presenter`

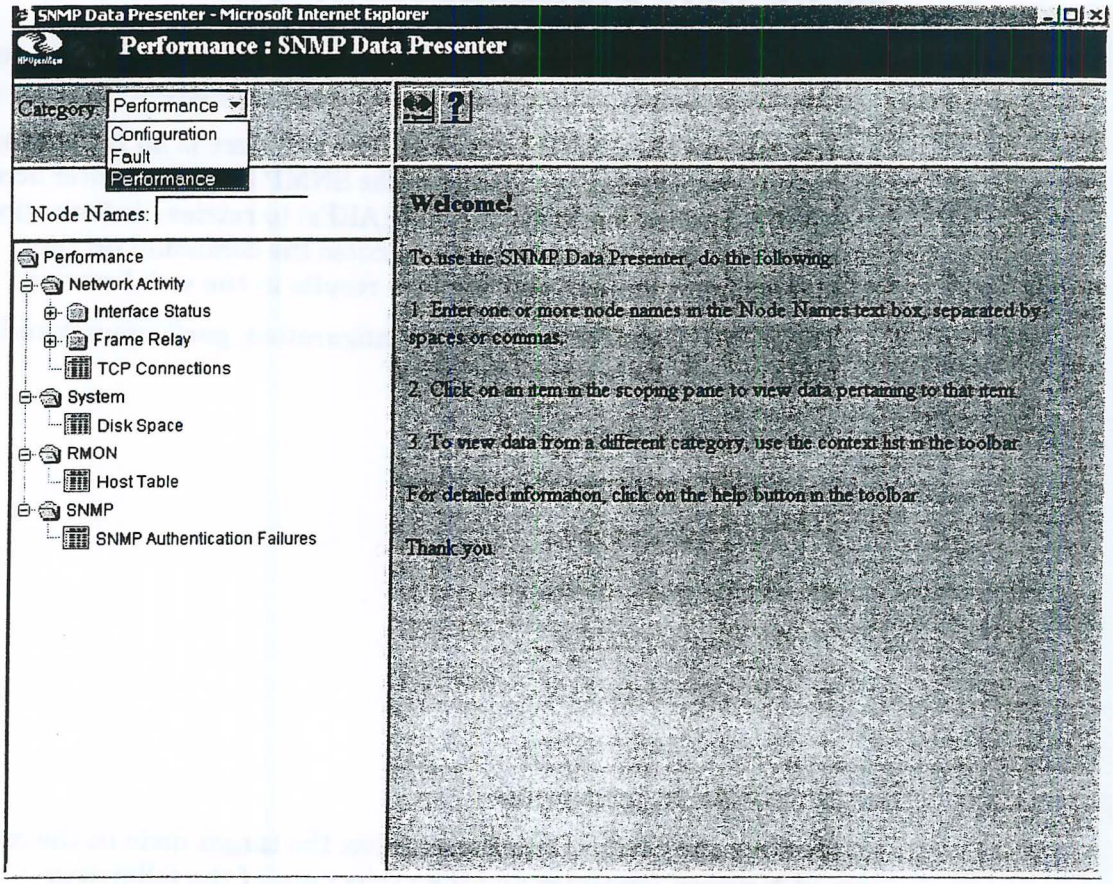
To start the SNMP Data Presenter from the Launcher, select:

- `Tools` tab, then `NNM:SNMP Data Presenter`

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1080
3740
Doc:

The SNMP Data Presenter window is shown in Figure 14-5.

Figure 14-5 SNMP Data Presenter Window



Scoping Pane Content Pane

When accessed from the `Tools` tab, the scoping pane contains categories and actions in a tree format. You can click on the category items to expand them and then click on an action to execute that action. You can also use the Category pull-down.

The results of an action are shown in the content area. A link at the bottom of this area allows you to display a new web browser window with the currently displayed information. This allows for easy comparing of data.

Configuring the SNMP Data Presenter

The SNMP Data Presenter uses NNM's Application Registration Files (ARFs) and the Application Builder. Because of this, you can execute the same SNMP monitoring operations as you do in NNM, and add new operation commands to the menu structure with Application Builder.

See NNM's online manual, *Creating and Using Registration Files,* for details about editing application registration files (ARFs). See "Using the MIB Application Builder" on page 443 for more information about the Application Builder feature.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1081
3740
Doc:

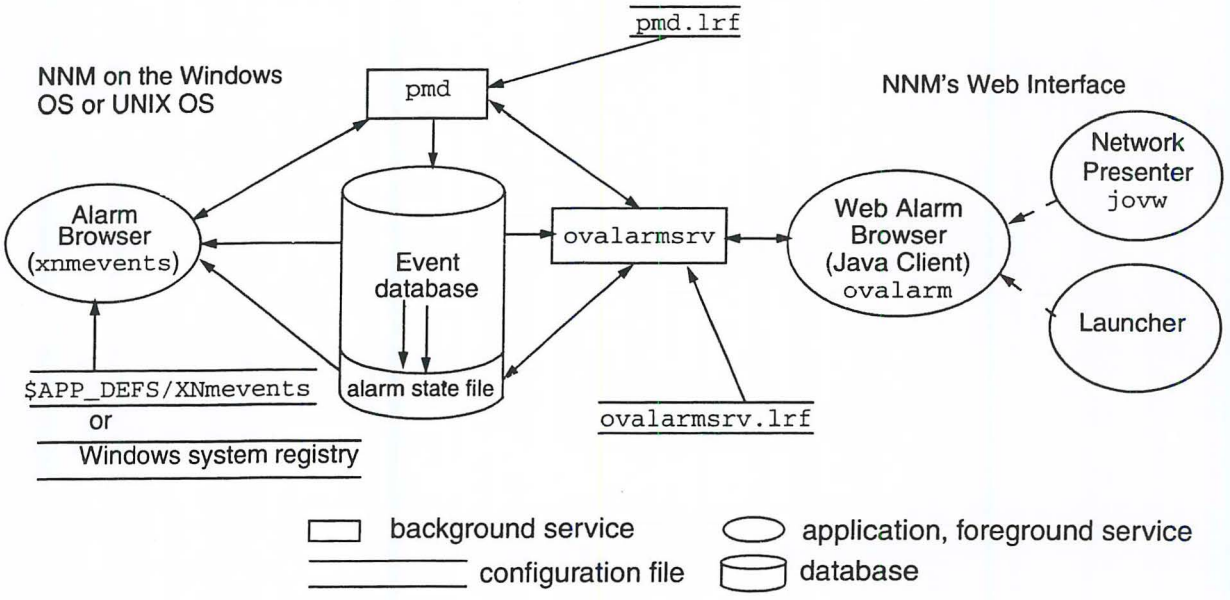
Alarm Browser

The Alarm Browser presents alarm data via the web interface. Through the Alarm Browser, you can filter alarms and take actions on specific alarms. All alarms are global to all web users, as are the acknowledge, delete, change category, and change severity functions.

The web-based Alarm Browser service, `ovalarmsrv`, is started by `ovstart` when you start an NNM session on the management station.

Figure 14-6 illustrates the relationship and data flow between the Alarm Browser application on a management station and the web-based Alarm Browser.

Figure 14-6 Relationship Between the Two Alarm Browsers

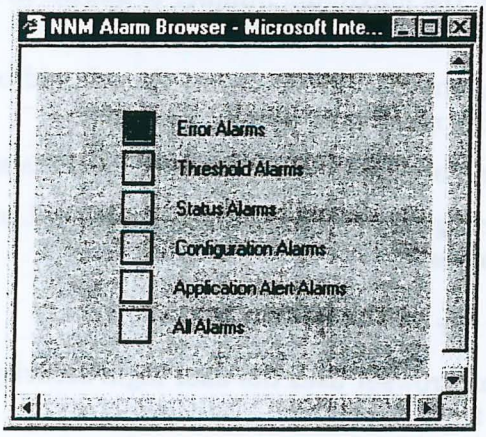


You access the Alarm Browser using one of the following methods:

- In the Launcher, select the `Tools` tab, then select `NNM:Alarm Browser`

- In Network Presenter, select the `Fault` menu, then select `Alarm Browser`.

Figure 14-7 Web-Based Alarm Browser's Category Window



Using and Configuring the Alarm Browser

You can use the Alarm Browser to perform the following:

- Acknowledge/Unacknowledge alarms.
- Move alarms to a different category.
- Assign alarm severities.
- Filter alarms.
- Delete alarms.
- Examine alarm details to find correlated events.

To move an existing alarm message to a different category. Select the alarm that you want to recategorize. Then select `Actions:Change Category` from the menu bar. Refer to the online help if you need more information.

This change affects only the selected alarms. Future alarms of the same type will continue to be posted in the old category's list.

You can configure an alarm to activate your web browser to a specific URL. See "Launching Specific Views or URLs from Alarms" on page 340 for more information.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1082
Doc: 3740

See Chapter 12, Customizing Events: Doing It Your Way, for configuration options:

- Setting the maximum size of the event database (default 16 MB).
- Setting the maximum number of alarms in the Alarm Browser's state file (default 3500).
- Setting the number of alarms that should be deleted each time the state file reaches maximum capacity.
- Copying or restoring the Alarm Browser's state file.
- Assigning alarms to other categories and creating new alarm categories.

Security for the Alarm Browser

The Alarm Browser uses the user login security mechanisms, described earlier in this chapter.

Event Reduction

Event reduction is the process by which the relationship between events is identified. Once identified, a smaller number of new events providing higher information content can be generated. This simplifies the task of diagnosing network faults. There are three event reduction strategies that are configured and working within NNM. You can access the configuration windows for two of them over the web:

- "ECS Correlations" on page 360
- "Correlation Composer Correlators" on page 386

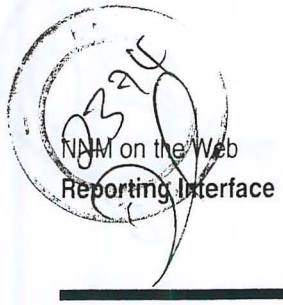
There are several ways to access these event correlation features. For more information, from any submap:

- Select `Toos:HP OpenView Launcher`.
- Select the `[?]` tab.
- Click `Tasks`, `Event Correlation Management`.

  Read the information under *Accessing the Event Correlation Configuration Windows*

For information about the NNM event reduction strategies, see Chapter 11, "Event Reduction Capabilities: Getting to the Root Cause," on page 351.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 3740
Doc:



Reporting Interface

The web Reporting interface is a graphical user interface that is available through a web browser. The Reporting interface consists of:

- Report Configuration-- create, modify, and view report schedules.
- Report Presenter-- view reports.

You can access the Report Configuration in one of the following ways:

- From NNM on a management station, select the `Options:Report Configuration` menu item.
- From Network Presenter, select the `Options:Report Configuration` menu item.
- From the Launcher, select the `Tools` tab, and expand the NNM category. Double-click on `Report Configuration`.
- From your browser, specify the following URL:

  `http://`*`hostname`* `[:`*`port`*`]/OvCgi/RptConfig.exe`

  You need to specify a port if you are running NNM on a UNIX machine.

You can access the Report Presenter in one of the following ways:

- From NNM on a management station, select the `Tools:Report Presenter` menu item.
- From Network Presenter, select the `Tools:Report Presenter` menu item.
- From the Launcher, select the `Tools` tab, and expand the NNM category. Double-click on `Report Presenter`.
- From your browser, specify the following URL:

  `http://`*`hostname`* `[:`*`port`*`]/OvCgi/RptPresenter.exe`

  You need to specify a port if you are running NNM on a UNIX machine.

The NNM Analysis and Reporting interface will be displayed in your browser window.

Refer to the online manual *Reporting and Data Analysis with HP OpenView NNM* and the web online help for more information.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: Nº 1084
3740
Doc:

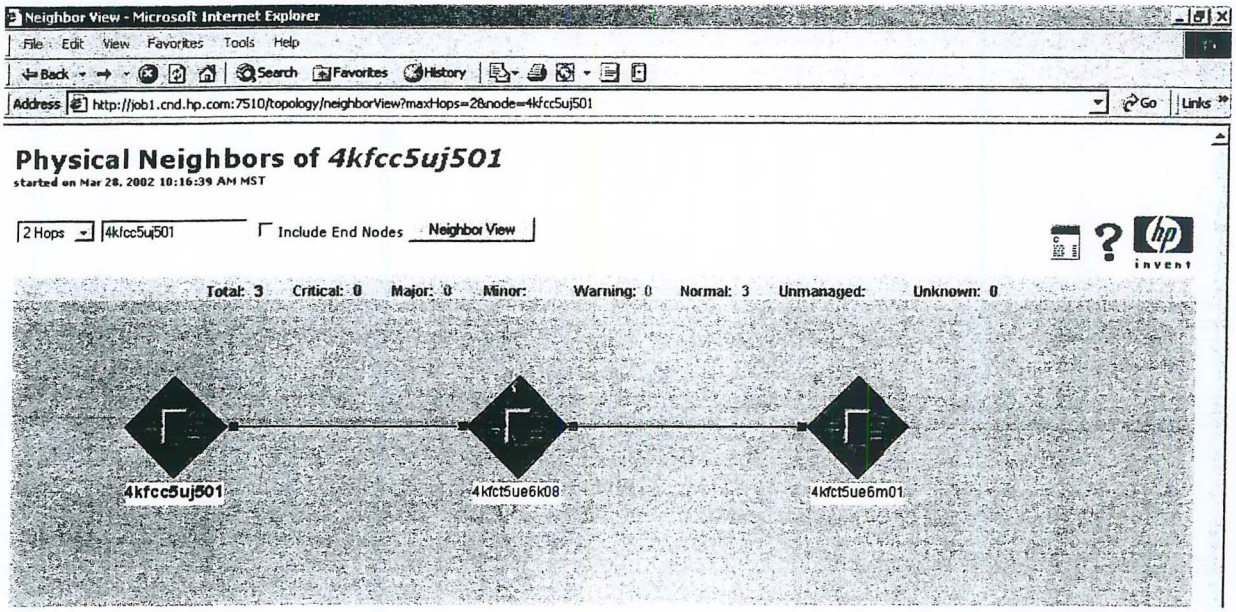
Additional Views

NNM presents several different views of discovered nodes. NNM's Neighbor view, Path view, Node view, Cisco Discovery Protocol view (CDP view), Station view, Internet view, and Port-Address Mapping capabilities show topology views that supplement NNM's map views.

Neighbor View

The Neighbor view shows you a graphical representation of the selected device and the connector devices related to it, within a specified number of hops of the selected device.

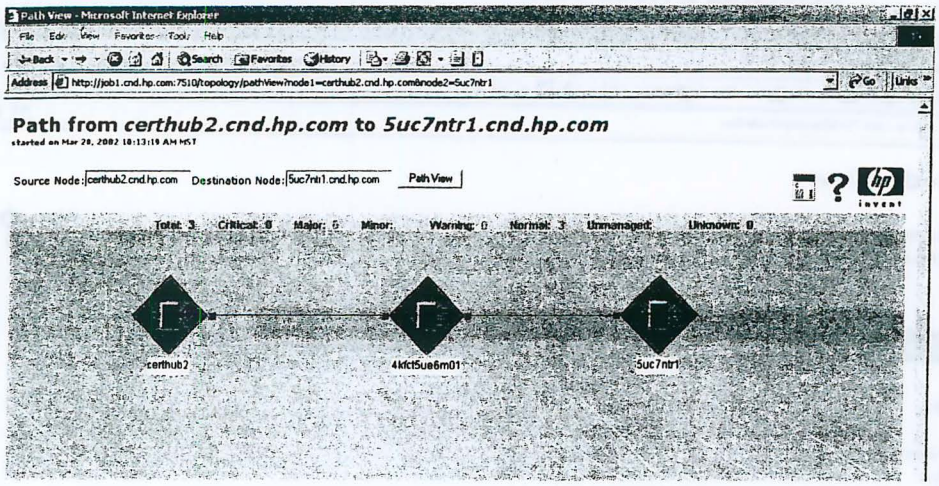
Figure 14-8 Neighbor View Example



Path View

The Path view shows you a graphical representation of the path between two nodes. NNM calculates the shortest path between the source and destination nodes from information contained in the topology database.

Figure 14-9 Path View Example

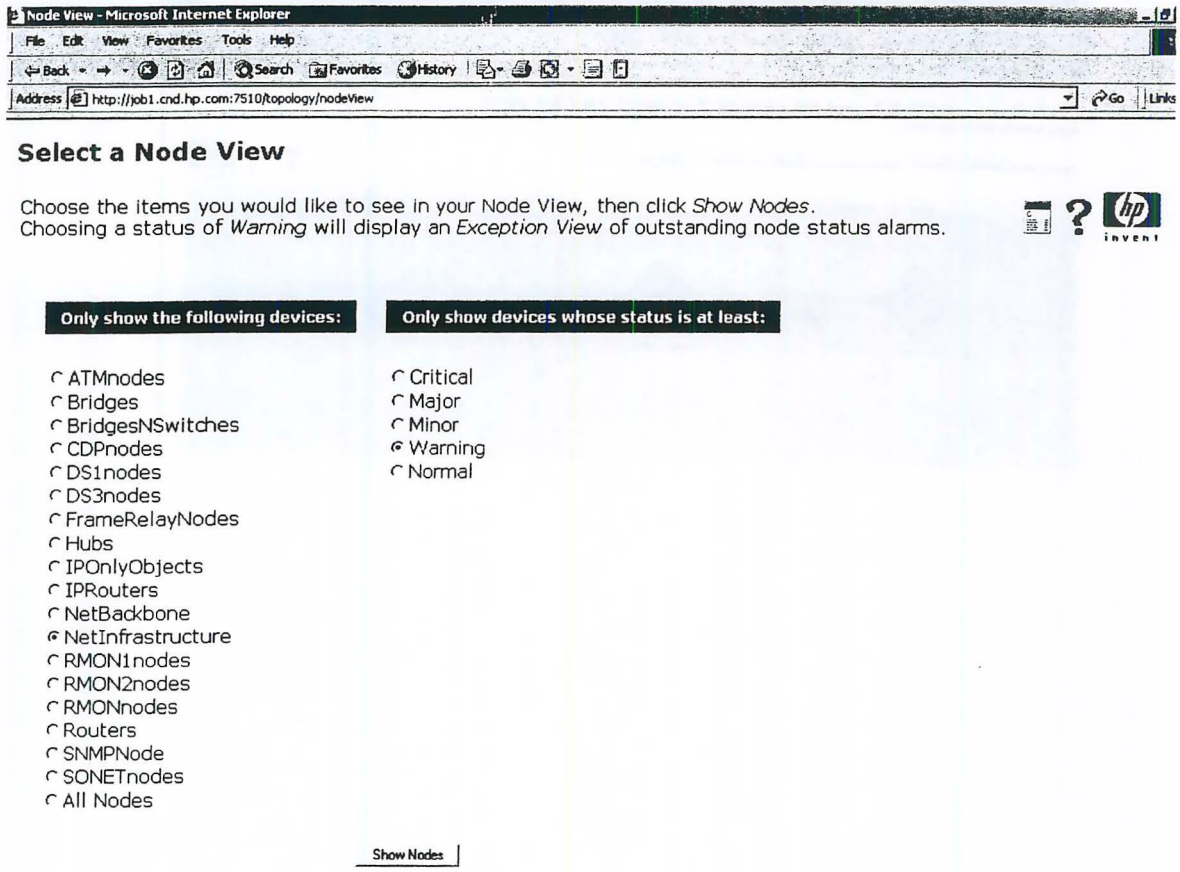


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1085
3740
Doc:

Node View

The Node view creates a visualization of a set of nodes and shows how they are connected. To create a visualization, use the NNM `Tools:Views->Node` menu item. The `Node View` interface contains device types and device status selections as shown in Figure 14-10.

Figure 14-10 Selecting a Node View



Device selection relies on filters contained within the `filters` file. This is the same file that contains filters such as discovery filters and DHCP filters. The filters file is found in the following locations:

- Windows: *install_dir*`\conf\C\filters`
- *UNIX:* `$OV_CONF/C/filters`

The information associated with each MIB object is displayed one MIB object per line with the MIB value to the right of the MIB label. Any type of MIB object is allowed.

— `Table`. Use this option to display MIB information that constructs a logical table in the MIB (for example, a routing table).

The MIB objects are laid out horizontally, making up the columns of the table. Each entry in the MIB table makes up the rows of the application table. Any type of MIB object is allowed.

NOTE You cannot create table applications which consist of MIB fields from multiple MIB tables.

— `Graph`. Use this option to display numeric MIB information that fluctuates over time (for example, interface statistics). Only numeric MIB values are allowed.

- Plan the menu structure. For example, if you have multiple devices from different vendors, you may want to organize the menu structure such that you have all MIB applications for routers grouped under one menu.

Procedure Tips

Refer to NNM's online help available within the `MIB Application Builder` window for information about how to add, modify, or delete applications.

When you build your applications, keep the following in mind:

- You must provide a unique name for the MIB application.
- You can perform MIB operations on one or more MIB objects at a time.
- Menu path. Decide which NNM menu your application belongs under, such as Performance, Fault, Configuration, or Tools. Use the character sequence -> to separate menu items in the menu path field.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1086
3740
Doc:

If the menu path field is blank, the application is created and automatically registered; however, the application will not appear in the menu bar. This is useful for creating applications to be used as the action for an executable symbol.

- You can specify selection rules for your application. Selection rules determine when a menu item is unavailable and when it is available. They are based upon defined capabilities of the nodes for which this application is compatible. If the application is registered in the menu bar, the menu item for this application is only accessible if the capabilities of the selected nodes match those defined in this selection rule; for example, `isSNMPSupported`. See NNM's online help within the `MIB Application Builder` window for more information.
- You can enter help text for your application. For example, you may want to give a general description of the MIB operation and how to interpret the information that is obtained. When you create the MIB operation menu item, the program automatically adds an entry under:
  - — *Windows:* `Help:On Application`.
  - — *UNIX:* `Help:Misc->Function` and in the dialog box help.

Data Collection & Thresholds

This section describes how to use NNM's Data Collections & Thresholds application to do the following:

- Collect MIB data from network nodes automatically at regularly scheduled intervals.
- Store the collected MIB data in a file.
- Set threshold monitoring on critical devices.

See page 469 for information about viewing the data after it is collected.

TIP You cannot configure Data Collections & Thresholds from NNM's web interface. However, the web-based Alarm Browser displays the alarms resulting from your configurations.

Prerequisites

- The node for which you want to collect data must support SNMP version 1 or version 2c.
- Make sure the correct version of the enterprise-specific MIB that you want to use to collect data is loaded into the MIB database on the management station. (The `Options:Load/Unload MIBs:SNMP` menu item lists all MIB modules currently in the MIB description file.) If the enterprise-specific MIB is not loaded, see "Loading MIBs in the MIB Database" on page 413.
- You can collect data or monitor thresholds on numeric MIB objects; that is, the MIB objects defined as `Counter`, `Gauge`, `INTEGER`, `IpAddress`, `Counter64`, or `TimeTicks`.
- You can collect data on MIB objects with a `String` data type; that is, monitor MIB objects such as `sysContact`.
- To configure your system to collect MIB data, you need to understand the definitions of the MIB objects and what they do.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1087
Doc: 3740



Most device vendors include documentation about their enterprise-specific MIB with their product. This documentation typically describes the MIB object and what the object means. In addition, some vendors include overview information describing strategies for how to manage their specific device. The vendor documentation can give you the conceptual understanding you need to configure your system to collect MIB data.

- Decide if it would be useful to collect the results of a MIB expression (MIB objects combined into a mathematical formula) rather than individual MIB objects. If you want to use a MIB expression, see "Creating and Using MIB Expressions" on page 460 for information about writing and using MIB expressions.
- Identify the nodes on which you will collect data. For example, for a network segment, you may want to collect data on the router, the hubs, and the key file server.
- Identify how often you want to collect data.
- Ensure the management station has enough room to store the data. NNM automatically collects data by default (select `Options: Data Collection and Thresholds` to see the list of current data collections). The amount of disk space required depends upon how much data you collect. For an example, say that you want to collect data for 10 MIB objects on 50 nodes, each with an average of 8 instances of these objects. If you choose a collection interval of half an hour, the collection rate will be 10x50x8x2 = 8000 values/hour. Since each value collected consumes 24 bytes of disk space, the disk consumption rate is 8000x24 = 192,000 bytes/hour.

  Windows: Data is stored in the *`install_dir`*`\databases\snmpCollect` directory.

  UNIX: Data is stored in the `$OV_DB/snmpCollect` directory. If you need more disk space, symbolically link to another file system.

TIP

For HP-UX systems only: You can expand the file system with Logical Volume Manager. Extend the logical volume, then use `extendfs` (hfs) or `fsadm` (vxfs).

2441

Procedure Tips

To access NNM's Data Collection & Thresholds application, from any submap, select `Options:Data Collection & Thresholds:SNMP`. Refer to NNM's online help available from the Data Collection & Thresholds window for directions and additional information.

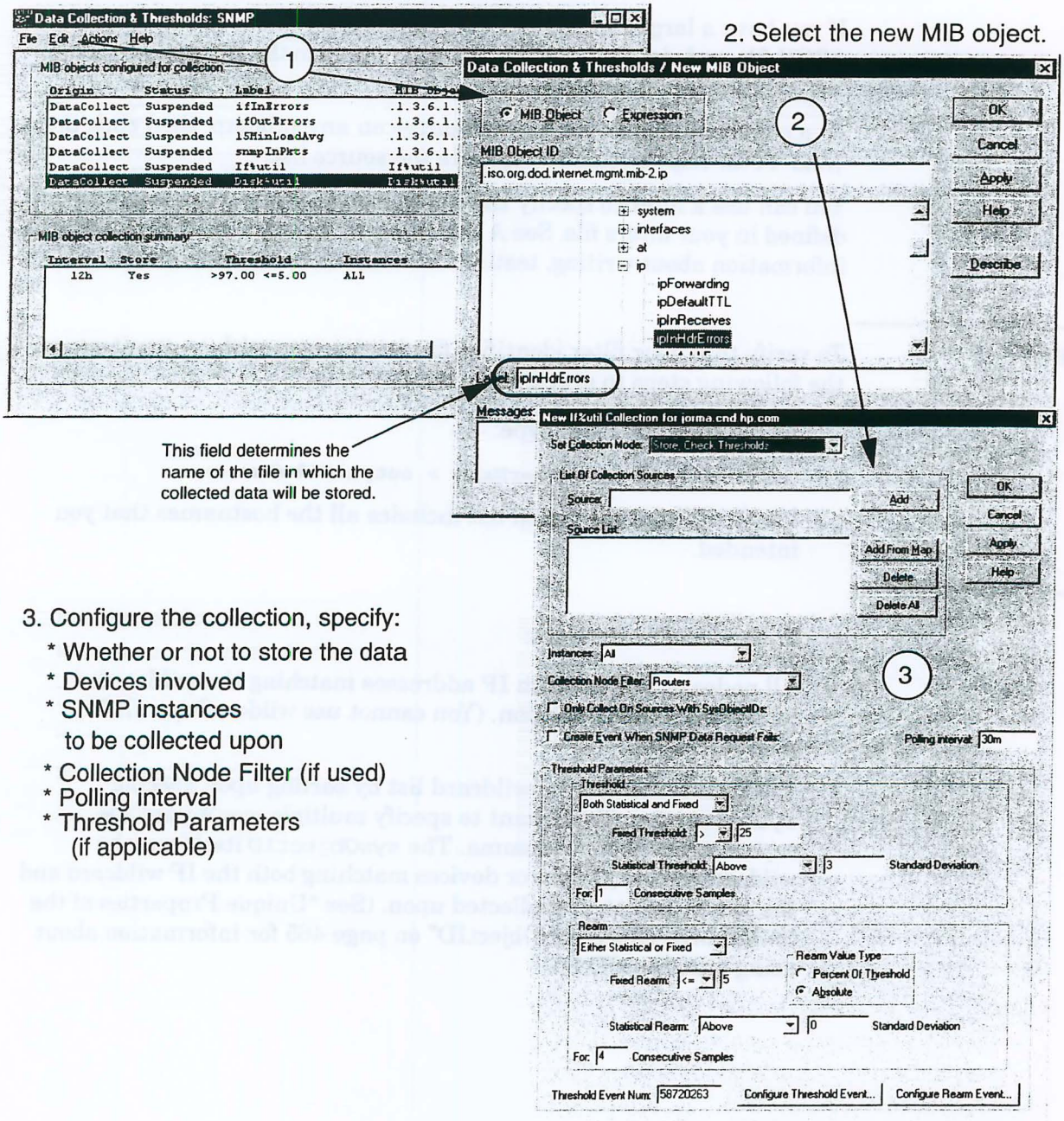
Select the MIB object or expression to be used for data collection. The `Label` field (circled in the following figure) in the MIB selection window determines the file name where the collected data will be stored. (Make

ROS nº 03/2005 CN -
CPMI - CORREIOS
Fls. Nº 1088
3740
Doc:

sure the label conforms with file naming conventions for your operating system.) The label defaults to the last component of the MIB mnemonic name.

Figure 12-11 Data Collection Configuration

1. Use Edit:Modify to reconfigure an existing MIB Object or MIB expression for collection.
   or use Edit:New to specify a New MIB Object or expression to collect upon (GET).



3. Configure the collection, specify:
   * Whether or not to store the data
   * Devices involved
   * SNMP instances
     to be collected upon
   * Collection Node Filter (if used)
   * Polling interval
   * Threshold Parameters
     (if applicable)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1089
3740
Doc:

Then, configure the collection and designate the devices to be monitored.

You specify the devices to be monitored by IP host name, `sysObjectID`, IP address, IP address wildcard (such as `15.21.*.*`), and/or (*NNM for Windows only*) IPX address.

If you have a large number of nodes to specify, you can list them in an ASCII file and simply place the full path name to the file in the `List of Collection Sources` field.

As a convenience, you can select sources on any submap, then click the `[Add From Map]` button to populate the source list.

You can use a filter to specify the list of objects. You may use any filter defined in your filters file. See *A Guide to Scalability and Distribution* for information about writing, testing, and implementing a filter.

TIP

To verify that your filter identifies the sources you wish to monitor, use the following steps to preview the list:

1. At the command line, type:

   ```
   ovfiltertest -f filterName > outputFileName
   ```

2. Verify that the generated list includes all the hostnames that you intended.

With wildcard IP addresses:

- All nodes or devices with IP addresses matching the wildcarded address are collected upon. (You cannot use wildcards on IPX addresses.)
- You can further limit a wildcard list by sorting upon specific `sysObjectIDs`. If you want to specify multiple `sysObjectIDs`, separate them with a comma. The `sysObjectID` itself may be wildcarded. Only nodes or devices matching both the IP wildcard and the `sysObjectID` are collected upon. (See "Unique Properties of the SNMP MIB Object sysObjectID" on page 465 for information about using sysObjectID.)

NOTE

You *must* save *any* changes for the new configuration to take effect. For example, if you suspend collection on a MIB object by selecting `Actions:Suspend Collection`, the `Status` column in the selection list indicates `Suspended`. However, even though the `Status` column displays a `Suspended` status, this change does not take effect until you select `File:Save`.

The data collection configuration is reanalyzed by `snmpCollect` each time you select `File:Save`. If you used IP wildcards, and you have a large number of managed nodes, there may be a significant delay before collections resume.

Counters are computed by calculating the change per second in the sampled values. Gauges and integers store the actual sampled value.

To view the collected data, open the Data Collection & Thresholds window, highlight the specific collection configuration in the list, and then select `Actions:Show Data`.

TIP

SNMP polling requests using the `Options:Data Collection & Thresholds:SNMP` menu item increase the amount of network traffic. If this becomes a problem:

- Change the status for particular collections to `Suspended` from within the Data Collection & Thresholds dialog box.
- Modify the details of your custom data collection by either deleting nodes, deleting instances, excluding nodes, or changing polling intervals.

Defining Thresholds for Monitored MIB Objects

Thresholds let you take a proactive approach to network management. You can manually define thresholds for specific MIB objects that you are monitoring, or have NNM calculate statistical thresholds for you. You can configure events to be posted in the Alarm Browser and/or automatic actions to be taken when the specified thresholds are exceeded. Once you have established a threshold and configured a threshold event, you can

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1090
3740
Doc:

use the web Reporting interface to create threshold violation reports. See NNM's online help for more information about the web Reporting interface.

If setting fixed thresholds, first determine what would constitute reasonable thresholds. To decide on a threshold value, you need to know what is normal and what is out of range. Only you can decide what is normal behavior for a device on your network. Generally, HP recommends that you collect information about a device throughout one complete business cycle before determining the normal high/low range. Consider collecting values such as error rates, retry limits, collisions, throughput, relation rates, and many more. Explore the MIB being used to determine which information to collect.

As soon as you install NNM, data collections on certain MIB objects are started. (You can see which objects are being collected from which devices by selecting `Options:Data Collection and Thresholds`.) This data is available for automatically setting thresholds based upon deviation from normal values. NNM uses the following process to establish statistical thresholds based upon the data being collected:

1. NNM gathers data as configured in Data Collection & Thresholds (the `snmpCollect` background process collects, compares, and stores requested SNMP MIB values).
2. NNM exports the collected *trend* data to the data warehouse every hour. See the *request_list* reference page in NNM's online help (or the UNIX manpage) for information about when NNM runs export tasks.
3. The data warehouse computes, for each instance of each configured collection:
   - The number of data points gathered in the past four days
   - The data summary
   - The sum of the squares for each collection

   This information, from the previous four days, is written to the `snmpColStats.txt` file. This file is recreated each time data is exported to the data warehouse. A notification event is sent to `snmpCollect`.

   These data points are sorted into three time periods, 8 p.m.-5 p.m., 5 p.m.-8 a.m., and weekends. See the *statTimeRanges.conf* reference page in NNM's online help (or the UNIX manpage) for information about controlling the definitions of the time periods.

4. When using automatic statistical threshold generation for a data collection configuration, `snmpCollect` reads `snmpColStats.txt` and calculates, one threshold standard deviation for each time period (bucket) for each data collection instance. Every time the `snmpColStats.txt` file is read, NNM compares the standard deviation calculations to the standard deviation that you specified. An alarm is generated if the current standard deviation exceeds the threshold standard deviation. See the *snmpCollect* reference page in NNM's online help (or the UNIX manpage) for more information.

   Multiple thresholds are allowed per node, one for each instance; for example, one threshold set for a primary hard drive, and a different threshold set for the secondary hard drive.

CAUTION If you are using `ovdwtrend -trim` or `-delete` options to manage the volume of your collected data, ensure that your schedule allows sufficient data history for the statistical threshold feature. See the *ovdwtrend* reference page in NNM's online help (or the UNIX manpage) for information.

Prerequisites

- Configure the data collection to which the threshold applies (see "Data Collection & Thresholds" on page 447).
- You can monitor thresholds on numeric MIB objects; that is, the MIB objects defined as `Counter`, `Gauge`, `INTEGER`, `IpAddress`, `Counter64`, or `TimeTicks`. You can also set thresholds on MIB expressions (see "Creating and Using MIB Expressions" on page 460).

Procedure Tips

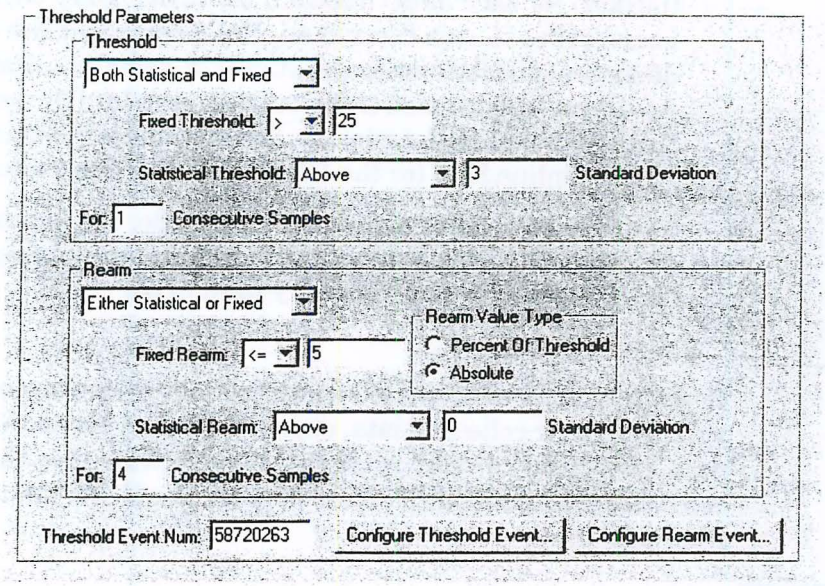
Access the collection configuration dialog box of the configured Data Collection you have been using to establish the normal operating range of your device. Select *one* of the following menu items from the `Option` menu next to the `Collection Mode` label:

- `Don't Store, Check Thresholds`
- `Store, Check Thresholds`
  (required if you want to use the statistical threshold feature)

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1091
3740
Doc:

The `Threshold` and `Rearm` fields are now available.

Figure 12-12 Threshold Area of Data Collection Window



To set up fixed-value threshold monitoring, select "Fixed" or "Both Statistical and Fixed" mode, specify a threshold value, and specify the number of consecutive samples required to violate the threshold. To set up fixed-value rearm monitoring, specify a fixed rearm value or percent, and the number of consecutive samples required to rearm the threshold.

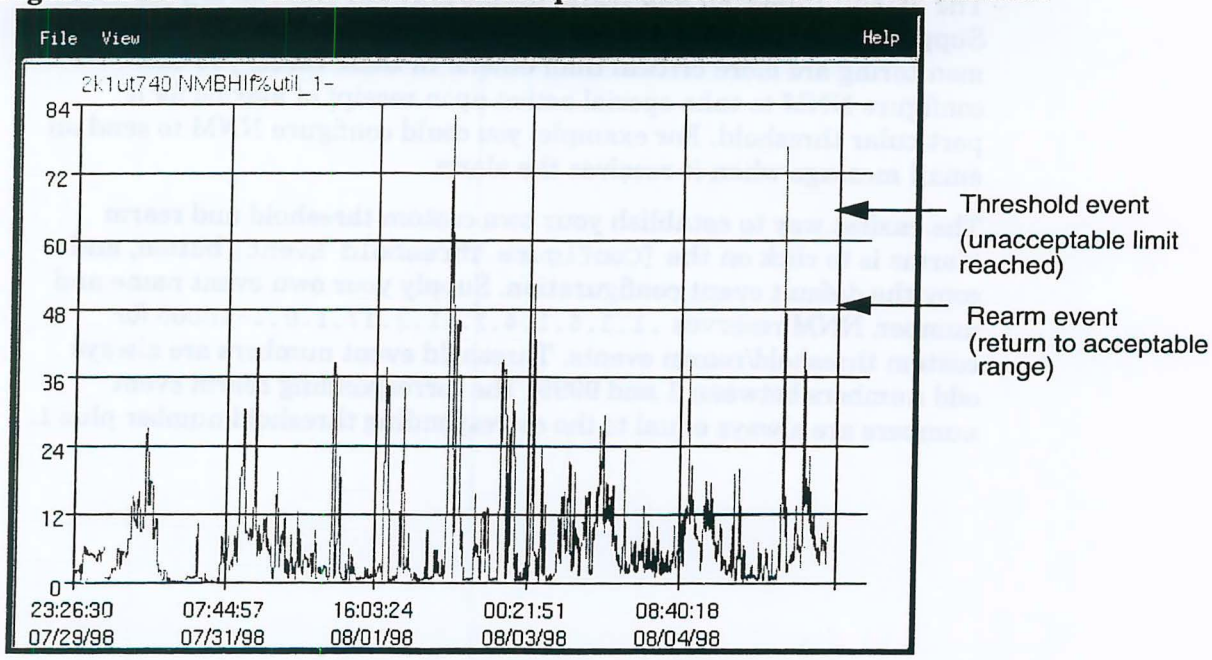
To set up automatic statistical threshold monitoring, select "Statistical" or "Both Statistical and Fixed" mode, specify the standard deviation, and specify the number of consecutive samples required to violate the threshold. To set up automatic statistical rearm monitoring, select "Both Statistical and Fixed" or "Either Statistical and Fixed" mode, specify standard deviation, and specify the number of consecutive samples required to violate the threshold. NNM automatically calculates the standard deviation according to the data warehouse's schedule for exporting trend data.

When the threshold setting is exceeded, a threshold-exceeded alarm is posted in the Alarm Browser, and any automatic actions (such as dialing a pager) that you specify in the Event Configuration are executed.

The *rearm value* controls how frequently a threshold event is generated. The *rearm* indicates that the device has returned to a non-critical state. A *rearm alarm* is posted in the Alarm Browser and any automatic

actions that you specified in the Event Configuration are executed. Another threshold event is not generated until the rearm event occurs and the collected value again reaches the threshold setting.

Figure 12-13 Data Collection Helps Establish Realistic Thresholds



For example, suppose you want to monitor interface percent-utilization. You can set a `Threshold` of 70% and a `Rearm` value of 50%. When the data collector detects a value above 70%, a threshold alarm is generated. Another threshold alarm will be generated only if the reading drops below 50% (sending a rearm alarm) and then goes above 70% again. Note that you can also specify absolute values rather than percentages.

Optionally, specify a value for the `Consecutive Samples` field. This value specifies the number of consecutive times the `Threshold` or `Rearm` expression must be satisfied before a corresponding alarm is generated. This field lets you distinguish sustained abnormality from a brief spike in behavior.

NNM uses two preconfigured events under the `OpenView` enterprise name (`.1.3.6.1.4.1.11.2.17.1.0`.) as the default events for thresholds and rearms:

```
OV_DataCollectThres (58720263)
```

RQS nº 03/2005 - CN - CPMI CORREIOS
Fls. Nº 1092
Doc: 3740



`OV_DataCollect_Rearm (58720264)`

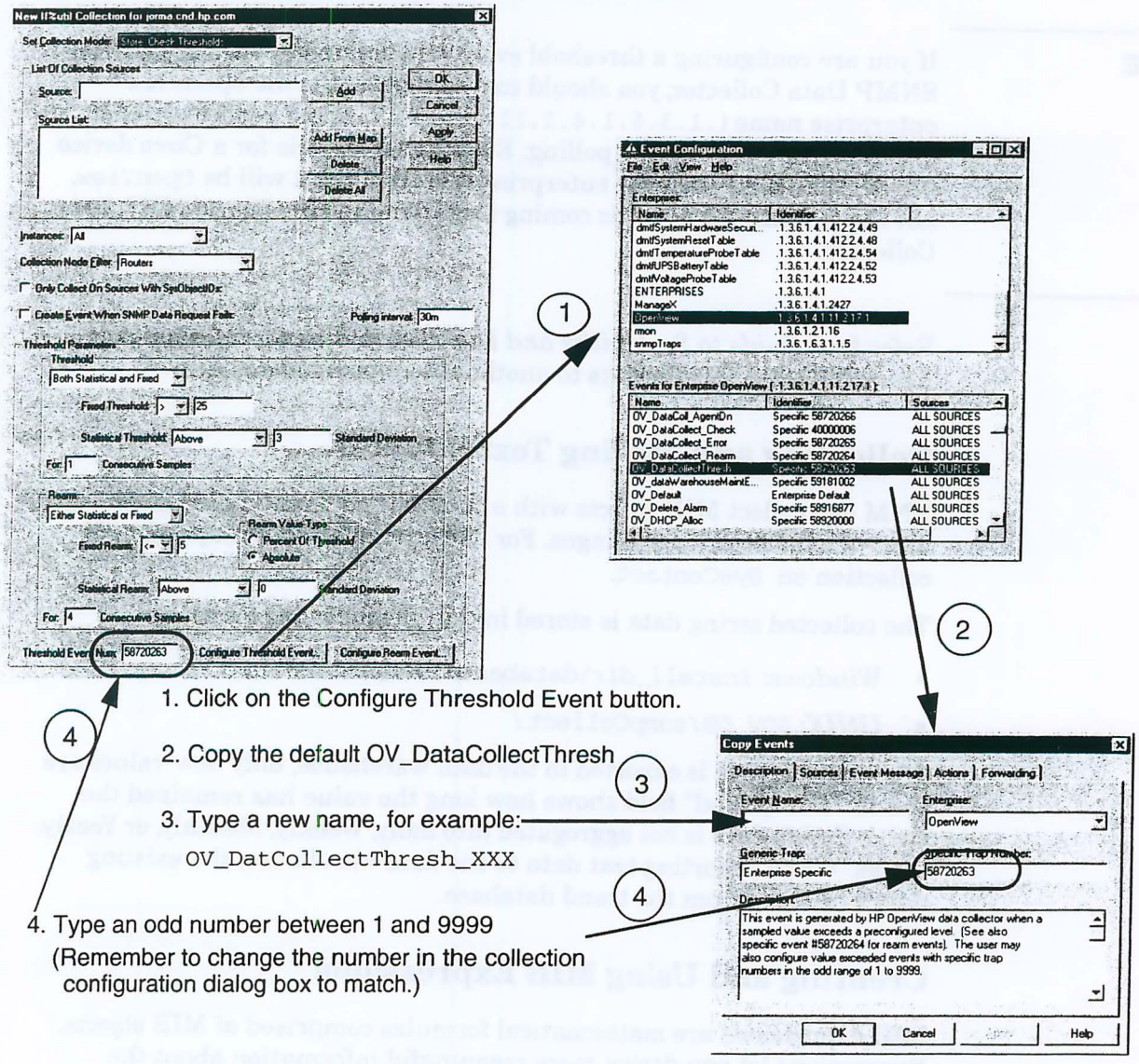
The default alarm is posted in the Alarm Browser's Threshold Alarms category.

The default threshold and rearm events may not meet all of your needs. Suppose, for example, that some of the threshold values you are monitoring are more critical than others. In these cases, you can configure NNM to take special action upon receipt of alarms for a particular threshold. For example, you could configure NNM to send an email message when it receives the alarm.

The easiest way to establish your own custom threshold and rearm alarms is to click on the `[Configure Threshold Event]` button, and copy the default event configuration. Supply your own event name and number. NNM reserves `.1.3.6.1.4.1.11.2.17.1.0.1-10000` for custom threshold/rearm events. Threshold event numbers are always odd numbers between 1 and 9999. The corresponding rearm event numbers are always equal to the corresponding threshold number plus 1.

NOTE If you create a custom threshold event, you must also create a matching rearm event.

Figure 12-14 Customizing the Threshold Event



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1093
3740
Doc:

For example, the threshold event ID 1005 will have a rearm event ID of 1006. These rearm event IDs are automatically assigned but *not* automatically configured in NNM. If you use one of the optional threshold event numbers, you must configure events for both the threshold and rearm event IDs (use the `[Configure Threshold Event]` and `[Configure Rearm Event]` buttons).

NOTE

If you are configuring a threshold event created by the HP OpenView SNMP Data Collector, you should configure it under the `OpenView` enterprise name (`.1.3.6.1.4.1.11.2.17.1.0.`), regardless of which node the Data Collector is polling. Even if the event is for a Cisco device exceeding a threshold, the enterprise ID of the event will be `OpenView`, not Cisco, since the event is coming from the HP OpenView SNMP Data Collector.

Refer to *A Guide to Scalability and Distribution* for information about forwarding threshold events to another management station.

Collecting and Storing Textual Data

NNM can collect MIB objects with a `String` data type. This data can be used to monitor device changes. For example, you can set up data collection on `SysContact`.

The collected string data is stored in the following locations.

- *Windows:* *`install_dir`*`\databases\snmpCollect\`
- *UNIX:* `$OV_DB/snmpCollect/`

When string data is exported to the data warehouse, only new values are stored. The "period" field shows how long the value has remained the same. String data is not aggregated into daily, Weekly, Monthly, or Yearly tables. When exporting text data to the data warehouse, the existing data is deleted from the trend database.

Creating and Using MIB Expressions

MIB expressions are mathematical formulas comprised of MIB objects. Expressions let you derive more meaningful information about the health of your network than you could gather using individual MIB objects. MIB expressions are used by several NNM components, and are

available for your use through the Data Collection & Thresholds window. You can also create your own and add them to the list by making additions to the `mibExpr.conf` file and the `mibExpr.conf` file.

Default MIB Expressions

NNM includes many default MIB expressions for your convenience. To explore the default MIB expressions, from any submap, select `Options:Data collection & Thresholds`, then select the following menu item:

Windows: `Edit:MIB Object->New`

UNIX: `Edit:Add->MIB Objects...`

Select the `Expressions` radio button. The list of predefined MIB expressions is displayed for your use. The following are a small sampling of the MIB expressions provided:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1094
3740
Doc:

Equation 12-1 **If%deferred (MIB II)**
The percent of packets on an interface which were deferred:

$$(\text{packets deferred rate} \div \text{packets transmitted rate}) \times 100$$

Equation 12-2 **If%collision (MIB II)**
Percent of packets on an interface which collided:

$$(\text{collision rate} \div \text{packets transmitted rate}) \times 100$$

Equation 12-3 **If%inErrors (MIB II)**
Percent of input packets on an interface which had an error:

$$\left(\frac{\text{input error rate}}{\text{received unicast packet rate} + \text{received non-unicast packet rate}}\right) \times 100$$

Equation 12-4 **If%outErrors (MIB II)**
Percent of output packets on an interface which had an error:

$$\left(\frac{\text{output error rate}}{\text{transmitted unicast packet rate} + \text{transmitted non-unicast packet rate}}\right) \times 100$$

Equation 12-5 **If%util (MIB II)**
Percent of available bandwidth utilized on an interface:

$$\left(\frac{(\text{received byte rate} + \text{transmitted byte rate}) \times 8}{\text{interface link speed}}\right) \times 100$$

Equation 12-6 **IfInOutOctets (MIB II)**
Total absolute traffic on an interface or the summation of octets (bytes) sent and received on an interface:

$$\text{received byte rate} + \text{transmitted byte rate}$$

Equation 12-7 **IfInOutPackets (MIB II)**
Total absolute traffic on an interface or summation of packets sent and received on an interface:

$$\left(\frac{\text{received unicast packet rate}}{\text{received non-unicast packet rate}} + \frac{\text{transmitted unicast packet rate}}{\text{transmitted non-unicast packet rate}}\right)$$

Equation 12-8 **Disk%util (HP-UX MIB)**
Percentage of disk utilization:

$$\left(\frac{\text{blocks} - \text{free blocks}}{\text{blocks} - \text{free blocks} + \text{available blocks}}\right) \times 100$$

Simply select one from the list and configure it for data collection and/or threshold monitoring on your network's devices.

TIP

There are seven additional MIB expressions defined specifically for use with the HP-extensible agent. They are located in:

- *Windows:* `install_dir\conf\extExpr.conf`
- *UNIX:* `$OV_CONF/extExpr.conf`

Open the file to read about them.

The mibExpr.conf File

The expressions are stored in an ASCII file:

- *Windows:* `install_dir\conf\mibExpr.conf`
- *UNIX:* `$OV_CONF/mibExpr.conf`

You can modify this file or create your own expressions using the `xnmcollect -loadExpr` utility. Best practice is to create a separate file with your new or revised MIB expressions, and then merge the expressions into the `mibExpr.conf file` using the following utility from the command prompt:

```
xnmcollect -loadExpr filename
```

The `-loadExpr` checks syntax, removes duplicate expressions, and rewrites the file.

See the *mibExpr.conf* reference page in NNM's online help (or the UNIX manpage) for information about writing your own MIB expressions; and see the *xnmcollect* reference page in NNM's online help (or the UNIX manpage) for information about updating the `mibExpr.conf` file.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1095
3740
Doc:

The mib.coerce File

The `mibExpr.conf` file works in partnership with the `mib.coerce` file. Entries in the `mib.coerce` file instruct NNM to convert (coerce) a received MIB value from one data type to another (for example, from a gauge or counter to an integer) for use in the mathematical formula defined in the `mibExpr.conf` file. The `mib.coerce` file is an editable ASCII file:

- *Windows:* `install_dir\conf\mib.coerce`
- *UNIX:* `$OV_CONF/mib.coerce`

After making changes to the `mib.coerce` file, you must force NNM to acknowledge the changes; from the command line, type:

```
xnmloadmib -event
```

See the *mib.coerce* reference page in NNM's online help (or the UNIX manpage) for more information about converting MIB values from one data type to another for use in your MIB expression.

Unique Properties of the SNMP MIB Object sysObjectID

The sysObjectID is an important SNMP MIB object to NNM operations. This section describes:

- What the sysObjectID is
- How network management operations use the sysObjectID

The sysObjectID is registered in the Internet-standard MIB-II module as iso.org.dod.internet.mgmt.mib-2.system.sysObjectID (1.3.6.1.2.1.1.2). The sysObjectID is used for administrative purposes to uniquely identify the type of SNMP agent software that is running on a given vendor's hardware. This object is different from most other MIB objects; when you query it, you get back an object identifier that describes the product. For example, when you query the iso.org.dod.internet.mgmt.mib-2.system.sysObjectID using the MIB Browser on an HP OpenView SNMP Agent that is running on an HP 9000 Series 700 or Sun SPARCstation, SNMP returns one of the following object identifiers:

```
iso.org.dod.internet.private.enterprises.hp.nm.system.hpsun.sparc.sun4
iso.org.dod.internet.private.enterprises.hp.nm.system.hpsun.sparc.sun5
iso.org.dod.internet.private.enterprises.hp.nm.system.hpux.hp9000s700
```

This result tells you how the HP 9000 Series 700 or Solaris agent is registered in the MIB. The numeric identifier for Solaris is 1.3.6.1.4.1.11.2.3.10.1.2

Note that there is no value associated with the object ID returned in sysObjectID. It is a unique identifier.

The sysObjectID includes both hardware and software information, and varies depending on the type of hardware and agent software. Some vendors have a different sysObjectID for every version of their agents. For example, Hewlett-Packard sells several SNMP agents, each uniquely identified. To distinguish the HP 9000 Series 800 agent from the HP 9000 Series 700 or Solaris agent, HP registered the HP 9000 Series 800 agent as:

```
iso.org.dod.internet.private.enterprises.hp.nm.system.hpux.hp9000s800
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1096
3740
Doc:

netmon, a service (background process) that automatically discovers the nodes on your network, obtains the sysObjectID when it queries SNMP nodes. NNM operations take advantage of this special object in the following ways:

- To identify the vendor; that is, the manufacturer of the hardware.
- To identify the source of the SNMP agent, which is the type of agent software running on the hardware. For example, if you do a GetRequest to a Sun SPARCstation, the vendor is Sun, but the SNMP agent may be
  - An HP OpenView SNMP Agent for SunOS
  - An SCO UNIX for SunOS agent
  - Other SNMP agent software
- To determine IP topology behavior. An agent's sysObjectID provides hints about what type of node the agent is; for example, a gateway, a bridge, or a host.
- To determine symbol type when putting symbols for newly discovered nodes on the map; for example, a bridge, a gateway, or a hub.
- To identify the source of an event. A sysObjectID is sent in every event. You can use the sysObjectID when you configure events and data collections. The reference in the Event Configuration dialog box to enterprise ID is generally synonymous with the sysObjectID of the agent that generated the event.

Like NNM, you can take advantage of the sysObjectID in many ways, such as:

- From any submap, select Find:Object By Attribute to locate quickly all of a certain manufacturer's model-X when they require a software upgrade.
- If you are writing a rules-based application or script, use the sysObjectID as a rule index.
- On any submap, select a node and use Edit:Object Properties to quickly determine which SNMP agent is running on that node.
- Use the sysObjectID in your filter definitions: discovery, topology, map, etc.

- Use the `sysObjectID` when using the `ovtopodump` command to generate useful lists.
- Customize NNM to display a symbol that you created for a specific type of object (see Appendix D, "Changing All the Symbols for a Particular Device," on page 661).
- If NNM displays an object on the map with a generic symbol (just the outside shape, no vendor-specific icon within the shape), you can specify the icon of your choice to be mapped to that device's `sysObjectID` (see Appendix D, "Changing All the Symbols for a Particular Device," on page 661).
- Specify nodes for which data should be collected, as described in the previous section.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1097
Fls. Nº 3740
Doc:

2422

Unique Properties of the SNMP MIB Object sysObjectID

13 Using Event Data

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1098
3740
Doc:

NNM provides several features that can assist you in analyzing the network data that has been collected:

- *Graph SNMP Data* (page 471)

  Display collected SNMP data in graphs. This can be SNMP data that has been collected over time and stored in a file, or real-time values that are graphed as they are collected, or both at the same time.

- *Data Warehouse* (page 476)

  Allows you to export collected historical data for use with other statistical analysis tools. Command line functions allow you to maintain the data warehouse database.

- *Web Reporting Interface*

  Allows you to use data from the data warehouse to create reports using a set of predefined templates. See the *Reporting and Data Analysis* online manual and the online help for more information.

NOTE For information about how to merge data from multiple NNM collection stations into a single database, see *A Guide to Scalability and Distribution*.

Ideas for utilizing your collected data:

- Anticipate the need for more network and computer resources, such as gateways and disk space.
- Detect deviations in normal activity.
- Isolate network faults and performance problems.
- Generate inventory reports.

Graphing SNMP Data

The NNM Grapher tool allows you to graph collected MIB data from within the SNMP MIB Browser. Once the Grapher window is displayed, you can set time intervals to continue the collection and even automatically establish a configuration for continuous monitoring by selecting `File:Configure in Data Collector`.

The NNM Grapher tool also enables you to organize MIB data that was collected by the Data Collections & Thresholds feature and view it in graph form. You can graph combinations of data values in the same graph. The data values can be different instances of MIB variables or different variables for different nodes. For example, you can graph instance 1 and instance 3 of a MIB variable for one system, or you could graph instance 3 of a MIB variable for one system, and a completely different variable for another system. You can also normalize the data over configurable time periods to identify trends in the historical data.

This section describes the following:

- Graphing collected data, which includes graphing all data or graphing selected data only, and updating data that has been graphed.
- Graphing historical and real-time data in the same graph.
- Zooming in and out of a specific period of time to view the data in greater or less detail.
- Modifying line attributes in a graph.
- Printing a graph.

NOTE The Grapher tool is available in NNM on a Windows or UNIX operating system. If you are using NNM on the Web, there is a Grapher tool available in the `contrib` directory. (See page 74 for information about using programs from the `contrib` directory.)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1099
Doc: 3740

Graphing Collected Data

You can graph the data collected in the Data Collector's database by using the `Performance:Graph SNMP Data->All` and `Performance:Graph SNMP Data->Selected Nodes` menu items. You can also access the Grapher tool from within the SNMP MIB Browser or by using the `xnmgraph` command. Refer to the *xnmgraph* reference page in NNM's online help (or the UNIX manpage) for more information.

Behavior

The Graph Selected Nodes dialog box consists of a line graph. The legend across the top of the graph identifies the currently graphed data. Time is shown on the X-axis.

The menu bar has functions that enable you to manipulate the data. The menu bar also has help entries explaining how to use the different menu options to manipulate the data.

The Graph SNMP Data operation does not update the graph with new information as the data is collected. To update the graph with the most current MIB data, select `File:Update Data` from the Grapher menu bar.

Refer to the online help within the graph window for additional information.

Graphing All Data

The `Performance:Graph SNMP Data->All` operation enables you to view collected data in graph form without first having to build an application. This is useful when you want to browse all the data in the Data Collector's database:

- *Windows:* Data is stored in the *`install_dir`*`\databases\snmpCollect` directory.
- *UNIX:* Data is stored in the `$OV_DB/snmpCollect` directory. (If you need more disk space, symbolically link to another file system.)

TIP

For HP-UX systems only: You can expand the file system with Logical Volume Manager. Extend the logical volume, then use `extendfs` (hfs) or `fsadm` (vxfs).

Use this operation when you want to graph some data points just once, or when you want to compare different variables across different systems. For example, let's say you want to compare the load averages to the number of packets, but had not used the Application Builder (see page 443) to set up your own application for this purpose. You can easily use the Graph All operation to graph these two variables together.

CAUTION This operation reads in *all* the collected data from the Data Collector database into its memory. Depending on the amount of data stored in the database, displaying the Graph All dialog box may take a long time.

Graphing Data on Selected Nodes

The `Performance:Graph SNMP Data->Selected Nodes` operation enables you to view collected data on the nodes that are currently selected on the map, without having to use the Application Builder (see page 443) to set up your own application for this purpose. This is useful when you want to browse the collected data for these nodes. Use this operation when you want to graph some data points just once, or when you want to compare different variables across different systems.

For example, let's say you want to compare the load averages to the number of packets on the selected systems, but had not used the Application Builder (see page 443) to set up your own application for this purpose. You can use the Graph Selected Nodes operation to easily graph these variables together.

Graphing Historical and Real-Time Data in the Same Graph

When you use the Grapher tool via an NNM-provided menu item, the Grapher displays both the collected data and real-time data in the same graph (for example, `Performance:Network Activity`).

When Grapher starts up, it does the following:

1. Reads in the data from the Data Collector's database.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1100
Doc. 3740

When the Grapher tool first comes up, it loads all the collected data from the Data Collector database and seeds its memory with the information in the database. The resolution of the collected data is determined by what the Data Collector was configured to collect.

Once the Grapher tool is running, the tool does not interact with the data in the Data Collector database again (unless you select `File:Update Data`). The Data Collector operates in the background and continues to collect data. This data is available for you to use in future operations.

2. Starts to graph the real-time data.

   The real-time data displayed is independent of the Data Collector. The Grapher tool processes SNMP requests based on the interval specified under `View:Time Intervals` and displays the data in the graph. Unless you save the graphed data to a file using the `File:Save As` menu item, the real-time data is lost as soon as you exit the Grapher.

Stopping Real-Time Data Graphing

To stop real-time data graphing, from the Graph window:

- *Windows:*

  Select `Options:Time Intervals->SNMP Polling Off`.

- *UNIX:*

  Select `View:Time Intervals->SNMP Polling Off`.

Grapher Operations

This section describes some common operations for manipulating a graph.

Selecting Time Intervals

To select time intervals, using the left mouse button:

- Click on the left edge of the graph to page back one screen.
- Click on the right edge of the graph to page forward one screen.
- Click within the graph to center the graph around the selected point in time. Holding the mouse button down and dragging enables you to fine tune the point that you want centered.

Zooming In and Out of a Graph

The Grapher allows you to zoom in and out of a specific period of time in order to view data in greater or lesser detail. To do so, using the right mouse button, click anywhere within the graph. An option menu appears. You can zoom in and out to different amounts of detail. You can also use the menu to page forward, page backward, or show different data points.

Modifying a Line Attribute

To access the `Line Configuration` dialog box, from the Graph window:

- *Windows:* Select `Options:Line Configuration`.

  Option buttons are arranged in rows and columns. Each item in the list controls the attributes for a particular line on the graph.

- *UNIX:* Select `View:Line Configuration`.

  Option buttons are arranged in rows and columns. Each row in the list controls the attributes for a particular line on the graph.

Printing a Graph

To Print a graph, from the Graph window:

- *Windows:* Select `File:Print`. The standard `Print` dialog box appears. Make your selections and click `[OK]`.
- *UNIX:* An `xwd`-compatible file is produced by the Grapher. The default `Print` command is configured in the Grapher print resource. The commands shown in the Print Command window are used to print that file. If the default command does not meet your needs, you can change it. Before you configure the default `Print` command, determine which command options will give you the best printouts. See NNM's online help for more information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1101
3740
Doc:



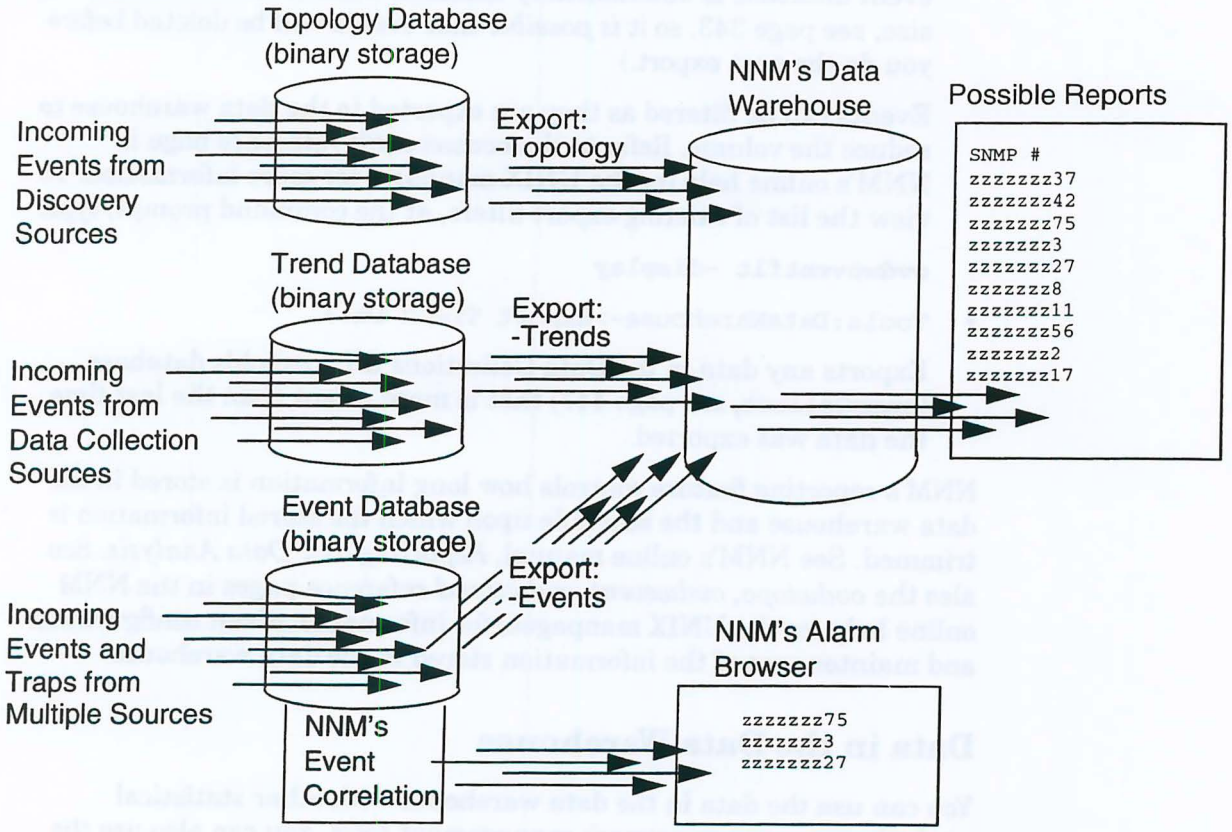
Data Warehouse

The NNM data warehouse is a relational database (RDBMS) provided with NNM. NNM stores a *copy* of the information from the NNM operational databases into the data warehouse so you can gain an historical perspective of your network information. The data warehouse information is accessible with standard SQL statements using ODBC tools. You can also create reports from the data using the NNM web Reporting interface.

By contrast, the information in the NNM *event database* is discarded when a certain volume is reached (see page 343). Information copied to the *data warehouse* is retained for as long as you need it. You can derive reports from hourly, daily, weekly, monthly, or even yearly information. The limit to the size of the data warehouse is up to you and the allotted hard drive space for the data warehouse.

2443

Figure 13-1 NNM's Event Flow



NNM periodically populates the data warehouse according to a schedule. See the *ovrequestd* and *request_list* reference page in NNM's online help (or the UNIX manpage) for more information. To view the current schedule, at the command prompt, type:

```
request_list schedule
```

You can also manually populate the data warehouse using the following pull-down menu items:

- `Tools:DataWarehouse->Export Topology`

  Exports the current network topology information, replacing any topology information previously sent to the data warehouse.

- `Tools:DataWarehouse->Export Events`

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1102
3740
Doc:

Exports any event database information that is more current than the last time the events database was exported. (Remember: NNM's event database is automatically trimmed when it reaches maximum size, see page 343, so it *is possible* that events will be deleted before you do the next export.)

Events can be filtered as they are exported to the data warehouse to reduce the volume. Refer to the *ovdweventflt* reference page in NNM's online help (or the UNIX manpage) for more information. To view the list of existing export filters, at the command prompt, type:

```
ovdweventflt -display
```

- `Tools:DataWarehouse->Export Trend Data`

  Exports any data in the Data Collections &Thresholds database (`snmpCollect`, see page 447) that is more recent than the last time the data was exported.

NNM's reporting feature controls how long information is stored in the data warehouse and the schedule upon which the stored information is trimmed. See NNM's online manual, *Reporting and Data Analysis*. See also the *ovdwtopo*, *ovdwevent*, *ovdwtrend* reference pages in the NNM online help (or the UNIX manpages) for information about configuration and maintenance of the information stored in the data warehouse.

Data in the Data Warehouse

You can use the data in the data warehouse with other statistical analysis programs or network management tools. You can also use the data to create reports with NNM's web Reporting interface.

See the NNM online manual, *Reporting and Data Analysis*. See also the NNM online help.

Reporting

Reporting is enabled by default when NNM is installed. Once the report data is collected, daily and month-to-date reports for general availability, threshold violation exceptions, and network performance are available from the `Tools:Report Presenter` command or from the HP OpenView Launcher. Daily Inventory reports are available as soon as the report data is collected. For more information about reporting see page 45 in this manual.

For more information about the Reporting feature, see the section labeled "Reporting Interface" on page 516 in this manual.

For more information about the NNM databases and the data warehouse, consult the online manual *Reporting and Data Analysis*.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1103
3740
Doc:

14 NNM on the Web

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1104
Fls. Nº
3740
Doc:



NNM on the Web

This chapter describes HP OpenView's Java™-based web interface, and tells you how to set up, configure, and administer NNM's web applications.

This chapter will not attempt to teach you how to use all the features of HP OpenView's web interface. You should consult the NNM online help within the web interface for usage instructions. For an introduction, explore the *Get Acquainted with HP OpenView Network Node Manager: Training for NNM Operators* CD provided with NNM.

This chapter refers to HP OpenView Application Registration Files (ARF) in several places. If you are not familiar with that file, review its functionality in the online manual *Creating and Using Registration Files*.

TIP If you make changes or additions to the web registration files ensure that your new files are properly backed up. They are *not* included in NNM's backup scripts. See "Backup/Restore to Protect Your Investment of Time" on page 165 for more information.

This chapter includes:

- An overview of the HP OpenView web applications, including setting up the web applications and security for the web applications (page 484).
- A description of the HP OpenView Launcher, the UI integration point for the web applications, including configuration details (page 492).
- A description of the Network Presenter, the web application that displays maps and map data (page 501).
- A description of the SNMP Data Presenter, which displays the results of operations that gather data from managed SNMP nodes (page 509).
- A description of the web-based Alarm Browser, a graphical interface that presents network alarm data, including a comparison of the web-based Alarm Browser and the Alarm Browser running on the management station (page 512).
- A description of Event Correlation Services, NNM's multi-protocol event correlator (page 515).

- A description of the Reporting interface, the web application that allows you to configure and view reports (page 516).
- A description of several supplemental views of discovered nodes (page 518).

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1105
3740
Doc:



Overview

HP OpenView's Java-based web interface further expands NNM's network management capabilities. A part of NNM's base product, the web interface and its applications present the same information about your network that is available from the NNM management station. This information is now presented in a familiar, operator-friendly format that you can access from a remote workstation running a web browser. From your web browser on any PC or UNIX operating system workstation, you can log onto the web and access NNM on the management station to display maps and alarm information. You can easily monitor the status of your network from any place at any time, a real advantage when your pager goes off in the middle of the night!

The HP OpenView Web lets you:

- Inquire about the status of your network and troubleshoot problems from anywhere via the World Wide Web.
- Obtain dynamic updates on map information.
- Share management data with others.
- Present both a graphical and tabular view of the network.
- Access and configure security for web applications.
- Launch NNM and other web-based applications.
- Interact with a familiar web interface.
- Configure and view reports.

The HP OpenView Web includes the following applications:

- HP OpenView Launcher
- HP OpenView Network Presenter
- HP OpenView SNMP Data Presenter
- HP OpenView Alarm Browser
- HP OpenView ECS Configuration
- HP OpenView Correlation Composer
- HP OpenView Reporting interface

An overview and the administration of each of these applications is discussed in the following sections of this chapter.

Setting Up the HP OpenView Web

When you install NNM on the management station the files and applications necessary to run the web interface are also installed. The management station must also have a web server running.

When you install NNM on a management station running Windows, a web server is not installed, since the Windows operating system comes with its own web server. The web server on the Windows operating system is automatically configured for NNM's use during the NNM installation.

When you install NNM on a management station with a UNIX operating system, a web server *is* installed. This server is fully configured to access scripting aliases and documentation aliases used by NNM. The web server uses port 3443 for communication.

If you want to set up your own web server, configure the port number and set up the aliases `OvCgi`, `OvDocs`, and `OvBackgrounds`, see NNM's release notes for additional information about installing a web server.

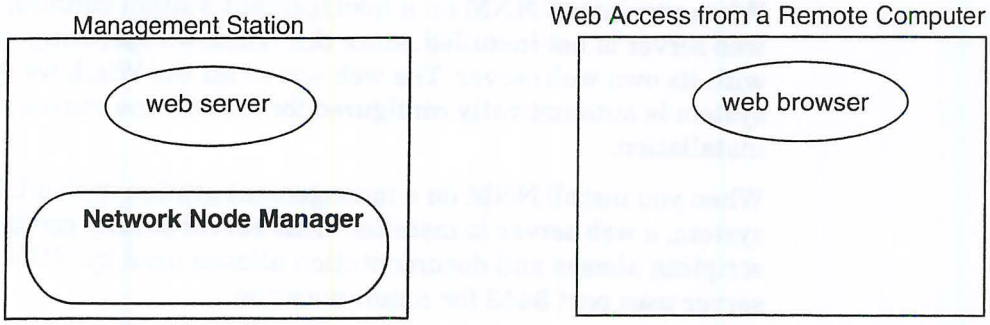
The client station only needs to have a web browser running. Supported web browsers are:

- Netscape
- Microsoft Internet Explorer

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: Nº 1106
3740
Doc:

NOTE Refer to the "Supported Configurations: Supported Web Browsers" section of the NNM Release Notes for specific information about supported web browsers.

Figure 14-1 Management Station and Remote Web Access



See Figure A-4, "Services and Files for the Web Components," on page 551 for more detailed information about the files and services (processes) on the management station and remote computer at installation time.

On the management station, there must be a non-web based version of NNM running for each map that will be accessible through remote web access. For example, if you want your team to be able to access the Home Office map and the map showing your operations in Germany, you must start NNM on the management station with your Home Office map displayed and start another instance of NNM on the management station with the Germany map displayed. See page 508 for more information.

From remote sites you can now use your web browser and NNM's Network Presenter to display the Home Office map or the Germany map.

Role Configuration Files for the HP OpenView Web

Since the HP OpenView Web can be accessed from virtually any system, security measures are in place to ensure that only authorized users log in to your NNM management station. The way the HP OpenView Launcher and the web applications use these mechanisms varies. The security mechanisms are:

- User authentication (password) file.
- User authorization (roles) file.
- Session configuration file.
- Audit log files.
- `ovw.auth` and `ovwdb.auth` files (used by the Network Presenter and discussed in the section "Configuring Security for the Network Presenter" on page 506).

Since the Launcher is the access point for all other web applications, it provides the first level of security. When security is enabled via the session configuration file, the user password file and user roles file are read to ensure that the user is authorized to access NNM on the management station. The user roles file ensures that only those applications approved for that user role are made available via the Launcher.

User Authentication (Password) File

User authentication is accomplished through a user name and user password. Users should not use the same password as their operating system password. Since the passwords are passed in cleartext format at the beginning of a session, it is possible that they may be intercepted. The Launcher uses the user password file when the user attempts to log on.

The user password file is located on the management station at:

Windows: `install_dir\www\etc\htpasswd`

UNIX: `/etc/opt/OV/share/www/etc/htpasswd`

Entries in the file appear as:

```
john: FXSD198sdfADS
sue: PO12ADFpoiuS
```

The file is installed with administrator-only (Windows operating system) or root-only (UNIX operating system) permission.

Set passwords as follows:

`ovhtpasswd` *`username`*

The command prompts you for the password for that user.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1107
Doc. 3740

See the *ovhtpasswd* reference page in NNM's online help (or UNIX manpage) for more information about this command.

User Authorization File

Users may be assigned to any number of groups for authorization purposes. These user groups are called user roles in NNM. A **user role** is a designation given to individuals who perform specific tasks with NNM. Users are assigned roles, and then those roles are given access to specific URLs. The Launcher uses the user roles file to define what list items are visible from the Launcher window. When a user logs in, his or her role is verified, and then he or she can access the URLs assigned to that specific role. User roles are valid only when a user accesses NNM via the web interface; they are not valid when a user accesses NNM directly on a management station.

Predefined user roles and their functions are listed below. You can change these roles, or add new roles.

- NetworkAdmin

  The role of NetworkAdmin is intended for individuals who have a higher level of knowledge of networks. Capabilities for configuration of the network and connecting devices, and advanced troubleshooting should be associated with this user role.

- NetworkOper

  The role of NetworkOper is intended for individuals who do routine troubleshooting and maintenance tasks associated with the network. Capabilities for monitoring the network, and routine troubleshooting and maintenance of the network and network devices should be associated with this user role.

- NTAdmin

  The role of NTAdmin is intended for individuals who have a higher level of knowledge of the Windows operating system. Capabilities for configuration of the Windows operating system and advanced troubleshooting should be associated with this role.

- NTOper

The role of NTOper is intended for individuals who do routine troubleshooting and maintenance tasks associated with Windows operating system. Capabilities for monitoring the system, and routine troubleshooting and maintenance of the Windows operating system should be associated with this user role.

- UNIXAdmin

  The role of UNIXAdmin is intended for individuals who have a higher level of knowledge of UNIX operating systems. Capabilities for configuration of UNIX operating systems and advanced troubleshooting should be associated with this user role.

- UNIXOper

  The role of UNIXOper is intended for individuals who do routine troubleshooting and maintenance tasks associated with UNIX operating systems. Capabilities for monitoring the system, and routine troubleshooting and maintenance of UNIX operating system should be associated with this user role.

- OVAdmin

  The role of OVAdmin is intended for individuals who do configuration and customization of the HP OpenView environment and management applications. Capabilities for configuring and customizing management applications should be associated with this role.

The user roles file is located on the management station at:

Windows: *install_dir*\www\etc\htgroup

UNIX: /etc/opt/OV/share/www/etc/htgroup

The format of the user roles file is:

```
NetworkAdmin: user1 user2

NetworkOper: user4 user5

NTAdmin:user1 user3

UNIXOper: user6
```

You can also use a plus sign (+) instead of specific user names. This allows any user access to the capabilities of that user role.

User roles work in conjunction with the Access specification in the Launcher Registration Files (WLRF). See "Action Block" on page 496.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1108
3740
Doc:

Session Configuration File

The session configuration file is used by the Launcher. A **session** is a group of applications associated with a particular user on a particular display. When a user logs in, all the applications started (directly or indirectly) from the Launcher are part of that session. The applications that are part of a session can share information, such as locale.

A session is terminated when the user exits the web browser, when the session has been inactive for some configurable period of time (the default is 9 hours), or when the management station is shut down.

The session configuration file allows you to enable or disable security for NNM's web applications (default is disabled). If you specify `Off` in the `UserLogin` field of this file, NNM's web applications open directly. If you specify `On` in the `UserLogin` field of this file, NNM's web applications display a login dialog box upon opening.

WARNING **The default is for the session configuration file to disable security. If the security mechanisms are disabled in this file, users will not be presented with a login screen, and will have access to all registered actions.**

The session configuration file is located on the management station at:

Windows: *`install_dir`*`\www\conf\session.conf`

UNIX: `/etc/opt/OV/share/www/conf/session.conf`

The session configuration file has the following format:

```
UserLogin: on|off
LoginLogging: on|off
AccessLogging: on|off
SessionTimeout: hours
```

The default values are `off` for the first three items, and 9 hours for the session timeout. Time should be specified in integer values. Open the editable ASCII `session.conf` file for more information.

If you modify this file while you have the Launcher running, you need to exit the web browser and restart the Launcher for the new information to take effect.

Audit Log Files

There are two audit log files — one for logging logins and one for logging URL access from the Launcher. These are useful for security auditing purposes, as you can check on which users are accessing the Launcher by monitoring these files.

There is no log file management; the files continue to grow. You should periodically check these files and when they get large, you should save them or trim them.

The files are located on the management station at:

Windows: *install_dir*\www\logs\login_log (login log)

install_dir\www\logs\access_log (access log)

UNIX: /var/opt/OV/www/logs/launch/login_log (login log)

/var/opt/OV/www/logs/launcher/access_log (access log)

Each log entry is a single line of text. If the session configuration file is set to LoginLogging:on, the following information is recorded:

- Host
- User name
- Date
- Session number
- Access permitted; either Allowed or DENIED
- URL accessed (for the access_log file only)

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 1109
3740
Doc:

The HP OpenView Launcher

The HP OpenView Launcher is the user interface integration point for the HP OpenView web applications. Just as with management station-based NNM, developers can tie their applications into NNM's web interface. Then users access those applications through the Launcher interface.

You can also create your own application that you access from the Launcher. If you create your own application, you can integrate it with the Launcher by creating a registration file for that application.

The Launcher provides functionality in three areas:

- Launching of management functionality and applications via a URL or via the web interface.
- User login and user roles.
- Maintenance of session information shared by all web interfaces.

Launcher User Interface

The Launcher interface is started from a web browser. The URL for the Launcher is:

`http://`*`hostname`*`:`*`[port]`*`/OvCgi/ovlaunch.exe`

For example, if the host system is a management station named `UX-manage1` running a UNIX operating system, you would enter:

`http://ux-manage1:3443/OvCgi/ovlaunch.exe`

A web server is automatically installed on UNIX management stations and configured to use port number 3443 for communication.

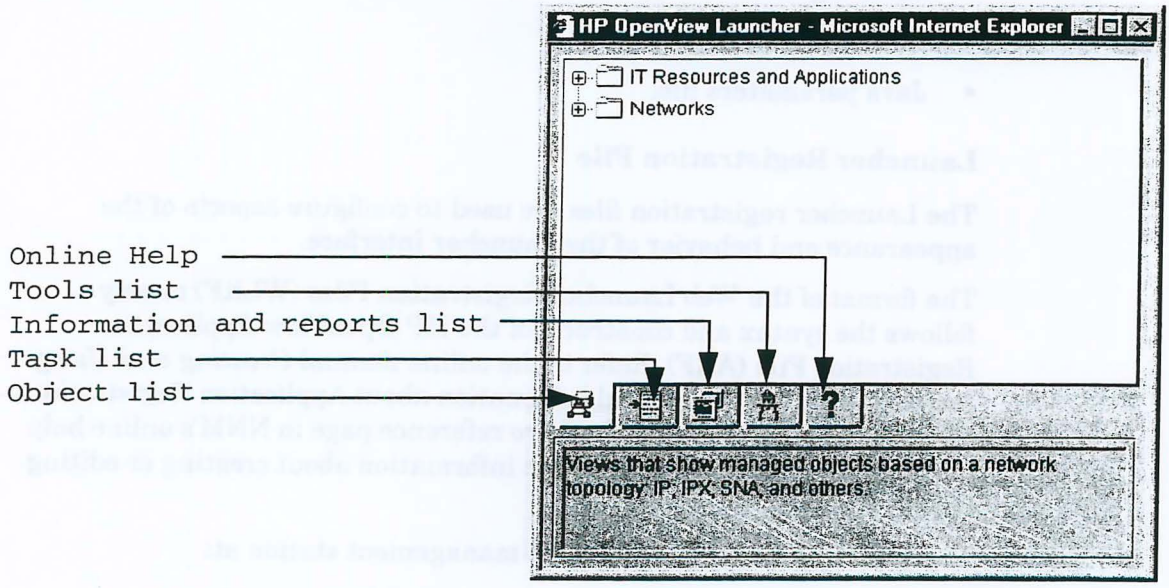
If the host system is a workstation named `nt-mgmt` running Windows, you would enter:

`http://nt-mgmt/OvCgi/ovlaunch.exe`

No port number is required for management stations running a Windows operating system.

If the management station has been configured for security, a login screen appears where the user enters his or her name and password. If no security has been configured, the Launcher window comes up without asking for login and password.

Figure 14-2 The Launcher Window



The Launcher window displays a tabular view of the capabilities available through the Launcher. The bottom tabs of the Launcher window contain the Task, Tool, Object Views, Management Areas, and Help categories. These categories correspond to the basic functionality of NNM on a management station. These are also the categories where other HP OpenView web applications will be linked.

Click on a category to expand it, or click on the expanded category to contract it. You can also click on the +/- indicator.

If you double-click on a list item, you execute the URL associated with that item.

The categories that are displayed in the tabular section of the Launcher window are determined by the user roles file and the Launcher Registration Files (WLRF), described next.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1110
3740
Doc:

Configuring the Launcher

There are several files you can use to customize the Launcher.

- Launcher registration files.
- Error log file.
- Installed locale file.
- Java parameters file.

Launcher Registration File

The Launcher registration files are used to configure aspects of the appearance and behavior of the Launcher interface.

The format of the Web Launcher Registration Files (WLRF) closely follows the syntax and constructs of the HP OpenView Application Registration File (ARF). Refer to the online manual *Creating and Using Registration Files* for general information about Application Registration files. Refer to the *LauncherRegIntro* reference page in NNM's online help (or the UNIX manpage) for specific information about creating or editing the WLRF files.

The WLRF files are located on the management station at:

Windows: `install_dir\www\registration\launcher\C\*.*`

UNIX: `/etc/opt/OV/share/www/registration/launcher/$LANG`

The bitmaps referenced in the WLRF are located in:

Windows: `install_dir\www\htdocs\C\images\*.*`

UNIX: `/opt/OV/share/www/htdocs/$LANG/bitmaps`

Components of the WLRF There are several sections of a WRLF that you might need to modify. Only those sections will be discussed here.

Once you have modified a WLRF file, you can check it for errors with the command `regverify`. See the *regverify* reference page in NNM's online help (or the UNIX manpage) for more information.This command is located on the management station at:

Windows: `install_dir\bin\regverify`

UNIX: `/opt/OV/bin/regverify`

Tab Block

The Launcher has several tabs at the bottom of its window. The tab block indicates under which of the tabs an application will appear.

The tab block allows an optional icon file name to display on the tab. If one is not specified, a default will be used. The icon appears in front of the name of the application in the Launcher content area. The format for icons is 16x16 GIF. The file name is relative to:

Windows: *install_dir*\www\htdocs\bitmaps

UNIX: $OV_WWW/htdocs/bitmaps

The tab block also contains optional active help text. This active help is presented when the mouse pointer is over the tab.

The tab block contains List Item entries instead of Menu Items (for the menu bar). Following is a sample of the tab block.

```
Tab <60> "Tools" Icon "launcher/toolsfold.20.gif"
        ActiveHelp { "tools" }
{
        <70> "Session"
                Icon "launcher/toolsfold.16.gif"
                ActiveHelp {"Session Info" }
                f.list "SESSION";
}
```

List Block

The list block of the WLRF corresponds to the menu block in the ARF.

The following statements are allowed in the list block:

- Precedence value

  This has the same definition as in the ARF.
- List Item Label

  This is the label that is displayed for the entry.
- Icon

  This is a locale-dependent icon that is displayed for the list item. The format for icons is 16x16 GIF.
- ActiveHelp

  This is the active help text that is displayed when the mouse pointer is placed over the entry.
- Functions

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1111
3740
Doc:

Two functions are supported:

— `f.action`

This indicates a terminal list item. It points to an Action block that has the action definition.

— `f.list`

This indicates a component list item. It points to a list block to allow the definition of a hierarchical tree list.

Following is a sample of the list block.

```
List "SESSION"{
     <80> "Session Info Viewer"
                Icon "launcher/tools.16.gif"
                ActiveHelp { "Session Info Viewer" }
                f.action "printsession";
}
```

Action Block

The action block of the WLRF serves the same function as in the ARF. The following statements are allowed in the action block:

- URL

  This is the URL to launch for the action. The URL may contain the special variable `$OVwWebServer`. This variable will be substituted with the name of the system from which the Launcher was loaded.

- Access

  This is a list of user roles that have access to this action. If a user does not belong to a group that has access, the user will not see the list item that invokes this action in their Launcher window. If the access statement is not present, all valid users can access this action. The user roles values correspond to entries in the user roles file. For example, `NetworkAdmin`. See "User Authorization File" on page 488.

- Window

  The Window statement specifies the characteristics of the window into which the URL will be loaded. If the WebWindow statement is not present, the URL will be loaded into an unnamed full web browser window.

  The Window definition has the following components:

2398

— Window name

This is a name for the window to allow window reuse by targeting a named window. The window name is a string of alphanumeric characters and underscores; it may not include blanks. If a new window is desired every time the URL is loaded, a blank window name (" ") may be given.

— Type (full, intermediate, or limited)

Type specifies the type of the window and determines which features it supports. If no type field is present in a window block, `full` is assumed. The values are:

— `full`, all window elements present and user configurable.

— `intermediate`, directories and menubar off, all other window elements present and user configurable.

— `limited`, all window elements off but user configurable.

— Toolbar (on or off)

— Location (on or off)

— Status (on or off)

— Scrollbars (on or off)

— Resizable (on or off)

— Width (integer value)

— Height (integer value)

Following is a sample of the action block.

```
Action printsession
{
    URL "/OvCgi/printsession.exe";
    WebWindow "OvPrintSession" {
        Type full;
        Toolbar off;
        Status off;
    }
}
```


RQS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 1112
3740
Doc:

Error Log File

The Launcher error log records internal errors from the Launcher. You can use the output from this file when discussing a problem with the HP Response Center or HP support personnel.

The Launcher error log file is located in:

Windows: `install_dir\www\logs\launcher\error_log`

UNIX: `$OV_WWW/launcher/error_log`

The error log contains the following information:

- Date
- Host
- User
- Session
- Reason or error

The error log file continues to grow without bounds. You need to watch the size of this file and truncate it as needed.

If the error log file does not give you sufficient information for troubleshooting, you can set a parameter in the URL for **ovlaunch.exe** that will enable more in-depth error logging on a session level. See "Troubleshooting Web Components" on page 613 for more information. The parameter is:

http://sysname:3443/OvCgi/ovlaunch.exe?Debug=/tmp/file

Language Selection

The Launcher and the Web applications started from the Launcher execute under a particular language, such as English or Japanese. The language used by the Launcher and the Web applications is based on the following:

- The language specified by the user when the security is enabled.
- The language specified by the user through the URL.
- The language specified by the browser.

Once a session is started, the language selection cannot be changed without restarting the browser with a different language.

Language Selection When Security is Enabled Security is enabled via the session configuration file. When security is enabled, the user is presented with a login page listing the languages available for the session under the `[Options]` button. This list represents the languages supported by the Launcher and other installed products that integrate into the Launcher. The languages presented in `[Options]` is based on the contents of the `locales.installed` file. This file is located in:

Windows: *`install_dir`*`\www\conf\locales.installed`

UNIX: `/etc/opt/OV/share/www/conf/locales.installed`

This file contains a list of locales for which the Web applications have been localized. For instance, if the Japanese NNM has been installed, this file will contain an entry for English and for Japanese, for example:

```
en
ja
```

This file can be modified by a developer or administrator. When an HP OpenView web application has been localized to a language not listed in this file, a locale entry should be added to this file. Refer to the *HP OpenView Windows Developer's Guide* for details on syntax.

Language Specified Through the URL The language for a session can be specified when the `ovlaunch.exe` URL is specified. This is done through the CGI parameter `AcceptLang`. This language specification will take precedence over the browser language specification, but can be overridden if security is on and the user chooses a different language on the login page. If security is not on, the login page will come up in the language specified by the `AcceptLang` parameter. For example:

```
http://mysystem:3443/OvCgi/ovlaunch.exe?AcceptLang=ja
```

Language Specified Through the Browser When security is not enabled, the Launcher uses language specified through the browser. For instance, if the browser has been configured to run in English, the Launcher will execute in English.

Java Parameters File

There are some Java parameters that you can modify to control Launcher appearance. You change these parameters by modifying the APPLET block in the following file, located on the management station at:

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1113
3740
Doc:

Windows: *install_dir*\www\htdocs\C\nnm\launcher\browser.html

UNIX: $OV_WWW/htdocs/$LANG/nnm/launcher/browser.html

The Java parameters that you can modify are:

- background
- foreground
- activeTabColor
- inactiveTabColor
- treeBackground
- treeForeground
- treeConnectingLineColor
- displayActiveHelp
- activeHelpLines
- fontName
- fontStyle
- fontSize
- displayInFrame

HP OpenView Network Presenter

The HP OpenView Network Presenter is a Java-based applet that connects to NNM for the purpose of displaying maps. It provides multiple views of map data on a management station from any system with a web browser that supports Internet Explorer or Netscape Navigator.

NOTE Refer to the "Supported Configurations: Supported Web Browsers" section of the NNM Release Notes for specific information about supported web browsers.

The Network Presenter communicates with the management station to get registration information, map data, and map object data. It provides read-only access to the map data and has dynamic updates to reflect the changes that occur on the management station. You can navigate through the map views, select and obtain status on symbols, and launch other web applications on the selected objects via the Network Presenter.

Starting the Network Presenter

You must start an NNM session on the management station for each map that you want available through the web, as described on page 485.

You can invoke the Network Presenter through the Launcher using either of the following tabs:

`Objects` tab, then choose `Networks:IP Network`

`Tools` tab, then choose `NNM:Network Presenter`

Alternatively, you can enter the URL for the Network Presenter:

`http://`*`hostname`*`[:`*`port`*`]/OvCgi/jovw.exe?[MapName=`*`mapname`*`&ObjectName=`*`selectionname`*`]`

On UNIX operating systems, you must specify port number `3443`. Ona Windows operating system, no port number is required. The `MapName` and `ObjectName` fields are optional.

The `MapName` field specifies which map to open. The `ObjectName` field specifies what object to show initially. Refer to the *OvWebURLIntro* reference page in NNM's online help (or UNIX manpage) for more information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1114
3740

NOTE When starting the Network Presenter directly from the URL, you lose the session information that the Network Presenter would have if it were started from the Launcher, including language information.

If a *mapname* is not specified in the URL used to start the Launcher, Network Presenter attempts to connect to an NNM session running with the default map. If there is no NNM session running with the default map, the Network Presenter displays an error message that says the map was not found.

If a *mapname* is specified in the URL, the Network Presenter attempts to connect to an NNM session on the management station with an open map called *mapname*. If there is no NNM session running on the management station with this map open, the Network Presenter displays an error message that says the map was not found.

If you close the NNM session or open a new map, the Network Presenter session attached to that NNM session is ended. The Network Presenter displays a dialog box informing the users that NNM is closing its map.

By default, the Launcher will start the Network Presenter with the `default` map displayed. To make a map other than `default` available to the Network Presenter, modify the `jovw` Web Launcher Registration File (WLRF) that specifies in the URL portion which map to open. See "Listing Multiple Maps in the Launcher" on page 508 and "Launcher Registration File" on page 494 for information.

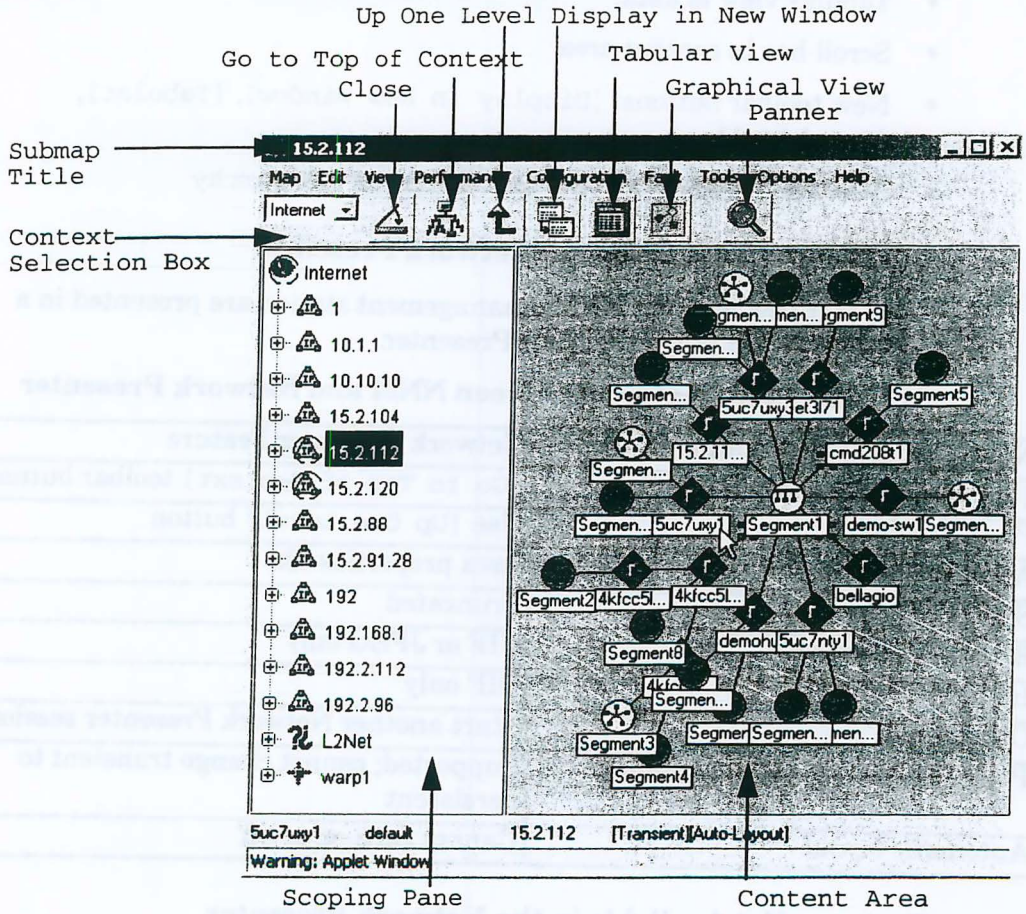
The Network Presenter Window

The Network Presenter window has the following components:

- Submap title
- Menu bar
- Context selection box
- Toolbar
- Content area
- Scoping pane

- Status bar

Figure 14-3 **Network Presenter Window**



Network Presenter versus NNM on a Management Station

There are some differences in the functionality and presentation of information between the Network Presenter and NNM on a management station.

Features in the Network Presenter

Following are features in the Network Presenter that are not available in NNM on a management station.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1115
3740
Doc:

- Context selection box to choose among the highest-level views.
- Scoping pane.
- Tabular view of data.
- Scroll bar in content area.
- New toolbar buttons: `[Display in New Window]`, `[Tabular]`, `[Graphical]`
- New menu items: `Up One Level`, `Top of Hierarchy`

Features That Differ in the Network Presenter

Some features from NNM on a management station are presented in a different format in the Network Presenter.

Table 14-1 Differences in Features Between NNM and Network Presenter

NNM Management Station Feature	Network Presenter Feature
`[Go to Root]` toolbar button	`[Go to Top of Context]` toolbar button
Parent toolbar	Use `[Up One Level]` button
App-defaults file	Java properties file
Symbol labels	Truncated
Background graphics	GIF or JPEG only
Inner shapes	GIF only
Open map	Start another Network Presenter session
Persistent and transient submaps	Supported; cannot change transient to persistent
Automatic layout	Cannot turn on or off

Features Not Available in the Network Presenter

The following features in NNM on a management station that are not available in the Network Presenter.

- `Map Description` dialog box.
- `Submap Properties` dialog box.
- `Locate Submap` dialog box.
- Home submap.
- `Symbol Properties` dialog box.
- Snapshots.

- Symbol enhancements (flashing, transparent, alerts, etc.).
- Menu collapsing.
- Symbol, submap editing.
- Invoking executable symbols.

Interaction Between NNM on the Management Station and the Network Presenter

Since the Network Presenter cannot do editing, the Network Presenter does not influence what happens to NNM on the management station; however, changes in the current session on the management station are dynamically reflected in the content area and scoping pane of the Network Presenter as appropriate. You will see changes in the content area if the submap that is displayed on the management station changes. You will see changes in the scoping pane if that level of hierarchy is displayed. Changes are not dynamically reflected in open dialog boxes.

Configuring the Network Presenter

You can modify the Network Presenter Registration Files (NPRF) to configure certain aspects of the Network Presenter.

The NPRFs are located on the management station at:

Windows: *install_dir*\www\registration\jovw\c*.*

UNIX: /etc/opt/OV/share/www/registration/jovw/$LANG

The format of the Network Presenter Registration Files (NPRF) closely follows the syntax and constructs of the HP OpenView Application Registration File (ARF). Refer to the online manual *Creating and Using Registration Files* for general information about Application Registration files. Refer to the *NetworkPresenterRegIntro* reference page in NNM's online help (or the UNIX manpage) for specific information about creating or editing the NPRF files.

You can add entries to the Action block to specify your own applications to be called when the Network Presenter is launched. You can also change the WebWindow properties in the Action block to control some aspects of the appearance of the Network Presenter (see "Components of the WLRF" on page 494 for sample contents of a registration file). You can add pull-down menus, toolbar buttons, and popup menus that operate on selected objects.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls! Nº 1116
3740
Doc:

Configuring Security for the Network Presenter

There are two levels of security for the Network Presenter.

- The `session.conf` file, described earlier in this chapter.
- The `ovw.auth` and `ovwdb.auth` files, described next.

The Network Presenter allows role-based, restricted access to menu items that have action blocks that contain access statements. See the *Action Block* description on page 496 for more information.

Authorization Files The `ovw.auth` and `ovwdb.auth` files specify which users are allowed access to which management stations. These files are located on the management station at:

Windows: *`install_dir`*`\conf\ovw.auth`

`install_dir``\conf\ovwdb.auth`

UNIX: `$OV_CONF/ovw.auth`

`$OV_CONF/ovwdb.auth`

Each of these files contain instructions for their use.

Using Symbol Registration Files and Bitmaps

Symbol registration files used by the Network Presenter are the same as those used by NNM on a management station. Therefore, if a symbol definition is added for NNM on a management station, it also appears in the Network Presenter. Symbol registration files are located in:

Windows: *`install_dir`*`\symbols\%LANG%`

UNIX: `$OV_SYMBOLS/$LANG`

See the *OVwRegIntro* reference page in NNM's online help (or the UNIX manpage) for more information about creating or editing symbol registration files.

The graphic files for the symbols, themselves, are stored in two places. One directory used by NNM on the management station (see page 664), and one directory used by NNM's web-based interface. The web-based interface requires GIF files. Other additional graphic file formats are supported on the management station. If you create your own GIF files, place a copy in each location.

The Network Presenter loads its bitmaps in GIF format from the directory:

Windows: *install_dir*\www\htdocs\bitmaps

UNIX: $OV_WWW/bitmaps

TIP

If you can see a symbol on the management station, but cannot see it over the web interface, check the `Contrib` directory (see page 74) for the `convertBitmaps.ovpl` script which walks through each graphic in the management station's symbol graphic directory and ensures that a corresponding GIF file exists or is created in the web interfaces's symbol directory.

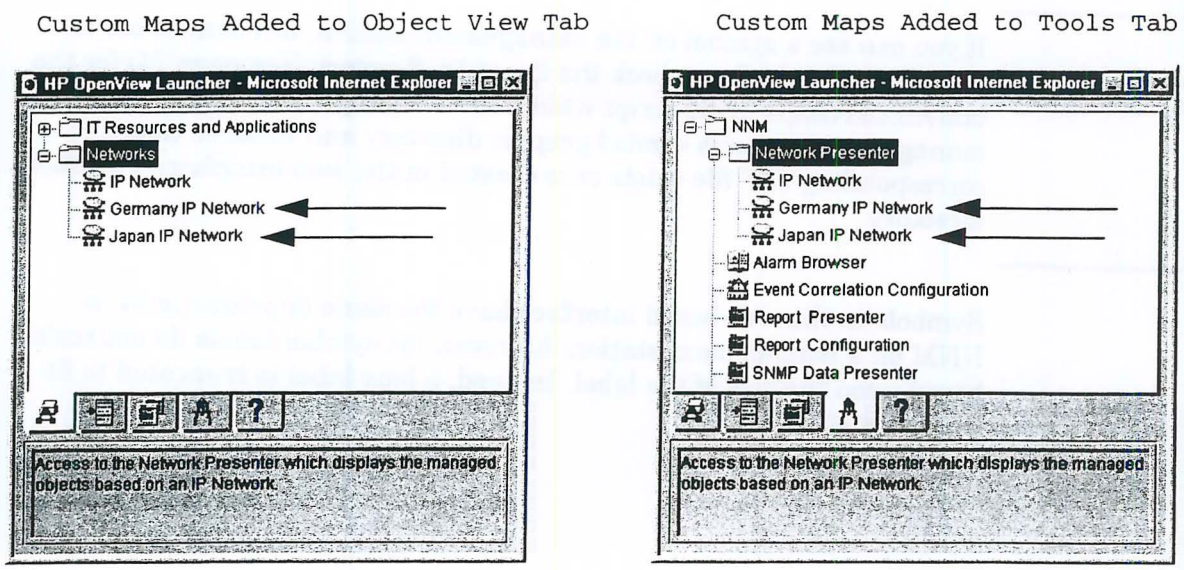
Symbols in the web-based interface have the same appearance as in NNM on a management station; however, the symbol labels do not scale based upon the size of the label. Instead, a long label is truncated to fit the space available.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 507
1117
3740

Listing Multiple Maps in the Launcher

You can modify the Launcher registration file for the Network Presenter so that each of your custom maps is listed.

Figure 14-4 Listing Multiple Maps in the Launcher Window



For each map, you must make additions to the `List` and `Action` blocks of the following file:

- Windows: *`install_dir`*`\www\registration\launcher\C\jovw`
- *UNIX:* `$OV_WWW_REG/launcher/$LANG/jovw`

Open this file and read the instructions provided for more information. See also the *LauncherRegIntro* reference page in NNM's online help (or the UNIX manpage) for specific information about creating or editing the WLRF files.

On the management station, there must be a non-web based version of NNM running for each map that will be accessible from the Network Presenter. For example, if you want your team to be able to access the Germany map and the map showing your operations in Japan, you must start NNM on the management station with your Germany map displayed and start another instance of NNM on the management station with the Japan map displayed.

SNMP Data Presenter

The SNMP Data Presenter displays results of operations that present tabular or textual data for managed SNMP nodes selected from the map.

You can use the SNMP Data Presenter even if there is no NNM session running on the management station. The SNMP Data Presenter accesses NNM's Application Registration Files (ARFs) to retrieve information about menu structure and actions, executes the command on the management station, and displays the results in the web browser.

The SNMP Data Presenter displays configuration, performance and fault information. Here are a few examples:

- Interface status.
- SNMP authentication failures.
- TCP connections.
- IP Network addresses.
- IP Routing tables.
- IP ARP cache table.
- System information.
- SNMP trap recipients.

To start the SNMP Data Presenter, select the target node in the content area of Network Presenter and then select one of the following:

- `Performance:SNMP Data Presenter`
- `Configuration:SNMP Data Presenter`
- `Fault:SNMP Data Presenter`

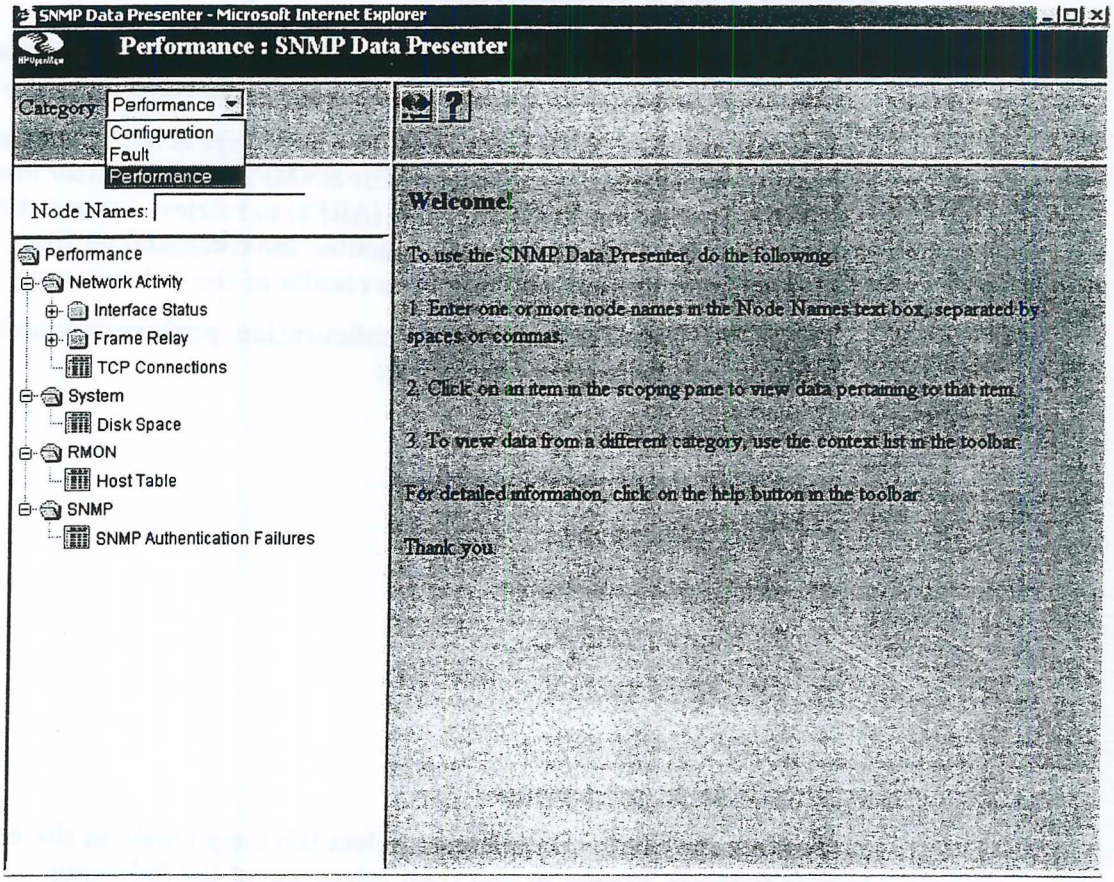
To start the SNMP Data Presenter from the Launcher, select:

- `Tools` tab, then `NNM:SNMP Data Presenter`

ROS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 1118
3740

The SNMP Data Presenter window is shown in Figure 14-5.

Figure 14-5 SNMP Data Presenter Window



Scoping Pane Content Pane

When accessed from the `Tools` tab, the scoping pane contains categories and actions in a tree format. You can click on the category items to expand them and then click on an action to execute that action. You can also use the Category pull-down.

The results of an action are shown in the content area. A link at the bottom of this area allows you to display a new web browser window with the currently displayed information. This allows for easy comparing of data.

Configuring the SNMP Data Presenter

The SNMP Data Presenter uses NNM's Application Registration Files (ARFs) and the Application Builder. Because of this, you can execute the same SNMP monitoring operations as you do in NNM, and add new operation commands to the menu structure with Application Builder.

See NNM's online manual, *Creating and Using Registration Files,* for details about editing application registration files (ARFs). See "Using the MIB Application Builder" on page 443 for more information about the Application Builder feature.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1119
3740
Doc:

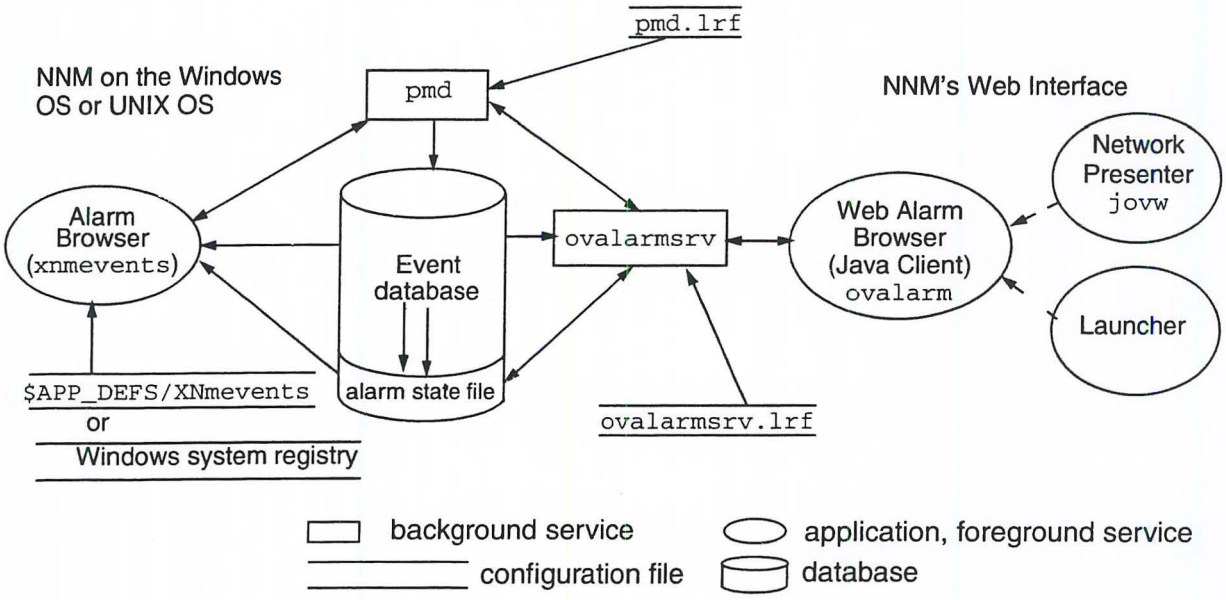
Alarm Browser

The Alarm Browser presents alarm data via the web interface. Through the Alarm Browser, you can filter alarms and take actions on specific alarms. All alarms are global to all web users, as are the acknowledge, delete, change category, and change severity functions.

The web-based Alarm Browser service, `ovalarmsrv`, is started by `ovstart` when you start an NNM session on the management station.

Figure 14-6 illustrates the relationship and data flow between the Alarm Browser application on a management station and the web-based Alarm Browser.

Figure 14-6 Relationship Between the Two Alarm Browsers

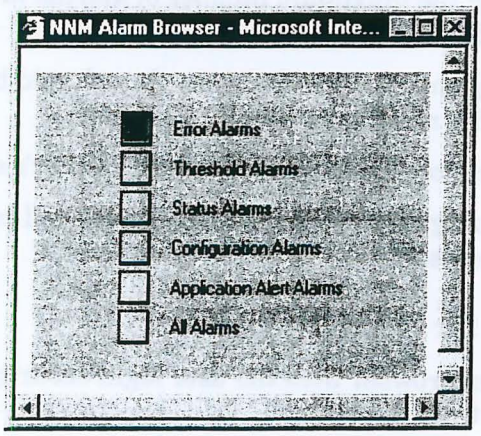


You access the Alarm Browser using one of the following methods:

- In the Launcher, select the `Tools` tab, then select `NNM:Alarm Browser`

- In Network Presenter, select the `Fault` menu, then select `Alarm Browser`.

Figure 14-7 Web-Based Alarm Browser's Category Window



Using and Configuring the Alarm Browser

You can use the Alarm Browser to perform the following:

- Acknowledge/Unacknowledge alarms.
- Move alarms to a different category.
- Assign alarm severities.
- Filter alarms.
- Delete alarms.
- Examine alarm details to find correlated events.

To move an existing alarm message to a different category. Select the alarm that you want to recategorize. Then select `Actions:Change Category` from the menu bar. Refer to the online help if you need more information.

This change affects only the selected alarms. Future alarms of the same type will continue to be posted in the old category's list.

You can configure an alarm to activate your web browser to a specific URL. See "Launching Specific Views or URLs from Alarms" on page 340 for more information.

RQS nº 03/2005 - CN
CPMI CORREIOS
Fls. Nº 1120
3740
Doc:

See Chapter 12, Customizing Events: Doing It Your Way, for configuration options:

- Setting the maximum size of the event database (default 16 MB).
- Setting the maximum number of alarms in the Alarm Browser's state file (default 3500).
- Setting the number of alarms that should be deleted each time the state file reaches maximum capacity.
- Copying or restoring the Alarm Browser's state file.
- Assigning alarms to other categories and creating new alarm categories.

Security for the Alarm Browser

The Alarm Browser uses the user login security mechanisms, described earlier in this chapter.

Event Reduction

Event reduction is the process by which the relationship between events is identified. Once identified, a smaller number of new events providing higher information content can be generated. This simplifies the task of diagnosing network faults. There are three event reduction strategies that are configured and working within NNM. You can access the configuration windows for two of them over the web:

- "ECS Correlations" on page 360
- "Correlation Composer Correlators" on page 386

There are several ways to access these event correlation features. For more information, from any submap:

- Select `Toos:HP OpenView Launcher`.
- Select the `[?]` tab.
- Click `Tasks`, `Event Correlation Management`.

  Read the information under *Accessing the Event Correlation Configuration Windows*

For information about the NNM event reduction strategies, see Chapter 11, "Event Reduction Capabilities: Getting to the Root Cause," on page 351.

ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls: Nº 1121
3740

Reporting Interface

The web Reporting interface is a graphical user interface that is available through a web browser. The Reporting interface consists of:

- Report Configuration-- create, modify, and view report schedules.
- Report Presenter-- view reports.

You can access the Report Configuration in one of the following ways:

- From NNM on a management station, select the `Options:Report Configuration` menu item.
- From Network Presenter, select the `Options:Report Configuration` menu item.
- From the Launcher, select the `Tools` tab, and expand the NNM category. Double-click on `Report Configuration`.
- From your browser, specify the following URL:

  `http://`*`hostname`* `[:`*`port`*`]/OvCgi/RptConfig.exe`

  You need to specify a port if you are running NNM on a UNIX machine.

You can access the Report Presenter in one of the following ways:

- From NNM on a management station, select the `Tools:Report Presenter` menu item.
- From Network Presenter, select the `Tools:Report Presenter` menu item.
- From the Launcher, select the `Tools` tab, and expand the NNM category. Double-click on `Report Presenter`.
- From your browser, specify the following URL:

  `http://`*`hostname`* `[:`*`port`*`]/OvCgi/RptPresenter.exe`

  You need to specify a port if you are running NNM on a UNIX machine.

The NNM Analysis and Reporting interface will be displayed in your browser window.

Refer to the online manual *Reporting and Data Analysis with HP OpenView NNM* and the web online help for more information.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1122
3740
Doc:

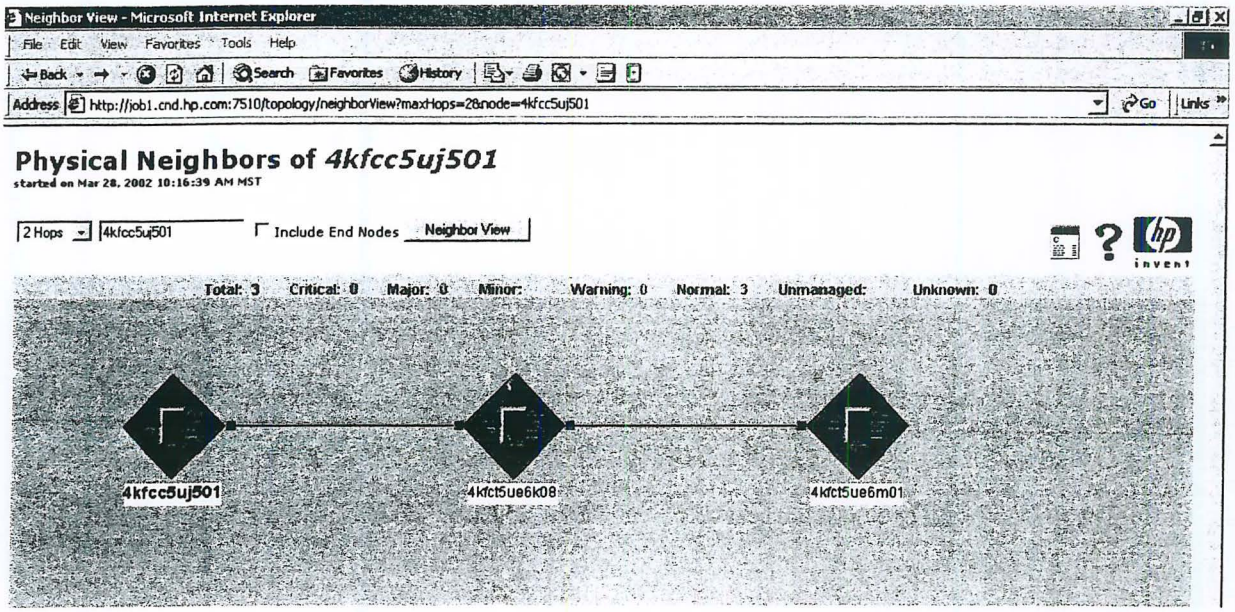
Additional Views

NNM presents several different views of discovered nodes. NNM's Neighbor view, Path view, Node view, Cisco Discovery Protocol view (CDP view), Station view, Internet view, and Port-Address Mapping capabilities show topology views that supplement NNM's map views.

Neighbor View

The Neighbor view shows you a graphical representation of the selected device and the connector devices related to it, within a specified number of hops of the selected device.

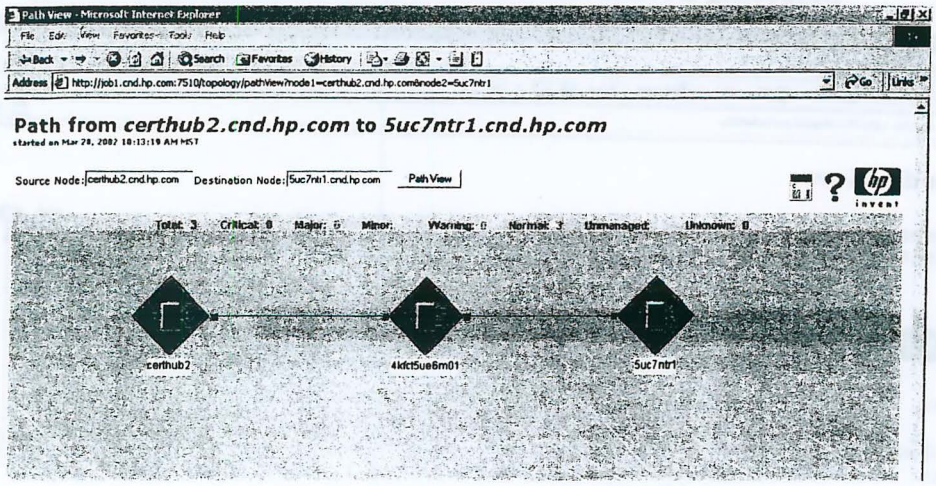
Figure 14-8 Neighbor View Example



Path View

The Path view shows you a graphical representation of the path between two nodes. NNM calculates the shortest path between the source and destination nodes from information contained in the topology database.

Figure 14-9 Path View Example

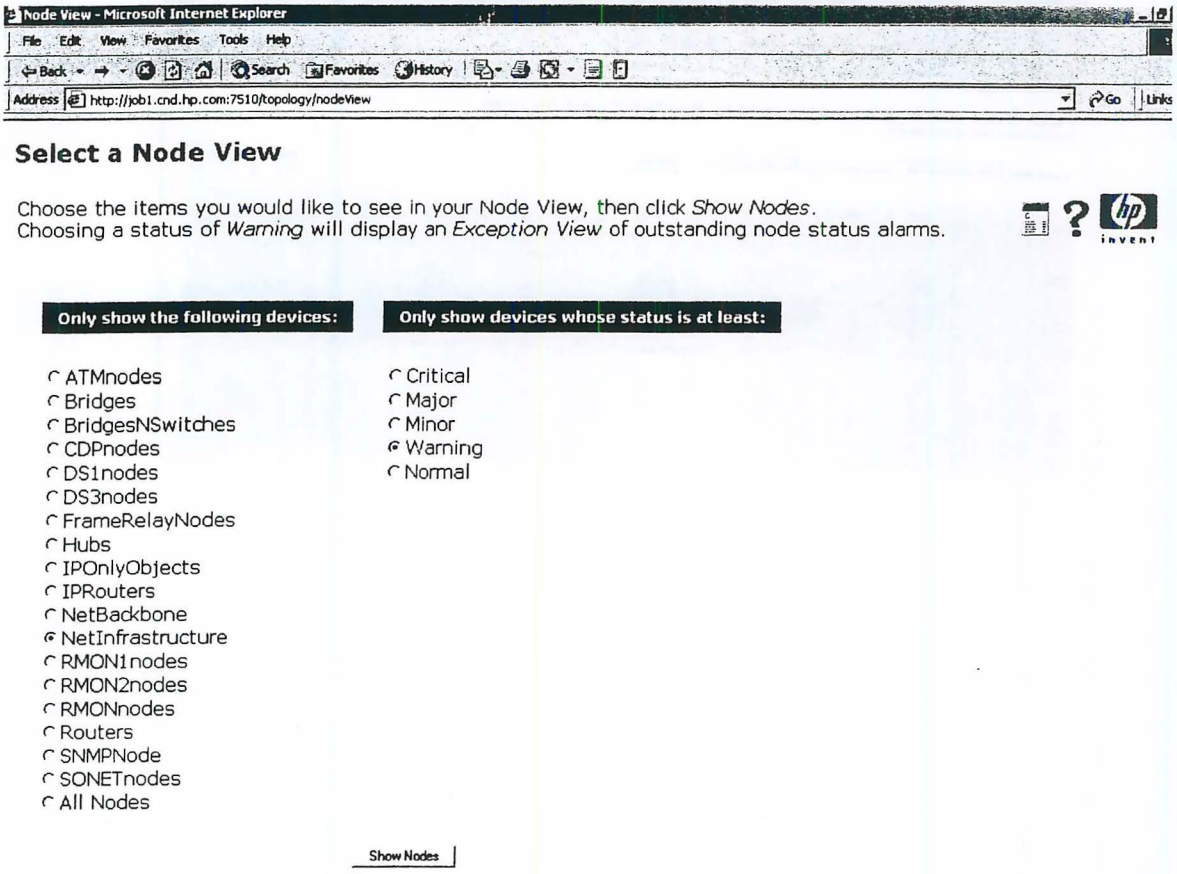


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls.: Nº 1123
Doc: 3740

Node View

The Node view creates a visualization of a set of nodes and shows how they are connected. To create a visualization, use the NNM `Tools:Views->Node` menu item. The `Node View` interface contains device types and device status selections as shown in Figure 14-10.

Figure 14-10 Selecting a Node View

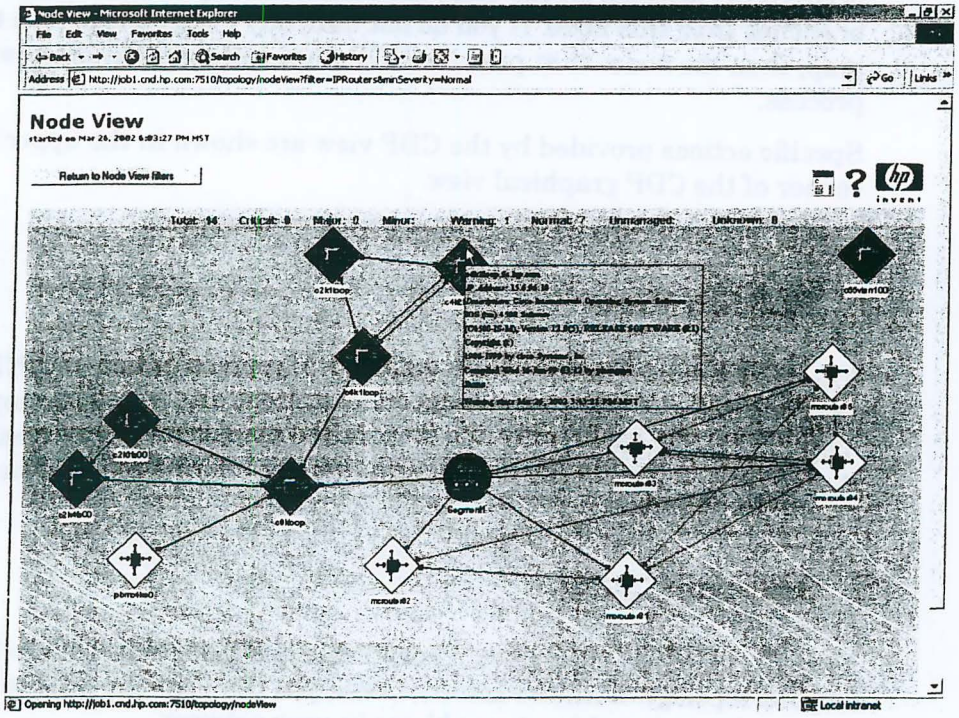


Device selection relies on filters contained within the `filters` file. This is the same file that contains filters such as discovery filters and DHCP filters. The filters file is found in the following locations:

- Windows: *`install_dir`*`\conf\C\filters`
- *UNIX:* `$OV_CONF/C/filters`

For detailed information about how to develop a filter, refer to *A Guide to Scalability and Distribution*.

Figure 14-11 Node View Example



When working with Node view, placing your mouse over a node displays additional information about the node, such as the hostname, IP address, model number and version, system location, and system contact, subject to availability. Single-clicking allows you to zoom in and zoom out on the display. Double-clicking a node shows the node's attributes from the `ovtopodump` command.

CDP View

Cisco Discovery Protocol (CDP) is a Cisco-proprietary protocol that enables the gathering of information about the types of devices in the network, the links between those devices, and the number of interfaces within each device. It runs on Cisco-manufactured devices, including routers, bridges, access servers, and switches.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1124
3740

You can view the CDP connectivity of your network by selecting `Tools:Views->CDP` from NNM, the HP OpenView Launcher, or from the Network Presenter. The `Tools:Views->CDP` menu item presents a graphical view of all the CDP nodes in the NNM topology. If a CDP node is currently selected on the map, then the discovery of CDP nodes branches from this node. If you do not have any nodes selected on the map, then the nodes that pass the CDP filter will start the discovery process.

Specific actions provided by the CDP view are shown in the upper left corner of the CDP graphical view.

See *CDP View* in NNM's online help for information.

Station View

The Station view shows you a graphical representation of the NNM collection stations and management stations discovered in your topology. This view is useful only in a distributed management environment. See *A Guide to Scalability and Distribution* for information about distributed environments.

Internet View

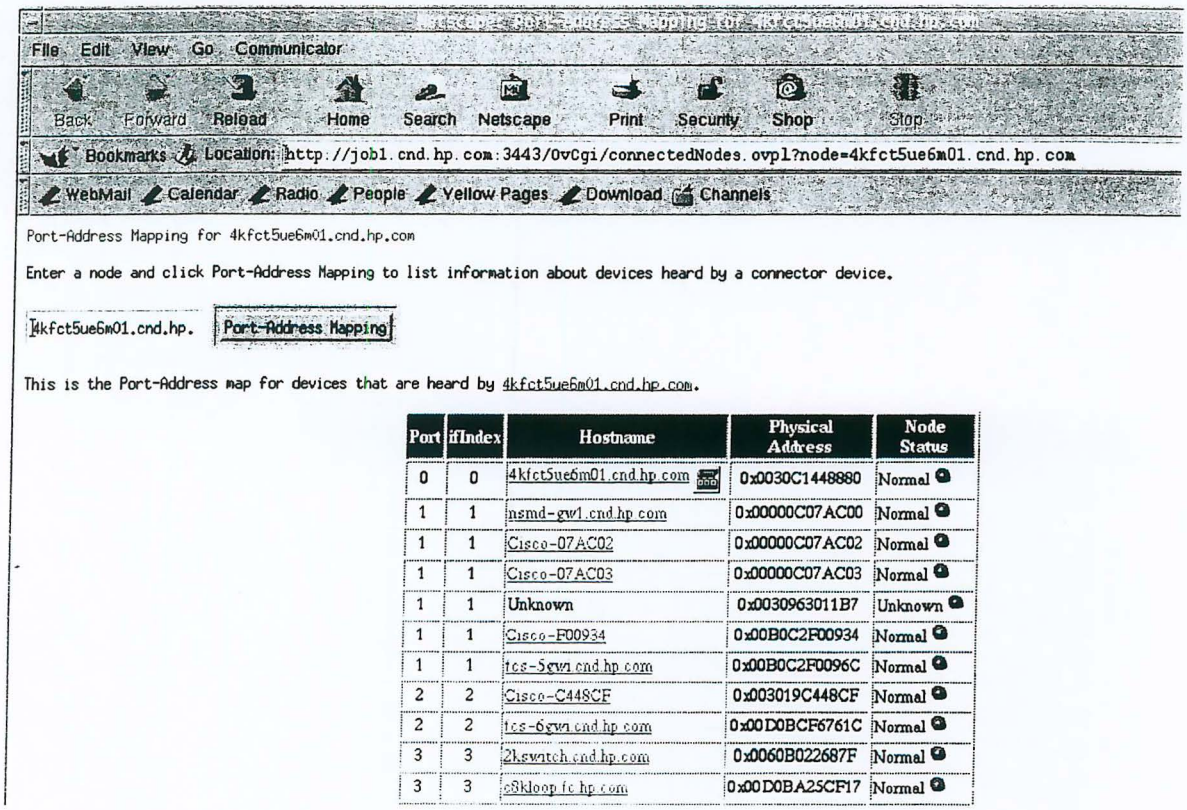
The Internet view shows you a graphical representation of the networks in your topology. With the Internet view, you can view the general status of your network and locate problems in your network.

Port-Address Mapping

By selecting a node and using the `Tools:Port-Address Mapping` menu item you'll see a table of all devices connected to the selected node. The menu item works for most devices that support the *Transparent Forwarding Database MIB* or the *Bridge MIB*.

In Figure 14-12 the user selected device `4kfct5ue6m01` from the NNM map, then used the `Tools:Port-Address Mapping` command to display a table of all of the devices connected to the selected node along with information associated with these connected devices.

Figure 14-12 Example of Port-Address Mapping Table



Port	ifIndex	Hostname	Physical Address	Node Status
0	0	4kfct5ue6m01.cnd.hp.com	0x0030C1448880	Normal
1	1	nsmd-gw1.cnd.hp.com	0x00000C07AC00	Normal
1	1	Cisco-07AC02	0x00000C07AC02	Normal
1	1	Cisco-07AC03	0x00000C07AC03	Normal
1	1	Unknown	0x0030963011B7	Unknown
1	1	Cisco-F00934	0x00B0C2F00934	Normal
1	1	tcs-5gw1.cnd.hp.com	0x00B0C2F0096C	Normal
2	2	Cisco-C448CF	0x003019C448CF	Normal
2	2	tcs-6gw1.cnd.hp.com	0x00D0BCF6761C	Normal
3	3	2kswitch.cnd.hp.com	0x0060B022687F	Normal
3	3	c8kloop1c.hp.com	0x00D0BA25CF17	Normal

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1125
3740
Doc:

2365
09

15 Maintaining NNM

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1126
3740
Doc:

This chapter gives you ideas and suggestions for maintenance tasks that, when performed on a regular basis, can help keep Network Node Manager running more smoothly and without errors.

Included are tasks for:

- Daily maintenance, including checking running services, checking disk space, and trimming files (page 527).
- Weekly tasks, including backing up NNM, cleaning up databases, and monitoring polling performance (page 531).
- Monthly tasks, including obtaining the latest patch releases and updating licensing requirements (page 533).
- Yearly tasks, including evaluating the latest product release (page 534).
- Other maintenance tasks that will help your NNM installation run smoothly (page 535).

For information about maintaining NNM's data warehouse, see the online manual *Reporting and Data Analysis with HP OpenView Network Node Manager*.

2363

Daily Tasks

You may wish to perform the following tasks on a daily basis.

Check Running Services

Each day you should check to see that all the required services (processes) are running. It is possible that a service has gotten "hung" or did not restart after a backup.

To check on the status of services use the `ovstatus` command. See the *ovstatus* reference page in NNM's online help (or the UNIX manpage) for command options.

If you encounter a service that fails on a regular basis and you cannot find a cause, refer to the service's reference page in NNM's online help (or the UNIX manpage) for more information. You can also use the Event Configuration feature to automatically restart the service whenever it fails. In the `Event Configuration` dialog box, open the `OpenView: OV_DaemonTerminated(.1.3.6.1.4.1.11.2.17.1.59180100)` event configuration and make the following entry in the `Command for Automatic Actions` field: `ovstart $4`.

Check Disk Space

You should check the available disk space on a daily basis. This will ensure that you have enough space to store collected data and to perform a backup.

To check available disk space:

- Use the `Performance:System->Disk Space` menu item.

  Since this information is generated by an HP enterprise-specific MIB, it is available only from an HP 9000 or Sun SPARCstation running the HP OpenView SNMP Agent software.

  If this menu item is not available, you can use the following:

  Windows: Use Windows Disk Administrator

  UNIX: Use the `df` or `bdf` command. See the appropriate manpage for more information.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1127
3740
Doc:

To regain disk space, you can trim certain files, described next.

Trim Files

Some files can grow large very quickly. This slows the discovery and map generation processes and affects overall system performance.

The NNM Data Warehouse and snmpCollect

NNM pre-configures several data collections for you. NNM exports data from pre-configured data collections as well as collections you have manually configured, to the data warehouse. NNM uses data from the data warehouse to generate pre-configured `General Availability`, `Threshold Violations`, `General Inventory`, and `Ping Response Time/Ping Retries` reports. NNM automatically trims data from the following directories as well as from the data warehouse on a regular basis.

- *Windows:* `install_dir\databases\snmpCollect\`
- *UNIX:* `$OV_DB/snmpCollect/`

NOTE

Select `Options: Data Collection and Thresholds` to see the list of current data collections. Event information is also exported to the data warehouse and trimmed from the Binary Event Store regularly. NNM automatically trims both collected data and event information to reduce disk usage.

TIP

HP uses trimming options that will satisfy a majority of your requirements. If you need to keep collected data and/or Data Warehouse data for longer time periods, you may need to manually complete the export and trimming functions using the `ovdwtrend` command. See the bulleted items on page 526.

To reduce the rate at which the `snmpCollect` directory fills up all available disk space, do the following:

- Reduce the polling intervals by using the `Options:Data Collection & Thresholds` operation. This slows the rate at which `snmpCollect` fills up available disk space. In addition, if you want to check fixed thresholds only, do not store the data.
- You can use the `ovdwtrend` command to reduce the size of files residing in the `snmpCollect` directory. For example, you can use the `ovdwtrend -export -delpriorto "2001-12-31 00:00:00"` command to export all new data collected since the last export while trimming snmpCollect data file information dated prior to December 31, 2001. Review the *ovdwtrend* reference page in NNM's online help (or the UNIX manpage) to plan your strategy for trimming files in the `snmpCollect` directory.
- You can use the `ovdwtrend -trim` command to delete SNMP trend data from the NNM data warehouse. For example, you can use the `ovdwtrend -trimpriorto [240]` command to trim data older than 240 hours from the *snmp_reduced_trend* table of NNM's data warehouse. Review the *ovdwtrend* reference page in NNM's online help (or the UNIX manpage) and the online manual *Reporting and Data Analysis with HP OpenView Network Node Manager* to plan your strategy for managing data in NNM's data warehouse.

Removing Reports

NNM automatically generates `General Availability`, `Threshold Violations`, `General Inventory`, and `Ping Response Time/Ping Retries` reports. You should review these reports and remove those reports that are no longer of use. See the online manual *Reporting and Data Analysis with HP OpenView Network Node Manager* for instructions on how to delete reports.

Trace and Log Files

Trace and log files can grow quite large, and should be periodically checked for size.

Tracing, especially in the case of `netmon`, can cause the trace file to grow extremely large (multiple megabytes in size) fairly quickly. If you use tracing, remember to monitor the size of the trace file frequently, and turn tracing off as soon as you are finished. The `netmon` trace file is *install_dir*`\log\netmon.trace` (`$OV_LOG/netmon.trace`).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1128
3740
Doc:

Windows: Run **netmon -MO** to disable polling. Use Notepad to edit the *netmon.trace* file, deleting all lines. Save the file. Then run **netmon -M** to enable polling.

UNIX: **cat /dev/null > $OV_LOG/netmon.trace**

Default Log Files

The log files in *install_dir*\analysis\default\log ($OV_DATABASE/analysis/default/log) are an audit trail of successful transactions since your last backup. These files are required for recovering the database at a point *other than* when the last backup was performed. These default log files are normally present with all relational databases.

If you are not performing backups on a regular basis, these log files could grow without bounds. If you are not concerned about recovering your database, you can remove these files at any time. New log files are constantly generated by your relational database software.

2359
Q

Weekly Tasks

You may wish to perform the following tasks on a weekly basis.

Back Up NNM

It is a good idea to do a full backup weekly (or as often as required at your site), so that you can restore to a relatively current state in the event of a system failure or a corrupted database. This will also ensure that you have all of the databases and configuration files together.

If you perform backups on a regular basis, you can restore to a relatively current state in the event of a system failure or a corrupted database.

There are a number of other situations when you should back up your NNM files. At a minimum, always do a full backup before starting any of the following tasks:

- Upgrading to a new version of NNM.
- Extensively editing or customizing your map.
- After performing initial or expanded discovery, once you think your map accurately reflects your network.

Refer to Chapter 6, "Preserve Your Sanity: Backup and Polling Configuration."

Check Polling Performance

You should periodically check to see how well `netmon` is keeping up with the changes in your network. Use `Performance:Network Polling Performance` to gauge how effectively netmon is collecting network data. If `netmon` is not keeping up with the network changes, you can adjust polling intervals and/or queue sizes (see "Fine-Tuning the Polling Services" on page 193 for more information). You can also consider reducing the size of the managed environment (see "Automatically Limit Your Management Domain" on page 124 for more information).

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1129
3740
Doc:

Check Web Launcher Log Files

The Web Launcher log files record errors and messages from the Launcher. These files will grow without bounds, and should be truncated as needed. The Launcher log files are:

Windows:

```
install_dir\www\logs\launcher\error_log
install_dir\www\logs\login_log
install_dir\www\logs\access_log
```

UNIX:

```
/var/opt/OV/www/logs/launcher/error_log
/var/opt/OV/www/logs/launcher/login_log
/var/opt/OV/www/logs/launcher/access_log
```

Monthly Maintenance Tasks

You should perform the following tasks on a monthly basis.

Check Patch Releases

Check the HP OpenView Web site for the latest patch releases or support updates. These can usually be downloaded at no charge. The HP OpenView Web site is:

`http://openview.hp.com`

Check License Requirements

When running NNM 250, it is a good idea to check to see if you are going to need more licenses. If your network is growing quickly and you have added many nodes, you could run out of available licenses. When the system gets within 25 nodes of the licensed nodes limit, an application alert will be generated. However, you can also check the number of nodes being managed and the number of nodes licensed before this alert is generated. To check the status of licenses:

1. In the NNM main window, right-click on the `Internet` object.
2. Select `Object Properties` from the pop-up menu.
3. Select `IP Map` and click `Edit:Attributes`. This will display the number of nodes that you are licensed for and the number of nodes that are currently being managed.

RQS nº 03/2005 - CN
CPMI CORREIOS
FLS. Nº 1130
3740
Doc:

Yearly Maintenance Tasks

You should perform the following tasks on a yearly basis.

Evaluate Latest Release

When new releases of Network Node Manager are announced, you should evaluate the new features that are included. If your network management needs have changed, the newest release may have new tools and features that will help you manage your network more effectively.

2355

Other Maintenance Tasks

There are other maintenance tasks that you may want to perform occasionally to improve the performance of the system, or just to make routine tasks easier.

Enabling/Disabling Automatic Startup

The NNM installation service creates the appropriate files such that the host operating system automatically starts NNM when the management station boots. Occasionally you may want to disable automatic NNM startup, such as during system maintenance when the system is going to be rebooted several times.

On a Windows Operating System:

1. From the Windows `Start` menu, select `Settings:Control Panel`.
2. In the `Control Panel`, click on `Services`.
3. Select `HP OpenView Process Monitor` and choose `Manual Startup`.

On a HP-UX Operating System:

Edit the startup file `/etc/rc.config.d/ov500` and set the variable `START_OV500` to either 1, to start NNM at boot up or to 0, to disable NNM boot at startup. You do not need to reboot the system after making this change.

On a Solaris Operating System:

To disable NNM from starting at boot time, rename the filename `S98netmgt` within the sequencing link `/etc/r3.d/S98netmgt` to a name that begins with a letter other than "S" or "K". To re-enable NNM starting at boot time, change the filename back to `S98netmgt` and reboot.

Customizing the Startup Configuration

The service `ovspmd` starts each service according to instructions it finds in the startup file *`install_dir`*`\conf\ovsuf ($OV_CONF/ovsuf)`. Depending on which services are configured to start, system response

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1131
3740
Doc:

time can be impaired, performance may be slower, and disk space can be rapidly consumed. If you encounter these problems, consider modifying the startup configuration.

Do not edit the `ovsuf` file directly. Instead, configure startup options in the local registration file (LRF) for the individual services. LRF files are then submitted to `ovsuf` through the `ovaddobj` command. Conversely, service startup instructions are disabled from `ovsuf` using the `ovdelobj` command.

Table 15-1 describes each LRF and any options applied as defaults in the LRF. The table does not contain a complete list of options. To learn about all the available options, see the reference page in NNM's online help (or the UNIX manpage) with the particular service's name.

The steps for customizing the startup configuration follow Table 15-1.

Table 15-1 Local Registration Files (LRFs)

LRF	Description
`netmon.lrf`	The LRF for `netmon`, the background service that polls agents to initially discover your network. Default option: `-P` which means that it is started through `ovstart`. You may want to use the following options. Be aware, however, that using these options can affect performance. `-b` *`burstcount`* — Add if you have an unreliable network. This allows you to do multiple pings on a node. `-s` *`seedfile`* — Add when you want the initial map to include specific networks in your administrative domain. `-J` — Add if you have few SNMP agents on your network to accelerate initial discovery.
`ovactiond.lrf`	The LRF for `ovactiond`, the background service that executes configured commands when an event is received. Default option: none.

2357

Table 15-1 Local Registration Files (LRFs) (Continued)

LRF	Description
ovcapsd.lrf	The LRF for ovcapsd, the background service that discovers Remote DMI nodes, Web-manageable nodes, and Web servers. Default option: none.
ovrepld.lrf	The LRF for ovrepld, the background service that replicates objects.
ovtopmd.lrf	The LRF for ovtopmd, the background service that controls the topology database. Default option: -O which means that it is started through ovstart. Use the -f *filter* option to specify a topology filter and make use of NNM's scalability and distribution feature.
ovtrapd.lrf	The LRF for ovtrapd, the background service that executes configured commands when an event is received. Default option: none.
ovuispmd.lrf	The LRF for ovuispmd, the background service that manages user interface services and distributes relevant ovspmd requests to OVW. Default option: none Use the -t option to change the time period that ovuispmd will wait for commands to complete.
ovwdb.lrf	The LRF for ovwdb, the background service that controls the object database. Default option: -O which means that is started by ovstart. You may want to use the *-n number of objects* option to reduce the amount of memory used by ovwdb when managing large numbers of nodes.
pmd.lrf	The LRF for pmd, the background service that multiplexes and logs events. Default option: none.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1132
3740
Doc:

Table 15-1 Local Registration Files (LRFs) (Continued)

LRF	Description
`snmpCollect.lrf`	The LRF for `snmpCollect`, the background service that collects MIB data. Default option: none.

Steps for Customizing the Startup Configuration

1. Stop NNM.
   a. Exit any currently-running ovw sessions.
   b. Run **`ovstop -c`**
2. Create a back-up copy of the service's LRF file.
3. Open the selected service's LRF file in a text editor:
4. Edit the lines that control the behavior you want to change. Save and close the file.
5. Submit the new LRF file with the ovaddobj command:

   `ovaddobj $OV_LRF/netmon.lrf`
6. Restart NNM. Run **`ovstart -c`**

2351
C

A NNM Services and Files

RQS nº 03/2005 - CN -
CPMI CORREIOS
Fls: Nº 1133
3740
Doc:

NNM Services and Files

This appendix describes key services (processes) and files in the operation of Network Node Manager.

Topics covered include:

- Differences between background services and foreground services (page 541).
- How the services interact at NNM startup and during operation (page 547).
- The web application services and how they interact (page 545).

2359
C

Services and Files

There are two types of services:

- Background services that run continuously independent of whether ovw is running.
- Foreground services that run while ovw is running.

The interaction among these services are shown in the figures in this appendix. A brief description of each service and file follows. For more information on these services and files, see the reference page in NNM's online help (or UNIX manpage) having the same name as the service you wish to learn about.

Background Services

The following services and files are involved with the startup of NNM.

ovstart	Starts the various services that make up the HP OpenView Network Node Manager product.
ovspmd	Launches and manages all background services. ovspmd interacts with the user commands ovstart, ovstop, ovstatus, ovpause, and ovresume, and performs the appropriate actions on the background services.
ovsuf	Contains the configuration information for ovspmd. Each entry in ovsuf is created by ovaddobj from information in the LRF (Local Registration File).

The following services run in the background during regular operation. All of the following files reside in *install_dir*\bin\ ($OV_BIN).

httpd	Handles http requests. This is a web server that is provided on the UNIX operating system only.
netmon	Polls SNMP agents to discover your network, and then detects topology, configuration, and status changes in the network.
ovactiond	Receives events from pmd and executes commands.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1134
3740
Doc:

ovalarmsrv	Provides event information to Java-based Alarm Browsers.
ovcapsd	Listens for new nodes and checks them for remote DMI capabilities, web-manageability, and web server capabilities.
ovas	Maintains topology and node status information for NNM Dynamic views.
ovrepld	Responsible for object replication. ovrepld is started only when monitoring remote collection stations in a DIDM environment.
ovrequestd	Executes the reports and data warehouse exports according to a predefined schedule. Once a report is configured, ovrequestd starts executing the exports and the reports.
ovsessionmgr.exe	Manages users' web sessions. ovsessionmgr.exe is started by ovstart.
ovtopmd	Maintains the network topology database. The topology database is a set of files that stores netmon polling status and information about network objects, including their relationships and status. ovtopmd reads the topology database at start-up.
ovtrapd	Receives SNMP traps and forwards them to pmd. ovtrapd also responds to SNMPv2 requests.
ovuispmd	Manages the NNM user interface services and distributes relevant ovspmd requests to each instance of ovw that is running. ovuispmd must be running for ovw to be started, and should be running whenever ovspmd is running.
ovwdb	Controls the object database. The object database stores semantic information about objects.
pmd	Receives and forwards events, and logs events to the event database. pmd also forwards events from the network to other applications that have connected to pmd using the SNMP API.

snmpCollect	Collects MIB data and performs threshold monitoring. snmpCollect stores the data it collects in the *install_dir*\databases\snmpcollect ($OV_DB/snmpcollect) directory and sends threshold events to pmd.

Foreground Services

This section describes the NNM foreground services that may be running after you execute ovw. All of these files reside in *install_dir*\bin\ ($OV_BIN):

ipmap	Runs under ovw to automatically draw IPX and IP topology maps representing your network.
mibform, mibtable, rnetstat, findroute, rbdf, rnetstat, rping	Commands executed by xnmappmon that enable you to monitor and diagnose problems in your TCP/IP network.
ovw	The service that provides map drawing, map editing, and menu management. When you start the OVW services by executing the ovw command, ovw automatically invokes ipmap, xnmevents, and the other applications, which register to be started by ovw.
xnmappmon	The Application Encapsulator that displays textual results of monitoring operations for managed SNMP objects selected from the map.
xnmbrowser	The Tools:SNMP MIB Browser menu item that enables you to get and set MIB values for Internet-standard and enterprise-specific MIB objects.
xnmbuilder	The Options:MIB Application Builder:SNMP menu item that enables you to build custom screens to manage multivendor MIB objects. The information you define using the MIB Application Builder is stored in registration files and help files using mibform, mibtable, and xnmgraph.
xnmcollect	The Options:Data Collection & Thresholds:SNMP menu item that enables you to configure snmpCollect to collect MIB data from network objects at regular, configurable intervals. The configuration information

2347
CPMI - CORREIOS
Fls.: Nº 1135
Doc: 3740

is stored in the *install_dir*\conf\snmpCol.conf ($OV_CONF/snmpCol.conf) and snmpRep.conf configuration files. The collected data are stored in files in the *install_dir*\databases\snmpCollect ($OV_DB/ snmpCollect) directory.

xnmevents	The alarm browser that is automatically invoked by ovw to display events that are being received by pmd. xnmevents reads the *install_dir*\log\xnmevents ($OV_LOG/xnmevents).*username.map* file only at start-up for events that occurred since the last time xnmevents was run. xnmevents reads the event database only at start-up to obtain those pending events. xnmevents also reads trapd.conf to obtain information about how to customize event messages.
xnmgraph	The tool that enables you to graph the results of monitoring operations for managed SNMP objects selected from the map. The results may be real-time or collected historical data.
xnmloadmib	The Options:Load/Unload MIBs:SNMP menu item used to load new Internet-standard or enterprise-specific MIBs into the loaded MIB database.
xnmpolling	The Options:Network Polling Configuration->IP/IPX menu item that updates the polling configuration.
xnmsnmpconf	The Options:SNMP Configuration menu item that enables you to add, delete, and modify SNMP configuration parameters and the netmon status polling interval. The SNMP configuration parameters include community name, set community name, timeout interval, number of retries, and proxy information.
xnmtrap	The event configurator invoked by the Options:Event Configuration menu item that enables you to define enterprise-specific events (traps). You can customize the alarm message displayed through xnmevents when a particular event arrives. You can also specify a command or a batch file that should be executed when

2345

a particular event arrives. Event configuration changes are stored in the *install_dir*\conf\C\trapd.conf ($OV_CONF/$LANG/trapd.conf) configuration file.

Web CGI Programs

The following programs are CGIs, which access HP OpenView's web applications. See the *OVWebURLIntro* reference page in NNM's online help (or the UNIX manpage) for more information about (*) only. The others are used internally by NNM and listed only for your information.

jovw.exe *	Starts the Network Presenter.
jovwreg.exe	Called by the Network Presenter to parse menu information from application registration files registered with the Network Presenter. Also parses symbol and enroll information from registration files registered with ovw.
nnmRptConfig.exe*	Launches the Report Configuration interface.
nnmRptPresenter.exe*	Launches the Report Presenter.
ovalarm.exe*	Launches the Alarm Browser user interface.
ovlaunchreg.exe	Reads the Launcher registration files (WLRFs), passing input to the Launcher window for display.
ovlaunch.exe*	Launches the HP OpenView Launcher and opens the user login screen, when UserLogin is set.
ovlogin.exe	Processes the user login screen. Should not be called as a standalone URL.
ovsessioninfo.exe	Collects session information from the ongoing session.
ovwebdata.exe	Tool for accessing NNM data stores via read-only http queries.
OvHelp	The NNM 5.0 help CGIs.
OvWebHelp.exe	The NNM 6.0 help CGIs.
printsession.exe	Browser-callable URL to present user session information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1136
3740
Doc:

`snmpviewer.exe` * Launches the SNMP Data Presenter, or displays textual or graphical results of SNMP monitoring operations on your browser.

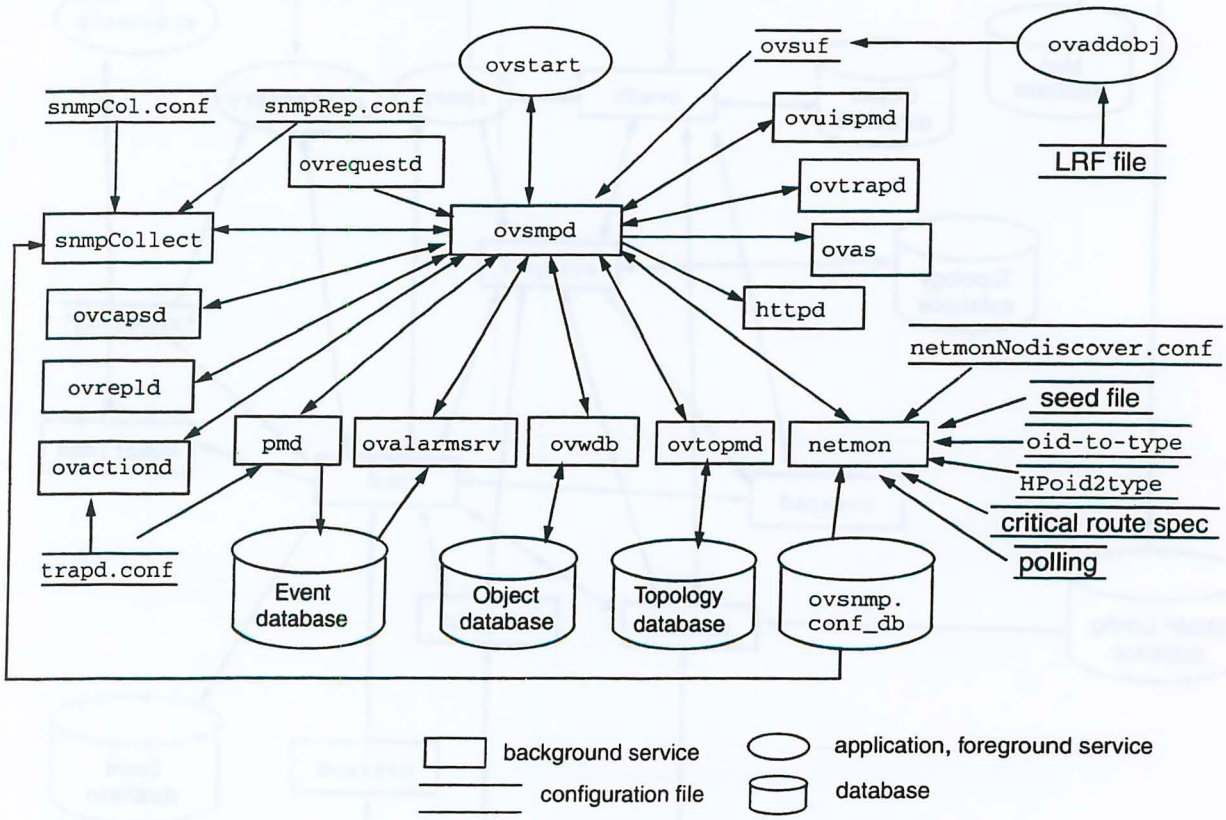
`webappmon.exe` Application encapsulator used by SNMP Data Presenter.

Figure A-4 on page 551 illustrates how the CGI programs interact with NNM's other services.

Behavior of the Services and Files

Figure A-1 shows the interactions and relationships among background services and files at start-up time. The arrows indicate the direction that communication flows.

Figure A-1 Services and Files at Start-up



ROS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1137
3740
Doc:

Figure A-2 and Figure A-3 show the interactions and relationships of background services and files during operation. The arrows indicate the direction that information flows.

Figure A-2 Services and Files During Operation (Part 1)

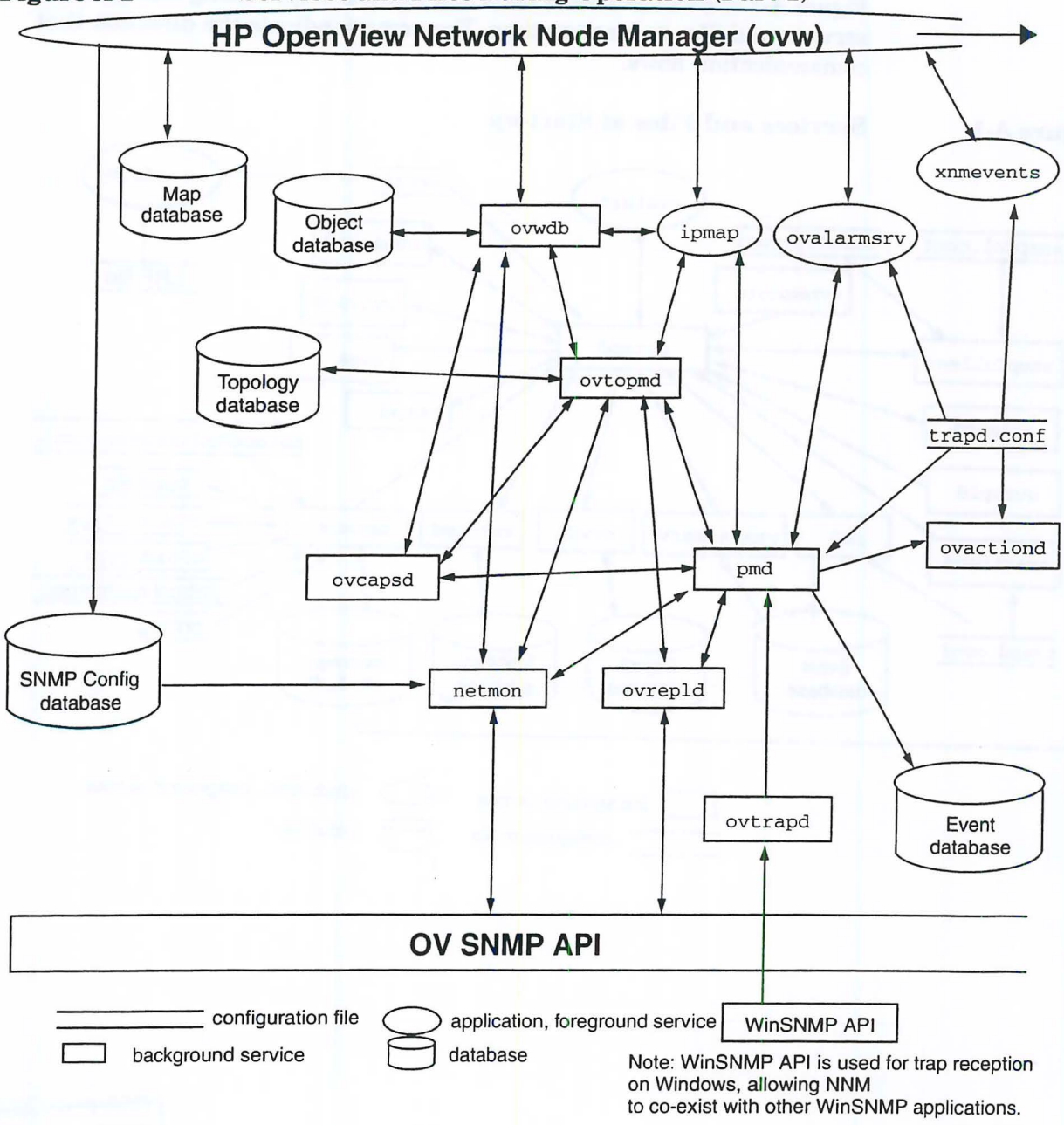
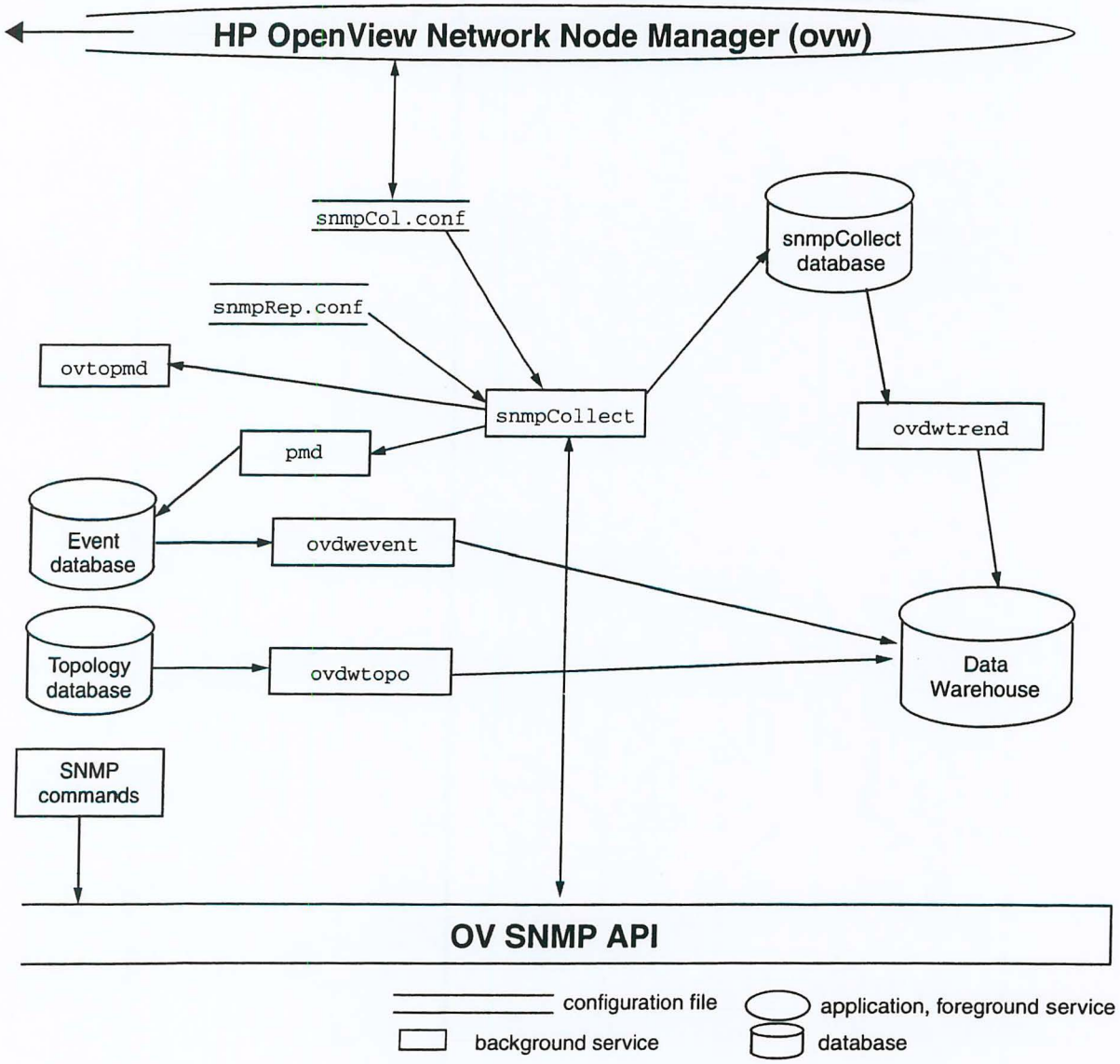


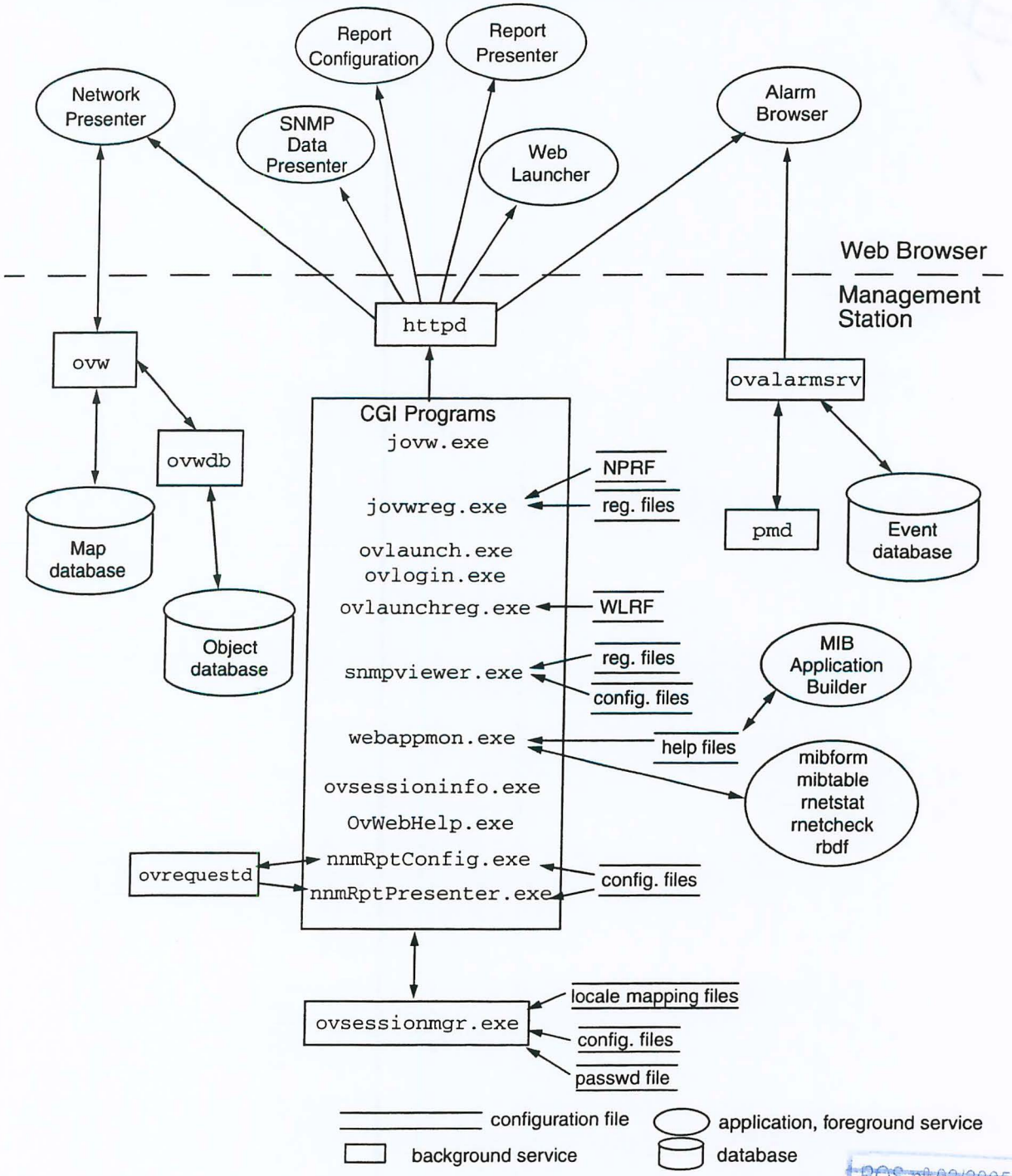
Figure A-3 Services and Files During Operation (Part 2)



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1138
3740
Doc:

Figure A-4 shows the interactions and relationships among the services and files of the web components.

Figure A-4 Services and Files for the Web Components



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1139
3740
Doc:

B Network Troubleshooting Tools

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1140
3740
Doc:

Network Node Manager includes many tools for your convenience. This appendix includes brief descriptions of the tools available for your use. For more information about each tool, access the online help within NNM, and search the index for the tool name.

To find out about easily creating your own custom SNMP tools and adding them to the pull-down menu choices, see "Using the MIB Application Builder" on page 443.

The tools in this appendix are organized as follows:

- Tools in NNM on a management station:
  - — Performance tools (page 556).
  - — Configuration tools (page 562).
  - — Fault management tools (page 566).
  - — Miscellaneous tools (page 569).
- Tools in NNM's web applications (page 575).

You can also run a variety of Microsoft diagnostic tools on a management station with a Windows operating system from the NNM menus. These tools will appear depending on whether your computer is a workstation or a server, and whether you have installed the tools on your computer.

The Windows operating system tools are:

- Registry Editor
- Performance Monitor
- Event Viewer
- Windows Diagnostics
- Server Manager
- User Manager
- SMS Properties
- Run SMS

NOTE The Microsoft System Management Server (SMS) does not come with the Windows operating system and must be purchased separately from Microsoft. Consult your Windows operating system documentation for details on using these tools.

Tools in NNM on a Management Station

The tools discussed in this section are located in the menu structure in NNM on a management station under the `Performance`, `Configuration`, `Fault`, and `Tools` pull-down menus. You simply highlight the node or nodes for which you want to gather information, then select the menu choice. NNM sends the MIB request and displays the responses for you in an easy to read graph, chart, or table.

Map Snapshots

Use `Map:Snapshot` to create a snapshot of a particular map frozen in time. A snapshot displays all persistent submaps showing the state of your network at the time you took the snapshot, including the status and location of all symbols. This may be useful to:

- Compare versions of your network and system map before and after a department is moved to a new building. You can use the snapshot as a reference to ensure that all connections are re-established correctly.
- Troubleshoot a network breakdown by reviewing multiple snapshots of a map showing the progression of the problem. This may give your team clues about the initial cause.

The map must be open with read-write access when the snapshot is created. Snapshots are read-only. You cannot edit a snapshot. However, you can traverse the submaps by double-clicking on symbols, locate objects, and keep an updated selection list for each submap. Only one snapshot may be open at a time. If a snapshot is already opened when you choose to open another snapshot, the previously opened snapshot is closed.

Use the `Map:Snapshot->Delete` command to remove old snapshots in order to free up memory and improve system performance.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1141
3740
Doc:

Performance Tools

Network Activity

Interface Status->Overview Select any node symbol on the map, then use this command to display a variety of information such as interface numbers, name, status, and last status change.

Select any interface symbol on the map, then select this command to display a wealth of information about the interface board.

Interface Status->DS1/E1 Serial Line Status Select a node that supports SNMP and the DS1 MIB, then use this command to list all interface status attributes for the interfaces on the selected node. This command is useful for determining the status of each selected node or interface on the map, which can be used in troubleshooting.

Interface Status->DS3/E3 Serial Line Status Select a node that supports SNMP and the DS3 MIB, then use this command to list all interface status attributes for the interfaces on the selected node. This command is useful for determining the status of each selected node or interface on the map, which can be used in troubleshooting.

Interface Errors->Error Rate Select any number of node or interface symbols on the map, then select this command to display a graph showing the number of bad packets dropped over time on each interface. This command is useful for troubleshooting data transmission problems.

Interface Errors->Error Percentage Select any number of node or interface symbols on the map, then select this command to display a graph comparing the percentage of bad packets dropped to the total number of packets received over time on each interface. This command is useful for troubleshooting data transmissions problems.

Interface Errors->Discard Rate Select any number of node or interface symbols on the map, then use this command to display a graph of the number of packets dropped by the selected node or interfaces for reasons other than errors in the packet over a period of time. This command is useful for troubleshooting data transmission problems.

Interface Errors->Discard Percentage Select any number of node or interface symbols on the map, then use this command to determine the percentage of packets dropped by the selected node or interfaces for reasons other than errors in the packet over a period of time. This command is useful for troubleshooting data transmission problems.

Interface Traffic->Packet Rate Select any number of node or interface symbols on the map, then use this command to display a graph showing the average number of packets successfully sent and received over time on each interface. For example, if you suspect network performance problems, you could monitor SNMP nodes to analyze interface traffic patterns over a period of time.

Interface Traffic->Utilization Select any number of node or interface symbols on the map, then use this command to display a graph that compares the percentage of traffic flowing on each interface as it relates to the overall capacity of the interface over a period of time. This command is useful for troubleshooting interface traffic problems.

Interface Traffic->Throughput Select any number of node or interface symbols on the map, then use this command to display a graph of the number of successful packets sent and received over each interface over a period of time. This command is useful for troubleshooting data transmission problems.

Interface Traffic->Data Rate Select any number of node or interface symbols on the map, then use this command to display a graph of the average number of bytes that are received or transmitted over the node or interface over a period of time. This command is useful for troubleshooting data transmission problems.

Interface Traffic->Avg. Packet Size Select any number of node or interface symbols on the map, then use this command to display a graph of the average size of packets sent or received on the node or interfaces over a period of time. This command is useful for troubleshooting data transmission problems

TCP Connections You can use the `TCP Connections` command to list the TCP Connections table for the remote SNMP nodes you select.

Ethernet (802.3)->Ethernet Errors Use the Ethernet Errors graph to monitor interface error statistics for a node running HP SNMP agent software. The graph is useful for viewing and tracking patterns. For

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1142
3740
Doc:

example, if you suspect performance problems, you could monitor HP SNMP agent nodes to analyze the pattern of interface card CRC errors versus frames received over a period of time.

Ethernet (802.3)->Ethernet Traffic Use the Ethernet Traffic graph to monitor interface statistics for a node running HP SNMP agent software.

Frame Relay->Circuit Traffic->Data Rate Select a node or interface that supports SNMP and the Frame Relay MIB, then use this command to display a graph of the average number of bytes that are received and transmitted on the virtual circuit over some period of time. This command is useful for troubleshooting problems with the interface and for assessing the performance of the interface.

Frame Relay->Circuit Traffic->Frame Rate Select a node or interface that supports SNMP and the Frame Relay MIB, then use this command to display a graph of the average number of frames sent and received on the Frame Relay virtual circuit. This command is useful for troubleshooting problems with the interface and for assessing the performance of the interface.

Frame Relay->Circuit Traffic->Avg. Frame Size Select a node or interface that supports SNMP and the Frame Relay MIB, then use this command to list the average frame size of packets sent and received on the Frame Relay virtual circuit. This command is useful for characterizing the type of traffic flowing on the interface.

Frame Relay->Circuit Congestion Select a node or interface that supports SNMP and the Frame Relay MIB, then use this command to display a graph that shows the percentage of Frame Relay Virtual Circuits that indicate forward and backward congestion in the Frame Relay network. This command is useful for characterizing the amount of traffic flowing through the Frame Relay network.

Frame Relay->Circuit Errors Select a node or interface that supports SNMP and the Frame Relay MIB, then use this command to display a graph that shows the percentage of received frames that are dropped, either because of format errors or because the circuit is not active. Data is expressed as a percentage of all received frames. This command is useful for troubleshooting data transmission problems.

Frame Relay->Data Link Errors Select a node or interface that supports SNMP and the Frame Relay MIB, then use this command to display a table that shows the data link errors for the selected interface. This command is useful for troubleshooting data transmission problems.

System

CPU Load Use this command to monitor and graph the average number of jobs in the run queue for each of the selected SNMP agent nodes. (Jobs are processes that are running on a system.) The graph is useful for viewing and tracking CPU utilization patterns. For example, you could monitor SNMP agent nodes to analyze the pattern of jobs performed over a period of time. By graphing the CPU load of several nodes, you may discover that some nodes are overworked, while others are underutilized. This information might be useful in determining how to distribute tasks among several nodes.

Since this information is generated by an HP enterprise-specific MIB, it is available only from an HP 9000 or Sun SPARCstation running the HP OpenView SNMP Agent software.

Disk Space You can list the disk space used and available for a remote SNMP agent node.

Since this information is generated by an HP enterprise-specific MIB, it is available only from an HP 9000 or Sun SPARCstation running the HP OpenView SNMP Agent software.

RMON

Segment Utilization Select one or more nodes that support SNMP and the RMON MIB, then use this command to monitor and graph the percent of the segment bandwidth that is currently being utilized. This graph is useful for finding segments that are being overutilized.

Segment Errors Select one or more nodes that support SNMP and the RMON MIB, then use this command to monitor and graph the rate of errors on the segment.

Segment Octets Select one or more nodes that support SNMP and the RMON MIB, then use this command to monitor and graph the rate of 8 byte octets in the segment. This graph is a good indication of the amount of traffic on the segment.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1143
3740
Doc:

Segment Packet Sizes Select one or more nodes that support SNMP and the RMON MIB, then use this command to monitor and graph the number of packets in six different predefined octet size ranges. This data can give you a breakdown of the packet sizes being transmitted and received on a network segment.

Segment Packet Types Select one or more nodes that support SNMP and the RMON MIB, then use this command to monitor and graph the rate of multicast packets versus broadcast packets.

Host Table Select one or more nodes that support SNMP and the RMON MIB, then use this command to show a table of the traffic patterns per physical address on the segment.

SNMP

SNMP Authentication Failures Select one or more nodes that are HP9000 or Sun SPARCstation systems running the HP OpenView Extensible SNMP Agent software. Then use this command to list the management stations that caused an authentication failure on the selected nodes. Authentication failures occur when a management station sends an SNMP request with an incorrect community name. This command is useful for troubleshooting SNMP authentication failures.

SNMP Traffic Select one or more nodes that support SNMP. Then use this command to monitor and graph the SNMP network traffic to and from selected nodes. This command is useful for comparing the SNMP traffic graph to interface traffic: packet rate graph to determine the percentage of traffic to and from the selected node that is attributed to the SNMP management of the selected node.

SNMP Operations Select one or more nodes that support SNMP. Then use this command to display a summary of the SNMP operations requested of and performed by the SNMP agent on the nodes you select. This command is useful for reporting the total number of operations for the given category that have occurred since the SNMP agent on the selected node was last started.

SNMP Errors Select one or more nodes that support SNMP. Then use this command to display a summary of the SNMP protocol errors detected by the SNMP agent on the nodes you select. This command is

useful for determining the total number of errors for the given category that have occurred since the SNMP agent on the selected node was last started.

Network Polling Statistics

This command graphs data based on interface status polling and SNMP node polling. This data can tell you how busy the management stations and collection stations are. Refer to A *Guide to Scalability and Distribution for Network Node Manager* for information on management stations and collection stations. The data being graphed is the data collected from the netmon service. The polling activities from the data Collector and other SNMP applications are not being shown in this graph. The polling activity that this graph displays is configured in the `Options:Network Polling Configuration` dialog box and in the `Options: Status Polling` field of the `SNMP Configuration` dialog box.

Graph SNMP Data

Selected Nodes This command graphs data that was previously collected with the MIB Data Collector and allows you to manipulate that data.

Use this command to view collected data on the selected nodes without having to first build an application to do so. This approach is useful when you want to browse the collected data for these nodes. Use this command when you want to graph some data points just once, or when you want to compare different variables across different systems.

For example, if you want to compare load averages to the number of packets on the selected systems and you have not built an application to do so, you can use this command to graph these two variables together.

All This command reads in ALL the collected data from the Data Collector database into its memory. Depending on how much data is stored in the database, displaying the Graph All Collected Data window may take a long time.

Windows Performance Monitor

On Windows operating systems only, use this command to run the Windows performance monitor. If NNM does not recognize the target node as one with a Windows operating system, the `Windows Performance Monitor` item is unavailable on your menu.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1144
3740
Doc.

Configuration

Network Configuration

Interface Properties Use this command to generate the list of attributes of all the interfaces within a selected node. The list includes information such as name, type, alias, and status.

IP Addresses Use this command to list the IP and link addresses for the selected remote SNMP nodes. This command is useful for determining IP and interface addresses associated with a node without looking through configuration files.

IP Routing Table You can list the routing table information for the remote SNMP nodes you select. This information determines how IP packets are routed on the nodes. Use the `IP Routing Table` command for diagnosing connectivity problems (for example, one node cannot communicate with another).

On UNIX operating systems, this information can be used to determine more efficient routes on the network, to assess the need for explicit routes, and to diagnose connectivity problems. The information you see is real-time data from the node rather than static information from a database.

On UNIX operating systems, if you want to reroute traffic on the network, you can either temporarily change the routing using the `route` command, or permanently change the routing by editing the `netlinkrc` file and rebooting the system. (Routing commands may vary across vendor systems.)

IP ARP Cache You can list the ARP (Address Resolution Protocol) cache table for the remote SNMP nodes you select. The `IP ARP Cache` command is useful for diagnosing connectivity problems because it indicates whether two nodes have a different link address for a third node. The information is real-time data taken from the node rather than static information from the database.

IP Services You can list the services that the remote SNMP-supported nodes you select are configured to support. This information tells you which configured services a node is currently running. The information is real-time data from the node rather than static information from the database.

For example, if you wanted to know if a node is executing the Telnet server, you could use the `IP Services` command to see if the node is listening with Telnet TCP port number 23.

Cisco Discovery Protocol->Interface Table Select one or more nodes that support SNMP and the CISCO-CDP MIB, then use this command to display device interface information contained in the Cisco Discovery Protocol Interface Table (cdpif). Refer to the `rnetstat` reference page in NNM's online help (or the UNIX manpage) for specific information about information contained in the Cisco Discovery Protocol Interface Table.

Cisco Discovery Protocol->Cache Table Select one or more nodes that support SNMP and the CISCO-CDP MIB, then use this command to display device interface information contained in the Cisco Discovery Protocol Cache Table (cdpcache). Refer to the `rnetstat` reference page in NNM's online help (or the UNIX manpage) for specific information about information contained in the Cisco Discovery Protocol Cache Table.

Cisco Discovery Protocol->Global Table Select one or more nodes that support SNMP and the CISCO-CDP MIB, then use this command to display device interface information contained in the Cisco Discovery Protocol Global Table (cdpglobal).Refer to the `rnetstat` reference page in NNM's online help (or the UNIX manpage) for specific information about information contained in the Cisco Discovery Protocol Global Table.

Cisco VLAN Membership Table Select one or more nodes that support SNMP and the CISCO-VTP MIB, then use this command to view the Cisco VLAN port membership table. There is one row for each bridge port that is assigned to at most one VLAN. Ports with more than one VLAN are not represented. An entry may be created and deleted when ports are created or deleted via SNMP or the management console on a device.

Bridge MIB->Base Table Select one or more nodes that support SNMP and the BRIDGE MIB, then use this command to view a table that contains information describing the basic bridging functionality provided by this device, regardless of the bridging protocol the device supports.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1145
3740
Doc:

Bridge MIB->Base Port Table Select one or more nodes that support SNMP and the BRIDGE MIB, then use this command to list all the ports on the device and basic information about each port.

Bridge MIB->Spanning Tree Table Select one or more nodes that support SNMP and the BRIDGE MIB, then use this command to view a table that contains configuration information about the Spanning Tree Protocol implementation.

Bridge MIB->Spanning Tree Port Table Select one or more nodes that support SNMP and the BRIDGE MIB, then use this command to view a table that contains information maintained by every port about the Spanning Tree Protocol state for that port.

Bridge MIB->Transparent Forwarding Table Select one or more nodes that support SNMP and the BRIDGE MIB, then use this command to view a table that contains information about unicast entries for which the bridge has forwarding and/or filtering information. This information is used by the transparent bridging function in determining how to propagate a received frame.

Bridge MIB->Transparent Port Table Select one or more nodes that support SNMP and the BRIDGE MIB, then use this command to view a table that contains transparent bridging protocol information about each port.

Bridge MIB->Static Table Select one or more nodes that support SNMP and the BRIDGE MIB, then use this command to view a table that contains filtering information configured into the bridge by (local or network) management, specifying the set of ports to which frames received from a specific port and containing a specific destination address are allowed to be forwarded.

Frame Relay-> Properties Select one or more nodes, then use this command to list information for all selected nodes or interfaces on a selected node.

Frame Relay->Virtual Circuits Select one or more nodes, then use this command to list the virtual circuit properties for all interfaces on the selected node. You can use this information for verifying the information related to each interface on the selected node.

ATM Properties Select one or more nodes, then use this command to list the common attributes for the selected nodes or for all interfaces on a selected node.

DS1/E1 Serial Line: Properties Select a node or interface, then use this command to list the attributes for the selected nodes or for all interfaces on a selected node.

DS3/E3 Serial Line: Properties Select a node or interface, then use this command to list the attributes for the selected nodes or for all interfaces on a selected node.

SONET/SDH: Properties Select a node or interface, then use this command to list the attributes for all interfaces on the selected node. You can use this list to verify the information about each interface on the selected node.

System: Information

Choose this command to display information about the selected system, such as system location and system contact.

System->HP-UX SAM

On HP-UX systems only, this command starts up a tool — System Administration Manager (SAM) — that enables you to administer and configure HP-UX systems. Although SAM is started on the remote HP-UX node that you selected, it appears in a window on your local node.

SNMP: Trap Recipients

Choose this command to list the management stations (by IP address) that are configured to receive events (traps) from the selected node.

Windows Registry Editor

Use this command to run the Windows operating system Registry Editor. If NNM does not recognize the target node as one with the Windows operating system, the `Windows Registry Editor` item is not on your menu.

RQS nº 03/2005 - CPMI - CORREIOS
Fls. Nº 1146
3740
Doc:

Fault Resolution Tools

Alarms

Choose this command to list all the undeleted alarms for a selected node. The `Alarms` command is particularly useful when you know that a specific node is at least partially responsible for certain problems (for example, connectivity or performance problems). Use this command to:

- Filter the selected alarms based on severity, time, source, message, or event type.
- Browse incoming alarms and alarms contained in the event database.

You must have a read-write Alarm Browser window to perform the following: Acknowledge, Unacknowledge, Delete, Assign Category, and Assign Severity.

Network Connectivity

Poll Node Choose this command to update the open map and database with information about selected objects. It is useful for diagnosing communication problems between NNM and the node. This command performs the following operations on node objects that are selected and managed:

- Provides information about the node.
- Updates the status of the selected node objects.
- Checks for exceeded thresholds and logs any events into the event log.

Status Poll Use this command to update the open map and database with status information about selected objects. This command performs a status poll on IP and IPX node objects that are selected and managed. It is useful for diagnosing communication problems between NNM and the node.

Capability Poll Use this command to check nodes for remote DMI devices, and web management and web server capabilities. If the node supports DMI, `ovcapsd` will register with that node for NNM to receive DMI events.

Ping Choose this command to send one ICMP Echo packet per second from the local management station to a remote node. (The transmitted packet size is 64 bytes.) The output displays the number of packets sent and lost, and the round-trip times.

Remote Ping Choose this command to check connectivity between two remote nodes by transmitting packets between the nodes. You must first select a source and destination node. The source node selected must be an HP 9000 or Sun SPARCstation running the HP OpenView SNMP Agent software.

Trace Route Select a node or interface, then use this command to track the route that packets follow from the NNM management station to the selected node. Trace Route utilizes the IP protocol time to live field and attempts to elicit an ICMP `time exceeded` response from each gateway along the path to the selected node or interface.

Locate Route via SNMP Choose this command to locate specific IP routes between selected nodes. The command does two things:

- Lists all the intermediate nodes in the dialog box.
- Highlights the route on the network map.

The `Locate Route` command is useful for diagnosing connectivity problems (for example, cases where one node cannot communicate with another).

Path View Select 2 nodes, then use this command to display a description of the path between the two selected nodes. If you select only one node, NNM uses the local node as the source node. Show Path lists the node name or interface name, the IP address, the physical address and the status of each node or interface along the path. This command is useful for diagnosing connectivity problems.

Test IP/TCP/SNMP

Choose this command to check the connection between the local management station and another node or nodes. This command is useful for diagnosing network connection problems by testing networking protocols.

The TCP test uses a telnet port to check TCP connectivity. This test may fail since some workstations with the Windows operating system may not have a telnet server installed.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls.! Nº 567 1147
Doc.: 3740

Interface Status

Interface Status->Overview Select any node symbol on the map, then use this command to display a variety of information such as interface numbers, name, status, and last status change.

Select any interface symbol on the map, then select this command to display a wealth of information about the interface board.

Interface Status->DS1/E1 Serial Line Status Select a node that supports SNMP and the DS1 MIB, then use this command to list all interface status attributes for the interfaces on the selected node. This command is useful for determining the status of each selected node or interface on the map, which can be used in troubleshooting.

Interface Status->DS3/E3 Serial Line Status Select a node that supports SNMP and the DS3 MIB, then use this command to list all interface status attributes for the interfaces on the selected node. This command is useful for determining the status of each selected node or interface on the map, which can be used in troubleshooting.

Interface Errors

Interface Errors->Error Rate Select any number of node or interface symbols on the map, then select this command to display a graph showing the number of bad packets dropped over time on each interface. This command is useful for troubleshooting data transmission problems.

Interface Errors->Error Percentage Select any number of node or interface symbols on the map, then select this command to display a graph comparing the percentage of bad packets dropped to the total number of packets received over time on each interface. This command is useful for troubleshooting data transmissions problems.

Interface Errors->Discard Rate Select any number of node or interface symbols on the map, then use this command to display a graph of the number of packets dropped by the selected node or interfaces for reasons other than errors in the packet over a period of time. This command is useful for troubleshooting data transmission problems.

Interface Errors->Discard Percentage Select any number of node or interface symbols on the map, then use this command to determine the percentage of packets dropped by the selected node or interfaces for reasons other than errors in the packet over a period of time. This command is useful for troubleshooting data transmission problems.

Frame Relay Circuits Select a node or interface that supports SNMP and the Frame Relay MIB, then use this command to display a graph that shows the percentage of received frames that are dropped, either because of format errors or because the circuit is not active. Data is expressed as a percentage of all received frames. This command is useful for troubleshooting data transmission problems.

Frame Relay Data Link Select a node or interface that supports SNMP and the Frame Relay MIB, then use this command to display a graph that shows the data link errors for the selected interface. This command is useful for troubleshooting data transmission problems.

Windows Event Viewer

Use this command to run the Windows operating system Event Viewer. If NNM does not recognize the target node as a one with the Windows operating system, the `Windows Event Viewer` item is not on your menu.

Windows Diagnostics

Use this command to run the Windows operating system diagnostics tools. If NNM does not recognize the target node as a one with the Windows operating system, the `Windows Diagnostics` item is not on your menu.

Miscellaneous Tools

Report Presenter

Use the `Report Presenter` command to access the NNM Report Presenter. The NNM Report Presenter is a presentation interface for viewing reports. Available report categories include device inventory, availability, performance, and exceptions.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1148
3740
Doc:

Remote Power On

New computers may have an energy-saving feature that automatically reduces the power after a specific idle time limit is reached. Some computers include a hardware-based feature in their network interface card that can be accessed to restart the computer remotely. Use `Remote Power On` to revive computers that respond to AMD Corporation's MagicPacket (`remotepoweron`) utility.

Highlight network devices on your map and select `Tools:Remote Power`. Then select one of the following.

Power On This command broadcasts the `remotepoweron` command for the highlighted device or devices. If the network interface card is capable of responding to the `remotepoweron` command, the computer will begin the power up process.

Power On and Ping This command broadcasts the `remotepoweron` command for the highlighted device or devices. NNM then waits a specified amount of time to allow for the power up process to complete, then issues a `ping` command to determine if the power-up was successful.

Note that this tool generates a lot of network traffic due to the broadcast.

TIP

Create a batch file that you can use to issue the `remotepoweron` command for all IP/IPX addresses of all devices on your network that contain hardware capable of responding to the `remotepoweron` command. Currently there is no way for NNM to detect which devices do or do not have this capability. You need to compile the list yourself.

For more information, refer to the *remotepoweron* reference page in NNM's online help (or UNIX manpage).

Terminal Connect

Choose this command to create a terminal emulator on a local system that is connected to a remote system using a network virtual terminal protocol.

Telnet (hpterm) On UNIX operating systems only, you can use this command to open an HP terminal window to telnet to other systems.

Telnet (xterm) On UNIX operating systems only, you can use this command to open an X terminal window to telnet to other systems.

Unused IP Addresses

The `Unused IP Addresses` command will display a list of IP addresses from networks NNM is managing that have not been recently heard from. You can configure the time in which a node must be heard from using the `Options:Network Polling Configuration:IP` command. In the Status Polling configuration area, check the `Delete nodes if down for` check box and specify a value.

HP OpenView Launcher

This command enables you to use the HP OpenView Launcher. The `HP OpenView Launcher` is an integration point with the HP OpenView web applications. It provides login security for HP OpenView applications and a central point from which you can launch all of the applications that have been integrated into the HP OpenView Web.

Port-Address Mapping

Select a node. Then use this command to display a table of the nodes that are connected to the node that you selected.

Data Warehouse

Export Topology This commands exports information from topology database to the data warehouse.

Export Events This command exports information from the event database to the data warehouse.

Export Trend Data This commands exports information from the trend database to the data warehouse.

Web Browser

Management Page Some servers can provide an alternative to their Home Page that is called the Management Page. The Management Page is semi-private, in that an individual wanting to browse it must know its URL.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 571
Doc: 3740

Choose this command to launch your web browser on the Management Page of the target node, provided that NNM recognizes the target node as an HTTP server that provides an alternative to its Home Page (`Attribute isHTTPmanaged = true`). If the target node is not recognized as such a server, this command remains grayed out.

Server Home Page Choose this command to launch your web browser on the Home Page of the target node, provided that NNM recognizes the target node as an HTTP server (`Attribute isHTTPsupported = true`).

If you choose the `Home Page` command with no node selected on the map, then it will open the default home page of your own web browser. If a target node is selected, then the command will open the target node's default home page.

SNMP MIB Browser

Use the MIB Browser as a general-purpose diagnostic tool to access the Management Information Base (MIB) on agents. The MIB is a collection of objects (management information) that encompasses configuration and status values.

Use the SNMP MIB Browser to:

- Learn what MIBs are available for building diagnostic applications that monitor MIB values.
- Query and display MIB objects that you use infrequently.
- Troubleshoot problems with other MIB commands.

For more information, refer to "SNMP MIB Browser" on page 412.

Views

Neighbor Select a node, then use this command to display a graphical representation of the selected device and the nodes connected to it, within a specified number of hops. The number of hops defaulted to two, however you can use the drop down list to modify the number of hops.This command is useful for understanding relative device connectivity and for diagnosing the root cause of abnormal device status alarms.

Path Select two nodes, then use this command to display a graphical representation of the path between the two selected nodes. If you select only one node, NNM uses the local node as the source node. The

2318

`Views:Path` command lists the node name or interface name, the IP address, the physical address and the status of each node or interface along the path. This command is useful for diagnosing connectivity problems.

Node The `Views:Node` command opens a menu that you can use to configure a topology view based upon the various filters available. A second selection criteria is the status of the managed devices that pass the selected filter.

CDP The `Views:CDP` command presents a graphical view of all the managed nodes supporting the CDP (Cisco Discovery Protocol) MIB. If a CDP node is currently selected on the map, then the discovery of CDP nodes will branch from this node. If you do not have any nodes selected on the map, then the nodes that pass the CDP filter will start the discovery process.

Station The `Views:Station` command shows you a graphical representation of the NNM collection stations and management stations discovered in your topology. This command is useful in a distributed management environment.

Internet The `Views:Internet` command shows you a graphical representation of the networks in your topology. This command lets you see the general status of your network, locate problems in your network, or proactively monitor all of your networks.

NOTE If you have not purchased and enabled the HP OpenView NNM Extended Topology product for UNIX operating systems, the OSPF Backbone, All HSRP Groups, All VLANs, and IPv6 Network views described below do not function as shown, but instead open a view that tells you how to purchase, install and enable Extended Topology.

OSPF Backbone For UNIX operating systems, the `Views:OSPF Backbone` command shows you a graphical and tabular representation of an OSPF area. By default, Extended Topology launches your web browser to the OSPF backbone (area 0.0.0.0).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1150
3740
Doc:

All HSRP Groups For UNIX operating systems, the `Views:All HSRP Groups` view presents both a graphical display and a table of HSRP groups. From the All HSRP Groups view you can open two other view, the HSRP Group Detail view and the HSRP Node Detail view.

All VLANs For UNIX operating systems, the `Views:All VLANs` command presents a table that lists all the VLANs in your network. From this table, you can link to two other VLAN views: a VLAN membership view and a switch centric view. You can use the VLAN membership view to observe the switches whose ports participate in a specific VLAN. You can use the switch centric view to observe a selected switch and the VLANs that it participates in.

IPv6 Network For UNIX operating sytems, the `Views:IPv6 Network` command shows you a graphical representation of an IPv6 network, including routers and end nodes that support IPv6. Lines connect IPv6 nodes to the prefix group or groups they logically connect to. From the IPv6 Network view, you can open two other views, the IPv6 Node Detail view and the IPv6 Prefix Groups view.

DMI Browser (Desktop Management Interface)

Some HP personal computers have a Desktop Management Interface (DMI) that you can query to determine the computer's status, configuration, and available resources. You can create queries for a single device, or a group of devices, using the DMI commands.

NOTE

Make sure the computers you select support Remote DMI. Select the `isRDMISupported` attribute from the `Find By Attribute` dialog box to see a list of HP PCs that support Remote DMI. For more information, see "DMI Events (Indications)" on page 327 and "DMI Browser" on page 417.

NNM uses Intel's DMI Explorer to browse DMI information. Refer to the DMI Explorer's online help for more information.

Tools in NNM's Web Applications

NNM's web applications also contain tools for managing your network. Some of the tools are accessed from tabs, while others are accessed through commands. For details about any of the following tools or commands, see the HP OpenView web online help.

HP OpenView Launcher

There are several tabs at the bottom of the `HP OpenView Launcher` window that can help you troubleshoot the network. The tabs listed below contain tools to help you manage your network.

Object Views

The Object Views tab provides access to applications that provide views. From the Object Views tab you can use the SNMP MIB Browser to retrieve and view SNMP data or you can view your network topology using the Network Presenter.

Tasks

The `Tasks` tab provides access to task presentation managers, wizards, and tabbed dialog boxes that perform tasks.

Information and Reports

The `Information and Reports` tab displays the containers for Accounting and Assets, Configuration Information, Faults and Alarms, and Resources and Performance. You can generate reports from these containers. This information can be instrumental in helping you diagnose network problems.

Tools

The pane associated with the `Tools` tab displays the container for NNM. Under the NNM container are the leaf nodes for the Network Presenter, Unused IP Addresses, Alarm Browser, Event Correlation Configuration, Report Presenter, Report Configuration, SNMP Data Presenter, SNMP MIB Browser, and Views. Accessing any of these tools will present additional useful network information.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 575
3740
Doc:

C Troubleshooting NNM Itself

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: Nº 1152
3740
Doc:

This appendix describes measures that you can use to identify and troubleshoot system and software problems that may occur during Network Node Manager operations. These measures include the following:

- General network management troubleshooting considerations (page 579).
- Characterizing various types of problems (page 582).
- Troubleshooting background services (processes), such as `netmon` and `ovtopmd` (page 584).
- Troubleshooting the Web applications (page 613).
- Troubleshooting various operations, such as MIBs and runtime components (page 623).
- Troubleshooting Windows operating system applications (page 637).
- Recommended practices for logging and tracing (page 639).
- Improving performance and traffic management (page 654).

These measures are not intended to be used for troubleshooting your network problems, but are only for system and software problems related to NNM operations.

Most of the steps you will take in troubleshooting NNM are the same for NNM on either a Windows or UNIX operating system; however, some files and services are different. In addition, there are considerations to NNM on Windows operating systems that do not apply to NNM on UNIX operating systems, and vice versa.

NOTE For troubleshooting NNM's databases and the data warehouse, refer to the online manual *Reporting and Data Analysis with HP OpenView Network Node Manager*.

General Troubleshooting Considerations

Consider the following when troubleshooting NNM:

- Network Node Manager is memory and page-file (swap-space) intensive. Problems may be due to resource exhaustion. Refer to "Performance" on page 656 for memory conservation tips.
- If you are using the Berkeley Internet Name Domain (BIND) Service on your network, each `gethostbyaddr` request for the hostname of a host with multiple IP addresses could return a different hostname.

When You Need More Information

Other information that may assist your troubleshooting is available in the following locations:

- The release note files (see page 71).
- The NNM online help.
- The Request for Comment (RFC) documents referenced in the introduction to this book (see page 33).

If a problem does not appear to be with the network management products themselves, see the following:

- Networking documentation for general network troubleshooting procedures.
- System documentation for system troubleshooting procedures.
- On UNIX operating systems only, X Windows documentation for X Windows troubleshooting procedures.

Preventive Practices

Following these recommended practices can help you prevent problems:

- Ensure that the management station meets the hardware, software and configuration prerequisites and recommendations.
- Maintain the system by regularly editing and deleting files. See Chapter 15 for maintenance tasks.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1153
3740
Doc

- Ensure that *install_dir*\bin\ ($OV_BIN) is in your path.
- On a UNIX operating system, source /opt/OV/bin/ov.envvars.sh into your environment.
- On a Windows operating system, source *install_dir*\bin\ov.envvars.bat into your environment.
- Do not modify Network Node Manager product files without retaining the original files. The original files provide a way of restoring a known good operational configuration. If you correct a problem by restoring the original files, you can isolate the problem to one of the changes you made to these files.

  When you back up original files, do not copy the files to a new file name in the same directory. All files in the following directories are considered "live;" that is, every file in these directories will be used and you will end up with duplicate definitions.

  install_dir\registration\ ($OV_REGISTRATION)
  install_dir\fields\ ($OV_FIELDS)
  install_dir\symbols\ ($OV_SYMBOLS)
  install_dir\bitmaps\ ($OV_BITMAPS)
  install_dir\conf\ ($OV_CONF)
  install_dir\help\ ($OV_HELP)
  install_dir\tmp\ovbackup ($OV_TMP/ovbackup)

  See the backup procedure in Chapter 6 for complete guidelines and procedures for backing up your files.
- Make sure that you are not using up too much of your management station's CPU and network resources by collecting too much MIB data or setting too frequent polling intervals for the netmon service. Use Performance:Network Polling Statistics to gauge how effectively netmon is collecting network data.
- Use logging and tracing of background services to help isolate problems, but be sure to clean up log and trace files regularly. For more information see "Recommended Logging and Tracing Practices" on page 639 in this appendix.
- Use ovstatus -c -v to check the status of background services and OVW sessions.
- Use ovstart -c to track the progress of the services being started by ovspmd.

- Use the `-d` option to `ovstart`, `ovstop`, `ovpause`, and `ovresume` to get additional debugging information.
- Use the `-verify` option to `ovw`. This option checks the syntax for all the installed application, symbol type, and field registration files. It also verifies the semantics of the application registration files and reports conflicts among application registration information. When started with this option, NNM does not start a normal "windowed" session; rather, it displays status messages in a text window.
- Use the `-mapcount` option to `ovw`. This option checks the consistency between the map database maintained by NNM and the object database maintained by `ovwdb`.
- Be careful when changing the permissions on files used by the management software. Restricting access could cause management services to be unable to access the file.
- On UNIX operating systems only, HP recommends that you not modify the files in `$APP_DEFS`. Instead, you can override the default X resources by modifying them in your `$HOME/.Xdefaults` file. If you are running HP VUE, modify your VUE resources. See `$APP_DEFS/XNm` for more details.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1154
3D0740

Characterizing the Problem

Symptoms are visible conditions that indicate a problem. Whenever you encounter a symptom, collect the basic information described in the following subsections. The problem can usually be characterized in one or more of the following ways: scope of the problem, what changed just before the problem occurred, duration of the problem, and what action was performed when the problem occurred.

Distinguish Local versus Remote Problems

If you suspect a problem on a remote node or agent system, try to duplicate it on a local node or management station, and vice-versa. If you cannot duplicate the problem on the local node, the problem is probably associated with the remote node. If you can duplicate the problem on the local node, the problem may be in the management station or somewhere in the link, or may be a problem common to the agents.

Remote Nodes' Level of Manageability

What type of remote node are you trying to communicate with when the problem occurs?

The amount of information that NNM can collect depends on whether a remote node:

- Supports SNMP or not (or is proxied).
- Supports all the mandatory objects in MIB-II.
- Supports a partial, full, or extended (non-standard) MIB.
- Is an HP node or not.
- Is a TCP/IP node or not.
- Is an IPX node or not.
- Is an IPX router/server or not.

The management station gets the most information from an HP SNMP node, less information from other SNMP nodes, least information from non-SNMP and TCP/IP nodes, and no information from non-SNMP and non-TCP/IP nodes.

Context: What Changed?

Determine what may have changed recently on your network or product configuration: hardware, software, files, security, utilization, etc. Keep a record of the software patches you install, so you can undo the changes in the order they occurred.

Also determine what is unique about a particular node that is having problems.

Duration: How Long or How Often?

Is the problem consistent (fails every time) or intermittent (fails sometimes)?

Context: What Action Was Performed?

When the problem occurred, what was happening? For instance:

- What operation was selected?
- What command was executed?
- What mouse operation was performed?
- What data was requested or sent?
- Was an alarm generated?
- Was an error or warning logged through the Windows Application Event Log (or `nettl`)?
- Was an error or warning logged through `ovconsole`, or the window from which `ovw` was started?
- Does `ovstatus -c` show all background services running?
- Does `ovstatus -v ovuispmd` list all of the OVW services that are expected to be running?

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1155
3740
Doc:

Troubleshooting Background Services

This section explains the background services of NNM and suggests actions to take if you have problems with one of the following background services. The background services are:

- hpptd
- netmon
- ovactiond
- ovalarmsrv
- ovcapsd
- ovrepld
- ovrequestd
- ovtopmd
- ovtrapd
- ovuispmd
- ovwdb
- pmd
- snmpCollect

In addition to explaining the background services, this section explains how to troubleshoot ovspmd, the service that monitors and controls the background services.

The background services and ovspmd should always be running whenever NNM is running. Normally, the background services are started through ovstart. See the *ovstart* reference page in NNM's online help (or the UNIX manpage) for all the options to ovstart. It may be particularly useful to use the -c or the -d options when troubleshooting.

To verify that the background services are running, enter the following:

```
ovstatus -c
```

See the *ovstatus* reference page in NNM's online help (or the UNIX manpage) for all the options to ovstatus.

The result should look similar to the following:

```
Name              PID   State       Last Message(s)
OVsPMD           3676   RUNNING     -
ovsessionmgr     3677   RUNNING     Initialization complete.
ovwdb            3678   RUNNING     Initialization complete.
ovuispmd         3701   RUNNING     Initialized. 1 ovw clients registered.
ovtrapd          3698   RUNNING     Initialization complete.
ovactiond        3699   RUNNING     Initialization complete.
ovalarmsrv       3700   RUNNING     Initialization complete.
pmd              3679   RUNNING     Initialization complete.
ovdbcheck        3680   RUNNING     Connected to embedded database.
ovrequestd       3681   RUNNING     Initialization complete.
httpd               -   unknown     (Does not communicate with ovspmd.)
ovtopmd          3697   RUNNING     Connected to native database "openview".

netmon           3702   RUNNING     Initialization complete.
snmpCollect      3703   RUNNING     No values configured for collection.
```

If ovstatus indicates that an object manager was not found, the problem may be caused by one of the following:

- The ovspmd configuration has been incorrectly modified or is corrupted. If the ovspmd configuration is corrupted, see "The ovspmd Background Service" on page 592.
- The executable file has been removed or moved from its expected location. ovsuf either has a pathname to each executable or expects them to be in *install_dir*\bin\ (%OV_BIN%). Make sure they exist where they are supposed to be.

If ovstatus indicates that a service is in a paused state, it may mean that a backup is currently being performed, or that the service did not restart as expected after a backup. In that case, the state will be one of the following: PAUSED, RESUME_ERROR, or DEPENDENCY_ERROR. In this case, check the backup log in *install_dir*\tmp (%OV_TMP%) to determine the cause of the error. You can then stop all services using ovstop, and restart all the services by typing:

```
ovstart -c
```

Some of the background services depend on other services to operate properly. Table C-1 shows the dependencies.

Table C-1 Background Service Dependencies

Background Service	Dependencies
httpd	no dependencies

RQS nº 03/2005 - CN - CPMI - CORREIOS 1156 Fls. Nº 3740 Doc:

Table C-1 Background Service Dependencies

Background Service	Dependencies
netmon	ovwdb, pmd, ovtopmd
ovactiond	pmd
ovalarmsrv	pmd
ovcapsd	ovwdb, pmd, ovtopmd
ovdbcheck	none
ovrepld	pmd, ovtopmd
ovrequestd	none
ovtopmd	ovwdb, pmd, snmpd
ovtrapd	pmd
ovuispmd	ovwdb, ovtopmd
ovwdb	no dependencies
pmd	snmpd
snmpCollect	ovwdb, pmd, ovtopmd

For problems with individual background services, see the appropriate subsection in this appendix on how to troubleshoot a specific background service.

The httpd Background Service

The `httpd` service handles http (web) requests. It is provided only on UNIX operating system installations of NNM. Here are some problems that can be caused by `httpd` and possible solutions to those problems.

`httpd` should be running wherever NNM is running. Normally it is started by `ovstart`. To verify that it is running, type:

```
ovstatus httpd
```

You can also see if `httpd` is running by typing **`ps -elf | grep httpd`** on UNIX operating systems. You should see multiple copies of `httpd` running, since the parent `httpd` service spawns multiple children to improve performance in handling `httpd` requests.

If `httpd` is running, you can validate that it is running correctly by entering the following into your web browser:

`http://`*`hostname`*`:3443/`

You should see a short web page with the title "It Worked!"

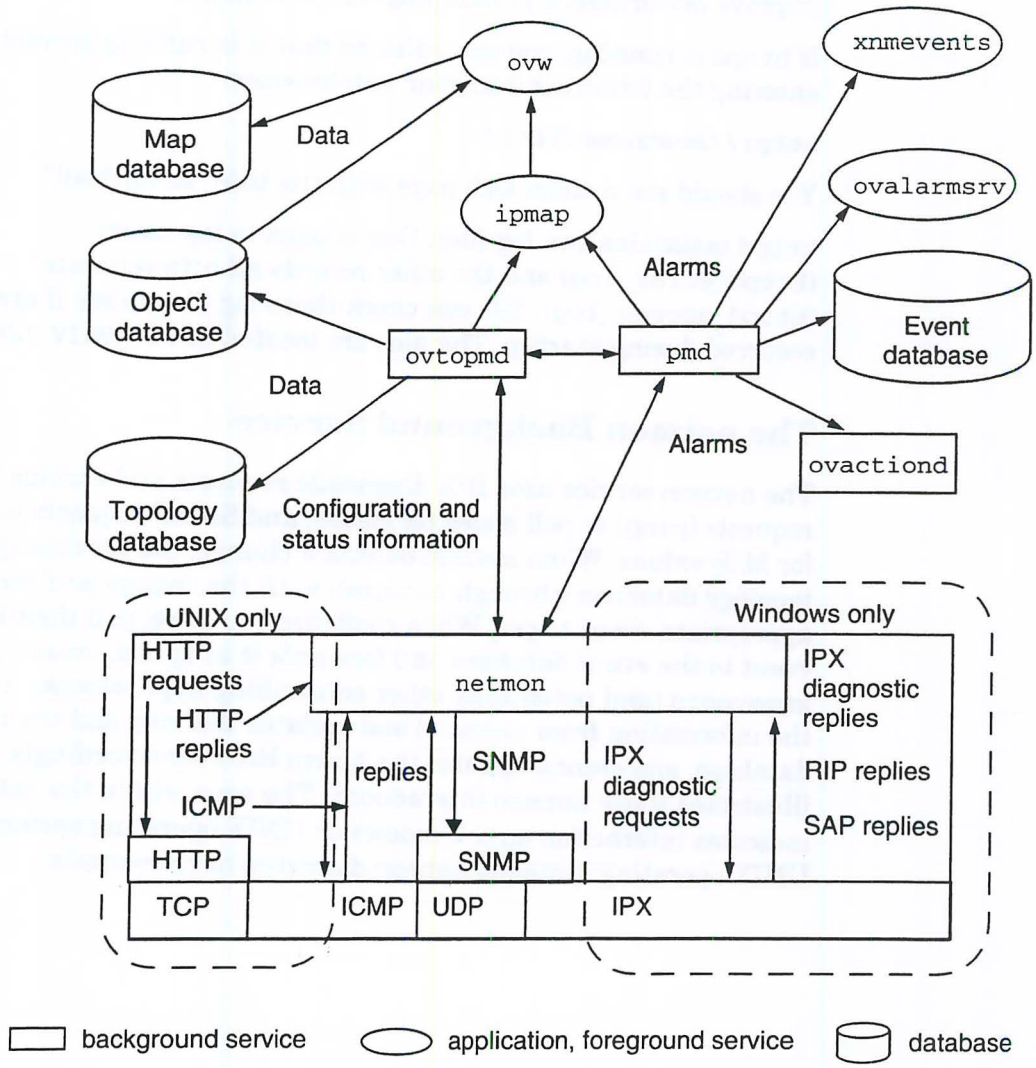
`httpd` maintains two log files. One is used to log errors (`httpd_error_log`) and the other records all http requests (`httpd_access_log`). You can check these log files to see if errors occurred during startup. The files are located in `$OV_PRIV_LOG`.

The netmon Background Service

The `netmon` service uses IPX diagnostic requests and various ICMP requests (`ping`) to poll nodes for status, and SNMP requests to poll nodes for MIB values. When `netmon` detects a change, the service updates the topology database (through `ovtopmd`) with the change and sends the appropriate event to `pmd`.When configured to do so, `pmd` then logs the event to the event database and forwards it to `ipmap`, `ovactiond`, and `xnmevents` (and potentially other subscribing applications). `ipmap` gets the information from `ovtopmd` and updates the map and the map database. `xnmevents` updates the Alarm Browser accordingly. Figure C-1 illustrates these `netmon` interactions. The area within the dotted oval indicates interaction on a Windows or UNIX operating system only. On UNIX operating systems, `netmon` discovers `http` requests.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1157
3740
Doc:

Figure C-1 netmon Interactions



You can control `netmon`'s polling through the map's `Options:SNMP Configuration` and the `Options:Network Polling Configuration:IP/IPX` menu item. The `SNMP Configuration` menu item modifies the *`install_dir`*`\conf\ovsnmp.conf_db` (`$OV_CONF/ovsnmp.conf_db`) database. The `Network Polling` menu item stores `netmon`'s polling intervals in the

install_dir\conf\polling ($OV_CONF/polling) file. Do not modify this file directly; use the command line options to the program xnmpolling.

The xnmevents service checks every five minutes to see if netmon and snmpCollect are running. If either service is not running, xnmevents will display a dialog box and report the inactive service. (For information on changing the five-minute default polling interval or on disabling this polling feature, see the System Registry on Windows operating systems, or the file /usr/lib/X11/app-defaults/XNmevents on UNIX operating systems.

Status polling is scheduled on a per node basis, but is not deterministic. Therefore, polling of a node may not occur when scheduled if netmon gets behind due to its polling load for a particular time interval. Also, polling of manually added nodes and nodes changed from unmanaged to managed may not occur immediately after they are added or managed.

While you are unmanaging a network or segment during active discovery, a few managed nodes may appear on that network. To avoid this problem, do one of the following:

- Wait until the program finishes active discovery of the map.
- Turn polling off while unmanaging the network.

Only one instance of netmon may run on the management station; the *install_dir*\conf\ ($OV_CONF) netmon.lock file enforces this restriction.

The following tools can help you troubleshoot netmon problems.

- Use the Fault:Network Connectivity:Poll Node or Status Poll menu item to test or cause immediate netmon polling activity to a node.
- Use ovdumpevents to check for netmon service errors.
- Use the Performance:Network Polling Statistics menu item to determine if netmon is able to perform its polling at the configured frequency. See the online help for an explanation of the output of this menu item.
- Use netmon tracing to help isolate problems. For information see "Logging and Tracing" on page 639, or see the *ovstatus* reference page in NNM's online help (or the UNIX manpage).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1158
3740
Doc:

Auto-configuration of SNMP Traps

When netmon detects a node running an HP OpenView SNMP agent, it attempts to add the IP address of the NNM system to the trap destination table using an SNMP set request. In order for this to work, the NNM system must be configured with the correct SNMP set community name using Options:SNMP Configuration.

The ovactiond Background Service

The ovactiond service is started when you start NNM. It receives events from pmd that have automatic actions defined. For each of these actions, ovactiond formats the command string, then passes it on for interpretation and execution.

When you configure events using the Options:Event Configuration menu item in NNM, you are configuring ovactiond. If the result of your configuration of events is not what you expected, you can check the status of ovactiond.

Use the command ovstatus ovactiond to see if the service is running. ovactiond requires that pmd is running, so you should also check the status of pmd.

You can check the log file ovactiond.log for error messages. The file is located in:

Windows: *install_dir*\logs

UNIX: $OV_LOG

The ovalarmsrv Background Service

The ovalarmsrv service is started when you start NNM, and is the service that forwards events to xnmevents on NNM on a management station, and to NNM's web-based Alarm Browser. ovalarmsrv relies on pmd to be running; therefore, if you have problems starting xnmevents or the Alarm Browser, first check to see if pmd is running using ovstatus pmd.

You can also check the status of ovalarmsrv by using the ovstatus command. If ovstatus shows that ovalarmsrv is not running, and it will not start using ovstart ovalarmsrv, check to see if the service is running but ovstatus is not reporting it.

On UNIX operating systems, type

ps -elf | grep ovalarmsrv.

On Windows operating systems, use the Task Manager. If you find an ovalarmsrv service running, kill that service and restart ovalarmsrv using **ovstart ovalarmsrv**.

If you still have problems starting ovalarmsrv, be sure that you do not have a port conflict. ovalarmsrv uses two ports for communications. You can check those values in the /etc/services file. Make sure that another application is not using one of the ports assigned to ovalarmsrv.

ovalarmsrv reads alarms from the event database, receives new alarms from pmd, and maintains the state of all user modifications (for example, acknowledge, delete, etc.) to presented alarms. If the event database or the state file have somehow become corrupted, or if the file permissions have changed such that those file can't be read, you will not receive any data in xnmevents or the Alarm Browser.

You can also check the ovalarmsrv log file, ovalarmsrv.trace for error and tracing messages. The file is located in:

Windows: *install_dir*\logs

UNIX: $OV_LOG

The ovcapsd Background Service

The ovcapsd service checks newly-discovered nodes for Remote Desktop Management Interface (remote DMI or RDMI) and Hypertext Transfer Protocol (HTTP) capabilities. It periodically rechecks all Normal-status nodes. Capabilities are stored in the ovwdb database. ovcapsd gets IP and IPX address information for nodes from ovtopmd.

See the *ovcapsd* reference page in NNM's online help (or the UNIX manpage) for the most complete information available. Here are two important troubleshooting tips:

- ovcapsd checks nodes' capabilities after netmon has added them to the topology database. It might not have checked a node before the node appears in your ovwdb database or your map. If you search on a capability such as isHTTPSupported, ovcapsd might not yet have had a chance to check the node in which you're interested. You can run ovcapsd from the command line to check individual nodes synchronously. Also, ovcapsd can be made to check nodes faster by

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1159
3740

increasing the number of threads it creates to check the nodes. See the *ovcapsd* reference page in NNM's online help (or the UNIX manpage) for more information.

- See the *install_dir*\log\ovcapsd.log file for ovcapsd service errors and on-exit messages.

The ovspmd Background Service

The ovspmd service monitors and controls the NNM background services. These background services are designed to run as children of ovspmd. The ovspmd service should be running whenever the background services are running. Normally, ovspmd is started by ovstart.

To verify the status of the services, type:

```
ovstatus -c
```

If ovstatus provides output indicating that all services are running, the problem is not ovspmd. If you do not receive the expected output, either ovspmd has a communication problem or the ovspmd service is not running. If the output indicates that ovsmpd is not running, start it using ovstart ovspmd.

Determining ovspmd Problems

You need to determine whether the problem is related to ovspmd or to a background service. If you determine you have an ovspmd problem, you need to determine what type of problem it is. Here are some indications of ovspmd problems:

- If the ovstatus output indicates that one of the background services is not running, type

  ```
  ovstart -v
  ```

  This should start any service that is not running. If any service fails to start, an error message will appear, indicating which service is not running. If this happens, use the Task Manager on a Windows operating system.

  On UNIX operating systems only, type **ps -ef** to list currently running services.

  Do *one* of the following:

— If the output indicates a certain service is running, but ovspmd says the service is not running (using ovstatus or ovstart), ovspmd does not know that service is running. This problem can occur when ovspmd is shut down unexpectedly.

— If the output indicates that a certain service is not running, that service has a problem. See the troubleshooting section for that service.

When you run ovstart, the error message you receive about the service should provide information that will help resolve the problem.

- If you receive an ovspmd error message in the following format:

```
ovspmd:conf\ovsuf: error message
($OV_conf/ovsuf: error message)
```

you may have a corrupt ovsuf configuration file.

On UNIX operating systems only, go to the next section "Recreating the ovspmd Sockets Directory (UNIX operating systems only)".

- On UNIX operating systems only, if you receive *one* of the following error messages

```
ovstart: ovspmd is not running.It may have failed to start.
ovstart: unable to contact ovspmd: error message
```

you need to verify that the ovspmd sockets directory exists. Go to "Recreating the ovspmd Sockets Directory (UNIX operating systems only)" below.

Recreating the ovspmd Sockets Directory (UNIX operating systems only)

This section is for UNIX operating systems only. If you are using NNM on a Windows operating system, see the section "The netmon Background Service" on page 587.

Use this procedure when ovstart is unable to start or connect to the ovspmd service.

1. Verify that the $OV_SOCKETS directory still exists. ovspmd creates the OVsPMD_MGMT and OVsPMD_REQ socket files in this directory, which enable ovspmd to communicate with the other background services. If this directory no longer exists, recreate it by typing

```
mkdir $OV_SOCKETS
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1160
3740
Doc:

2. Find out if any of the background services are running by typing

   ps -ef

3. Kill all the NNM background services that are running using the `kill` command. *Do not* use `kill -9`. For a list of the services, see "Troubleshooting Background Services" on page 584 in this appendix.

4. To restart the services and verify that they are starting properly, type

   ovstart -c

The ovrepld Background Service

`ovrepld` is a service that manages the discovery and monitoring of objects done on behalf of the local management station by remote collection stations. This remote topology information is merged with information obtained locally by `netmon` to create a more comprehensive topology database. If objects known to be present on remote collection stations are not appearing on your map, or are not being updated as expected, it is possible that `ovrepld` has stopped functioning.

Use `ovstatus ovrepld` to determine if `ovrepld` is running. If it is not, you can start it using `ovstart ovrepld`. In addition, `ovrepld` relies on `pmd` and `ovtopmd` to be running, so check to be sure that those services are also running.

`ovrepld` writes errors to a log file, `ovrepld.log`. The file is located in:

Windows: `install_dir\logs`

UNIX: `$OV_LOG`

The ovtopmd Background Service

The `ovtopmd` service is responsible for maintaining the topology database that is used by `netmon` and `ipmap`. It provides both enforcement of rules for correctness of the IP topology, and caching of the data to improve the performance of the system.

`ovtopmd` should be running whenever NNM is running. Normally it is started through `ovstart`. To verify that it is up and running, type

ovstatus ovtopmd

You should see something like this:

```
object manager name:    ovtopmd
state:                  RUNNING
PID:                    4119
last message:           Connectedto native database "openview"
exit status:            -
```

If ovstatus gives an error similar to this:

```
ovspmd:install_dir\conf\ovsuf:object manager ovtopmd not found
($OV_CONF/ovsuf:object manager ovtopmd not found)
```

The problem may be that the ovspmd configuration is corrupted. If the ovspmd configuration is corrupted, see "The ovspmd Background Service" on page 592 in this appendix.

If ovstatus reports the following message:

```
Running. Lost connection to master agent.
```

This could indicate that ovtopmd is still executing, but has lost its connection to the master SNMP agent (snmpd). Usually this is because the master agent (snmpdm) exited or has been shut down.

Restart the master agent on the Windows operating system using the Services applet in the Control Panel. Start the SNMP EMANATE Master Agent and SNMP EMANATE Adapter for NT/2000 services.

On UNIX operating systems only, restart snmpd by executing

```
/usr/sbin/snmpd
```

If the master agent is executing, try executing the following commands:

```
ovstop ovtopmd
```

```
ovstart ovtopmd
```

If ovstatus knows about ovtopmd, but indicates that it is not running, enter the following:

```
ovstart -c
```

Normally, this should start ovtopmd and all background services on which ovtopmd depends. In particular, ovtopmd depends on ovwdb and pmd being started. If ovwdb does not start, ovtopmd will not be able to execute successfully. In addition to ovwdb executing, ovtopmd relies on the field definitions being loaded into ovwdb, which normally happens through the configuration scripts at installation time.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1161
3740
Doc:

If ovtopmd gives an error indicating that it was unable to map a field name into a field ID, do the following:

- Verify that $LANG is set correctly and that the *install_dir*\fields\C ($OV_FIELDS/$LANG) directory exists and contains at least the following files: ovw_fields, ip_fields, snmp_fields, topm_fields, and misc_fields. The $LANG environment variable provides support for localizing native languages. If not otherwise defined, $LANG is assumed to be C, which means that no native language support is provided. (UNIX systems only: For more information on native language localization, see the *lang* manpage.)
- Type the following commands:

  ```
  ovstop -c
  ovstart ovwdb
  ovw -fields
  ovstart -c
  ```

  This should load any necessary field definitions into ovwdb, and then start ovtopmd and netmon (as well as any other background services).

By default, ovtopmd uses a TCP socket bound to port 2532. If ovtopmd indicates an error attempting to bind to this port number because another application is already using it, follow these steps:

1. Make sure that you do not have another ovtopmd service using port 2532.

   The most common reason for errors binding to the TCP socket is the presence of another ovtopmd service. If an ovtopmd service was started outside of ovstart, the ovstop, ovstart, and ovstatus commands will not recognize this service. To prevent this problem, always start all NNM background services with the ovstart command and stop them with the ovstop command.

   If another application is using port 2532, continue with the next step.

2. Change the port number to any unused port by changing the entry for ovtopmd in %SystemRoot%\system32\drivers\etc\services (/etc/services):

   ```
   ovtopmd 2532/tcp  # OpenView IP Topology daemon
   ```

   Choose a number other than 2532 that does not conflict with other services listed in services (/etc/services).

3. Reconfigure NNM by typing the following commands:

   ovstop

   ovstart

4. If ovtopmd still fails to run successfully from ovstart, contact your HP support representative.

NOTE On UNIX operating systems only, if you are using the Network Information Service (NIS), make sure you update your NIS Master Server.

Once ovtopmd has been started through ovstart, you can verify that it is responding to requests by executing *install_dir*\bin\ovtopodump ($OV_BIN/ovtopodump). By default, ovtopodump will print a single line of output for each object in the topology. You can also get verbose listings and summary information. For more information see the *ovtopodump* reference page in NNM's online help (or the UNIX manpage). For example, if you type

ovtopodump -l

or, for remote collection stations

ovtopodump -c *nodename*

your result will look something like

```
TOPO OBJECT ID: 70
TIME CREATED: Fri Apr 10 14:52:02 1995
TIME MODIFIED: Fri Apr 10 14:52:02 1995
GLOBAL FLAGS:
NUMBER OF NETWORKS: 13
NUMBER OF SEGMENTS: 19
NUMBER OF NODES: 238
NUMBER OF INTERFACES: 281
NUMBER OF GATEWAYS: 21
```

This prints the summary information for the entire topology. If ovtopodump fails, this indicates some problem with ovtopmd. Try stopping all background services with ovstop, and then restarting them with ovstart.

If ovstart succeeds, but ovtopodump still fails, verify that at least one of the following is true:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1162
3740
Doc:

- The IP address of the loopback interface is `127.0.0.1`.
- There is an entry for `localhost` that has the correct address for the loopback interface.
- The IP address for the `localhost`'s hostname is correct. (That is, do an `ipconfig /all`, ping the hostname that was returned, and verify that the address returned is correct.)

  On UNIX operating systems only, do a `hostname`, and then look up that name with `nslookup`, and verify that the address returned is correct.

If `ovtopodump` still fails, contact your HP support representative.

In addition, `ovtopmd` maintains consistency with the object database maintained by `ovwdb`. You can use the `ovtopofix` command to do the following consistency checks and updates:

- Check object existence in both the topology and `ovwdb` databases.
- Ensure that the managed state is consistent.
- Remove incomplete interface objects and incomplete nodes created by the discovery process from the object database.
- Update the presentation time to force `ipmap` to update the object's status during map synchronization.
- Update the creation time of the object to force `ipmap` to add the object during map synchronization.

To run `ovtopofix` and check for problems, type

`ovtopofix -n`

To run `ovtopofix` and fix any problems found, follow these steps:

1. Exit `ovw` using the `Map:Exit` menu item.
2. Stop `netmon` by typing **`ovstop netmon`**.
3. Type **`ovtopofix`**.
4. Restart `netmon` by typing **`ovstart netmon`**.

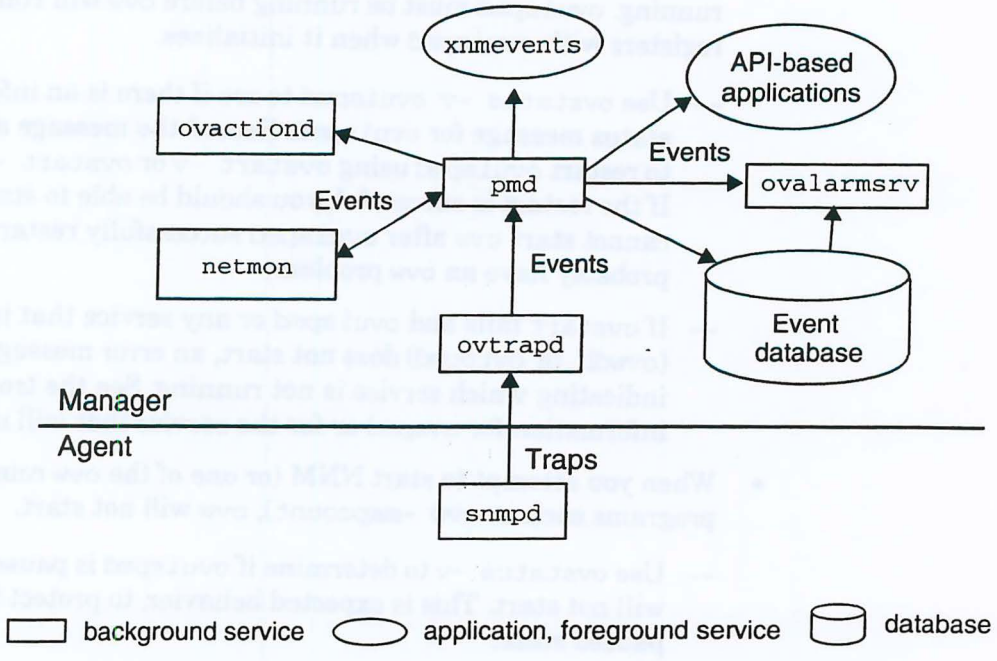
For more information, see the *ovtopofix* reference page in NNM's online help (or the UNIX manpage).

A license problem could also cause ovtopmd to fail. In this situation, verify that the license in *install_dir*\conf\.license ($OV_CONF/.license) is correct.

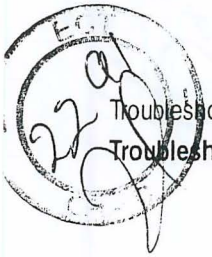
The ovtrapd Background Service

SNMP traps generated by an agent (snmpd in the case of the HP OpenView SNMP Agent) go to ovtrapd (via UDP port 162), which forwards them to pmd. ovtrapd acts as a buffer for traps that could potentially be dropped when pmd is busy. pmd logs and forwards the traps (in the form of an event) to netmon, ovactiond, ovtopmd, ipmap, and xnmevents (and potentially other subscribing applications). Figure C-2 illustrates this interaction.

Figure C-2 ovtrapd Event Interactions with SNMP Agent



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1163
3740
Doc:



The ovuispmd Background Service

You are most likely to see ovuispmd problems when you are trying to start ovw, since you cannot start ovw if ovuispmd is not running. You may also see ovuispmd problems when you use ovpause and ovresume, which are invoked when you perform a backup.

Problems that appear to be ovuispmd problems can actually be the result of:

- Problems with ovuispmd itself.
- Problems with one of the services on which ovuispmd depends.
- Problems with ovw, which depends on ovuispmd.

The easiest way to determine if the problem is with ovuispmd itself, or with another service, is to look at the symptom, as follows.

- When starting NNM, you get a dialog box saying that registration with the UI process manager failed. This is because ovuispmd is not running. ovuispmd must be running before ovw will run because ovw registers with ovuispmd when it initializes.
  - Use `ovstatus -v ovuispmd` to see if there is an informative exit status message for ovuispmd. Record the message and then try to restart ovuispmd using `ovstart -v` or `ovstart -v ovuispmd`. If the restart is successful, you should be able to start ovw. If you cannot start ovw after ovuispmd successfully restarts, then you probably have an ovw problem.
  - If `ovstart` fails and ovuispmd or any service that it depends on (ovwdb or ovtopmd) does not start, an error message will appear, indicating which service is not running. See the troubleshooting information for ovspmd or for the service that will not start.
- When you attempt to start NNM (or one of the ovw command line programs such as `ovw -mapcount`), ovw will not start.
  - Use `ovstatus -v` to determine if ovuispmd is paused. If it is, ovw will not start. This is expected behavior, to protect the NNM's paused state.

    It should not take long for ovpause to complete. If the pause was initiated by the automated backup program, you can determine how long the system has been paused from the log file, *install_dir*`\tmp\ovbackup.log` (`$OV_TMP/ovbackup.log`).

If the paused state persists and there is no ovbackup in progress you can attempt to ovresume the system. Do not do this if a backup is in progress because it can result in corruption of the data store copies that are being created.

- You attempt an ovpause or ovbackup.ovpl when an ovw command line client is running, and ovuispmd denies the pause. This is expected behavior. Under these conditions the command ovstatus ovuispmd tells you that ovuispmd's state is PAUSE_ERROR and ovuispmd's last message field indicates that it denied the pause because a command line client is running.

  To prevent database inconsistency or inaccurate reporting, ovuispmd denies a pause request if the pause request is received when one of ovuispmd's registered ovw services is an ovw that was invoked with the -mapcount, -deleteMap, or -copyMap option.

  — To resolve this problem, issue a new pause request after the ovw service terminates. These ovw command line services are designed to do specific, short tasks and then exit.

- There are ovw sessions that seem to be stuck pausing. If you have run ovbackup.ovpl and you find ovw sessions still paused after the background services have resumed, ovuispmd may have exited or been killed during the pause.

  If a resume request is issued when ovuispmd is not running, then ovw sessions will not be notified of the resume and will remain paused, even when the background services have resumed. When ovuispmd terminates ungracefully it leaves a state file containing information about the registered ovw sessions. You can examine this file in *install_dir*\conf\ovuispmd.state ($OV_CONF/ovuispmd.state). *Do not modify this file!* It is used by ovuispmd when it is restarted.

  — Use ovstatus to determine if ovuispmd is still running. If it is not running, restart it. When it initializes, it will automatically attempt to resume all of the ovw sessions that were registered with it when it terminated ungracefully.

- The ovw session information reported by ovuispmd is not correct. When you run ovstatus -v ovuispmd, it includes ovw sessions that are no longer running.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1164
Doc. 3740

Under some termination conditions, ovw sessions are unable to unregister with ovuispmd before they terminate. In those cases, ovuispmd's list of ovw sessions will not be corrected until ovuispmd attempts to communicate with the registered sessions.

— If no ovw sessions are running locally or remotely then it is safe to stop ovuispmd and restart it. Its ovw session information will be updated when it is restarted.

- ovuispmd exits ungracefully. This may be due to a termination signal from ovspmd.

  — See the *ovuispmd* reference page in NNM's online help (or the UNIX manpage) for information about forced termination. Also refer to the file *install_dir*\lrf\ovuispmd.lrf ($OV_LRF/ovuispmd.lrf) for useful comments about configuring the timeout field to prevent this occurrence.

- When you try to start ovw, ovw will not start or ovuispmd exits.

  — If ovuispmd is running but ovw does not start, or if ovw startup causes ovuispmd to abort, there may be useful information in the ovuispmd logging messages. The log messages may help you characterize the problem as an ovw problem, an ovuispmd problem, or an application problem.

  Detailed instructions for using the Windows Application Event Log and the UNIX operating tracing and logging facilities, nettl and netfmt, are found in this appendix in the section "Logging and Tracing" on page 639. Examine the logging output for ovuispmd errors in the OVEXTERNAL subsystem section. Also refer to the diagnostics in the *ovuispmd* reference page in NNM's online help (or the UNIX manpage).

The ovwdb Background Service

The ovwdb service controls the object database. Here are some problems that can be caused by ovwdb and possible solutions to the problems.

ovwdb should be running whenever NNM is running. Normally it is started through ovstart. To verify that it is up and running, type:

```
ovstatus ovwdb
```

You should see something like this:

```
object manager name:    ovwdb
state:                  RUNNING
PID:                    4115
last message:           Initialization complete.
exit status:            -
```

By default, ovwdb uses a TCP socket bound to port 9999. If ovwdb indicates an error attempting to bind to this port number because another application is already using it, follow these steps:

1. Make sure that you do not have another ovwdb service using port 9999. Check the /etc/services file for a listing of ports being used.

   The most common reason for errors binding to the TCP socket is the presence of another ovwdb service. If an ovwdb service was started outside of ovstart, the ovstop, ovstart, and ovstatus commands will not recognize this service. To prevent this problem, always start all NNM background services with the ovstart command and stop them with the ovstop command.

   If another application is using port 9999, continue with the next step.

2. Change the port number to any unused port by changing the entry for ovwdb in %SystemRoot%\system 32\drivers\etc\services (/etc/services).

   ```
   ovwdb    9999/tcp      # OpenView Object Database daemon
   ```

3. Reconfigure NNM by typing the following commands:

   ovstop

   ovstart

4. If ovwdb still fails to run successfully from ovstart, contact your HP support representative.

NOTE If you are using the Network Information Service (NIS), make sure you update your NIS Master Server.

If you notice a great deal of swapping and the system performance does not meet your expectations, you can do one of two things:

- Edit the *install_dir*\lrf\ovwdb.lrf ($OV_LRF/ovwdb.lrf) file to configure the maximum number of objects that will be in the ovwdb cache.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1165
3740
Doc:

- Change the system parameters (kernel parameters and regenerate the kernel). For more information, see "Improving Traffic Management and Performance" on page 654 in this appendix.

To verify the status of ovwdb, first run the `ovstatus -v` command to determine if everything is working correctly. If ovwdb stops running, netmon and ovtopmd will also stop running because these services are dependent on ovwdb. On UNIX operating systems only, if ovwdb is no longer running, check the `nettl` log using `netfmt`. Note that this assumes `nettl` was running when the problem occurred. To verify that `nettl` is running, execute the `nettl -status` command. See "Using nettl and netfmt (UNIX operating systems only)" on page 643 for more information on using `nettl`.

If you exhaust all available memory, the ovwdb service will stop running. To solve this problem, follow the suggestions described above for solving problems with excessive swapping; that is, either edit the `ovwdb.lrf` file or change the system (kernel) parameters.

If ovwdb stopped running due to memory problems, a disaster message will be logged into the Application Event Log (through `nettl`).

If the object database gets corrupted in any way, for example, by removing the files in the *`install_dir`*`\databases\ovwdb` (`$OV_DB/ovwdb`) directory, you need to restart the automatic map generation from the beginning.

The pmd Background Service

The pmd service is the postmaster background service. It provides event (trap) forwarding and message passing between services. When pmd receives an event, it forwards it to all the services that are registered to receive the event. Events are generated by these services:

- ipmap and ovtopmd when you edit the map or when nodes' status propagates to segments and networks.
- netmon, when it detects a change as a result of polling nodes or as a result of receiving a trap forwarded by pmd.
- ovtrapd, when ovtrapd receives a trap from agent services.
- ovtopmd, when topology changes occur.
- snmpCollect, when a threshold is exceeded or reset.
- ovevent, when this command is called from a batch file (shell script).

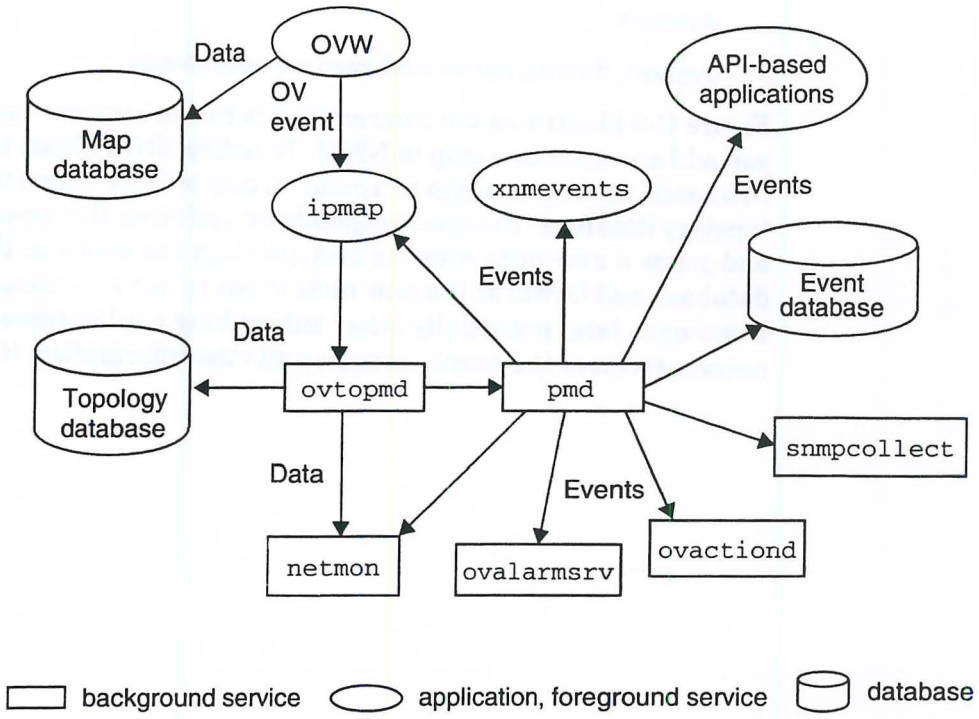
- Configuration operations such as `xnmloadmib`, `xnmtrap`, `xnmsnmpconf`, and `xnmcollect` when you edit configuration files.
- `ovrepld` as a result of a change detected on a remote collection station. Refer to *A Guide to Scalability and Distribution* for information on the `ovrepld` background service and collection stations.
- `ovspmd`, during pause and resume operations.

Figure C-3 illustrates the interactions between services and `pmd` when you add an object to a map in NNM. To notify NNM about the new object, `ovw` sends an `ovw` message to `ipmap`. `ipmap` tells `ovtopmd` to update the topology database. `ovtopmd` responds by updating the topology database and sends a new node event to `pmd`. `pmd` logs the event in the event database and forwards the new node event to `netmon`, `snmpcollect`, and `xnmevents` (and potentially other subscribing applications). When `netmon` receives the event, `netmon` pulls the information it needs from

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1166
3740
Doc:

the topology database through ovtopmd. When snmpCollect receives the event, it checks to see if the new node should be collected from (that is, whether it matches any configured IP wildcards).

Figure C-3 pmd Event Interactions



For a discussion of pmd's interactions and operation concerning events generated by netmon, see "The netmon Background Service" on page 587.

If you suspect a problem with the pmd background service, try the following actions to further isolate the problem:

- If pmd is not configured to write to eventdb, you'll first need to execute ovdumpevents to write the contents of the event database to a log file.
- Look for events logged to the event database, using xnmevents or the Alarm Browser.

- Add a node to the map and then check to see if the event was recorded in the event database, using `xnmevents` on a management station or the Alarm Browser through the Web UI.
- Run `ovstatus` and check the status of `pmd`. If the `pmd` service appears to be hung, stop the service using `ovstop` and restart all background services with `ovstart`.
- Check `pmd.log0` to see any messages related to the `pmd` service.
- Turn on tracing as described in the "Recommended Logging and Tracing Practices" on page 639 in this chapter. Your HP support representative can help you interpret the trace results.
- Verify that events can be generated. Use the `popupMsg` contributed script in `$OV_CONTRIB/NNM/popupMsg` to generate an event.

The ovrequestd Background Service

The `ovrequestd` service executes reports and data warehouse exports according to a predefined schedule. Once a report is configured, `ovrequestd` starts executing the exports and the reports.

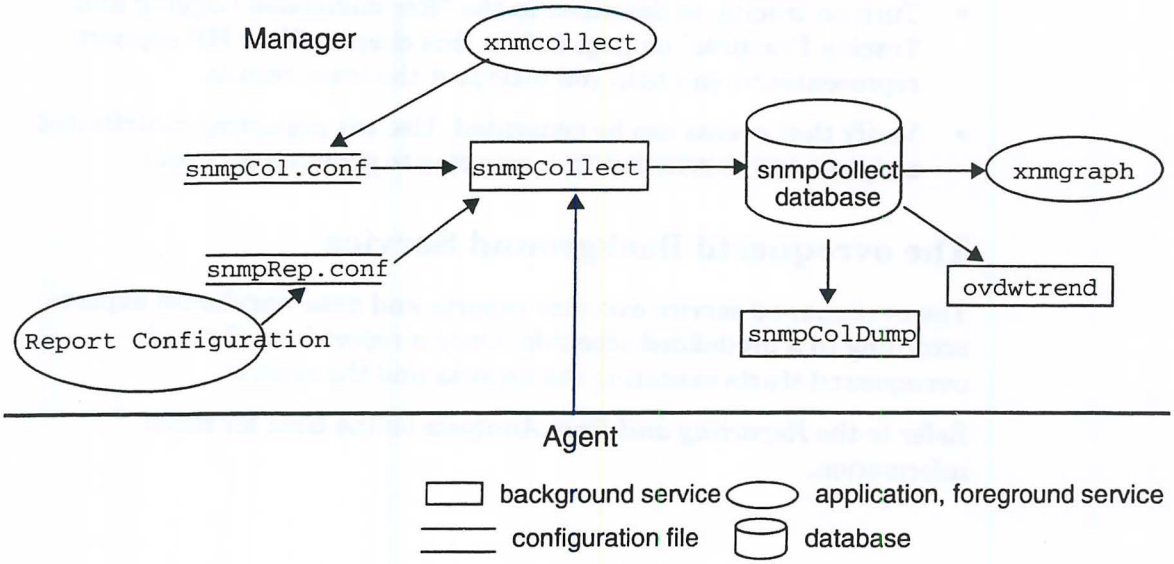
Refer to the *Reporting and Data Analysis* online book for more information.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1167
Doc: 3740

Troubleshooting Data Collector Problems

Figure C-4 shows the interactions among the services `xnmcollect`, `xnmgraph`, `snmpCollect`, `snmpColDump`, and an SNMP agent.

Figure C-4 snmpCollect Interactions with SNMP Agents



If you have problems collecting MIB data, check for these problems:

- The service for the data collector, `snmpCollect`, may not be running on the management station.
  - — Make sure that you are not out of disk space. The data collector stops running when the disk is full. See page 610 for information about what to do if the disk is full.
  - — Verify the `snmpCollect` service is running by executing the `ovstatus snmpCollect` command. If the `snmpCollect` service is not running, restart the data collector using the `ovstart` command.
- Data is not being collected from the node it should be or thresholds are not being generated.
  - — Make sure the target node supports SNMP.

ECT 2280

- Make sure the node is managed, or that the `-u` option to `snmpCollect` is used.
- Verify that the MIB object is configured for collection. Use the `Options:Data Collection & Thresholds:SNMP` menu item to verify the configuration.
- Verify that the target node is configured to collect data or generate threshold events. You can configure the node to collect data by explicitly specifying the node name, by specifying a wildcard, or by specifying the name of an ASCII file that contains the node name. Also, verify that the target node has not been excluded for collection. Use the `Options:Data Collection & Thresholds:SNMP` menu item to verify the configuration.
- Ensure that collections for the MIB object are not in `Suspended` state.
- Ensure that the desired instances are specified for the MIB object and node combination.
- Perform `Fault:Test IP/TCP/SNMP` on the collection in question. This checks the connection between the local management station and other SNMP nodes.
- If `sysObjectID` filtering is being used, make sure the correct `sysObjectID` is being used.
- See if other collections or thresholds from that node are working. If none are working, the problem is probably with the node. From the `Options:Data Collection & Thresholds:SNMP` window, select the MIB object, and then select `Actions:Show Data` to see if data is being collected from the node.
- Try to access the MIB object using the `Tools:SNMP MIB Browser` dialog box.
- Run `snmpCollect -S` and look at the *`install_dir`*`\log\(`$OV_LOG`)snmpCol.trace` file. This command lists the configuration of the data collection.
- Try turning on verbose tracing. Execute `ovstop snmpCollect`. Then execute `ovstart snmpcollect -V`. Check the output in the `snmpCol.trace` file.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1168
Doc: 3740

— If you expect threshold events to occur, but they do not, start a data collection on the MIB variable. The problem may be that the threshold value is not set correctly. For example, if the normal value for this variable is 20 and you set the threshold value to 100, you will probably never see a threshold event.

— If you can't resolve the problem, use the tracing command. To use the tracing command, try restarting the data collector with the same command as in the *install_dir*\lrf\snmpCollect.lrf (`$OV_LRF/snmpCollect.lrf`) file, but add the `-t` *filename* option. The `-t` option is a tracing option that logs the results to the *filename*. Run `snmpCollect -T` to toggle the tracing. To determine whether or not tracing is on, look at the trace file. See the *snmpCollect* reference page in NNM's online help (or the UNIX manpage) for more information.

— For more information about troubleshooting threshold events, see the section "Configuring Events" on page 631 in this appendix.

- The disk is full. The data collector stops running when the disk is full. To solve this problem and to prevent this problem from happening again, do the following:
  - Use `ovdwtrend -delpriorto` *date/time*. This command will export `snmpCollect` data to the data warehouse and then delete the `snmpCollect` data after it has been exported. See the *ovdwtrend* reference page in NNM's online help (or the UNIX manpage) for more information on using this command.
  - Free up disk space by removing files in the *install_dir*\databases\snmpCollect (`$OV_DB/snmpCollect`) directory. Note, however, when you remove files you lose the data you have saved. If you don't want to remove the whole file, you can edit the file and keep only the most recent data by deleting older entries in the file. Once you have freed up disk space, as `root` restart the data collector with the `ovstart` command.
  - Edit files in the *install_dir*\databases\snmpCollect (`$OV_DB/snmpCollect`) directory using the `snmpColDump` command. For example, to retain the last 100 entries of a file, use the following commands (available in the MKS Toolkit on a Windows operating system):

```
snmpColDump -tTI snmpCollect\filename\
awk -F\t '{printf("%d\t%d\t%s\t%lg\n", $4, $5, $6, $3)}' | \
  tail -100 > \tmp\save
snmpColDump -r \tmp\save install_dir\databases\snmpCollect/
```

On UNIX operating systems only:

```
snmpColDump -tTI $OV_DB/databases/snmpCollect/filename\
awk -F\t '{printf("%d\t%d\t%s\t%lg\n", $4, $5, $6, $3)}' | \
  tail -100 > /tmp/save
snmpColDump -r /tmp/save $OV_DB/databases/snmpCollect/
```

- If you want to stop all data collection, kill the `snmpCollect` service with the `ovstop snmpCollect` command, or suspend all data collections using the `Options:Data Collection & Thresholds:SNMP` menu item.

To prevent the problem in the future:

- Lengthen the polling intervals. Using the `Options:Data Collection & Thresholds:SNMP` menu item and set the polling interval to not collect as often. In addition, if you only want to check thresholds, don't store the data.
- Reduce the number of MIB objects you are collecting on.
- Reduce the number of nodes you are collecting on.
- Reduce the number of instances you are collecting for some or all nodes.
- Set up programs (`cron`) to periodically either remove files in the *install_dir*`\databases\snmpCollect` (`$OV_DB/snmpCollect`) directory or export and trim them with `ovdwtrend`.

- There is no response when querying DMI devices.
  - Make sure that DMI is configured correctly on the remote device.
  - The Data Collector supports only SNMP devices. Install an SNMP agent and a DMI-to-SNMP mapping agent on the DMI system.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1169
3740
Doc:

Set-community Name and Trap-dest Loss Upon Re-Installation

The emanate SNMP agent uses the following two configuration files in the *install_dir*\conf\SnmpAgent ($OV_CONF/SnmpAgent) directory:

- snmpd.cnf — the SNMPR-format emanate configuration file.
- snmpd.conf — the HP-format SNMPD configuration file.

emanate uses the union of configuration information from both files. However, some of the information is in both—sysDescr, sysName, sysContact, and sysLocation. When emanate starts up, it uses the snmpd.conf values (if defined) and copies them to snmpd.cnf; otherwise, it uses the values in snmpd.cnf.

The get-community, set-community, and trap-dest fields in snmpd.conf are not replicated in snmpd.cnf, so they are appended (in emanate run-time memory) to the set of configurations in snmpd.cnf because it is allowable to have more than one value for each.

Thus, upon installation, the default snmpd.cnf file is conditionally installed by Setup (only if one doesn't already exist)—but the default snmpd.conf file is always installed. After uninstallation and re-installation, the result is that sysContact and sysLocation get taken from the existing snmpd.cnf file, but the set-community and trap-dest are taken from the new/default snmpd.conf file (in which they are not defined).

The solution is to conditionally install snmpd.conf only when it does not already exist.

Troubleshooting Web Components

If you experience problems starting any of the web components, you should first check the following before doing further troubleshooting.

- Make sure that NNM is installed on the host specified in the URL, and that the host is running.
- Make sure that you are using a supported web server, and that it is configured properly and is running. Supported web servers include Microsoft Peer Web Services, Microsoft Internet Information Server, and Apache (shipped with NNM for UNIX operating systems.) Try entering the simplest URL (`http://hostname[:port]`) in the web browser and see if the server is accepting connections.
- Make sure that you are using a web browser that supports NNM. Supported web browsers include Netscape 4.6 or greater and Microsoft Internet Explorer 5.0 or greater.
- If starting the web component directly from a URL, make sure the full URL was entered correctly. If NNM is running on a UNIX operating system, check that port 3443 is specified in the URL.
- Make sure that the hostname in the URL is fully qualified. Do not use the short version of the hostname. For example, use `mysystem.home.com` instead of just `mysystem`.
- Exit and restart the browser, and then re-enter the URL.
- Clear the memory and disc caches for the browser, and restart the browser.

  In Netscape Navigator, select the `Edit:Preferences` menu item. In the dialog box, click on `Advanced`, then click on `Cache`. In the next dialog box, click on `Clear Disk Cache` and `Clear Memory Cache`.

  In Internet Explorer, select the `View:Internet Options` menu item. On the `General` page, select the `Temporary Internet Files` field. Then click on the `Delete Files` button.
- Check the contents of all of the web log files for possible errors.

  Windows:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1170
3740
Doc:

install_dir\www\logs\launcher\error_log
install_dir\www\logs\launcher\login_log
install_dir\www\logs\launcher\access_log

UNIX:

/var/opt/OV/www/logs/launcher/error_log
/var/opt/OV/www/logs/launcher/login_log
/var/opt/OV/www/logs/launcher/access_log

- If an http proxy server is in use, try disabling the web browser from using it.

  In Netscape, select the `Edit:Preferences` menu item. In the dialog box, click on `Advanced`, then click on `Proxies`. In the dialog box, select `Direct connection to the Internet`.

  In Internet Explorer, from the `General` page select the `View:Internet Options` menu item. On the Connection page, deselect `Access the Internet using a proxy server`.

- For errors in the Reporting interface, refer to the *Reporting and Data Analysis* online manual.

Language Selection Problems

NNM's web applications are available in English and Japanese. However, it is possible to integrate and use other web applications that have been translated into other languages while NNM's web applications remain in English. If you expect the web applications to be in a language other than English and they are not, it could be due to one of the following problems:

- If the strings are appearing in English, check the browser's language configuration.

  In Netscape, `Languages` is configured through the `Netscape:Preferences` menu item.

  In Internet Explorer, `Languages` is configured through the `Internet:Options` menu item.

  In both cases, the language that you expect to see should be listed at the top of the `Languages` window. To see NNM's web applications in Japanese, be sure that the Japanese entry (`ja`) is listed before the English entry (`en` or `en-us`). Restart the browser after making changes.

- If the non-English strings appear garbled in the window, check the following:

  — The browser's encoding or font configuration may be incorrect.

  In Netscape, the encoding is specified through the `View:Encoding` menu item.

  In Internet Explorer, the font is specified through the `View:Font` menu item.

  To choose Japanese, one of the Japanese fonts or encodings should be selected.

  — On UNIX systems only, the browser was not started with the correct environment variable settings.

  The browser process should be started with the correct `$LANG` setting. For Japanese, `XMODIFIERS` must also be set. These variables are usually set by the desktop environment.

  — On Japanese on UNIX systems only, the default codeset in use by the server may be incompatible with the Web applications.

  By default, NNM's web applications expect the data from the servers to be in Shift-JIS codeset for HP-UX and Windows operating systems. On Solaris, EUC is the default. Use the `ovchange_locale_mapping` command to switch the default configuration. See the *ovchange_locale_mapping* manpage for details.

HP OpenView Launcher

User Login Problems

If you expected to get a user login screen when the Launcher starts, but you did not, then the file `session.conf` probably has not been set up for user logins. See Chapter 14, NNM on the Web, for information on setting up users and logins.

If you get the user login screen and the Launcher does not accept the login, check the following:

- Make sure you typed the user name and password correctly.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1171
3740
Doc:

- Make sure the password file, `htpasswd`, includes the user name and password. See Chapter 14, NNM on the Web, for information on setting up the `htpasswd` file.
- If running NNM in a non-English language, be sure that the environment variable `XMODIFIERS` is set correctly.

Starting the Launcher

If you have problems starting the Launcher, check the error log file for potential errors. The Launcher error log records internal errors from the Launcher. You can use the output from this file when discussing a problem with the HP Response Center or support personnel.

If the error log file does not give you sufficient information for troubleshooting, you can set a parameter in the URL for `ovlaunch.exe` that will enable more in-depth error logging on a session level.

The parameter is:
`http://`*`hostname`*`:[`*`port`*`]/OvCgi/ovlaunch.exe?Debug=/tmp/`*`file`*

The output of this file is less "friendly" than other error log files, but it contains valuable information that may be useful to a support person who is trying to assess the problem.

If the Launcher does not start and you get an error message indicating that there is a CGI problem, then the problem could be with one of the Launcher's CGI programs. Try executing each of the following programs from the command line. These programs are located in:

Windows: `install_dir\www\cgi-bin`

UNIX: `/opt/OV/www/cgi-bin`

- `ovlaunch.exe`
- `ovlogin.exe`
- `ovsessioninfo.exe`
- `ovlaunchreg.exe`

You can tell if these programs are running if they output ASCII text to the screen. If one of these programs is not running, contact HP Support.

Launcher Window Problems

If the Launcher window comes up with no content (blank), it could be one of the following problems:

- The correct patches have not been installed on the system. Check the system requirements section of the Installation Guide.
- You could have a conflict if you had an older version of Netscape installed on your system. If you have set the `CLASSPATH` environment variable when running an older version of Netscape, it will cause Java access problems when you run the recommended version of Netscape. If you have set this variable, you should unset it before running the newer version of Netscape.
- You could have a Java applet problem. Check the Java log as follows:
  - In your web browser, check to see that the items Java and Java script are enabled. In Netscape Navigator, check this by using `Edit:Preferences->Advanced`. In Internet Explorer, check this by using `View:Advanced`.
  - Bring up a Java console and view the messages it contains. In Netscape Navigator, use `Window:Java Console`. In Internet Explorer, use `View:Java Console`.
  - Try starting the Launcher without going through a proxy.

    In Internet Explorer, select the `View:Internet Options` menu item. Choose the `Connection` tab, then turn off the proxy server.

    In Netscape Navigator, select the `Edit:Preferences` menu item, choose `Advanced`, and disable the proxy server.
  - The Java console also provides a method of logging information about the Java virtual machine interpretation of the Java code that is executing. Both of the supported web browsers allow you to turn on Java error logging from the browser menu. In Netscape Navigator, look under the `Window` menu item. In Internet Explorer, select the `View:Internet Options` menu item under the `Advanced` tab.

If you encounter errors when reading in registration files, run the `regverify` command in *`install_dir`*`\bin\` (`$OV_BIN`) against the Launcher Registration File (WLRF) in the following directory:

Windows: *`install_dir`*`\www\registration\launcher\%LANG%`

UNIX: `/etc/opt/OV/share/www/registration/launcher/$LANG`

You can also hold down the **Shift** key and press the `[Reload]` button on your browser to force the registration files to reload.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1172
3740

Other Sources of Information

Web server log files are available that provide you with information about server-related problems. The error log is located at:

Windows: `\WINNT\System32\Logfiles`

UNIX: `/opt/OV/httpd/logs`

This is the default location, but it may vary depending on where your web service is set to log errors. Check your web server properties to verify the location.

Network Presenter

If the Network Presenter does not start, check the items on page 613, and the following:

- If the Network Presenter progress bar does not appear, it could indicate web server problems. Try connecting to the web server from your browser without starting Network Presenter. For example:

`http://hostname:3443`

- Make sure the Network Presenter is registered with NNM. In NNM on a management station, use the `Help:About HP OpenView` menu. In the dialog box, click `Applications`. Verify that the Network Presenter appears in the list. Alternatively, check the registration directory to ensure that the file `netpresenter` appears. The location is:

  Windows: *`install_dir`*`\share\registration\%LANG%`

  UNIX: `/etc/opt/OV/share/registration/$LANG`

- Make sure that NNM is running on the management station, with the map opened to which the Network Presenter is trying to connect.
- If you tried starting the Network Presenter from the `Tools` or the `Objects` selection in the Launcher, try starting it directly from the URL instead.

If there are missing menu bar or toolbar items, do the following:

- Check the permissions on the registration files registered with Network Presenter. The permissions need to be read by all, and the owner and the group should be set to `bin`. The registration files are located in:

C Troubleshooting NNM Itself

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1173
3740
Doc:

This appendix describes measures that you can use to identify and troubleshoot system and software problems that may occur during Network Node Manager operations. These measures include the following:

- General network management troubleshooting considerations (page 579).
- Characterizing various types of problems (page 582).
- Troubleshooting background services (processes), such as `netmon` and `ovtopmd` (page 584).
- Troubleshooting the Web applications (page 613).
- Troubleshooting various operations, such as MIBs and runtime components (page 623).
- Troubleshooting Windows operating system applications (page 637).
- Recommended practices for logging and tracing (page 639).
- Improving performance and traffic management (page 654).

These measures are not intended to be used for troubleshooting your network problems, but are only for system and software problems related to NNM operations.

Most of the steps you will take in troubleshooting NNM are the same for NNM on either a Windows or UNIX operating system; however, some files and services are different. In addition, there are considerations to NNM on Windows operating systems that do not apply to NNM on UNIX operating systems, and vice versa.

NOTE For troubleshooting NNM's databases and the data warehouse, refer to the online manual *Reporting and Data Analysis with HP OpenView Network Node Manager*.

General Troubleshooting Considerations

Consider the following when troubleshooting NNM:

- Network Node Manager is memory and page-file (swap-space) intensive. Problems may be due to resource exhaustion. Refer to "Performance" on page 656 for memory conservation tips.
- If you are using the Berkeley Internet Name Domain (BIND) Service on your network, each `gethostbyaddr` request for the hostname of a host with multiple IP addresses could return a different hostname.

When You Need More Information

Other information that may assist your troubleshooting is available in the following locations:

- The release note files (see page 71).
- The NNM online help.
- The Request for Comment (RFC) documents referenced in the introduction to this book (see page 33).

If a problem does not appear to be with the network management products themselves, see the following:

- Networking documentation for general network troubleshooting procedures.
- System documentation for system troubleshooting procedures.
- On UNIX operating systems only, X Windows documentation for X Windows troubleshooting procedures.

Preventive Practices

Following these recommended practices can help you prevent problems:

- Ensure that the management station meets the hardware, software and configuration prerequisites and recommendations.
- Maintain the system by regularly editing and deleting files. See Chapter 15 for maintenance tasks.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1174
3740
Doc

- Ensure that *install_dir*\bin\ ($OV_BIN) is in your path.
- On a UNIX operating system, source /opt/OV/bin/ov.envvars.sh into your environment.
- On a Windows operating system, source *install_dir*\bin\ov.envvars.bat into your environment.
- Do not modify Network Node Manager product files without retaining the original files. The original files provide a way of restoring a known good operational configuration. If you correct a problem by restoring the original files, you can isolate the problem to one of the changes you made to these files.

  When you back up original files, do not copy the files to a new file name in the same directory. All files in the following directories are considered "live;" that is, every file in these directories will be used and you will end up with duplicate definitions.

  install_dir\registration\ ($OV_REGISTRATION)
  install_dir\fields\ ($OV_FIELDS)
  install_dir\symbols\ ($OV_SYMBOLS)
  install_dir\bitmaps\ ($OV_BITMAPS)
  install_dir\conf\ ($OV_CONF)
  install_dir\help\ ($OV_HELP)
  install_dir\tmp\ovbackup ($OV_TMP/ovbackup)

  See the backup procedure in Chapter 6 for complete guidelines and procedures for backing up your files.
- Make sure that you are not using up too much of your management station's CPU and network resources by collecting too much MIB data or setting too frequent polling intervals for the netmon service. Use Performance:Network Polling Statistics to gauge how effectively netmon is collecting network data.
- Use logging and tracing of background services to help isolate problems, but be sure to clean up log and trace files regularly. For more information see "Recommended Logging and Tracing Practices" on page 639" in this appendix.
- Use ovstatus -c -v to check the status of background services and OVW sessions.
- Use ovstart -c to track the progress of the services being started by ovspmd.

- Use the `-d` option to `ovstart`, `ovstop`, `ovpause`, and `ovresume` to get additional debugging information.
- Use the `-verify` option to `ovw`. This option checks the syntax for all the installed application, symbol type, and field registration files. It also verifies the semantics of the application registration files and reports conflicts among application registration information. When started with this option, NNM does not start a normal "windowed" session; rather, it displays status messages in a text window.
- Use the `-mapcount` option to `ovw`. This option checks the consistency between the map database maintained by NNM and the object database maintained by `ovwdb`.
- Be careful when changing the permissions on files used by the management software. Restricting access could cause management services to be unable to access the file.
- On UNIX operating systems only, HP recommends that you not modify the files in `$APP_DEFS`. Instead, you can override the default X resources by modifying them in your `$HOME/.Xdefaults` file. If you are running HP VUE, modify your VUE resources. See `$APP_DEFS/XNm` for more details.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1175
3740

Characterizing the Problem

Symptoms are visible conditions that indicate a problem. Whenever you encounter a symptom, collect the basic information described in the following subsections. The problem can usually be characterized in one or more of the following ways: scope of the problem, what changed just before the problem occurred, duration of the problem, and what action was performed when the problem occurred.

Distinguish Local versus Remote Problems

If you suspect a problem on a remote node or agent system, try to duplicate it on a local node or management station, and vice-versa. If you cannot duplicate the problem on the local node, the problem is probably associated with the remote node. If you can duplicate the problem on the local node, the problem may be in the management station or somewhere in the link, or may be a problem common to the agents.

Remote Nodes' Level of Manageability

What type of remote node are you trying to communicate with when the problem occurs?

The amount of information that NNM can collect depends on whether a remote node:

- Supports SNMP or not (or is proxied).
- Supports all the mandatory objects in MIB-II.
- Supports a partial, full, or extended (non-standard) MIB.
- Is an HP node or not.
- Is a TCP/IP node or not.
- Is an IPX node or not.
- Is an IPX router/server or not.

The management station gets the most information from an HP SNMP node, less information from other SNMP nodes, least information from non-SNMP and TCP/IP nodes, and no information from non-SNMP and non-TCP/IP nodes.

Context: What Changed?

Determine what may have changed recently on your network or product configuration: hardware, software, files, security, utilization, etc. Keep a record of the software patches you install, so you can undo the changes in the order they occurred.

Also determine what is unique about a particular node that is having problems.

Duration: How Long or How Often?

Is the problem consistent (fails every time) or intermittent (fails sometimes)?

Context: What Action Was Performed?

When the problem occurred, what was happening? For instance:

- What operation was selected?
- What command was executed?
- What mouse operation was performed?
- What data was requested or sent?
- Was an alarm generated?
- Was an error or warning logged through the Windows Application Event Log (or `nettl`)?
- Was an error or warning logged through `ovconsole`, or the window from which `ovw` was started?
- Does `ovstatus -c` show all background services running?
- Does `ovstatus -v ovuispmd` list all of the OVW services that are expected to be running?

RQS nº 03/2005 - CN - CPMI 583 CORREIOS
Fls. Nº 1176
3740
Doc:

Troubleshooting Background Services

This section explains the background services of NNM and suggests actions to take if you have problems with one of the following background services. The background services are:

- hpptd
- netmon
- ovactiond
- ovalarmsrv
- ovcapsd
- ovrepld
- ovrequestd
- ovtopmd
- ovtrapd
- ovuispmd
- ovwdb
- pmd
- snmpCollect

In addition to explaining the background services, this section explains how to troubleshoot ovspmd, the service that monitors and controls the background services.

The background services and ovspmd should always be running whenever NNM is running. Normally, the background services are started through ovstart. See the *ovstart* reference page in NNM's online help (or the UNIX manpage) for all the options to ovstart. It may be particularly useful to use the -c or the -d options when troubleshooting.

To verify that the background services are running, enter the following:

```
ovstatus -c
```

See the *ovstatus* reference page in NNM's online help (or the UNIX manpage) for all the options to ovstatus.

The result should look similar to the following:

```
Name            PID   State       Last Message(s)
OVsPMD         3676   RUNNING     -
ovsessionmgr   3677   RUNNING     Initialization complete.
ovwdb          3678   RUNNING     Initialization complete.
ovuispmd       3701   RUNNING     Initialized. 1 ovw clients registered.
ovtrapd        3698   RUNNING     Initialization complete.
ovactiond      3699   RUNNING     Initialization complete.
ovalarmsrv     3700   RUNNING     Initialization complete.
pmd            3679   RUNNING     Initialization complete.
ovdbcheck      3680   RUNNING     Connected to embedded database.
ovrequestd     3681   RUNNING     Initialization complete.
httpd             -   unknown     (Does not communicate with ovspmd.)
ovtopmd        3697   RUNNING     Connected to native database "openview".

netmon         3702   RUNNING     Initialization complete.
snmpCollect    3703   RUNNING     No values configured for collection.
```

If ovstatus indicates that an object manager was not found, the problem may be caused by one of the following:

- The ovspmd configuration has been incorrectly modified or is corrupted. If the ovspmd configuration is corrupted, see "The ovspmd Background Service" on page 592.
- The executable file has been removed or moved from its expected location. ovsuf either has a pathname to each executable or expects them to be in *install_dir*\bin\ (%OV_BIN%). Make sure they exist where they are supposed to be.

If ovstatus indicates that a service is in a paused state, it may mean that a backup is currently being performed, or that the service did not restart as expected after a backup. In that case, the state will be one of the following: PAUSED, RESUME_ERROR, or DEPENDENCY_ERROR. In this case, check the backup log in *install_dir*\tmp (%OV_TMP%) to determine the cause of the error. You can then stop all services using ovstop, and restart all the services by typing:

```
ovstart -c
```

Some of the background services depend on other services to operate properly. Table C-1 shows the dependencies.

Table C-1 Background Service Dependencies

Background Service	Dependencies
httpd	no dependencies

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1177
3740
Doc:

Table C-1 Background Service Dependencies

Background Service	Dependencies
netmon	ovwdb, pmd, ovtopmd
ovactiond	pmd
ovalarmsrv	pmd
ovcapsd	ovwdb, pmd, ovtopmd
ovdbcheck	none
ovrepld	pmd, ovtopmd
ovrequestd	none
ovtopmd	ovwdb, pmd, snmpd
ovtrapd	pmd
ovuispmd	ovwdb, ovtopmd
ovwdb	no dependencies
pmd	snmpd
snmpCollect	ovwdb, pmd, ovtopmd

For problems with individual background services, see the appropriate subsection in this appendix on how to troubleshoot a specific background service.

The httpd Background Service

The `httpd` service handles http (web) requests. It is provided only on UNIX operating system installations of NNM. Here are some problems that can be caused by `httpd` and possible solutions to those problems.

`httpd` should be running wherever NNM is running. Normally it is started by `ovstart`. To verify that it is running, type:

```
ovstatus httpd
```

You can also see if `httpd` is running by typing **`ps -elf | grep httpd`** on UNIX operating systems. You should see multiple copies of `httpd` running, since the parent `httpd` service spawns multiple children to improve performance in handling `httpd` requests.

If `httpd` is running, you can validate that it is running correctly by entering the following into your web browser:

`http://`*`hostname`*`:3443/`

You should see a short web page with the title "It Worked!"

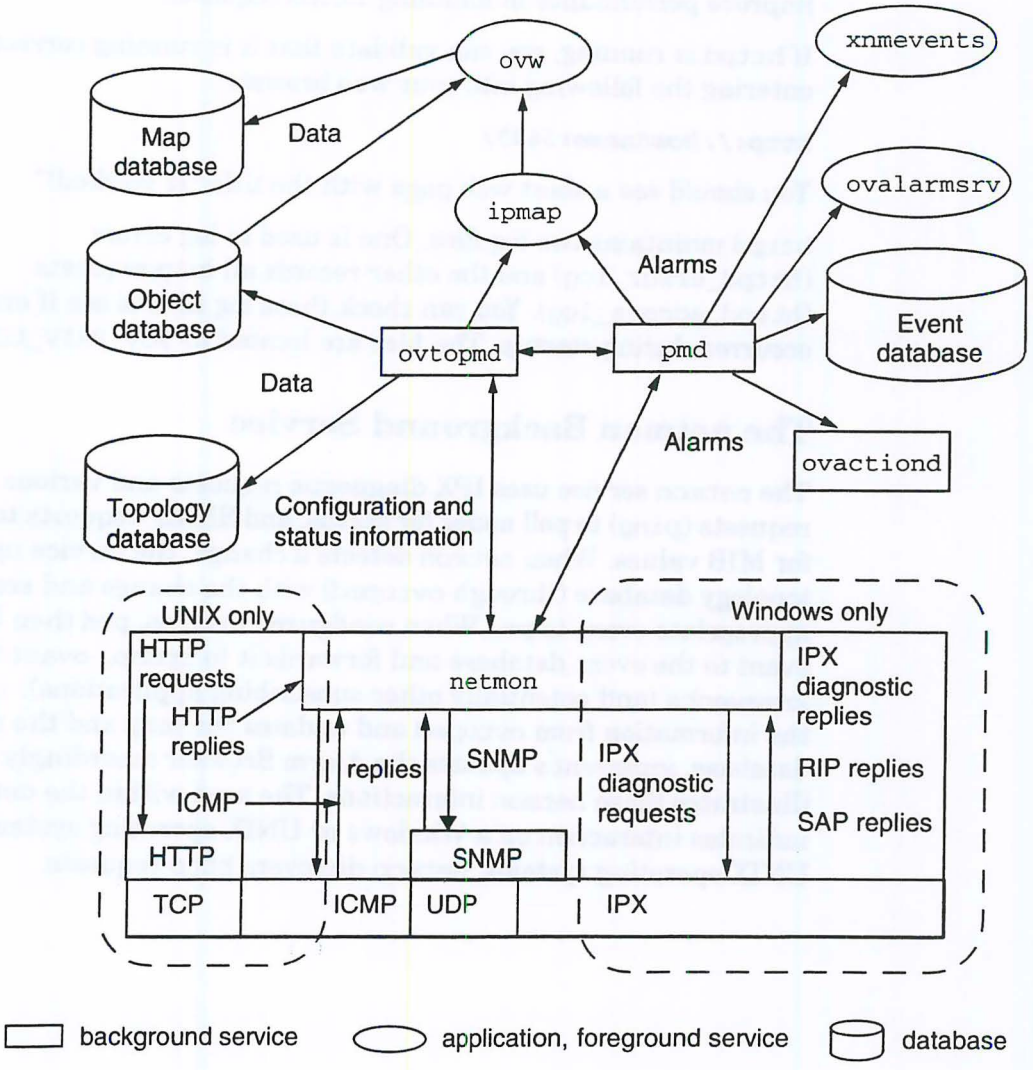
`httpd` maintains two log files. One is used to log errors (`httpd_error_log`) and the other records all http requests (`httpd_access_log`). You can check these log files to see if errors occurred during startup. The files are located in `$OV_PRIV_LOG`.

The netmon Background Service

The `netmon` service uses IPX diagnostic requests and various ICMP requests (`ping`) to poll nodes for status, and SNMP requests to poll nodes for MIB values. When `netmon` detects a change, the service updates the topology database (through `ovtopmd`) with the change and sends the appropriate event to `pmd`.When configured to do so, `pmd` then logs the event to the event database and forwards it to `ipmap`, `ovactiond`, and `xnmevents` (and potentially other subscribing applications). `ipmap` gets the information from `ovtopmd` and updates the map and the map database. `xnmevents` updates the Alarm Browser accordingly. Figure C-1 illustrates these `netmon` interactions. The area within the dotted oval indicates interaction on a Windows or UNIX operating system only. On UNIX operating systems, `netmon` discovers `http` requests.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1178
3740

Figure C-1 netmon Interactions



You can control `netmon`'s polling through the map's `Options:SNMP Configuration` and the `Options:Network Polling Configuration:IP/IPX` menu item. The `SNMP Configuration` menu item modifies the *`install_dir`*`\conf\ovsnmp.conf_db` (`$OV_CONF/ovsnmp.conf_db`) database. The `Network Polling` menu item stores `netmon`'s polling intervals in the

install_dir\conf\polling ($OV_CONF/polling) file. Do not modify this file directly; use the command line options to the program xnmpolling.

The xnmevents service checks every five minutes to see if netmon and snmpCollect are running. If either service is not running, xnmevents will display a dialog box and report the inactive service. (For information on changing the five-minute default polling interval or on disabling this polling feature, see the System Registry on Windows operating systems, or the file /usr/lib/X11/app-defaults/XNmevents on UNIX operating systems.

Status polling is scheduled on a per node basis, but is not deterministic. Therefore, polling of a node may not occur when scheduled if netmon gets behind due to its polling load for a particular time interval. Also, polling of manually added nodes and nodes changed from unmanaged to managed may not occur immediately after they are added or managed.

While you are unmanaging a network or segment during active discovery, a few managed nodes may appear on that network. To avoid this problem, do one of the following:

- Wait until the program finishes active discovery of the map.
- Turn polling off while unmanaging the network.

Only one instance of netmon may run on the management station; the *install_dir*\conf\ ($OV_CONF) netmon.lock file enforces this restriction.

The following tools can help you troubleshoot netmon problems.

- Use the Fault:Network Connectivity:Poll Node or Status Poll menu item to test or cause immediate netmon polling activity to a node.
- Use ovdumpevents to check for netmon service errors.
- Use the Performance:Network Polling Statistics menu item to determine if netmon is able to perform its polling at the configured frequency. See the online help for an explanation of the output of this menu item.
- Use netmon tracing to help isolate problems. For information see "Logging and Tracing" on page 639, or see the *ovstatus* reference page in NNM's online help (or the UNIX manpage).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1179
3740
Doc:

Auto-configuration of SNMP Traps

When netmon detects a node running an HP OpenView SNMP agent, it attempts to add the IP address of the NNM system to the trap destination table using an SNMP set request. In order for this to work, the NNM system must be configured with the correct SNMP set community name using Options:SNMP Configuration.

The ovactiond Background Service

The ovactiond service is started when you start NNM. It receives events from pmd that have automatic actions defined. For each of these actions, ovactiond formats the command string, then passes it on for interpretation and execution.

When you configure events using the Options:Event Configuration menu item in NNM, you are configuring ovactiond. If the result of your configuration of events is not what you expected, you can check the status of ovactiond.

Use the command ovstatus ovactiond to see if the service is running. ovactiond requires that pmd is running, so you should also check the status of pmd.

You can check the log file ovactiond.log for error messages. The file is located in:

Windows: *install_dir*\logs

UNIX: $OV_LOG

The ovalarmsrv Background Service

The ovalarmsrv service is started when you start NNM, and is the service that forwards events to xnmevents on NNM on a management station, and to NNM's web-based Alarm Browser. ovalarmsrv relies on pmd to be running; therefore, if you have problems starting xnmevents or the Alarm Browser, first check to see if pmd is running using ovstatus pmd.

You can also check the status of ovalarmsrv by using the ovstatus command. If ovstatus shows that ovalarmsrv is not running, and it will not start using ovstart ovalarmsrv, check to see if the service is running but ovstatus is not reporting it.

On UNIX operating systems, type

ps -elf | grep ovalarmsrv.

On Windows operating systems, use the Task Manager. If you find an ovalarmsrv service running, kill that service and restart ovalarmsrv using **ovstart ovalarmsrv**.

If you still have problems starting ovalarmsrv, be sure that you do not have a port conflict. ovalarmsrv uses two ports for communications. You can check those values in the /etc/services file. Make sure that another application is not using one of the ports assigned to ovalarmsrv.

ovalarmsrv reads alarms from the event database, receives new alarms from pmd, and maintains the state of all user modifications (for example, acknowledge, delete, etc.) to presented alarms. If the event database or the state file have somehow become corrupted, or if the file permissions have changed such that those file can't be read, you will not receive any data in xnmevents or the Alarm Browser.

You can also check the ovalarmsrv log file, ovalarmsrv.trace for error and tracing messages. The file is located in:

Windows: *install_dir*\logs

UNIX: $OV_LOG

The ovcapsd Background Service

The ovcapsd service checks newly-discovered nodes for Remote Desktop Management Interface (remote DMI or RDMI) and Hypertext Transfer Protocol (HTTP) capabilities. It periodically rechecks all Normal-status nodes. Capabilities are stored in the ovwdb database. ovcapsd gets IP and IPX address information for nodes from ovtopmd.

See the *ovcapsd* reference page in NNM's online help (or the UNIX manpage) for the most complete information available. Here are two important troubleshooting tips:

- ovcapsd checks nodes' capabilities after netmon has added them to the topology database. It might not have checked a node before the node appears in your ovwdb database or your map. If you search on a capability such as isHTTPSupported, ovcapsd might not yet have had a chance to check the node in which you're interested. You can run ovcapsd from the command line to check individual nodes synchronously. Also, ovcapsd can be made to check nodes faster by

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1180
3740
Doc:

increasing the number of threads it creates to check the nodes. See the *ovcapsd* reference page in NNM's online help (or the UNIX manpage) for more information.

- See the *install_dir*\log\ovcapsd.log file for ovcapsd service errors and on-exit messages.

The ovspmd Background Service

The ovspmd service monitors and controls the NNM background services. These background services are designed to run as children of ovspmd. The ovspmd service should be running whenever the background services are running. Normally, ovspmd is started by ovstart.

To verify the status of the services, type:

```
ovstatus -c
```

If ovstatus provides output indicating that all services are running, the problem is not ovspmd. If you do not receive the expected output, either ovspmd has a communication problem or the ovspmd service is not running. If the output indicates that ovsmpd is not running, start it using ovstart ovspmd.

Determining ovspmd Problems

You need to determine whether the problem is related to ovspmd or to a background service. If you determine you have an ovspmd problem, you need to determine what type of problem it is. Here are some indications of ovspmd problems:

- If the ovstatus output indicates that one of the background services is not running, type

  ```
  ovstart -v
  ```

  This should start any service that is not running. If any service fails to start, an error message will appear, indicating which service is not running. If this happens, use the Task Manager on a Windows operating system.

  On UNIX operating systems only, type **ps -ef** to list currently running services.

  Do *one* of the following:

— If the output indicates a certain service is running, but ovspmd says the service is not running (using ovstatus or ovstart), ovspmd does not know that service is running. This problem can occur when ovspmd is shut down unexpectedly.

— If the output indicates that a certain service is not running, that service has a problem. See the troubleshooting section for that service.

When you run ovstart, the error message you receive about the service should provide information that will help resolve the problem.

- If you receive an ovspmd error message in the following format:

```
ovspmd:conf\ovsuf: error message
($OV_conf/ovsuf: error message)
```

you may have a corrupt ovsuf configuration file.

On UNIX operating systems only, go to the next section "Recreating the ovspmd Sockets Directory (UNIX operating systems only)".

- On UNIX operating systems only, if you receive *one* of the following error messages

```
ovstart: ovspmd is not running.It may have failed to start.
ovstart: unable to contact ovspmd: error message
```

you need to verify that the ovspmd sockets directory exists. Go to "Recreating the ovspmd Sockets Directory (UNIX operating systems only)" below.

Recreating the ovspmd Sockets Directory (UNIX operating systems only)

This section is for UNIX operating systems only. If you are using NNM on a Windows operating system, see the section "The netmon Background Service" on page 587.

Use this procedure when ovstart is unable to start or connect to the ovspmd service.

1. Verify that the $OV_SOCKETS directory still exists. ovspmd creates the OVsPMD_MGMT and OVsPMD_REQ socket files in this directory, which enable ovspmd to communicate with the other background services. If this directory no longer exists, recreate it by typing

```
mkdir $OV_SOCKETS
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1181
3740
Doc:

2. Find out if any of the background services are running by typing

   ps -ef

3. Kill all the NNM background services that are running using the `kill` command. *Do not* use `kill -9`. For a list of the services, see "Troubleshooting Background Services" on page 584 in this appendix.

4. To restart the services and verify that they are starting properly, type

   ovstart -c

The ovrepld Background Service

`ovrepld` is a service that manages the discovery and monitoring of objects done on behalf of the local management station by remote collection stations. This remote topology information is merged with information obtained locally by `netmon` to create a more comprehensive topology database. If objects known to be present on remote collection stations are not appearing on your map, or are not being updated as expected, it is possible that `ovrepld` has stopped functioning.

Use `ovstatus ovrepld` to determine if `ovrepld` is running. If it is not, you can start it using `ovstart ovrepld`. In addition, `ovrepld` relies on `pmd` and `ovtopmd` to be running, so check to be sure that those services are also running.

`ovrepld` writes errors to a log file, `ovrepld.log`. The file is located in:

Windows: *`install_dir`*`\logs`

UNIX: `$OV_LOG`

The ovtopmd Background Service

The `ovtopmd` service is responsible for maintaining the topology database that is used by `netmon` and `ipmap`. It provides both enforcement of rules for correctness of the IP topology, and caching of the data to improve the performance of the system.

`ovtopmd` should be running whenever NNM is running. Normally it is started through `ovstart`. To verify that it is up and running, type

ovstatus ovtopmd

You should see something like this:

```
object manager name:    ovtopmd
state:                  RUNNING
PID:                    4119
last message:           Connectedto native database "openview"
exit status:            -
```

If ovstatus gives an error similar to this:

```
ovspmd:install_dir\conf\ovsuf:object manager ovtopmd not found
($OV_CONF/ovsuf:object manager ovtopmd not found)
```

The problem may be that the ovspmd configuration is corrupted. If the ovspmd configuration is corrupted, see "The ovspmd Background Service" on page 592 in this appendix.

If ovstatus reports the following message:

```
Running. Lost connection to master agent.
```

This could indicate that ovtopmd is still executing, but has lost its connection to the master SNMP agent (snmpd). Usually this is because the master agent (snmpdm) exited or has been shut down.

Restart the master agent on the Windows operating system using the Services applet in the Control Panel. Start the SNMP EMANATE Master Agent and SNMP EMANATE Adapter for NT/2000 services.

On UNIX operating systems only, restart snmpd by executing

```
/usr/sbin/snmpd
```

If the master agent is executing, try executing the following commands:

```
ovstop ovtopmd
```

```
ovstart ovtopmd
```

If ovstatus knows about ovtopmd, but indicates that it is not running, enter the following:

```
ovstart -c
```

Normally, this should start ovtopmd and all background services on which ovtopmd depends. In particular, ovtopmd depends on ovwdb and pmd being started. If ovwdb does not start, ovtopmd will not be able to execute successfully. In addition to ovwdb executing, ovtopmd relies on the field definitions being loaded into ovwdb, which normally happens through the configuration scripts at installation time.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1182
3740
Doc:

If ovtopmd gives an error indicating that it was unable to map a field name into a field ID, do the following:

- Verify that $LANG is set correctly and that the *install_dir*\fields\C ($OV_FIELDS/$LANG) directory exists and contains at least the following files: ovw_fields, ip_fields, snmp_fields, topm_fields, and misc_fields. The $LANG environment variable provides support for localizing native languages. If not otherwise defined, $LANG is assumed to be C, which means that no native language support is provided. (UNIX systems only: For more information on native language localization, see the *lang* manpage.)
- Type the following commands:

  ```
  ovstop -c
  ovstart ovwdb
  ovw -fields
  ovstart -c
  ```

  This should load any necessary field definitions into ovwdb, and then start ovtopmd and netmon (as well as any other background services).

By default, ovtopmd uses a TCP socket bound to port 2532. If ovtopmd indicates an error attempting to bind to this port number because another application is already using it, follow these steps:

1. Make sure that you do not have another ovtopmd service using port 2532.

   The most common reason for errors binding to the TCP socket is the presence of another ovtopmd service. If an ovtopmd service was started outside of ovstart, the ovstop, ovstart, and ovstatus commands will not recognize this service. To prevent this problem, always start all NNM background services with the ovstart command and stop them with the ovstop command.

   If another application is using port 2532, continue with the next step.

2. Change the port number to any unused port by changing the entry for ovtopmd in %SystemRoot%\system32\drivers\etc\services (/etc/services):

   ```
   ovtopmd 2532/tcp  # OpenView IP Topology daemon
   ```

   Choose a number other than 2532 that does not conflict with other services listed in services (/etc/services).

3. Reconfigure NNM by typing the following commands:

   ovstop

   ovstart

4. If ovtopmd still fails to run successfully from ovstart, contact your HP support representative.

NOTE On UNIX operating systems only, if you are using the Network Information Service (NIS), make sure you update your NIS Master Server.

Once ovtopmd has been started through ovstart, you can verify that it is responding to requests by executing *install_dir*\bin\ovtopodump ($OV_BIN/ovtopodump). By default, ovtopodump will print a single line of output for each object in the topology. You can also get verbose listings and summary information. For more information see the *ovtopodump* reference page in NNM's online help (or the UNIX manpage). For example, if you type

ovtopodump -l

or, for remote collection stations

ovtopodump -c *nodename*

your result will look something like

```
TOPO OBJECT ID: 70
TIME CREATED: Fri Apr 10 14:52:02 1995
TIME MODIFIED: Fri Apr 10 14:52:02 1995
GLOBAL FLAGS:
NUMBER OF NETWORKS: 13
NUMBER OF SEGMENTS: 19
NUMBER OF NODES: 238
NUMBER OF INTERFACES: 281
NUMBER OF GATEWAYS: 21
```

This prints the summary information for the entire topology. If ovtopodump fails, this indicates some problem with ovtopmd. Try stopping all background services with ovstop, and then restarting them with ovstart.

If ovstart succeeds, but ovtopodump still fails, verify that at least one of the following is true:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1183
3740
Doc:

- The IP address of the loopback interface is `127.0.0.1`.
- There is an entry for `localhost` that has the correct address for the loopback interface.
- The IP address for the `localhost`'s hostname is correct. (That is, do an `ipconfig /all`, ping the hostname that was returned, and verify that the address returned is correct.)

  On UNIX operating systems only, do a `hostname`, and then look up that name with `nslookup`, and verify that the address returned is correct.

If `ovtopodump` still fails, contact your HP support representative.

In addition, `ovtopmd` maintains consistency with the object database maintained by `ovwdb`. You can use the `ovtopofix` command to do the following consistency checks and updates:

- Check object existence in both the topology and `ovwdb` databases.
- Ensure that the managed state is consistent.
- Remove incomplete interface objects and incomplete nodes created by the discovery process from the object database.
- Update the presentation time to force `ipmap` to update the object's status during map synchronization.
- Update the creation time of the object to force `ipmap` to add the object during map synchronization.

To run `ovtopofix` and check for problems, type

`ovtopofix -n`

To run `ovtopofix` and fix any problems found, follow these steps:

1. Exit `ovw` using the `Map:Exit` menu item.
2. Stop `netmon` by typing **`ovstop netmon`**.
3. Type **`ovtopofix`**.
4. Restart `netmon` by typing **`ovstart netmon`**.

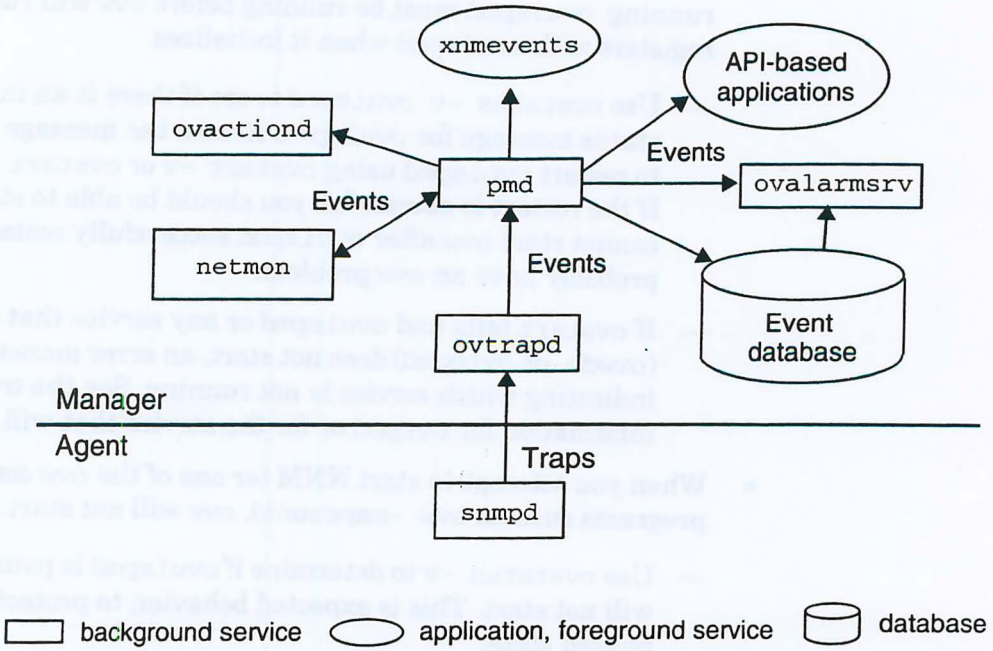
For more information, see the *ovtopofix* reference page in NNM's online help (or the UNIX manpage).

A license problem could also cause `ovtopmd` to fail. In this situation, verify that the license in *`install_dir`*`\conf\.license` (`$OV_CONF/.license`) is correct.

The ovtrapd Background Service

SNMP traps generated by an agent (`snmpd` in the case of the HP OpenView SNMP Agent) go to `ovtrapd` (via UDP port 162), which forwards them to `pmd`. `ovtrapd` acts as a buffer for traps that could potentially be dropped when `pmd` is busy. `pmd` logs and forwards the traps (in the form of an event) to `netmon`, `ovactiond`, `ovtopmd`, `ipmap`, and `xnmevents` (and potentially other subscribing applications). Figure C-2 illustrates this interaction.

Figure C-2 ovtrapd Event Interactions with SNMP Agent



ECT
ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1184
3740
Doc.

The ovuispmd Background Service

You are most likely to see ovuispmd problems when you are trying to start ovw, since you cannot start ovw if ovuispmd is not running. You may also see ovuispmd problems when you use ovpause and ovresume, which are invoked when you perform a backup.

Problems that appear to be ovuispmd problems can actually be the result of:

- Problems with ovuispmd itself.
- Problems with one of the services on which ovuispmd depends.
- Problems with ovw, which depends on ovuispmd.

The easiest way to determine if the problem is with ovuispmd itself, or with another service, is to look at the symptom, as follows.

- When starting NNM, you get a dialog box saying that registration with the UI process manager failed. This is because ovuispmd is not running. ovuispmd must be running before ovw will run because ovw registers with ovuispmd when it initializes.
  - Use `ovstatus -v ovuispmd` to see if there is an informative exit status message for ovuispmd. Record the message and then try to restart ovuispmd using `ovstart -v` or `ovstart -v ovuispmd`. If the restart is successful, you should be able to start ovw. If you cannot start ovw after ovuispmd successfully restarts, then you probably have an ovw problem.
  - If ovstart fails and ovuispmd or any service that it depends on (ovwdb or ovtopmd) does not start, an error message will appear, indicating which service is not running. See the troubleshooting information for ovspmd or for the service that will not start.
- When you attempt to start NNM (or one of the ovw command line programs such as `ovw -mapcount`), ovw will not start.
  - Use `ovstatus -v` to determine if ovuispmd is paused. If it is, ovw will not start. This is expected behavior, to protect the NNM's paused state.

    It should not take long for ovpause to complete. If the pause was initiated by the automated backup program, you can determine how long the system has been paused from the log file, *install_dir*`\tmp\ovbackup.log` (`$OV_TMP/ovbackup.log`).

If the paused state persists and there is no ovbackup in progress you can attempt to ovresume the system. Do not do this if a backup is in progress because it can result in corruption of the data store copies that are being created.

- You attempt an ovpause or ovbackup.ovpl when an ovw command line client is running, and ovuispmd denies the pause. This is expected behavior. Under these conditions the command ovstatus ovuispmd tells you that ovuispmd's state is PAUSE_ERROR and ovuispmd's last message field indicates that it denied the pause because a command line client is running.

  To prevent database inconsistency or inaccurate reporting, ovuispmd denies a pause request if the pause request is received when one of ovuispmd's registered ovw services is an ovw that was invoked with the -mapcount, -deleteMap, or -copyMap option.

  — To resolve this problem, issue a new pause request after the ovw service terminates. These ovw command line services are designed to do specific, short tasks and then exit.

- There are ovw sessions that seem to be stuck pausing. If you have run ovbackup.ovpl and you find ovw sessions still paused after the background services have resumed, ovuispmd may have exited or been killed during the pause.

  If a resume request is issued when ovuispmd is not running, then ovw sessions will not be notified of the resume and will remain paused, even when the background services have resumed. When ovuispmd terminates ungracefully it leaves a state file containing information about the registered ovw sessions. You can examine this file in *install_dir*\conf\ovuispmd.state ($OV_CONF/ovuispmd.state). *Do not modify this file!* It is used by ovuispmd when it is restarted.

  — Use ovstatus to determine if ovuispmd is still running. If it is not running, restart it. When it initializes, it will automatically attempt to resume all of the ovw sessions that were registered with it when it terminated ungracefully.

- The ovw session information reported by ovuispmd is not correct. When you run ovstatus -v ovuispmd, it includes ovw sessions that are no longer running.

ROS nº 03/2005 - CN - CPMI CORREIOS
Fls. Nº 1185
3740
Doc:

Under some termination conditions, ovw sessions are unable to unregister with ovuispmd before they terminate. In those cases, ovuispmd's list of ovw sessions will not be corrected until ovuispmd attempts to communicate with the registered sessions.

— If no ovw sessions are running locally or remotely then it is safe to stop ovuispmd and restart it. Its ovw session information will be updated when it is restarted.

- ovuispmd exits ungracefully. This may be due to a termination signal from ovspmd.

  — See the *ovuispmd* reference page in NNM's online help (or the UNIX manpage) for information about forced termination. Also refer to the file *install_dir*\lrf\ovuispmd.lrf ($OV_LRF/ovuispmd.lrf) for useful comments about configuring the timeout field to prevent this occurrence.

- When you try to start ovw, ovw will not start or ovuispmd exits.

  — If ovuispmd is running but ovw does not start, or if ovw startup causes ovuispmd to abort, there may be useful information in the ovuispmd logging messages. The log messages may help you characterize the problem as an ovw problem, an ovuispmd problem, or an application problem.

  Detailed instructions for using the Windows Application Event Log and the UNIX operating tracing and logging facilities, nettl and netfmt, are found in this appendix in the section "Logging and Tracing" on page 639. Examine the logging output for ovuispmd errors in the OVEXTERNAL subsystem section. Also refer to the diagnostics in the *ovuispmd* reference page in NNM's online help (or the UNIX manpage).

The ovwdb Background Service

The ovwdb service controls the object database. Here are some problems that can be caused by ovwdb and possible solutions to the problems.

ovwdb should be running whenever NNM is running. Normally it is started through ovstart. To verify that it is up and running, type:

```
ovstatus ovwdb
```

You should see something like this:

```
object manager name:    ovwdb
state:                  RUNNING
PID:                    4115
last message:           Initialization complete.
exit status:            -
```

By default, ovwdb uses a TCP socket bound to port 9999. If ovwdb indicates an error attempting to bind to this port number because another application is already using it, follow these steps:

1. Make sure that you do not have another ovwdb service using port 9999. Check the /etc/services file for a listing of ports being used.

   The most common reason for errors binding to the TCP socket is the presence of another ovwdb service. If an ovwdb service was started outside of ovstart, the ovstop, ovstart, and ovstatus commands will not recognize this service. To prevent this problem, always start all NNM background services with the ovstart command and stop them with the ovstop command.

   If another application is using port 9999, continue with the next step.

2. Change the port number to any unused port by changing the entry for ovwdb in %SystemRoot%\system 32\drivers\etc\services (/etc/services).

   ```
   ovwdb    9999/tcp      # OpenView Object Database daemon
   ```

3. Reconfigure NNM by typing the following commands:

   ovstop

   ovstart

4. If ovwdb still fails to run successfully from ovstart, contact your HP support representative.

NOTE If you are using the Network Information Service (NIS), make sure you update your NIS Master Server.

If you notice a great deal of swapping and the system performance does not meet your expectations, you can do one of two things:

- Edit the *install_dir*\lrf\ovwdb.lrf ($OV_LRF/ovwdb.lrf) file to configure the maximum number of objects that will be in the ovwdb cache.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1186
3740



- Change the system parameters (kernel parameters and regenerate the kernel). For more information, see "Improving Traffic Management and Performance" on page 654 in this appendix.

To verify the status of ovwdb, first run the `ovstatus -v` command to determine if everything is working correctly. If ovwdb stops running, netmon and ovtopmd will also stop running because these services are dependent on ovwdb. On UNIX operating systems only, if ovwdb is no longer running, check the `nettl` log using `netfmt`. Note that this assumes `nettl` was running when the problem occurred. To verify that `nettl` is running, execute the `nettl -status` command. See "Using nettl and netfmt (UNIX operating systems only)" on page 643 for more information on using `nettl`.

If you exhaust all available memory, the ovwdb service will stop running. To solve this problem, follow the suggestions described above for solving problems with excessive swapping; that is, either edit the `ovwdb.lrf` file or change the system (kernel) parameters.

If ovwdb stopped running due to memory problems, a disaster message will be logged into the Application Event Log (through `nettl`).

If the object database gets corrupted in any way, for example, by removing the files in the *`install_dir`*`\databases\ovwdb` (`$OV_DB/ovwdb`) directory, you need to restart the automatic map generation from the beginning.

The pmd Background Service

The pmd service is the postmaster background service. It provides event (trap) forwarding and message passing between services. When pmd receives an event, it forwards it to all the services that are registered to receive the event. Events are generated by these services:

- ipmap and ovtopmd when you edit the map or when nodes' status propagates to segments and networks.
- netmon, when it detects a change as a result of polling nodes or as a result of receiving a trap forwarded by pmd.
- ovtrapd, when ovtrapd receives a trap from agent services.
- ovtopmd, when topology changes occur.
- snmpCollect, when a threshold is exceeded or reset.
- ovevent, when this command is called from a batch file (shell script).

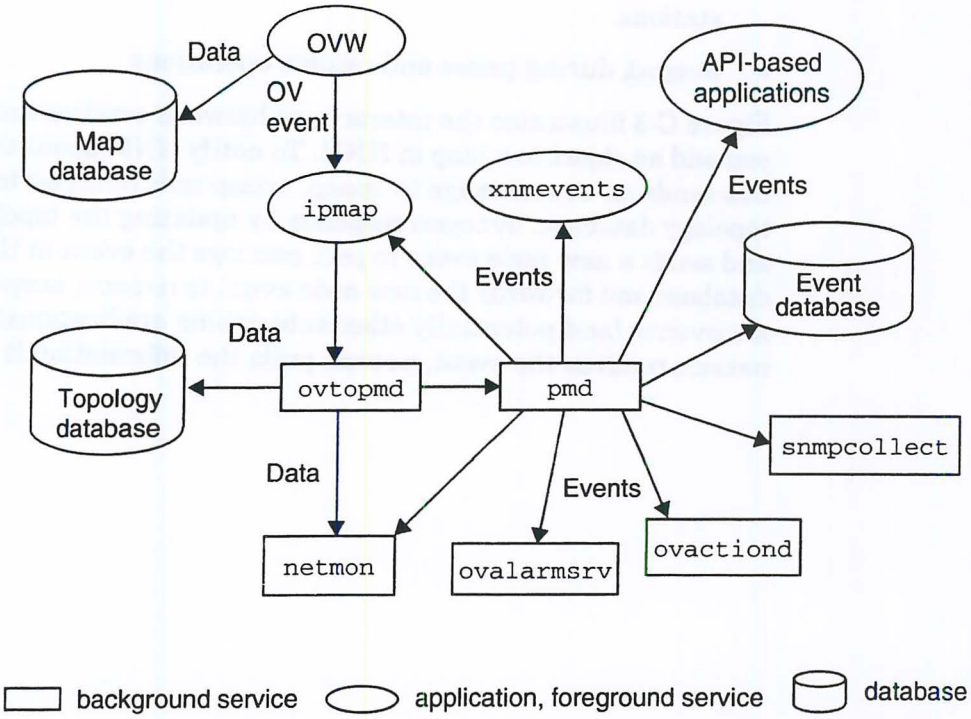
- Configuration operations such as `xnmloadmib`, `xnmtrap`, `xnmsnmpconf`, and `xnmcollect` when you edit configuration files.
- `ovrepld` as a result of a change detected on a remote collection station. Refer to *A Guide to Scalability and Distribution* for information on the `ovrepld` background service and collection stations.
- `ovspmd`, during pause and resume operations.

Figure C-3 illustrates the interactions between services and `pmd` when you add an object to a map in NNM. To notify NNM about the new object, `ovw` sends an `ovw` message to `ipmap`. `ipmap` tells `ovtopmd` to update the topology database. `ovtopmd` responds by updating the topology database and sends a new node event to `pmd`. `pmd` logs the event in the event database and forwards the new node event to `netmon`, `snmpcollect`, and `xnmevents` (and potentially other subscribing applications). When `netmon` receives the event, `netmon` pulls the information it needs from

ECT 2280 21
ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1187
3740
Doc:

the topology database through ovtopmd. When snmpCollect receives the event, it checks to see if the new node should be collected from (that is, whether it matches any configured IP wildcards).

Figure C-3 pmd Event Interactions



For a discussion of pmd's interactions and operation concerning events generated by netmon, see "The netmon Background Service" on page 587.

If you suspect a problem with the pmd background service, try the following actions to further isolate the problem:

- If pmd is not configured to write to eventdb, you'll first need to execute ovdumpevents to write the contents of the event database to a log file.
- Look for events logged to the event database, using xnmevents or the Alarm Browser.

- Add a node to the map and then check to see if the event was recorded in the event database, using `xnmevents` on a management station or the Alarm Browser through the Web UI.
- Run `ovstatus` and check the status of `pmd`. If the `pmd` service appears to be hung, stop the service using `ovstop` and restart all background services with `ovstart`.
- Check `pmd.log0` to see any messages related to the `pmd` service.
- Turn on tracing as described in the "Recommended Logging and Tracing Practices" on page 639 in this chapter. Your HP support representative can help you interpret the trace results.
- Verify that events can be generated. Use the `popupMsg` contributed script in `$OV_CONTRIB/NNM/popupMsg` to generate an event.

The ovrequestd Background Service

The `ovrequestd` service executes reports and data warehouse exports according to a predefined schedule. Once a report is configured, `ovrequestd` starts executing the exports and the reports.

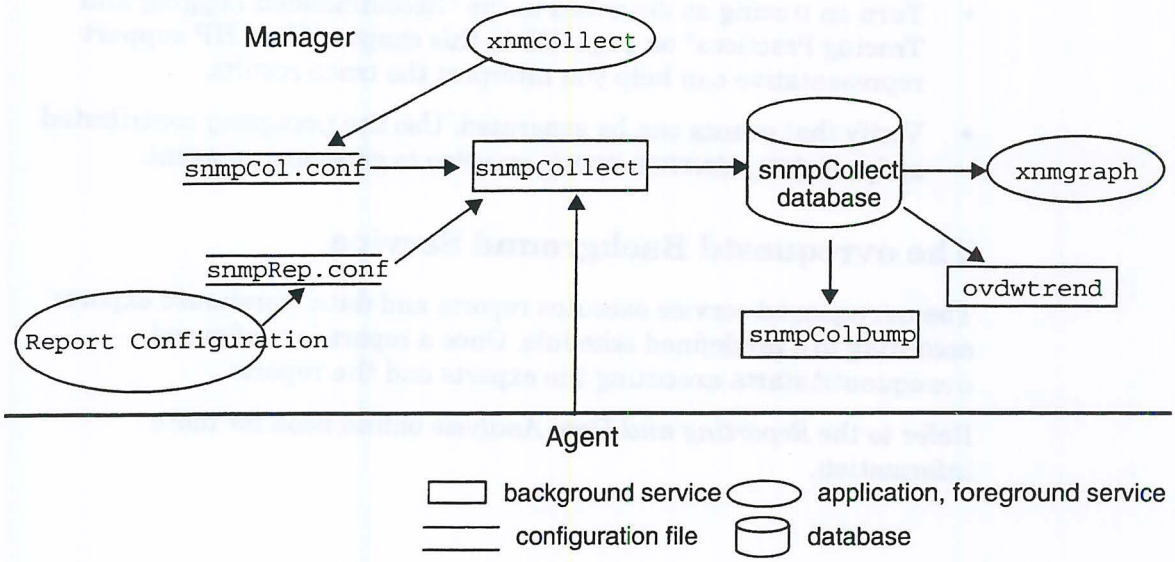
Refer to the *Reporting and Data Analysis* online book for more information.

RQS nº 03/2003 - CN - CPMI - CORREIOS
Fls. Nº 1188
Doc. 3740

Troubleshooting Data Collector Problems

Figure C-4 shows the interactions among the services `xnmcollect`, `xnmgraph`, `snmpCollect`, `snmpColDump`, and an SNMP agent.

Figure C-4 snmpCollect Interactions with SNMP Agents



If you have problems collecting MIB data, check for these problems:

- The service for the data collector, `snmpCollect`, may not be running on the management station.
  - — Make sure that you are not out of disk space. The data collector stops running when the disk is full. See page 610 for information about what to do if the disk is full.
  - — Verify the `snmpCollect` service is running by executing the `ovstatus snmpCollect` command. If the `snmpCollect` service is not running, restart the data collector using the `ovstart` command.
- Data is not being collected from the node it should be or thresholds are not being generated.
  - — Make sure the target node supports SNMP.

- Make sure the node is managed, or that the `-u` option to `snmpCollect` is used.
- Verify that the MIB object is configured for collection. Use the `Options:Data Collection & Thresholds:SNMP` menu item to verify the configuration.
- Verify that the target node is configured to collect data or generate threshold events. You can configure the node to collect data by explicitly specifying the node name, by specifying a wildcard, or by specifying the name of an ASCII file that contains the node name. Also, verify that the target node has not been excluded for collection. Use the `Options:Data Collection & Thresholds:SNMP` menu item to verify the configuration.
- Ensure that collections for the MIB object are not in `Suspended` state.
- Ensure that the desired instances are specified for the MIB object and node combination.
- Perform `Fault:Test IP/TCP/SNMP` on the collection in question. This checks the connection between the local management station and other SNMP nodes.
- If `sysObjectID` filtering is being used, make sure the correct `sysObjectID` is being used.
- See if other collections or thresholds from that node are working. If none are working, the problem is probably with the node. From the `Options:Data Collection & Thresholds:SNMP` window, select the MIB object, and then select `Actions:Show Data` to see if data is being collected from the node.
- Try to access the MIB object using the `Tools:SNMP MIB Browser` dialog box.
- Run `snmpCollect -S` and look at the *`install_dir`*`\log\(`$OV_LOG`)snmpCol.trace` file. This command lists the configuration of the data collection.
- Try turning on verbose tracing. Execute `ovstop snmpCollect`. Then execute `ovstart snmpcollect -V`. Check the output in the `snmpCol.trace` file.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1189
3740
Doc:

— If you expect threshold events to occur, but they do not, start a data collection on the MIB variable. The problem may be that the threshold value is not set correctly. For example, if the normal value for this variable is 20 and you set the threshold value to 100, you will probably never see a threshold event.

— If you can't resolve the problem, use the tracing command. To use the tracing command, try restarting the data collector with the same command as in the *install_dir*\lrf\snmpCollect.lrf (`$OV_LRF/snmpCollect.lrf`) file, but add the `-t` *filename* option. The `-t` option is a tracing option that logs the results to the *filename*. Run `snmpCollect -T` to toggle the tracing. To determine whether or not tracing is on, look at the trace file. See the *snmpCollect* reference page in NNM's online help (or the UNIX manpage) for more information.

— For more information about troubleshooting threshold events, see the section "Configuring Events" on page 631 in this appendix.

- The disk is full. The data collector stops running when the disk is full. To solve this problem and to prevent this problem from happening again, do the following:

  - Use `ovdwtrend -delpriorto` *date/time*. This command will export `snmpCollect` data to the data warehouse and then delete the `snmpCollect` data after it has been exported. See the *ovdwtrend* reference page in NNM's online help (or the UNIX manpage) for more information on using this command.

  - Free up disk space by removing files in the *install_dir*\databases\snmpCollect (`$OV_DB/snmpCollect`) directory. Note, however, when you remove files you lose the data you have saved. If you don't want to remove the whole file, you can edit the file and keep only the most recent data by deleting older entries in the file. Once you have freed up disk space, as `root` restart the data collector with the `ovstart` command.

  - Edit files in the *install_dir*\databases\snmpCollect (`$OV_DB/snmpCollect`) directory using the `snmpColDump` command. For example, to retain the last 100 entries of a file, use the following commands (available in the MKS Toolkit on a Windows operating system):

```
snmpColDump -tTI snmpCollect\filename\
awk -F\t '{printf("%d\t%d\t%s\t%1g\n", $4, $5, $6, $3)}' | \
  tail -100 > \tmp\save
snmpColDump -r \tmp\save install_dir\databases\snmpCollect/
```

On UNIX operating systems only:

```
snmpColDump -tTI $OV_DB/databases/snmpCollect/filename\
awk -F\t '{printf("%d\t%d\t%s\t%1g\n", $4, $5, $6, $3)}' | \
  tail -100 > /tmp/save
snmpColDump -r /tmp/save $OV_DB/databases/snmpCollect/
```

- If you want to stop all data collection, kill the `snmpCollect` service with the `ovstop snmpCollect` command, or suspend all data collections using the `Options:Data Collection & Thresholds:SNMP` menu item.

To prevent the problem in the future:

- Lengthen the polling intervals. Using the `Options:Data Collection & Thresholds:SNMP` menu item and set the polling interval to not collect as often. In addition, if you only want to check thresholds, don't store the data.
- Reduce the number of MIB objects you are collecting on.
- Reduce the number of nodes you are collecting on.
- Reduce the number of instances you are collecting for some or all nodes.
- Set up programs (`cron`) to periodically either remove files in the *install_dir*`\databases\snmpCollect` (`$OV_DB/snmpCollect`) directory or export and trim them with `ovdwtrend`.

- There is no response when querying DMI devices.
  - Make sure that DMI is configured correctly on the remote device.
  - The Data Collector supports only SNMP devices. Install an SNMP agent and a DMI-to-SNMP mapping agent on the DMI system.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1190
Doc: 3740

Set-community Name and Trap-dest Loss Upon Re-Installation

The emanate SNMP agent uses the following two configuration files in the *install_dir*\conf\SnmpAgent ($OV_CONF/SnmpAgent) directory:

- snmpd.cnf — the SNMPR-format emanate configuration file.
- snmpd.conf — the HP-format SNMPD configuration file.

emanate uses the union of configuration information from both files. However, some of the information is in both—sysDescr, sysName, sysContact, and sysLocation. When emanate starts up, it uses the snmpd.conf values (if defined) and copies them to snmpd.cnf; otherwise, it uses the values in snmpd.cnf.

The get-community, set-community, and trap-dest fields in snmpd.conf are not replicated in snmpd.cnf, so they are appended (in emanate run-time memory) to the set of configurations in snmpd.cnf because it is allowable to have more than one value for each.

Thus, upon installation, the default snmpd.cnf file is conditionally installed by Setup (only if one doesn't already exist)—but the default snmpd.conf file is always installed. After uninstallation and re-installation, the result is that sysContact and sysLocation get taken from the existing snmpd.cnf file, but the set-community and trap-dest are taken from the new/default snmpd.conf file (in which they are not defined).

The solution is to conditionally install snmpd.conf only when it does not already exist.

Troubleshooting Web Components

If you experience problems starting any of the web components, you should first check the following before doing further troubleshooting.

- Make sure that NNM is installed on the host specified in the URL, and that the host is running.
- Make sure that you are using a supported web server, and that it is configured properly and is running. Supported web servers include Microsoft Peer Web Services, Microsoft Internet Information Server, and Apache (shipped with NNM for UNIX operating systems.) Try entering the simplest URL (`http://`*`hostname`*`[:`*`port`*`]`) in the web browser and see if the server is accepting connections.
- Make sure that you are using a web browser that supports NNM. Supported web browsers include Netscape 4.6 or greater and Microsoft Internet Explorer 5.0 or greater.
- If starting the web component directly from a URL, make sure the full URL was entered correctly. If NNM is running on a UNIX operating system, check that port 3443 is specified in the URL.
- Make sure that the hostname in the URL is fully qualified. Do not use the short version of the hostname. For example, use `mysystem.home.com` instead of just `mysystem`.
- Exit and restart the browser, and then re-enter the URL.
- Clear the memory and disc caches for the browser, and restart the browser.

  In Netscape Navigator, select the `Edit:Preferences` menu item. In the dialog box, click on `Advanced`, then click on `Cache`. In the next dialog box, click on `Clear Disk Cache` and `Clear Memory Cache`.

  In Internet Explorer, select the `View:Internet Options` menu item. On the `General` page, select the `Temporary Internet Files` field. Then click on the `Delete Files` button.
- Check the contents of all of the web log files for possible errors.

  Windows:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1191
3740
Doc:

```
install_dir\www\logs\launcher\error_log
install_dir\www\logs\launcher\login_log
install_dir\www\logs\launcher\access_log
```

UNIX:

```
/var/opt/OV/www/logs/launcher/error_log
/var/opt/OV/www/logs/launcher/login_log
/var/opt/OV/www/logs/launcher/access_log
```

- If an http proxy server is in use, try disabling the web browser from using it.

  In Netscape, select the `Edit:Preferences` menu item. In the dialog box, click on `Advanced`, then click on `Proxies`. In the dialog box, select `Direct connection to the Internet`.

  In Internet Explorer, from the `General` page select the `View:Internet Options` menu item. On the Connection page, deselect `Access the Internet using a proxy server`.

- For errors in the Reporting interface, refer to the *Reporting and Data Analysis* online manual.

Language Selection Problems

NNM's web applications are available in English and Japanese. However, it is possible to integrate and use other web applications that have been translated into other languages while NNM's web applications remain in English. If you expect the web applications to be in a language other than English and they are not, it could be due to one of the following problems:

- If the strings are appearing in English, check the browser's language configuration.

  In Netscape, `Languages` is configured through the `Netscape:Preferences` menu item.

  In Internet Explorer, `Languages` is configured through the `Internet:Options` menu item.

  In both cases, the language that you expect to see should be listed at the top of the `Languages` window. To see NNM's web applications in Japanese, be sure that the Japanese entry (`ja`) is listed before the English entry (`en` or `en-us`). Restart the browser after making changes.

- If the non-English strings appear garbled in the window, check the following:

  — The browser's encoding or font configuration may be incorrect.

  In Netscape, the encoding is specified through the `View:Encoding` menu item.

  In Internet Explorer, the font is specified through the `View:Font` menu item.

  To choose Japanese, one of the Japanese fonts or encodings should be selected.

  — On UNIX systems only, the browser was not started with the correct environment variable settings.

  The browser process should be started with the correct `$LANG` setting. For Japanese, `XMODIFIERS` must also be set. These variables are usually set by the desktop environment.

  — On Japanese on UNIX systems only, the default codeset in use by the server may be incompatible with the Web applications.

  By default, NNM's web applications expect the data from the servers to be in Shift-JIS codeset for HP-UX and Windows operating systems. On Solaris, EUC is the default. Use the `ovchange_locale_mapping` command to switch the default configuration. See the *ovchange_locale_mapping* manpage for details.

HP OpenView Launcher

User Login Problems

If you expected to get a user login screen when the Launcher starts, but you did not, then the file `session.conf` probably has not been set up for user logins. See Chapter 14, NNM on the Web, for information on setting up users and logins.

If you get the user login screen and the Launcher does not accept the login, check the following:

- Make sure you typed the user name and password correctly.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1192
3740
Doc:

- Make sure the password file, `htpasswd`, includes the user name and password. See Chapter 14, NNM on the Web, for information on setting up the `htpasswd` file.
- If running NNM in a non-English language, be sure that the environment variable `XMODIFIERS` is set correctly.

Starting the Launcher

If you have problems starting the Launcher, check the error log file for potential errors. The Launcher error log records internal errors from the Launcher. You can use the output from this file when discussing a problem with the HP Response Center or support personnel.

If the error log file does not give you sufficient information for troubleshooting, you can set a parameter in the URL for `ovlaunch.exe` that will enable more in-depth error logging on a session level.

The parameter is:
`http://`*`hostname`*`:[port]/OvCgi/ovlaunch.exe?Debug=/tmp/`*`file`*

The output of this file is less "friendly" than other error log files, but it contains valuable information that may be useful to a support person who is trying to assess the problem.

If the Launcher does not start and you get an error message indicating that there is a CGI problem, then the problem could be with one of the Launcher's CGI programs. Try executing each of the following programs from the command line. These programs are located in:

Windows: *`install_dir`*`\www\cgi-bin`

UNIX: `/opt/OV/www/cgi-bin`

- `ovlaunch.exe`
- `ovlogin.exe`
- `ovsessioninfo.exe`
- `ovlaunchreg.exe`

You can tell if these programs are running if they output ASCII text to the screen. If one of these programs is not running, contact HP Support.

Launcher Window Problems

If the Launcher window comes up with no content (blank), it could be one of the following problems:

- The correct patches have not been installed on the system. Check the system requirements section of the Installation Guide.
- You could have a conflict if you had an older version of Netscape installed on your system. If you have set the `CLASSPATH` environment variable when running an older version of Netscape, it will cause Java access problems when you run the recommended version of Netscape. If you have set this variable, you should unset it before running the newer version of Netscape.
- You could have a Java applet problem. Check the Java log as follows:
  - In your web browser, check to see that the items Java and Java script are enabled. In Netscape Navigator, check this by using `Edit:Preferences->Advanced`. In Internet Explorer, check this by using `View:Advanced`.
  - Bring up a Java console and view the messages it contains. In Netscape Navigator, use `Window:Java Console`. In Internet Explorer, use `View:Java Console`.
  - Try starting the Launcher without going through a proxy.

    In Internet Explorer, select the `View:Internet Options` menu item. Choose the `Connection` tab, then turn off the proxy server.

    In Netscape Navigator, select the `Edit:Preferences` menu item, choose `Advanced`, and disable the proxy server.
  - The Java console also provides a method of logging information about the Java virtual machine interpretation of the Java code that is executing. Both of the supported web browsers allow you to turn on Java error logging from the browser menu. In Netscape Navigator, look under the `Window` menu item. In Internet Explorer, select the `View:Internet Options` menu item under the `Advanced` tab.

If you encounter errors when reading in registration files, run the `regverify` command in *`install_dir`*`\bin\` (`$OV_BIN`) against the Launcher Registration File (WLRF) in the following directory:

Windows: *`install_dir`*`\www\registration\launcher\%LANG%`

UNIX: `/etc/opt/OV/share/www/registration/launcher/$LANG`

You can also hold down the **Shift** key and press the `[Reload]` button on your browser to force the registration files to reload.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1193
3740
Doc:

Other Sources of Information

Web server log files are available that provide you with information about server-related problems. The error log is located at:

Windows: `\WINNT\System32\Logfiles`

UNIX: `/opt/OV/httpd/logs`

This is the default location, but it may vary depending on where your web service is set to log errors. Check your web server properties to verify the location.

Network Presenter

If the Network Presenter does not start, check the items on page 613, and the following:

- If the Network Presenter progress bar does not appear, it could indicate web server problems. Try connecting to the web server from your browser without starting Network Presenter. For example:

`http://hostname:3443`

- Make sure the Network Presenter is registered with NNM. In NNM on a management station, use the `Help:About HP OpenView` menu. In the dialog box, click `Applications`. Verify that the Network Presenter appears in the list. Alternatively, check the registration directory to ensure that the file `netpresenter` appears. The location is:

  Windows: *`install_dir`*`\share\registration\%LANG%`

  UNIX: `/etc/opt/OV/share/registration/$LANG`

- Make sure that NNM is running on the management station, with the map opened to which the Network Presenter is trying to connect.
- If you tried starting the Network Presenter from the `Tools` or the `Objects` selection in the Launcher, try starting it directly from the URL instead.

If there are missing menu bar or toolbar items, do the following:

- Check the permissions on the registration files registered with Network Presenter. The permissions need to be read by all, and the owner and the group should be set to `bin`. The registration files are located in:

- Check your web server configuration. Verify the port number, alias names, directory names, and permissions. For more information, consult your web server documentation.

If you receive a message that you have a CGI Error or an Internal Server Error, please contact HP Support.

If No Data or Wrong Tree Structure Appears

If no data or the wrong tree structure is shown on the scoping pane:

- Verify the application registration files (ARFs) on the management station. Type:

  Windows: ***install_dir*\bin\regverify**

  UNIX: **$OV_BIN/regverify**

  (Set the LANG environment if necessary.)

  Alternatively, you can enter **http://*hostname*:*[port]*/OvCgi/snmpviewer.exe?ins=check** in your browser.

  If there are errors, fix the errors by editing the ARFs.

New Applications Not Displayed

If you added new applications with Application Builder, but they are not displayed on the scoping pane, clear the cache on your browser following the instructions on page 615, then launch SNMP Data Presenter again.

Results Not Shown, or are Incorrect

If the scoping pane is blank after resizing the browser window or frames:

- Click with the right mouse button on the scoping pane and select `Frame Reload`.

If you click an item in the scoping pane, but the results are not shown in the results pane:

- Check if the target nodes are healthy. Try `ping` or SNMP commands on the management station to the target nodes. See "Network Management Operations" on page 626 for more information.

If results are shown, but errors are indicated:

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1194
Doc. 3740

- All the operations in SNMP Data Presenter are defined in ARFs on the management station. NNM on the management station has the same menu items as in SNMP Data Presenter. Try the operation on the management station. If you still encounter errors, see the sections "Network Management Operations" on page 626 and "Executing MIB Applications" on page 629.

If the format in the results pane is unappealing:

- Make sure a fixed font is specified in the fixed width font setting. In Internet Explorer, select the `View:Internet Options->Fonts` menu item to change fonts. In Netscape Navigator, select the `Edit:Preferences->Appearance->Fonts` menu item.

Troubleshooting NNM Operations

This section suggests actions to take if you suspect a problem with one of the operations of NNM. This section also discusses the sequence of interactions and/or the flow of data associated with an operation when such information may help you to isolate the problem. This section covers the following:

- Runtime components.
- Network management operations.
- Browsing MIBs.
- Building MIB applications and executing MIB applications built by the MIB Application Builder.
- Collecting MIB information from network nodes at regular intervals.
- Configuring events.
- Event Reduction Capabilities
- Loading MIBs.
- X Windows components.
- Online help.

For detailed information on a command or service mentioned in this section, see its associated reference page in NNM's online help (or the UNIX manpage).

Runtime Components

If you are having problems running NNM, you should check file permissions, start-up scripts, and error log. These topics are discussed below.

Manager File Permissions

By default, the `ovw` (graphical network map) program is executable by anyone; the `ovwdb`, `pmd`, `snmpCollect`, `ovactiond`, `ovtopmd`, and `netmon` background services are executable only by `root`.

The remainder of this section is for UNIX operating systems only.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 1195
Doc: 3740

You may restrict the permissions on the map files using the `$OV_BIN/ovwchmod`, `$OV_BIN/ovwchgrp`, and `$OV_BIN/ovwchown` commands. These commands, along with the `ovwls` command, are explained in the *ovwperms* reference page in NNM's online help (or the UNIX manpage). These commands change all of the map data files associated with a map. You use the commands the same way as the operating system `chmod`, `chgrp`, and `chown` commands, except that you follow them with a map name instead of a file name. Note that these commands do not change permissions on the product's directories or executable files, nor on other configuration and data files.

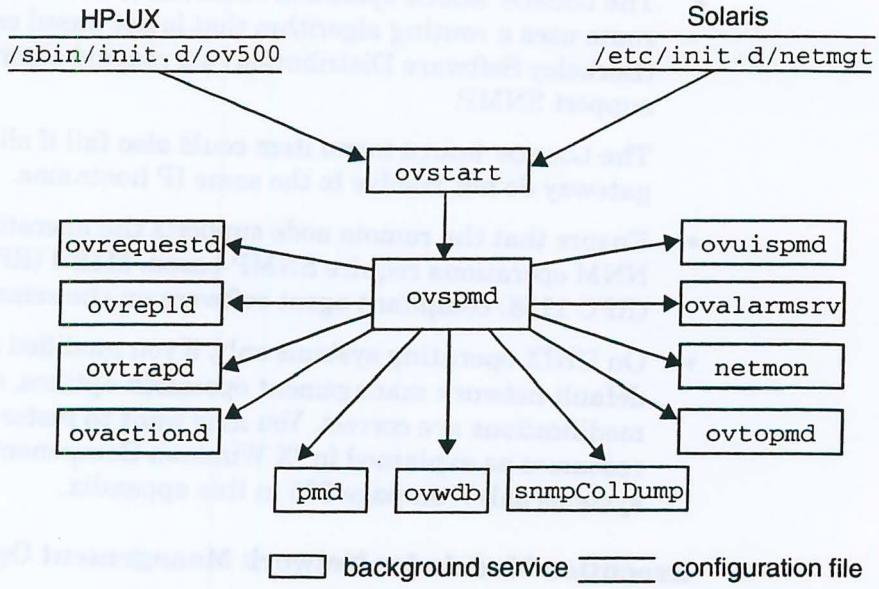
NOTE Do not change map permissions when NNM is running.

If you are having problems running NNM, try restoring the map file permissions to their default using the `ovwchmod` command with mode `0777`.

Start-Up Scripts (UNIX operating systems only)

Check to see if some component in the execution sequence is "broken," such as a syntax error in one of the product's start-up scripts. Figure C-5 shows the start-up execution sequence for NNM. All files are in the `$OV_BIN` directory.

Figure C-5 Manager Startup



A script file automatically executes `ovstart` when you reboot the system. The script file has the following name:

- *HP-UX*: `/sbin/init.d/ov500`
- *Solaris 2.X*: `/etc/init.d/netmgt`

If `ovstart` does not execute, the problem may be with the start-up script. The script file is created during installation. If the file already exists, the existing file is moved to another file, and the new one is copied to the original file name. For example, on HP-UX systems the existing file would be moved to `/sbin/init.d/#ov500`, and the new file would be copied to `/sbin/init.d/ov500`.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1196
3740
Doc:

Network Management Operations

If you are having problems running an operation to a remote node, check the following items.

- If you configured agent community names, verify that the node's community name listed in the `Options: SNMP Configuration` dialog box matches the community name configured on that node.
- The `Locate Route` operation could fail if one of the nodes in the route uses a routing algorithm that is not based on the BSD (Berkeley Software Distribution) 4.2 routing algorithm or does not support SNMP.

  The `Locate Route` menu item could also fail if all IP addresses for a gateway do not resolve to the same IP hostname.
- Ensure that the remote node supports the operation. Most of the NNM operations require SNMP-based, MIB-I (RFC 1156) or MIB-II (RFC 1158) compliant agent software on the remote node.
- On UNIX operating systems only, if you modified any X resources for default network management operation options, ensure that the modifications are correct. You may want to restore the default X resources as explained in "X Windows Components (UNIX operating systems only)" on page 635 in this appendix.

Execution Models for Network Management Operations

Some of the NNM operations start directly from `ovw`; others are started by an integrating service, `xnmappmon`.

Figure C-6 shows some of the network management operations started (or startable) directly by ovw.

Figure C-6 Applications Started Directly by the ovw Service

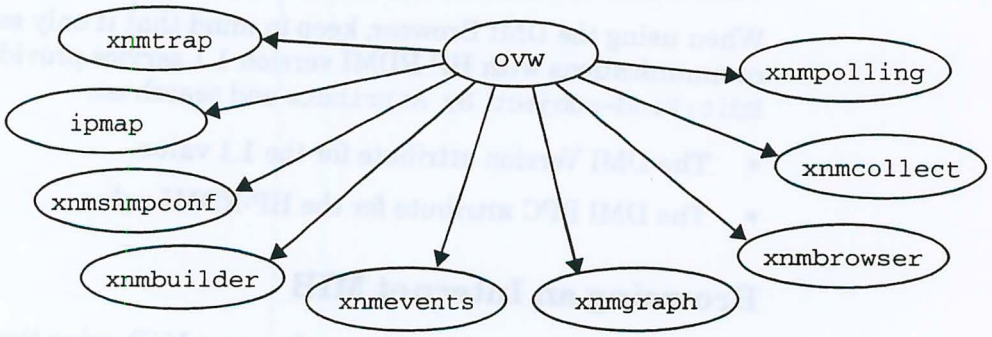
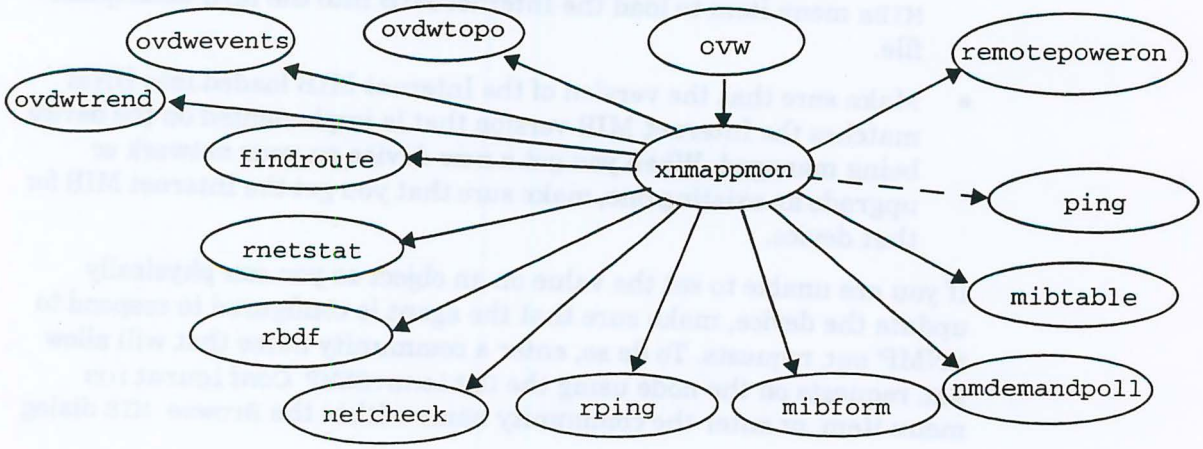


Figure C-7 shows those operations started by xnmappmon.

Figure C-7 Applications Started by xnmappmon



Many of the services shown in the previous two figures may be run as commands for remote troubleshooting. For information about which commands are executed for the different services, see each service's reference page in NNM's online help (or the UNIX manpage). ping is shown as a dotted line because it is a system command.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1197
3740
Doc:

Managing DMI Devices

NNM supports SNMP communications. In order to access DMI devices, you must install a DMI-to-SNMP mapping agent on the DMI system. Then SNMP requests will get processed.

When using the DMI Browser, keep in mind that it only supports DMI communications with HP-RDMI version 1.1 service providers. Use `Edit:Find->Object By Attribute` and search on:

- The DMI Version attribute for the 1.1 value.
- The DMI RPC attribute for the HP-RDMI value.

Browsing an Internet MIB

If you have problems browsing an Internet MIB using the `Tools:SNMP MIB Browser` menu item, check the following:

- Make sure the Internet MIB is loaded. Use the `Options:Load/Unload MIBs:SNMP` menu item to see what modules are currently loaded. If the MIB is not listed, use the `Load/Unload MIBs` menu item to load the Internet MIB into the MIB description file.
- Make sure that the version of the Internet MIB loaded into NNM matches the Internet MIB version that is implemented on the device being managed. When you get a new device on your network or upgrade an existing one, make sure that you get the Internet MIB for that device.

If you are unable to set the value on an object so you can physically update the device, make sure that the agent is configured to respond to SNMP `set` requests. To do so, enter a community name that will allow `set` requests on the node using the `Options:SNMP Configuration` menu item, or enter the community name within the `Browse MIB` dialog box.

Building and Executing MIB Applications

The problems you may encounter while building MIB applications and executing MIB applications built by the MIB Application Builder are closely related.

For example, some errors made while building an application may not show up until you actually execute the application. If the problem is an incorrectly built application, you need to modify your application.

This section is organized as follows:

- Things to check when you have problems building an application.
- Things to check when you have problems executing an application. Problems executing applications can be caused by either an error in the way the application was built, or by independent things such as the community name not being configured correctly.

Building MIB Applications

If you have problems building MIB applications using the `Options:MIB Application Builder:SNMP` menu item, check the following:

- Make sure to read the instructions in online help about adding MIB applications.
- Make sure you have the enterprise-specific MIB loaded. Use the `Options:Load/Unload MIBs:SNMP` menu item to see what modules are currently defined. If the MIB is not listed, use the `Load/Unload MIBs` menu item to include the MIB in the loaded MIB database.
- Make sure the MIB object ID you select is supported by the device you are trying to monitor. To verify this, use the `Tools:SNMP MIB Browser` menu item.
- When you create a Table application, you can only select fields from a single table in the MIB tree.
- Make sure that the version of the MIB loaded into NNM matches the MIB version that is implemented on the device being managed. When you get a new device on your network or upgrade an existing one, make sure that you get the MIB for that device.

Executing MIB Applications

If you have problems executing applications built using the `Options:MIB Application Builder:SNMP` menu item, check the following:

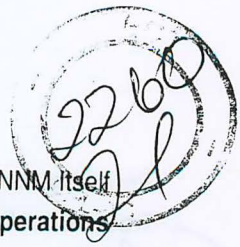
- Make sure you have the enterprise-specific MIB loaded. The application does not come up when the MIB for that particular application is not loaded. Use the `Options:Load/Unload MIBs:SNMP`

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1198
3740
Doc:

menu item to see what modules are currently defined. If the MIB is not listed, use the `Load/Unload MIBs` menu item to load the MIB into the MIB description file.

The MIB may be missing; for example, if you load a MIB, build an application, and then unload the MIB or if you copy the application to a new machine and the MIB is not on that machine. Make sure that if you copy the MIB application to another system, you also load the enterprise-specific MIB on that system.

- Make sure the MIB object ID you select is supported by the device you are trying to monitor. To verify this, use the `Tools:SNMP MIB Browser` menu item.
- Make sure the application was built to monitor the device you have selected. The problem may be that the application was built to monitor a different device than the one you are trying to monitor. For example, the application was built for an HP-UX agent, and you are trying to run that application on a Fred Router from Flintstones Company.
- Verify that the management station can talk to the agent. Use the `Tools:SNMP MIB Browser` menu item to verify that the manager station can actually talk to the agent and that the agent is responding with the values. Also, use the `Fault:Test IP/TCP/SNMP` menu item.
- Verify that the community name is set up properly in the `Options:SNMP Configuration` menu item. If you get a message indicating no response from the device, the management station may not have the proper community name defined for that device.
- Make sure that the version of the MIB loaded into NNM matches the MIB version that is implemented on the device being managed. When you get a new device on your network or upgrade an existing one, make sure that you get the MIB for that device.
- Verify that the following three files created by the MIB Application Builder are intact:
  - The registration file in *`install_dir`*`\registration\C\ovmib` (`$OV_REGISTRATION/$LANG/ovmib`, where `$LANG` is the language NNM is set to use). Make sure the registration file name for the application is the same as the application name that was specified when the application was created.



— The help file name is the same as the application name that was specified when the application was created.

The help file is:

Windows: `install_dir\help\C\ovmib\OVW\Functions`

UNIX: `$OV_HELP/$LANG/ovmib/OVW/Functions`

— On UNIX operating systems only, the line entry in the help index file in the `$OV_HELP/$LANG/OVW/functions/INDEX` directory corresponds to your specific MIB application.

- If you typed the object identifier in the MIB selection field, make sure you enter a full object identifier. For example, you cannot create a form application for `.iso.org.dod.internet`. The object ID must correspond to an object supported by the selected device.
- If you configured your Application Builder program to query DMI devices using the corresponding mapped MIB values, and there is no response from the DMI devices, do one of the following:

  — Use the DMI Browser feature of NNM.

  — Install an SNMP agent along with a DMI-to-SNMP mapping agent on the DMI device.

Configuring Events

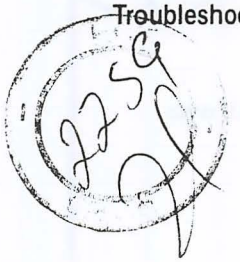
If you have problems configuring events using the `Options:Event Configuration` menu item, first see the vendor documentation that describes the traps generated by that specific device to make sure the enterprise and trap number correspond to what you have indicated.

To get a description of the NNM events shipped with the product, use the `Options:Event Configuration` menu item. From the `Event Configuration` dialog box, select `OpenView` as the `Enterprise Name`, then select an event name and select `Edit:Events->Describe (Describe Event)`.

If you have defined an action for an event, but the action is never taken or it is not executed the way it was intended to, check the following:

- Verify the configuration. When you save the configuration for a new event, the entire `trapd.conf` file is rewritten, and an event is sent to `xnmevents`, `ovactiond`, and `pmd`. Common configuration problems are:





  - The command is typed wrong.
  - The arguments are not specified properly.
- Make sure the format message for a particular trap is intact. For example, if the format message for the `coldStart` trap has been erased, you will not see that trap in the event log file or the Alarm Browser window.
- Make sure you do not edit the `trapd.conf` file. The `trapd.conf` file contains the logging and action definitions. If this file is corrupted, the events you have configured may not be logged.
- Use `ovdumpevents` to see if the trap was decoded properly. Each time NNM receives an event, the `pmd` service logs an entry in the event database. For example, the event database identifies ASN.1 coding problems in enterprise-specific traps.
- Verify that the event is logged to the expected category. For example, if you selected `log only`, you will not see the event in the event browser window. If you selected `ignore`, you will not see the event.
- On UNIX operating systems only, compare your `$OV_CONF/C/trapd.conf` file with the default configuration file, `/usr/OV/newconfig/OVEVENT-MIN/conf/C/trapd.conf`.

Event Reduction Capabilities

Event reduction is the process by which you can identify relationships between events. Once identified, a smaller number of new events with the same or higher information content can be generated.

Two event reduction strategies that NNM uses are ECS correlations and Correlation Composer correlators. For more information about these strategies, see "ECS Correlations" on page 360 or "Correlation Composer Correlators" on page 386.

Troubleshooting ECS Correlations

If you are having problems with any of the ECS correlations, see "Troubleshooting" on page 381 for more information.

Troubleshooting Correlation Composer Correlators

If you are having problems with any of the Correlation Composer correlators, see "Troubleshooting" on page 397 for more information.

Loading Internet MIBs

When you load an Internet MIB, the `Options:Load/Unload MIBs:SNMP` menu item takes all vendors' Internet MIBs and puts them into one single loaded MIB database, *install_dir*`\conf\ ($OV_CONF) snmpmib`. The `Load/Unload MIBs` menu item creates a binary file, *install_dir*`\conf\snmpmib.bin (`$OV_CONF`/snmpmib.bin)`. The SNMP MIB Browser, MIB Data Collection, MIB Application Builder, and the MIB applications built using the MIB Application Builder access the loaded MIB database for their routines.

NOTE Always use the `Options:Load/Unload MIBs:SNMP` menu item to modify the loaded MIB database; do *not* edit the loaded MIB database directly.

If you have problems including Internet MIBs in the MIB description file using the `Options:Load/Unload MIBs:SNMP` menu item, check the following:

- Make sure that the format of the MIB definition is correct. For example, it must have an ASN.1 module `DEFINITIONS` clause. The enterprise-specific files should only contain modules that are unique to that vendor.

  The format must conform to *RFC 1155*, *RFC 1212*, *RFC 1902*, *RFC 1903* or *RFC 1904*. *RFC 1155* and *RFC 1212* apply to the SNMPv1 SMI, while *RFC 1902*, *RFC 1903*, and *RFC 1904* apply to the SNMPv2 SMI.

- Make sure that the syntax is correct. Hewlett-Packard has verified that the syntax of the MIB modules included with the NNM product is correct. However, if you get the MIB module directly from the vendor, you may have to correct syntax errors. The `Options:Load/Unload MIBs:SNMP` menu item checks for syntax errors and displays an error that tells you where the error is and how to fix it. The most common syntax errors are typing errors and non-conformance to the RFCs.
- Compare the MIB with the Hewlett-Packard MIB to look for errors. By comparing the MIB that does not load with the Hewlett-Packard MIB, you may be able to troubleshoot the problem. The Hewlett-Packard MIB loads correctly.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1200
Doc: 3740

Known Limitations

The object label in a MIB module must be unique. Due to lack of standards this is not clearly identified by SNMP. If you have mnemonic names for an object ID component that is used elsewhere in the module, the second object shows up in the MIB tree under the first object that has the common component name. Furthermore, the translation from the mnemonic object name to the numeric object ID will be incorrect, causing SNMP queries to fail.

For example, suppose the xyzCorp has the enterprise MIB `device` object defined in a module XYZCORP-MIB under `.iso.org.dod.internet.private.` as

```
enterprises.xyzCorp.bridge.device.name
                                 .number
                                 .ROMid
```

and another `device` object defined as

```
enterprises.xyzCorp.hub.device.model
                                .serialNumber
                                .otherInfo
```

The MIB parser cannot distinguish between the two `device` objects. As a result, the xyzCorp fields `model`, `serialNumber`, and `otherInfo` will appear incorrectly in the Internet MIB tree as

```
enterprises.xyzCorp.bridge.device.model
                                .serialNumber
                                .otherInfo
```

To circumvent the problem, patch the enterprise-specific MIB to use a unique component name. For this example, change `.hub.device` to `.hub.hubdevice`. When the object name is translated to the numeric object ID used in the SNMP query, the proper object ID will be used and the SNMP query should work.

A second (and more contrived) alternative is to put the second and any subsequent occurrences of duplicate object labels (and any objects based on them) in a separate ASN.1 module with a fully-qualified reference as to their proper position in the global Internet MIB tree.

For example, the first occurrence of `device` could be defined in a module as

```
XYZCORP1-MIB DEFINITIONS ::= BEGIN
xyzCorp OBJECT IDENTIFIER ::= { iso org(3) dod(6) internet(1) private(4)
                                enterprises(1) 999 }
```

```
    bridge  OBJECT IDENTIFIER ::= { xyzCorp 1 }
    device  OBJECT IDENTIFIER ::= { bridge  1 }
     -- all subsequent children...
        .
        .
        .
END
```

and the second in a module as

```
XYZCORP2-MIB DEFINITIONS ::= BEGIN
hub OBJECT IDENTIFIER ::= { iso org(3) dod(6) internet(1) private(4)
                                              enterprises(1) xyzCorp(999) }

   device  OBJECT IDENTIFIER ::= { hub  1 }
    -- all subsequent children...
        .
        .
        .
END
```

X Windows Components (UNIX operating systems only)

This section discusses X Windows-related files for NNM only. If the problem does not appear to be with this product, refer to your X Windows documentation for further troubleshooting information.

To verify the status of the background services, run the `ovstatus` command. For more information about `ovstatus` and how to troubleshoot the background services, see "Troubleshooting Background Services" on page 584 in this appendix.

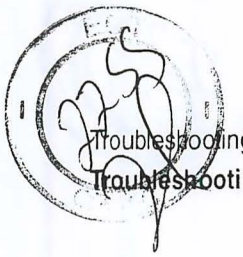
To determine whether there is a problem with the X Windows component of NNM, try restoring the default X resources for this product, and see if this solves the problem.

1. Ensure that the files in the `$APP_DEFS` directory contain the installed X resource defaults for the product: `XNm`, `OVw`, `XNmevents`, `XNmgraph`, `OVHelp`, etc.

   The X resource defaults are listed in the *ovw* and *ovhelp* manpages. The `XNm` resource defaults are listed in the `XNm` resource file itself.

2. Ensure that the `XENVIRONMENT` shell variable is not set.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1201
3740
Doc:



3. Remove resources starting with `XNm`, `XNmevents`, `XNmgraph`, `OVw`, or `ovhelp` from your `$HOME/.Xdefaults` file. Or, temporarily rename this file.
4. Restart X Windows.
5. Restart `ovw` (`$OV_BIN/ovw`) without any X resources specified as arguments.

Online Help

The text files used for the NNM Help operations (not including reference pages or UNIX manpages) are below the directory *`install_dir`*`\help\C\help\C` (`$OV_HELP/help/C`). On UNIX operating systems only, you can also use the `man` command on the manpage name.

Troubleshooting Windows Applications

This section discusses troubleshooting applications on Windows operating system.

Problems Launching Applications

If you experience problems launching the Event Viewer, Performance Monitor, Registry Editor, or Windows Diagnostics, and an error message like `Permission denied` or `Access denied` appears after launching the application, it may be that you do not have enough privileges to be able to administer or view the remote computer's properties.

Windows Operating System Tools

The Windows operating system tools, listed below, can assist you in troubleshooting Windows applications. These tools appear on NNM's menus, depending on the applications on your system. There can be up to eight Windows tools menu items:

- `Fault:Windows Event Viewer` — always present
- `Performance:Windows Performance Monitor` — always present
- `Configuration:Windows Registry Editor` — present only if the currently logged-on user has Administrative privileges
- `Fault:Windows Diagnostics`
- `Server Manager` and `User Manager` — present only if running on a Windows server (as opposed to a Windows workstation)
- `SMS Properties` and `Run SMS` — present only if SMS Administrator software has been installed

  If you launch SMS and do not see an OpenView icon when viewing the properties on a node, verify that NNM is running.

  If you have installed SMS Administrator software on your system and the two SMS-related menu items are missing, ensure that you installed SMS version 1.2 — only version 1.2 is supported.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1202
3740
Doc:

In order to be able to view SMS properties for a node selected on the NNM map, you must copy the `machview.exe` utility from your SMS CD-ROM to the `smsadmin\x86.bin` directory where SMS Administrator software is installed.

Recommended Logging and Tracing Practices

The following sections discuss the logging and tracing practices of Network Node Manager.

Logging and Tracing

Table C-2 lists the two logging and tracing facilities used by NNM.

Table C-2 Logging and Tracing Facilities

For this service	Use this facility

`pmd`
`netmon`
`ovactiond`
`ovalarmsrv`
`ovcapsd`
`ovrepld`
`ovrequestd`
`snmpCollect`
	Command line options.
	See the reference pages in NNM's online help (or the UNIX manpages) for the command options for these background services.

`ipmap`
`ovspmd`
`ovtopmd`
`ovuispmd`
`ovwdb`
	Windows Event Viewer. Also see the *ovtracelog* reference page in NNM's online help (or the UNIX manpage).
	`nettl` for logging and tracing.
	`netfmt` to format and view the logged data.

NOTE Tracing is normally used only by support personnel. Tracing, especially in the case of `netmon`, can cause the trace file to grow extremely large (multiple megabytes in size) fairly quickly. If you use tracing, remember to monitor the size of the trace file frequently, and turn tracing off as soon as you are finished.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1203
3740
Doc:

Using Command Line Options

The following section describes logging and tracing options for the NNM background services pmd, netmon, ovactiond, snmpCollect, and ovalarmsrv.

The *install_dir*\bin\pmd (`$OV_BIN/pmd`) event logging facility has the following characteristics:

- The default logging is set to ON. Specify the `n` option in the `pmd.lrf` to prevent event logging.
- The event log database is, by default, set to 16 MB. When this space is used up, the oldest log is truncated, and new events are written into the reclaimed space. Refer to the *ov_event* reference page in NNM's online help (or the UNIX manpage) for more information.

The *install_dir*\bin `$OV_BIN/pmd` background service logging facility has the following characteristics:

- The default logging is set to log WARNING, ERROR, and DISASTER.
- The log file is *install_dir*\log\pmd.log0 (`$OV_LOG/pmd.log0`). When this log file is filled to a user-configurable size, its contents are automatically moved to the file *install_dir*\log\pmd.log1 (`$OV_LOG/pmd.log1`).

The *install_dir*\bin\pmd (`$OV_BIN/pmd`) event and service tracing facility has the following characteristics:

- The default tracing is set to OFF. Specify the `T` option in the `pmd.lrf` file to enable tracing.
- The trace file is *install_dir*\log\pmd.trc0 (`$OV_LOG/pmd.trc0`). When this trace file is filled to a user configurable size, its contents are automatically moved to the file *install_dir*\log\pmd.trc1 (`$OV_LOG/pmd.trc1`).
- When tracing is turned on, event traces are also found in the trace file.

The *install_dir*\bin\netmon (`$OV_BIN/netmon`) tracing facility has the following characteristics:

- The default tracing is set to OFF.

- The default trace and hexdump file is *install_dir*\log\netmon.trace ($OV_LOG/netmon.trace).
- To turn tracing on, run netmon -M *tracemask* at the command line, or add the -m *tracemask* option to netmon.lrf.
- To turn tracing off, specify netmon -M 0 (zero).

The following information explains the variable *tracemask* discussed in the netmon tracing facility. Trace masks specify the type of output listed in netmon's trace file. To select multiple output types, add the individual *tracemask* values together and enter the sum. netmon has the following tracing options:

0	Turn off tracing.
1	Trace ICMP echo requests.
2	Trace ICMP echo replies and timeouts.
4	Trace SNMP requests.
8	Trace SNMP replies and timeouts.
16	Trace traps generated.
32	Trace traps received.

Some examples follow. These assume netmon is already running.

To trace ICMP echo replies and timeouts, enter the following command:

```
netmon -M 2
```

To trace ICMP echo replies and timeouts, as well as SNMP replies and timeouts, add their *tracemask* values (2 + 8) to determine the *tracemask* value to enter:

```
netmon -M 10
```

The *install_dir*\bin\ovactiond ($OV_BIN/ovactiond) tracing facility has the following characteristics:

- The default tracing is set to ON.
- The default tracing file is *install_dir*\log\ovactiond.log ($OV_LOG/ovactiond.log) and *install_dir*\log\ovactiond.log.old ($OV_LOG/ovactiond.log.old).
- To turn verbose tracing on and off when tracing is on, specify ovactiond -V (toggle ON/OFF).

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1204
3740
Doc:

- The `-t` option must have a value greater than 0 (zero) to see the return value of the event actions.

The *install_dir*`\bin\ovalarmsrv` (`$OV_BIN/ovalarmsrv`) tracing facility has the following characteristics:

- By default, logs only errors.
- Logs errors to *install_dir*`\log` (`$OV_LOG`) `ovalarmsrv.trace`.

  To change the level of logging that is performed, edit the LRF file and add `-D2` as a parameter. This will increase the logging information (for example, add tracing information as well).

The *install_dir*`\bin\snmpCollect` (`$OV_BIN/snmpCollect`) logging facility has the following characteristics:

- The default logging is set to ON.
- The data that is collected is stored in the file *install_dir*`\log\snmpCol.trace` (`$OV_LOG/snmpCol.trace`).

The *install_dir*`\bin\snmpCollect` (`$OV_BIN/snmpCollect`) tracing facility has the following characteristics:

- The default tracing is set to OFF.
- The default tracing is limited.
- The default trace file is *install_dir*`\log` (`$OV_LOG`) `snmpCol.trace` and *install_dir*`\log` (`$OV_LOG`) `snmpCol.trace.old`.
- To turn the tracing on and off, specify `snmpCollect -T` (toggle ON/OFF) while `snmpCollect` is running.
- To turn verbose tracing on and off when tracing is on, specify `snmpCollect -V` (toggle ON/OFF) while `snmpCollect` is running.
- To trace `snmpCollect` initialization, add the options `-T -V` to *install_dir*`\lrf\snmpCollect.lrf` (`$OV_LRF/snmpCollect.lrf`). This turns off verbose tracing from the moment `snmpCollect` starts up.

Using the Windows Application Event Log

NNM services perform logging (to capture network activities such as state changes, errors and connections) and tracing (to capture inbound and outbound packets going though the network, as well as loopback or header information). All tracing and logging is directed to the Windows

Event Log and can be accessed through the Windows Event Viewer application. See the *ovtracelog* reference page in NNM's online help (or the UNIX manpage) for further details. You can use the following troubleshooting tools:

- **tracing**, which records a detailed record of internal events taking place within the software. Tracing of the NNM background services is generally only used on the advice of HP Support to diagnose difficult problems, with the aid of the source code. API tracing is used by developers to determine whether they are using the HP OpenView APIs correctly.
- **logging**, which records externally-observable events such as connection establishment or termination of child services, and errors, which background services ordinarily have no other way of reporting.

Users should run tracing only when something is seriously wrong, and only on the advice of your HP support representative when it is necessary to reconstruct in detail the sequence of events that caused the problem. The trace output is intended to be interpreted by the developers of the NNM product, with the source code at hand. It is not intended to be meaningful to the ordinary user.

Using nettl and netfmt (UNIX operating systems only)

`nettl` and `netfmt` enable system administrators and developers to gather and view data about the operation of NNM software. `nettl` is the administrative interface to the tracing and logging facilities discussed previously.

It is recommended that you run the `nettl` logging facility at all times. This way, you can view the constantly updated log file to help you determine what happened when something goes wrong. Also, paradoxically, performance is better when logging is turned *on*.

`netfmt` formats the log and trace output into human-readable form.

Services use `nettl` to log or trace in particular subsystems. To examine the log or trace output of a service, you need to know the name of the subsystem the service uses. Table C-3 shows the subsystems and services.

NOTE The `nettl` and `netfmt` commands are in `$OV_BIN`. For example, to run the `nettl -status` command, you would type:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1205
3740
Doc:

```
$OV_BIN/nettl -status
```

Table C-3 Subsystem Services

Subsystem	Services Using this Subsystem	Purpose of Service
OVS	ovspmd	Starts and stops NNM background services.
OVW	ovwdb, ipmap	Provides access to object database. Automatically draws IP topology maps.
OVEXTERNAL	ovuispmd; ovtopmd; also any third-party-developed software using the OVuTL facility.	Maintains the topology database.
OVWAPI	Any software using the OVw (HP OpenView Windows) API.	Provides programmatic application integration points.

Capturing Logging and Tracing Output with nettl (UNIX operating systems only)

1. To determine whether the logging/tracing facilities are currently running, type the following command as root:

   nettl -status

   The output includes the log and trace status for each active subsystem.

2. If necessary, use the nettl command to start the logging/tracing facilities. As root, type the following command:

   nettl -start

   This command initializes the logging/tracing facilities and starts the default logging. By default, the OVS, OVW, OVWAPI, and OVEXTERNAL subsystems log error and disaster messages; the OVS subsystem also logs informative messages.

3. Once nettl is running, you can use command options to customize the kind of data you want to capture for any of the nettl subsystems shown in the previous table. The next section contains examples of various nettl commands.

Examples of nettl Commands Use the following examples to get started. After you have captured the data you want, go to "Formatting Network Data with netfmt" on page 649 in this section.

- **Logging Facility** - Turning it on.

  There are four classes of logging messages: informative (i), warning (w), error (e), and disaster (d). Default logging always includes disaster-class messages; you can turn on any of the other three classes by typing a nettl command for a specific subsystem.

  The command syntax is:

```
nettl -log class -entity subsystem OVEXTERNAL
```

`-log class`

Specifies the classes of logging to be turned on for the specified subsystems.

`-entity subsystem`

Specifies the subsystems for which logging is to be modified. *For logging done by HP OpenView products,* OVEXTERNAL *must always be in the list.*

Example 1:

Turn on logging of informative messages for the ovw subsystem. As root, type the following command:

```
nettl -log i -entity OVW OVEXTERNAL
```

Note that this command will turn off any log classes not listed in the command (in this example, the warning and error messages would be turned off). The one exception is disaster logging, which cannot be turned off.

Example 2:

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1206
3740
Doc:

Turn on logging of informative, warning, and error messages for the OVS subsystem. As root, type the following command:

```
nettl -log i w e -entity OVS OVEXTERNAL
```

- **Tracing Facility** - Turning it on.

  There are eight kinds of tracing that nettl can turn on, as shown in the following table.

Table C-4 Tracing Facilities Activated by nettl

Type of Tracing	Keyword	Mask Number
inbound header tracing	hdrin	0x80000000
outbound header tracing	hdrout	0x40000000
inbound PDU tracing	pduin	0x20000000
outbound PDU tracing	pduout	0x10000000
procedure entry/exit tracing	proc	0x08000000
state machine tracing	state	0x04000000
error tracing	error	0x02000000
log call tracing	logging	0x01000000

The command syntax is:

nettl -traceon *kind* -entity *subsystem* OVEXTERNAL -file *filename*

-traceon *kind*

Specifies the kinds of tracing to be turned on for the specified subsystems.

-entity *subsystem*

Specifies the subsystems for which tracing is to be turned on. *For tracing done by HP OpenView products,* OVEXTERNAL *must always be in the list.*

-file *filename*

Specifies the prefix of the trace file you want to create. Trace output will be written to *file*.TRC0 and *file*.TRC1. (See "How nettl Generates the Binary Data Files" on page 648 for a description of these two trace files.)

Example 1:

Do error tracing for the OVW subsystem, putting the data in the trace files, /tmp/nettl.TRC0 and /tmp/nettl.TRC1. As root, type the following all on one line:

```
nettl -traceon error -entity OVW OVEXTERNAL -file /tmp/nettl
```

Example 2:

Do both inbound and outbound PDU tracing for the ovw subsystem, putting the data in the trace files, /tmp/nettl.TRC0 and /tmp/nettl.TRC1. To enable more than one kind of tracing, either specify all the appropriate keywords, all the appropriate mask numbers, or the logical OR of the mask numbers. As root, type one of the following command variations:

```
nettl -traceon pduin pduout -entity OVW OVEXTERNAL -file /tmp/nettl
```

or

```
nettl -traceon 0x20000000 0x10000000 -entity OVW OVEXTERNAL -file /tmp/nettl
```

or

```
nettl -traceon 0x30000000 -entity OVW OVEXTERNAL -file /tmp/nettl
```

NOTE Do not leave off the -file argument to nettl -trace on! If you do, unformatted trace output will be sent to your screen.

- **Tracing Facility** - Turning it off.

  While logging should always remain on, you should run the tracing facility only when a serious problem occurs, and it is necessary to reconstruct in detail the sequence of events that caused the problem. After you have completed a trace, you should turn tracing off.

  The command syntax is:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1207
3740
Doc:

```
nettl -traceoff -entity subsystem
```

`-traceoff` Specifies that tracing is to be turned off for the specified subsystems.

`-entity subsystem`

Specifies the subsystems for which tracing is to be turned off. To turn tracing off completely, specify all subsystems for which tracing is currently on.

Note that you cannot turn off trace kinds individually. To change the trace kinds enabled for a subsystem, turn tracing off for that subsystem, then turn tracing back on for the particular kinds in which you are interested.

Example 1:

Disable tracing for the `OVEXTERNAL` subsystem. As `root`, type the following command:

```
nettl -traceoff -entity OVEXTERNAL
```

- **Logging and Tracing Facilities** - Turning both off.

  To stop the logging/tracing facilities, as `root`, type the following command:

  ```
  nettl -stop
  ```

How nettl Generates the Binary Data Files The first time you run a `nettl` command for capturing logging data, the log file `nettl.LOG00` is generated. Binary data captured from each successive `nettl` logging command is appended to this file, until it is filled. Then a second log file with the suffix `.LOG01` is created in which new data is stored. When this second file fills up, the `.LOG00` file is overwritten.

When you run a `nettl` command for capturing trace data, you specify a filename prefix, to which the suffix `.TRC0` is added. For each successive `nettl` tracing command, you can have the binary data appended to this file, or you can specify a new file in which to store the data. If you append binary data from successive traces to the same file, it will eventually fill up. A new file with the same prefix and the suffix `.TRC1` will then be created for storing new data. If this second file fills up, then a new trace file with the same prefix and the `.TRC0` suffix is created.

If you need to check the name of a log file before formatting it with `netfmt`, use a `nettl -status` command.

Formatting Network Data with netfmt The command syntax is:

`netfmt -f binary_file`

`-f binary_file`

Specifies the log or trace file containing the binary data

It is possible to do elaborate filtering of the output, as `netfmt` has many other options that cannot be described here. Some of these options, for example, let you specify the output of a log or trace file to be filtered by timestamp, subsystem, or message class. UNIX only: for more information, see the *netfmt* manpage.

Examples of netfmt Commands The following example will help you start using the `netfmt` command.

To format the log file, `$NETFMT_LOG_FILE`, type

`$NETFMT/netfmt -f $NETMFT_LOG_FILE | more`

The next section shows what the output of `netfmt` looks like.

Log and Trace File Output Below are two complete examples of using the `nettl` and `netfmt` commands, and the final output you might see.

Example 1:

1. You ran a `nettl` logging command for informative messages in the OVW subsystem, in order to observe the startup of the `ovspmd` service, by typing:

   `nettl -log i e d -entity OVS OVEXTERNAL`

   The binary data was stored in the `$NETFMT_LOG_FILE` log file.

2. You formatted and displayed the binary log file by typing:

   `netfmt -f $NETFMT_LOG_FILE | more`

   The output would be similar to the following:

```
**********OpenView**********@#%

Timestamp         : Wed Nov 17 1995 17:28:58.441517
Process ID        : 22756          Subsystem     : OVS
User ID ( UID )   : 0              Log Class     : INFORMATIVE
Device ID         : -1             Path ID       : -1
Connection ID     : -1             Log Instance  : 0
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1208
3740
Doc:

```
Software          : ovspmd
Hostname          : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Initialized successfully:
ovspmd

**********OpenView**********@#%

Timestamp         : Wed Nov 17 1995 17:28:59.352086
Process ID        : 22756          Subsystem      : OVS
User ID ( UID )   : 0              Log Class      : INFORMATIVE
Device ID         : -1             Path ID        : -1
Connection ID     : -1             Log Instance   : 0
Software          : ovspmd
Hostname          : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Accepted request connection (fd 5)

**********OpenView**********@#%

Timestamp         : Wed Nov 17 1995 17:28:59.355761
Process ID        : 22756          Subsystem      : OVS
User ID ( UID )   : 0              Log Class      : INFORMATIVE
Device ID         : -1             Path ID        : -1
Connection ID     : -1             Log Instance   : 0
Software          : ovspmd
Hostname          : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Received request,  fd 5
[9]  [START] ""

**********OpenView**********@#%

Timestamp         : Wed Nov 17 1995 17:28:59.358398
Process ID        : 22756          Subsystem      : OVS
User ID ( UID )   : 0              Log Class      : INFORMATIVE
Device ID         : -1             Path ID        : -1
Connection ID     : -1             Log Instance   : 0
Software          : ovspmd
Hostname          : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Building master M table from $OV_CONF/ovsuf

**********OpenView**********@#%

Timestamp         : Wed Nov 17 1995 17:28:59.366810
Process ID        : 22756          Subsystem      : OVS
User ID ( UID )   : 0              Log Class      : INFORMATIVE
Device ID         : -1             Path ID        : -1
Connection ID     : -1             Log Instance   : 0
```

```
Software          : ovspmd
Hostname          : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Reporting M status,  code = SUCCESS
    object manager name:  OVsPMD
    behavior:             OVs_PMD
    state:                RUNNING
    PID:                  22756
    exit status:          -
```

Example 2:

1. You ran a nettl tracing command for procedure tracing in the OVEXTERNAL subsystem, in order to observe some procedure calls in ipmap, by typing:

```
nettl -traceon proc -entity OVEXTERNAL -file $NETFMT_LOG_FILE
```

The binary data was stored in the trace file $NETTL_TRC_FILE.

2. You formatted the binary trace file by typing:

```
netfmt -f $NETTL_TRC_FILE > outfile
```

A brief fragment of the output appears below:

```
*********************OpenView*************************************@#%

Timestamp         : Wed Nov 17 1993  18048:44.443027
Process ID        : 23059          Subsystem      : OVW
User ID ( UID )   : 214          Trace Kind       : Proc. Entry/Exit
Device ID         : -1               Path ID      :  -1
Connection ID     : -1
Software          : $OV_BIN/ipmap
Hostname          : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

FieldBinding::FieldBinding(OVwFieldBinding) entered

*********************OpenView*************************************@#%

Timestamp         : Wed Nov 17 1993  18:04:44.444646
Process ID        : 23059          Subsystem      : OVW
User ID ( UID )   : 214            Trace Kind     : Proc. Entry/Exit
Device ID         : -1             Path ID        : -1
Connection ID     : -1
Software          : $OV_BIN/ipmap
Hostname          : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

FieldBinding::init() entered

*********************OpenView*************************************@#%
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1209
3740
Doc:

```
Timestamp         : Wed Nov 17 1993  18:04:44.446053
Process ID        : 23059          Subsystem      : OVW
User ID ( UID )   : 214            Trace Kind     : Proc. Entry/Exit
Device ID         : -1             Path ID        : -1
Connection ID     : -1
Software          : $OV_BIN/ipmap
Hostname          : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

FieldBinding::init() exit

*********************OpenView*********************************@#%

Timestamp         : Wed Nov 17 1993  18:04:44.447404
Process ID        : 23059          Subsystem      : OVW
User ID ( UID )   : 214            Trace Kind     : Proc. Entry/Exit
Device ID         : -1             Path ID        : -1
Connection ID     : -1
Software          : $OV_BIN/ipmap
Hostname          : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

FieldBinding::copyFieldValue() entered

*********************OpenView*********************************@#%

Timestamp         : Wed Nov 17 1993  18:04:44.448754
Process ID        : 23059          Subsystem      : OVW
User ID ( UID )   : 214            Trace Kind     : Proc. Entry/Exit
Device ID         : -1             Path ID        : -1
Connection ID     : -1
Software          : $OV_BIN/ipmap
Hostname          : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

FieldBinding::copyFieldValue() exit

*********************OpenView*********************************@#%

Timestamp         : Wed Nov 17 1993  18:04:44.450233
Process ID        : 23059          Subsystem      : OVW
User ID ( UID )   : 214            Trace Kind     : Proc. Entry/Exit
Device ID         : -1             Path ID        : -1
Connection ID     : -1
Software          : $OV_BIN/ipmap
Hostname          : pinetum.cnd.hp.com
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

FieldBinding::FieldBinding(OVwFieldBinding) exit
```

Web Launcher Error Log

The Launcher error log records internal errors from the Launcher. You can use the output from this file when discussing a problem with HP support personnel.

The Launcher error log file is located in:

Windows: `install_dir\www\logs\launcher\error_log`

UNIX: `/var/opt/OV/www/launcher/error_log`

The error log contains the following information:

- Date
- Host
- User
- Session
- Reason or error

The error log file continues to grow without bounds. You need to watch the size of this file and truncate it as needed.

If the error log file does not give you sufficient information for troubleshooting, you can set a parameter in the URL for `ovlaunch.exe` that will enable more in-depth error logging on a session level.

The parameter is:

`http://hostname:[port]/OvCgi/ovlaunch.exe?Debug=/tmp/file`

The output of this file is less "friendly" than other error log files, but it contains valuable information that may be useful to an HP support person who is trying to assess the problem.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1210
3740
Doc:

Improving Traffic Management and Performance

Traffic Management

Status polling generates the most network traffic. You can monitor the traffic generated by NNM by using the `netstat -s` command. Run the `netstat -s` command several times and observe the differences in the number of packets sent and received. Be sure that the management station is not generating any other outbound traffic. Note that the command used to show the number of packets sent and received may be different depending on the operating system you use. Make sure that you are using the appropriate command.

You can regulate the traffic generated by NNM through the following methods:

- Adjust polling intervals through the `Options:SNMP Configuration` or `Options:Network Polling Configuration` menu item. Reducing the amount of polling traffic by lengthening polling intervals may delay real-time map updates, resulting in a less accurate map.
- Apply a discovery filter to ensure that you are monitoring only what needs to be monitored.
- Unmanage nodes with the `Edit:Unmanage Objects` menu item such that you are monitoring only what really needs to be monitored. Note that this tactic decreases the amount of available management information for unmanaged nodes.
- Adjust the amount of MIB data that is collected through the `Options:Data Collection & Thresholds:SNMP` menu item. You can:
  - — Stop collecting MIB data on some of the MIB objects that are configured to collect data by changing the status to `Suspend`.
  - — Modify the details of the configured MIB objects by either deleting nodes, deleting instances, excluding nodes, or changing polling intervals.

If NNM starts to use excessive swap space, performance may decrease. To check the size of ovw (and other services), use `Help:About HP OpenView`, and click `More Info`. If the service grows too large, exit NNM and restart it. (The program automatically saves the map between invocations.)

`netmon` will generate some network broadcast traffic; how much traffic depends on several factors.

- If you use `netmon` without the `-J` option, `netmon` generates, if necessary, just an ARP Request. There are several factors that determine whether `netmon` needs to generate an ARP Request.
  - For nodes that are up, but not on the same subnet where the management station is, `netmon` generates just one ICMP echo request packet and gets back one response. In this case, no ARP Request is generated.

    Because the management station is on a different subnet, a request will go through a gateway. Gateways always have large ARP caches. `netmon` knows the gateway's link-level address and does not have to broadcast an ARP Request to that gateway. `netmon` only has to send one ICMP echo request through the gateway and gets back one response.
  - For devices that are on the same subnet as the management station, `netmon` may generate just one ICMP echo request, or it may also generate one ARP Request as well. Because the nodes are on the same subnet, `netmon` does not have to go through a gateway. Broadcasting an ARP Request will depend on whether or not `netmon` has in its own ARP cache in the device's link-level address.
  - `netmon` will generate an ARP Request based on whether the address that is being polled for status is still in the ARP cache of that system.

    The presence of the address in the ARP cache is affected by how many nodes are on the subnet, and by how much physical memory is in the system (some systems will automatically adjust the size of their ARP table).
- If invoked with the `-J` option, `netmon` may cause up to three broadcast ICMP echo requests to be broadcast on each subnet it discovers. These broadcasts will only be issued on a subnet if:

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1211
3740
Doc:

  - No broadcast ICMP echo request has ever been issued on this subnet on behalf of this management station.
  - An agent capable of issuing a broadcast ICMP echo request on netmon's behalf has been discovered on this subnet. All HP-UX SNMP agents have this capability.
- The amount of netmon's broadcast traffic also depends on your network's configuration, including:
  - How many nodes are up and how many are down.
  - How many nodes are on the same subnet.
  - How many nodes are on other subnets.
  - How large the permanent ARP cache is.
  - How probable it is that a particular IP address can be found in the permanent ARP cache.
- For IPX discovery, netmon uses broadcast IPX packets as the basis of its discovery. The following broadcasts occur for each discovery interval:
  - A single broadcast RIP request.
  - A single broadcast SAP request.
  - Two broadcast IPX diagnostic requests for each known IPX network, 10 seconds apart.
  - You can change or schedule the IPX discovery interval using `Options:Network Polling Configuration` operation

Performance

The performance of NNM is limited primarily by three factors:

- The amount of memory installed in the manager system.
- The management station's processor (CPU) speed.
- The performance of the graphical display adapter (X Windows).

Minimum system requirements and memory recommendations are detailed in the *Performance and Configuration* guides for NNM.

One good way to find out if your management station has sufficient memory is to select the icon for your management station on the map. Then select the `Performance:Network Polling Statistics` menu item. If the graph shows negative numbers, the polling queue has fallen behind because of resource shortage.

Following are some tips to conserve memory and increase performance:

- You may want to install additional memory and/or upgrade your CPU.
- Reduce the number of devices that need to be monitored, thus decreasing the polling load. Refer to "Controlling the Amount of Traffic Generated by NNM" on page 178 for more information.
- Change the polling interval setting to a less frequent interval. Refer to "Controlling the Amount of Traffic Generated by NNM" on page 178 for more information.
- If you are currently running OVW sessions directly on a management station, you can improve system performance by running OVW sessions on an NNM remote console instead.
- You can reduce NNM's memory usage by changing `ipmap`'s persistence level to a higher level than `All Levels`. See *A Guide to Scalability and Distribution* for more information.
- Run `ipmap` with the `-D 2` option. This option prevents the automatic creation of node submaps for end nodes (unless an end node is a gateway). Nodes with submaps that have not been created are marked with an empty string on the label. See the *ipmap* reference page in NNM's online help (or the UNIX manpage) for information on how to use the `-l` or `-L` options to modify this empty string. Double-clicking on such a node will result in the creation of the submap. The advantage of this option is that no memory is used for end node submaps that are never viewed. The disadvantage is that the locate operation will not work for addresses for end nodes.

  The option can be set in:

  Windows: `install_dir\registration\C\ipmap`

  UNIX: `$OV_REGISTRATION/C/ipmap`
- Partition the environment into multiple maps. See "Partitioned Internet Submaps" on page 248 for more information on partitioning submaps.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1212
3740
Doc:

- Delete unwanted nodes. After the nodes on a particular network have been discovered, you may want to delete some of the nodes, for example, PCs that are not being managed directly.
- Restart the system after active discovery. Some extra memory is consumed in the source of active discovery. After active discovery is finished, it may help to stop and restart the system to recover memory used during the discovery process.
- Use the on-demand submap feature, which may greatly reduce the amount of memory required. The drawback is that when opening transient submaps, some extra processor work will be expended and some delay may be noticeable.
- NNM on a Windows operating system performs best if you use DNS. If you are going to use DNS, enable DNS for Windows Resolution and configure DNS correctly. In particular, when installing NNM, the IP hostname and Windows computer name of the intended NNM Manager must be correct and identical.

Performance on UNIX Operating Systems

On UNIX operating systems only, you can also increase performance in some cases by minimizing file system swapping. NNM performance is best when there is no file system swapping required. With no file swapping, `ovwdb` is running as efficiently as possible; all the object information it is managing is residing in physical memory. Any system swapping that must be done is affected by two factors: the number of objects maintained in physical memory, and the service size limit.

- If you have a system where NNM performance is poor due to file system swapping, you may use the `-n` option for `ovwdb` to limit the maximum number of objects that `ovwdb` can keep in physical memory, while storing the rest in a database.

  Note that this option is not always an appropriate solution for memory problems due to file swapping, and it is not a good performance enhancement because `ovwdb` database queries are often random. For example, a `locate` operation will cause a query over many objects in searching for a field value. In this operation, using the `-n` option would cause `ovwdb` to update the cache with each object involved in the search, as well as with all the field values for those objects. The best way to correct poor performance due to file system

swapping is to increase the amount of physical memory available to ovwdb. More physical memory reduces the amount of swapping needed.

If the -n option is not used (the default state), ovwdb will continue to grow as new objects are created until either:

— The maximum service size limit is reached.

— The system swap space is exhausted.

- Another factor that can limit the number of objects managed by ovwdb is the service size limit. If the maximum service size limit is reached, ovwdb will terminate. For information on increasing the service size limit, see the appropriate UNIX operating system administration guide.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1213
3740
Doc:

D Changing All the Symbols for a Particular Device

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1214
3740
Doc:

Procedure

Each of the following steps is explained in more detail in the example beginning on page 663.

NOTE Back up any files before you modify them.

1. Create a *symbol registration file* to add a new symbol subclass.
2. Copy and modify a set of GIF graphic files for your new symbol and place the new set of GIF files into two locations.
3. Map a specific `sysObjectID` to the new symbol by editing the `oid_to_sym` file.
4. Create a *field registration file* to define the appropriate capabilities for each new database field specified in the symbol registration file (step 1).
5. Force NNM to add the new field definitions to the database.
6. Ensure that the `sysObjectID` is listed in the `oid_to_type` file (or `HPoid2type` file) to provide information to NNM about the vendor and SNMP agent for the device you are mapping to the new symbol. This file can also be used to provide NNM with additional useful information about the device.
7. Force NNM to acknowledge your changes and update the map.
8. Open the NNM map and verify the changes.

Complete information about registration files is available in NNM's online manual, *Creating and Using Registration Files*.

Example

In this example, you will make NNM display customized symbols for HP 9000 Series 700 workstations, rather than the predefined HP-UX workstation symbol.

If you follow this example, be sure that you back up any files before modifying them. You will modify the following files in this example:

- *Windows:*

  install_dir\symbols\C\Computer\Computer_workstation

  install_dir\www\htdocs\bitmaps\C\computer\workst.16.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.20.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.26.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.32.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.38.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.44.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.50.gif

  install_dir\conf\oid_to_sym

  install_dir\conf\oid_to_type

- *UNIX:*

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.16.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.20.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.26.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.32.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.38.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.44.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.50.gif

  $OV_CONF/oid_to_sym

  $OV_CONF/oid_to_type

ECT 2228
ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1215
3740
Doc:

Create a Symbol Registration File

Because NNM provides a rich set of classes (shape outlines), you will rarely create an entirely new class of symbols. You almost always will be adding subclasses (graphics imposed over the shape) to an existing class.

To create a new subclass, create a new symbol registration file:

1. Copy the following file and name it **`Computer_workstation_700`**. Place the new file in the same directory as the original file:
   - *Windows:*

     install_dir`\symbols\C\Computer\Computer_workstation`
   - *UNIX:*

     `$OV_SYMBOLS/$LANG/Computer/Computer_workstation`
2. Edit the new symbol registration file named `Computer_workstation_700`. Modify the file to look like this:

```
SymbolType "Computer" : "HP700"
{
  Filebase "HP700";
  CursorSize 38;

  Capabilities {
    isHP700 = 1;
  }
}
```

   Any file found in this directory is assumed to be a registration file. If you used a text editing program that makes an automatic backup of any file you edit, be sure to remove the backup file.
3. Change the permissions on the file to read-only.

Copy and Modify the Symbol Graphics

You need a *set* of GIF files to provide multiple sizes of the same graphic so that when you resize the map, the graphics grow and shrink. The easiest way to create custom graphics is to copy an existing set and modify each file. Open NNM and select `Help:Display Legend` to see the existing collection of symbol graphics.

Each set of GIF files contains several files by the same name with different numbers. The numbers indicate the pixel size of the square GIF image (20x20, 50x50). For this example, use:

- *Windows:*

  install_dir\www\htdocs\bitmaps\C\computer\workst.16.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.20.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.26.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.32.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.38.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.44.gif

  install_dir\www\htdocs\bitmaps\C\computer\workst.50.gif

- *UNIX:*

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.16.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.20.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.26.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.32.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.38.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.44.gif

  $OV_WWW/htdocs/bitmaps/$LANG/computer/workst.50.gif

1. Copy this set of `workst.##.gif` files and give them new meaningful names (for this example, use the name `HP700.##.gif`). Place them in the same directory as the ones you copied. Be sure to follow the naming scheme using the numbers in the file extensions
2. Change the permissions on the new GIF files so that you can modify them using the graphics program of your choice.

   Start with size 16. Because of size, this one is the hardest to modify. Write `700` inside the workstation's display screen in each GIF image.
3. Set the file permissions on the finished HP700 GIF files to read-only.
4. The graphic files for the symbols, themselves, are stored in two places: one directory used by NNM on the management station, and one directory used by the NNM web-based interface. (The web-based interface requires GIF files. Other additional graphic file formats are supported on the management station.)

ECT
ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1216
3740
Doc:

Place a copy of the new GIF files into the following directory for use by NNM on the management station. Don't worry if they are the only GIF files in this directory, because NNM ships with pixmaps:

Windows: `install_dir\bitmaps\C\computer`

UNIX: `$OV_BITMAPS/$LANG/computer`

TIP

Symbols in the web-based interface have the same appearance as in NNM on a management station, except that the symbol labels do not scale in the web-based interface. Instead, a long label is truncated to fit the space available.

Map a sysObjectID to the New Symbol

NNM determines which symbol to draw on the map for a particular `sysObjectID` by referencing the entries in the `oid_to_sym` file. For additional information, refer to the comments at the top of the `oid_to_sym` file or the *oid_to_sym* reference page in NNM's online help (or the UNIX manpage).

NOTE

While you are editing the file, note the many-to-one relationship between `sysObjectIDs` and symbols in the `oid_to_sym` file. You can specify "leaf" values of `sysObjectIDs` in the `oid_to_sym` file. For example, specify two `sysObjectIDs` separately:

```
1.3.6.1.4.1.11.2.3.2.2:Computer:HP-UX # 300
1.3.6.1.4.1.11.2.3.2.5:Computer:HP-UX # 700
```

A limited use of wildcards is allowed. Only a single * can exist as the last entry in a `sysObjectID` number sequence.

```
1.3.6.1.4.1.9.1.*:Computer:XX #Cisco devices use XX symbol
```

1. Locate the following file:
   - *Windows:* `install_dir\conf\oid_to_sym`
   - *UNIX:* `$OV_CONF/oid_to_sym`

2. Make a backup copy of the `oid_to_sym` file, if you have not already done so.
3. Edit the `oid_to_sym` file to modify the line referring to HP 9000 Series 700 workstations. Your changes map this device to the new HP700 subclass instead of the existing HP-UX workstation subclass.

   Old line:

```
1.3.6.1.4.1.11.2.3.2.5:Computer:HP-UX #700
```

   New line:

```
1.3.6.1.4.1.11.2.3.2.5:Computer:HP700 #700
```

Define the Capabilities for Computer_workstation_700

Now create a *field registration file* to define the `isHP700` capabilities field referred to in your `Computer_workstation_700` *symbol registration file*. Whenever the discovery and layout process creates a symbol of type `Computer:HP700`, it will automatically set the `isHP700` field to `TRUE`.

Complete information about field registration files is available in the NNM online manual, *Creating and Using Registration Files*.

Fields are defined in field registration files:

- *Windows:* *`install_dir`*`\fields\C\*.*`
- *UNIX:* `$OV_FIELDS/`*`$LANG`*`/*`

1. In this directory, create a new file called `HP700` and enter this information:

```
Field "isHP700" {
  Type  Boolean;
  Flags Capability;
}
```

   Any file found in this directory is assumed to be a registration file. If you used a text editing program that makes an automatic backup of any file you edit, be sure to remove the backup file.

2. *UNIX operating systems only:* Make sure the file is readable. At the command prompt, type:

```
chmod 644 HP700
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
1217
Fls. Nº
5740

NOTE You can specify directories other than the default directories by using environment variables, such as `OVwRegDir`, `OVwFieldDir`, and `OVwSymbolDir`.

For each registration file found, NNM executes the following steps:

a. Opens the file

b. Parses it for correctness

c. Prints any error information to the `Console` window when using a Windows operating system (to `stdout` on UNIX systems) indicating the file and line where the error occurred. Possible errors include:

- Duplicate entries
- Ill-formed entries

NOTE If you see error messages, verify the contents in the `HP700` file. Return to step 1 in "Define the Capabilities for Computer_workstation_700" on page 667 to correct sytax errors.

Provide Additional Information in the oid_to_type File

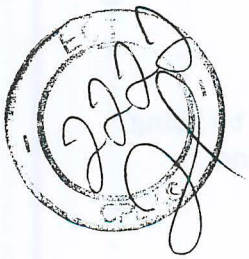
The `oid_to_type` file is used by `netmon` to map `sysObjectIds` to the correct vendor and SNMPAgent values for use with `ovw` and `ovwdb`. Applications integrated with NNM use the `vendor` and `SNMPAgent` values to determine which menu options are active for particular devices.

This file can also be used to provide topological information to NNM. For example, use this file to automatically set all devices with this `sysObjectId` to *unmanaged* or fine-tune the manner in which NNM identifies devices with this `sysObjectId`.

The file is located in:

- *Windows:* *install_dir*`\conf\oid_to_type`
- *UNIX:* `$OV_CONF/oid_to_type`

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1218
3740
Doc:



Their are four fields for each entry in the file:

sysObjectId:vendor:SNMPAgent:IP Map Topology Attributes

For information about controlling the vendor and SNMPAgent values, see Appendix E, "Changing an Object's Vendor and SNMP Agent," on page 675. For information about providing IP Map topology attributes for a specific device, refer to the comments at the top of the `oid_to_type` file and refer to the *oid_to_type* reference page in NNM's online help (or the UNIX manpage).

In general, you will not need to modify the `oid_to_type` file because extensive information by `sysObjectIds` is already included.

There are actually two files that NNM uses for this purpose: `oid_to_type` and `HPoid2type`. The `HPoid2type` file contains the HP `sysObjectId` list. The important difference between these files is:

- `oid_to_type`

  If you make changes to this file, your changes will be preserved the next time you install a patch or upgrade for NNM.

- `HPoid2type`

  If you make changes to this file, your changes will be lost the next time you install a patch or upgrade for NNM.

For this example, you do not need to make any changes. Since the HP 9000 Series 700 workstation is an HP device, the `sysObjectId`: `1.3.6.1.4.1.11.2.3.2.5` is located in the `HPoid2type` file.

Update the Database

You must now ask the topology manager to update the database, so the new symbols you created appear on the map.

1. Log in as:
   - *Windows:* `Administrator`
   - *UNIX:* `root`
2. With all the NNM processes running, shut down just the `netmon` service. From the command prompt, type:

   `ovstop -c -v netmon`
3. Update the database by using the `ovtopofix` command.

3. Resize a submap window that contains one of the HP 700 symbols. Does resizing the submap cause the different bitmap sizes to be used? Do the bitmaps look acceptable?

Back Up Your Efforts

The next regularly scheduled backup will save some of the files associated with your new symbols. See "Backup/Restore to Protect Your Investment of Time" on page 165.

TIP

The following *analytical data* directories are *not* included in NNM's backup scripts:

- *Windows:*

  ```
  install_dir\backgrounds
  install_dir\bitmaps
  install_dir\www\htdocs\bitmaps
  install_dir\www\registration
  ```

- *UNIX:*

  ```
  $OV_BACKGROUNDS
  $OV_BITMAPS
  $OV_WWW/htdocs/bitmaps
  $OV_WWW_REG
  ```

If you make changes or additions to map backgrounds, bitmap files, or web registration files ensure that your new files are properly backed up.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1219
3740
Doc:



Changing All the Symbols for a Particular Device

Example

ECT
22
CT-02

E Changing an Object's Vendor and SNMP Agent

RQS nº 03/2000 - CN -
CPMI - CORREIOS
Fls. Nº 1220
3740

How NNM Discovers Vendor and SNMP Agent Values

This appendix describes how to modify the appropriate files to correctly set the vendor and SNMP agent fields for a particular device.

NNM automatically discovers all IP-addressable devices on your network (and IPX-addressable devices, if configured to do so on a management station running a Windows operating system). If the device has a responding SNMP agent (or proxy) that supports MIB II, then NNM will query the agent to find more information about the device. One of the pieces of information retrieved from the agent is the SNMP system object ID (`sysObjectID`) of the device:

```
iso.org.dod.internet.mgmt.mib-2.system.sysObjectID (1.3.6.1.2.1.1.2)
```

See "Unique Properties of the SNMP MIB Object sysObjectID" on page 465.

The discovery service then looks at the mappings defined in the `HPoid2type` and `oid_to_type` files. These ASCII files are used to set the value of the vendor and SNMP agent fields for the object.

NOTE The `HPoid2type` file contains entries that are *required* by NNM. You should *never* modify `HPoid2type`.

If no `sysObjectID` is returned by the device (that is, there is no SNMP agent running on the device) or no entry is found in these files that match the returned `sysObjectID`, the vendor and SNMP agent fields are not set. These fields are important because they can be used in the *selection rule* for certain menu items. This means that if these fields are not set, certain menu items may not be available.

These fields can also be used in `Edit:Find->Objects By Attribute`. This allows you to locate all the devices from a specific vendor. Or you can locate all the devices running a particular SNMP agent.

The vendor and SNMP agent fields for an object can be viewed from the main menu bar by selecting a symbol and `Edit:Object Properties`. Double-clicking on `General Attributes` in the `Object Attributes` list displays the `SNMPAgent` and `vendor` fields.

When the Vendor and SNMP Agent Would Not Be Set

The vendor and SNMP agent fields for a particular object are not set if:

- There is no SNMP agent running on the device; therefore the `sysObjectID` value was never passed to NNM.
- The device's `sysObjectID` does not have a corresponding entry in either the `oid_to_type` file or the `HPoid2type` file.
- The entry in the `oid_to_type` file does not contain valid values for the vendor and SNMP agent fields of the entry.

If the `oid_to_type` file contains an entry for the `sysObjectID` but the values specified for the vendor and SNMP agent are not in the corresponding field registration files, an error will be generated when NNM is started, and the fields for that object will not be set.

The vendor and SNMP agent field values are enumerated types that are defined in the following files:

- *Windows:*

  install_dir`\fields\C\ovw_fields` and

  install_dir`\fields\C\snmp_fields`

- *UNIX:*

  `$OV_FIELDS/$LANG/ovw_fields` and

  `$OV_FIELDS/$LANG/snmp_fields`

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 677
1221
Doc 3740

Procedure

This is the procedure for correctly modifying the appropriate files to set the vendor and SNMP agent fields for a particular device. These steps are explained in greater detail in the example that follows.

NOTE Most systems require `sysadmin` or `root` access to perform the following tasks.

During this procedure, you should not start any new sessions. If you do, the new sessions will use the partially built files and exit with errors. It is not necessary to shut down any NNM services. *You do need to* stop and restart NNM sessions, but not until the last step in the procedure. This minimizes loss of service.

1. Three files need to be examined and possibly modified:
   a. `oid_to_type`

      Add or modify the entry for the `sysObjectID`.
   b. `ovw_fields`

      Add the new vendor value.
   c. `snmp_fields`

      Add the new SNMP agent value.
2. Reinitialize the field values.
3. Force the `netmon` service to reread the `oid_to_type` file.
4. Force the `ipmap` service to use the new `oid_to_sym` mapping by closing and reopening the map.

TIP See Appendix D, "Changing All the Symbols for a Particular Device," on page 661 for information about creating and assigning your own custom symbols to a particular `sysObjectID`.

Example

The following example takes you through all the required steps in greater detail.

oid_to_type

NNM identifies each device by referencing the information contained in two configuration files:

- *Windows:*

  install_dir\conf\oid_to_type

  install_dir\conf\HPoid2type (Do *not* edit this one.)

- *UNIX:*

  $OV_CONF/oid_to_type

  $OV_CONF/HPoid2type (Do *not* edit this one.)

Although the entries in these files are already extensive, you may encounter a situation where you want to make additions or changes to the oid_to_type file.

See the instructions at the beginning of the oid_to_type ASCII file. See also the *oid_to_type* reference page in NNM's online help (or the UNIX manpage) for more information.

For this example, the sysObjectID is: 1.3.6.1.4.1.99.1.1

In the oid_to_type file, use an ASCII editor to add the following entry:

```
1.3.6.1.4.1.99.1.1:NewVendor:New SNMP Agent:B
```

ovw_fields and snmp_fields

The field registration files contain valid values for the object fields. The ovw_fields files contain the valid values for the vendor field. The snmp_fields files contains the valid values for the SNMP agent field.

ovw_fields For this example, modify the following ASCII file to add the new vendor information:

- *Windows:*
  install_dir\fields\c\ovw_fields
- *UNIX:*
  $OV_FIELDS/$LANG/ovw_fields

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1222
Doc: 3740

$LANG refers to the setting of the $LANG language shell environment variable. To check the value of $LANG on your system, from the command prompt, enter:

echo $LANG

Use the value returned. If no value is returned, then use the default, which is C.

The following example illustrates how the ovw_fields file could be modified. Note the new entry in the file.

NOTE These entries are case-sensitive and must exactly match the field in the oid_to_type file.

```
 Field "vendor" {

Type      Enumeration;
  Flags   capability, general, locate;
  Enumeration "Unset",
  "Hewlett-Packard",
  "HP/Apollo",
  "ACC",
  "Cayman",
  "cisco Systems",
    :
  "NetWare",
  "NewVendor",              <-- new entry
  "Novell",
  "NRC",
  "SGI",
  "SynOptics",
  "Ungermann-Bass",
  "Wellfleet",
  "Xyplex",
   ;
  }
```

snmp_fields For this example, modify the following ASCII file to add the new SNMP agent information:

- *Windows:*
  install_dir\fields\c\snmp_fields

- *UNIX:*
  `$OV_FIELDS/$LANG/snmp_fields`

  `$LANG` refers to the setting of the `$LANG` language shell environment variable. To check the value of `$LANG` on your system, from the command prompt, enter:

  `echo $LANG`

  Use the value returned. If no value is returned, then use the default, which is `C`.

The following example illustrates how an `snmp_fields` file could be modified. Note the new entry in the file.

NOTE These entries are case-sensitive and must exactly match the field in the `oid_to_type` file.

```
Field "SNMPAgent" {
  Type      Enumeration;
  Flags     capability, general, locate;
  Enumeration "Unset",
  "HP 3000/XL",
  "HP 386",
  "HP 700/[R]X X-Terminal",
  "HP 9000/HP-UX",
    :
  "cisco Terminal Server",
  "cisco T-Router",
  "cisco Protocal Translator",
  :
  "Netware 386 TCP/IP",
  "New SNMP Agent",      <-- new entry
  "Novell Lantern",
  "NRC Fusion Xenix agent",
  "Process Software Corp. VMS agent",
    :
  "Xyplex Remote Ethernet Bridge",
  "4BSD ISODE";
  }
```

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1223
3740
Doc:

Configure the Database

It is not necessary to shut down the NNM services or to exit NNM when performing this step.

It is necessary to reinitialize the fields so that the new ones in the `snmp_fields` and `ovw_fields` files are loaded into the object database.

To reinitialize the fields, at the command prompt, type:

```
ovw -fields
```

Updating Field Values

It is not necessary to shut down the NNM services or to exit NNM when performing this step.

To force the `netmon` service to reread the `oid_to_type` file, at the command prompt type:

```
xnmpolling -event
```

Updating the Map

To update the map to reflect the changes, close and then reopen the map.

If the device has already been discovered, the vendor and SNMP agent changes will be detected during the next regularly scheduled configuration check. Those fields will be updated at that time to reflect the new values. You can set the intervals between configuration checks using `xnmpolling` or using the `Options:Network Polling Configuration->IP` menu item.

Alternately, you can delete the device's symbol from the map and let it be rediscovered. When the device is rediscovered, the new values will be used.

Backing Up Your Efforts

The following *analytical data* directories are *not* included in NNM's backup scripts:

- *Windows:*

  install_dir\backgrounds
  install_dir\bitmaps
  install_dir\fields
  install_dir\symbols

- *UNIX operating system:*

```
$OV_BACKGROUNDS
$OV_BITMAPS
$OV_FIELDS
$OV_SYMBOLS
```

When you make changes or additions to map backgrounds, bitmap files, field registration files, or symbol registration files ensure that your new files are properly backed up. See "Backup/Restore to Protect Your Investment of Time" on page 165 for more information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 683
3740
Doc:



Changing an Object's Vendor and SNMP Agent

Procedure

Symbols

.login file
  modifying, 101
.profile file
  modifying, 101
.vueprofile file
  modifying, 101

A

access
  no access, 293
  read-only, 292
  read-write, 292
  to maps, 292
accessing
  alarm information from the map, 339
  map information from alarms, 338
  MIB information, 52
accounting management
  components, 43
acknowledging alarms, 334
action block, WLRF, 496
adding
  background graphic, 262
  features to NNM, 278
  IP interface object, 260
  new symbols, 263, 662
  node object, 259
  segment object, 258
additional actions
  alarms, 339
  configuring, 339, 441
  See also Alarm Browser
additional views
  cdp view, 521
  internet view, 522
  neighbor view, 518
  node view, 520
  path view, 519
  Port-Address mapping command, 522
  station view, 522
address
  resolution, 579
  table poll operations in netmon, 179
  well-configured, 90
Address Resolution Protocol. See ARP/RARP
administrative symbol status, 271
agent. See SNMP agent
Alarm Browser
  acknowledging alarms, 334
  All Alarms category, 331
  assign category, 348
  configuring, 342
    automatic delete, 345
    event database, 343
    state file, 344
  correlated alarms, 352
  de-duplicated alarms, 352
  deleting alarms, 337
  features, 512
  filtering alarms, 335
  overview, 329
  starting, 513
  troubleshooting, 619
  window, 330, 332, 337
alarm categories
  configuring, 349
  window, 329, 331
alarm to map connection, 338
alarms, 323, 330, 338, 423
  accessing information, 338
  acknowledging, 334
  adding, 423
  additional actions, 339
  automatic actions, 433
  automatic delete configuration, 345
  categories, 348
  categories, new, 349
  configuration
    sources, 432
  configuring, 423
  copying, 423
  correlated
    see event reduction capabilities
  de-duplicated
    see event reduction capabilities
  definition, 323
  deleting, 337, 423
  deleting automatically, 345
  displaying, 329
  filtering, 335
  highlighting, 339
  monitoring devices, 326
  moving to a different category, 348
  using to diagnose problems, 566
  using to filter events, 566
  using to launch specific URLs, 340
  zoom to highlighted object, 338
Alarms command, 566

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1225
3740
Doc:

aliases, for web server, 485
All command, 561
All HSRP Groups command, 574
All VLANs command, 574
analytical data backup, 166
app-default files, 269
Application Builder. See MIB Application Builder
application layer
  hardware used in, 26
  in OSI model, 22
  protocols, 22
application registration files (ARF)
  control menu choices, 299
archive
  implement your plan, 170
  importance of, 165
ARF files for menu control, 299
ARP cache, viewing, 562
ARP/RARP, described, 23
attributes
  changing, 235
  locating objects by, 113
  object, 205
audit log file, 491
  format, 491
  location, 491
automatic actions, 433
  using trusted commands, 433
automatic discovery, 56
automatic thresholds, 453

B

background graphic
  adding, 262
  formats, 260
background processes
  See services
backup
  adding scripts, 176
  archive
    implement your plan, 170
    importance of, 165
  directory (staging area), 166
  disk space requirements, 168
  frequency, 167
  how it works, 166
  procedure, 167
  SOLID database, 175
  troubleshooting, 171, 174
backup routers
  missing from map, 136
Berkeley Internet Name Domain (BIND) Service, 579
Bridge MIB
  Base Port Table command, 564
  Base Table command, 563
  Spanning Tree Port Table command, 564
  Spanning Tree Table command, 564
  Static Table command, 564
  Transparent Forwarding Table command, 564
  Transparent PortTable command, 564
bridge MIB
  described, 28
  for topology polling, 184
bridges, 26
  discovery of, 103
  display of, 217
Browse MIB operation, SNMP Set requests, 628
browser
  DMI, 417
  MIB, 412
  See Alarm Browser
browsing
  alarms, 335
browsing MIBs
  problems with, 628
  See also SNMP MIB Browser
browsing MIFs. See DMI Browser
building new MIB applications, 43
bundled
  correlations, 360
  correlators, 386
bus layout, 242

C

cache, clearing from browser, 613
capabilities, 206
categories for alarms
  assigning, 348
  changing default, 348
  creating new, 349
  moving an alarm, 348
CDP command, 573
cdp view
  description, 521
CGI errors, 616
CGI programs, described, 545

change management
tools, 46
characteristics, symbol, 209
checking disk space, 527
checkpoint phases for backup, 166
child submaps
creating, 245
Cisco Discovery Protocol
Cache Table command, 563
Global Table command, 563
Interface Table command, 563
class, symbol, 207
client station, web components installed on, 485
collecting
historical MIB information, 45
MIB information, problems, 608
collecting data
See data collection
collecting SNMP data. See data collection
colors, status, 271
command
xnmevents, 341
communications problems diagnosing, 566
community names
configuring NNM, 93, 146
configuring SNMP agents, 93, 146
defined, 52
GET/SET, 93, 146
problems with, 626
requests for information, 52
testing with netmon.cmstr, 93, 147
Community-based SNMP version 2, 52
Composer, 386
compound status propagation, 275
configuration check
operations in netmon, 179
polling, 183
configuration management
components, 42
tools, 46
configuring
additional actions, 441
alarm categories, 349
alarms, 423
automatic actions, 433
correlations, 352
correlators, 352
de-duplications, 352
events, 422, 423
polling, 178, 194
print command, 475
problems with events, 631
SNMP events, 423
connection labels
defined, 223
connection symbol, 208
connections, multiple connections between symbols, 245
connectivity problems, diagnosing, 556, 557, 562, 567, 568
connector topology
polling, 184
Connector-Down correlation
behavior, 361
setting parameters, 362
important node filter, 192, 362
secondary failures, 192, 363
conserving memory, 657
container object, 248, 251
containment realm
editing guidelines, 253
example of Internet submap, 253
example of Partitioned Internet submap, 255
maintaining, 255
overview of, 252
context for menu items, 296
contrib programs
accessing, 74
controlling management traffic, 178
copying
events, 423
symbols, 257
correlating events, 352
correlation
background information, 354
command line control, 380
ConnectorDown, 361
files, 381
FrameRelay, 365
MgXServerDown, 369
new, 382
PairWise, 371
RepeatedEvent, 375
ScheduledMaintenance, 379
troubleshooting, 381
Correlation Composer, 386
correlator
background information, 354
files, 397

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1226
3740
Doc:



new, 398
OV_Chassis_Cisco, 387
OV_Connector_IntermittentStatus, 393
OV_HSRP_(group), 394
OV_MultipleReboots, 388
OV_NodeIf_(group), 390
troubleshooting, 397
CPU
load operation, problems with, 626
speed, performance impact, 656
viewing load, 559
CPU Load command, 559
CRC errors, viewing, 558
creating
child submaps, 245
correlations, 383
correlators, 398
de-duplication configurations, 358
executable symbols, 280
independent submaps, 245
Quick Navigator, 287
submaps, 244
critical status, 275
customizing
background graphic, 262
setting a user default map, 287
setting the home submap, 287
startup files, 535
cutting symbols, 257

D

data collection
configuring, 450
disk space usage, 168
graph, 472
graphing, 472, 473
reducing file size with ovdwtrend, 529
scheduling, 451
setting thresholds, 456
storing results, 448
using the data collector, 447
viewing results, 453
Data Collector, 473
data graphing, 473
data link layer
discovery of devices, 59
hardware used in, 26
in OSI model, 21
protocols, 23
Data Warehouse
Export Events command, 571
Export Topology command, 571
Export Trend Data command, 571
data warehouse, described, 63
database files
changing permissions, 295
databases
corrupted OVW object database, 604
event, 63
map, 62
NNM, 62
object, 62
topology, 63
trend, 63
de-duplicated, 358
deleting, 423
alarms, 337
nodes, 658
old snapshots, 555
description
Composer correlators, 386
de-duplication, 358
ECS correlations, 360
object, 236
Desktop Management Interface. See DMI
destination
SNMP trap, 325, 326
developing
additional actions, 441
automatic actions, 433
de-duplication configurations, 358
new correlations, 383
new correlators, 398
devices
discovery of, 104
supporting SNMP, 43
DHCP
described, 24
filter, 183
polling, 179, 181, 183
well-configured, 91
dialog boxes
General Attributes, 205
discovery, 103
automatic, 56
description of, 56
DIscover Level-2 Objects check box, 185
duplicate IP Address, 159
expanding, 117, 119

incorrect IPX node names, 157
IP and IPX, 58
IP Network 0.0.0.0, 156
IPX failure, 154
IPX node discoverd as two nodes, 159
Level 2, 59, 185
limiting, 117, 124
MAC address, 59
missing IPX routers, 156
netmon -k options, 185
no vendor translation, 159
non-IP devices, 59
non-IPX devices, 59
partial IPX, 157
problems with, 154
recommendations, 134, 153
requirements for IP, 56
requirements for IPX, 58
routing tables, 144
start again, 161
unmanaging a network, 589
verify accuracy, 109
discovery filter
procedure, 128
to improve performance, 531
disk space
checking, 527
regaining, 527, 529
viewing usage, 559
Disk Space command, 559
displaying alarms, 330
distributed event correlation, 357
DMI
configuring, 95, 417
described, 30
event, 54, 327
features, 30
MIF, 54, 327
See MIF
service provider, 54, 327
viewing status, 574
DMI Browser
accessing, 574
querying DMI values, 417
DMI devices
can't communicate with, 628
problems querying, 611, 628, 631
DNS
caching-only name server, 91
quick check, 92
secondary name server, 91
well-configured, 91, 133
documenting a map, 555
dynamic correlation parameters, 355
Dynamic Host Configuration Protocol. See DHCP

E

ECS, 360
e-mail message generation. See automatic actions
Enterprise Identification, 423
Enterprise MIB
adding, 423
correlating, 352
deleting, 423
environment variables
setting up, 101
error log file
contents, 498
Launcher, 653
using for troubleshooting, 498
Web Launcher, 616, 653
errors
monitoring SNMP, 561
viewing Ethernet, 558
Ethernet
statistics, monitoring, 558
traffic, monitoring, 558
Ethernet Errors command, 558
Ethernet Traffic command, 558
Event Browser
See Alarm Browser
Event Configuration
operation, 631
overview, 422
event correlation
bundled edition
Connector-Down, 192, 361
Frame-Relay, 365
ManageX Server-Down, 369
Pair-Wise, 371
Repeated-Event, 375
Scheduled-Maintenance, 379
developing your own, 383, 398
disabling, 354
distributed, 357
enabling, 354
settling time, 354
files, 381

ECT 2207 CPL-06
RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1227
3740
Doc:

general recommendations, 356
introduction, 353
parameters
dynamic, 355
static, 355
See event reduction capabilities
sources for more, 382
streams, 356, 380
event database
configuration, 343
event database, described, 63
Event Identification, 423
event log, browsing, 566
event reduction capabilities
Correlation Composer, 386
de-duplication, 358
described, 61, 352
ECS, 360
web based, 515
event storm prevention
Composer correlators, 386
Connector-Down correlation, 361
de-duplication, 358
ManageX Server-Down correlation, 369
Pair-Wise correlation, 371
Repeated-Event correlation, 375
Scheduled-Maintenance correlation, 379
events, 423
actions, 441
adding, 423
automatic actions, 433
configuration, 631
sources, 432
configuring, 423
correlating, 352
de-duplication, 358
definition, 323
deleting, 423
listing, 566
management stations receiving, 565
processes that generate, 591
propagation of, 591, 604
services that generate, 604
exact match, 114
executable symbols
adding, 280
described, 279
executing MIB applications, problems, 628
expanding maps
containment realm, 252
creating Partitioned Internet submap, 251
higher level maps, 247
IP interface object, adding, 260
node object, adding, 259
See Also containment realm
segment object, adding, 258
explodable symbols
defined, 279
export map, 256
Extended Topology, 44

F

fault management
components, 42
event reduction capabilities, 352
HP OpenView IT/Operations, 44
tools, 43
faults on network, diagnosing, 44, 45
field definitions, problems with, 595
field registration files, 667
file
backing up originals, 580
modifying default X resources, 581
original product, 580
permissions, 623
filters
alarms, 335
DHCP, 183
discovery, 128, 183
important node, 192
Connector-Down correlation, 362
OV_NodeIf_(group) correlator, 390
map, 232
persistence, 231
find
attributes, 235
entering text for exact match, 114
entering text for pattern match, 114
entering text for regular expressions, 114
objects, 113, 114
forwarding
SNMP trap from NNM, 326
SNMP trap to NNM, 325
Frame Relay
Circuit Congestion command, 558
Circuit Errors command, 558
Circuit Traffic Avg. Frame Size command, 558
Circuit Traffic Data Rate command, 558

Circuit Traffic Frame Rate command, 558
correlation of health, 365
Data Link Errors command, 559
Properties command, 564
Virtual Circuits command, 564
frequency of discovery value, in netmon, 179
FRF, 667
full restore of NNM data, 171

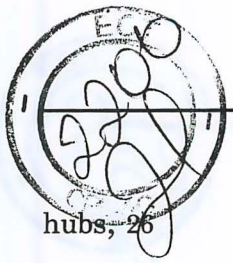
G

gateways
described, 26
discovery of, 103
General Attributes dialog box, 205
generating
alarms, 323
geometry of submaps, 266
get request, 53
get response, 53
getBulk request, 53
getNext request, 53
GIF graphics format, 260
graph
CPU load, 559
Ethernet errors, 558
Ethernet traffic, 558
Frame Relay circuit congestion, 558
Frame Relay circuit errors, 558
Frame Relay circuit traffic data rate, 558
Frame Relay circuit traffic frame rate, 558
interface discard percentage, 557, 569
interface discard rate, 556, 568
interface error percentage, 556, 568
interface error rate, 556, 568
interface statistics, 556, 568
interface traffic avg. packet size, 557
interface traffic data rate, 557
interface traffic packet rate, 557
interface traffic throughput, 557
interface traffic utilization, 557
printing, 475
selected data, 473
SNMP data, 561
SNMP errors, 561
SNMP operations, 560
SNMP traffic, 560
Graph All Data, 472
Graph SNMP Data command, 561
graphics
backgrounds for maps, 260
graphing
data, 472
historical data, 473
MIB data, 45
real-time data, 473
with xnmgraph, 544
greyed menu items, 206

H

help system, 67
files, viewing, 636
overview, 67
printing, 68
searching, 68
using separately from NNM, 69
using to create manuals, 68
hiding objects on map, 233
highlighting
alarms, 339
sources, 338
historical data, 473
holding area, 244
home submap
defined, 202
setting, 287
hotlist
creating, 287
HP Agent
trap recipients, 326
HP Education, 77
HP OpenView Grapher, 472
HP OpenView IT/Operations, for fault management, 44
HP OpenView Launcher. See Launcher
HP OpenView Web
applications, 484
Correlation Composer, 386
event correlation, 515
features, 484
requirements, 485
security, 486
setting up, 485
web browser, 485
web server, 485
HP-RDMI service provider, 417
hpterm, accessing, 570
HP-UX SAM command, 565
HSRP Group Detail view, 574
HSRP Node Detail view, 574
httpd service, troubleshooting, 586

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1228
3740
Doc:



hubs, 26

I

ICMP
  polling, 179, 181
ICMP, described, 23
icon symbols
  described, 207
import map, 256
important node filter
  Connector-Down correlation, 362
  OV_NodeIf_(group) correlator, 390
  setting, 192
independent submaps, creating, 245
initial discovery
  process, 107
  start again, 161
  troubleshooting
    IP, 131
  verify information, 109
instance
  query for, in MIB Browser, 412
instance, MIB, 29
interface
  status of interface, 556, 568
  status of node, 556, 568
Interface Avg. Packet Size command, 557
Interface Error Percentage command, 556, 568
Interface Error Rate command, 556, 568
Interface Errors
  Data Link Errors command, 569
  Discard Percentage command, 557, 569
  Discard Rate command, 556, 568
  Frame Relay Circuits command, 569
interface object, 112
Interface Status command, 556, 568
Interface Traffic
  Data Rate command, 557
  Throughput command, 557
  Utilization command, 557
Interface Traffic command
  uses of, 654
Interface Traffic Packet Rate command, 557
Internet command, 573
Internet Control Message Protocol. See ICMP
Internet level, 230
Internet Packet Exchange. See IPX
internet view
  description, 522
inventory network objects
  internet object properties, 111
inventory report, 107
IP
  addressing, 579
  described, 23
  discovery, 56
  forwarding, 140
  interaction with IPX, 58
  internet object, 111
  objects, discovery of, 103
  requirements for discovery, 56
  routes, locating, 567
  secondary addresses, 137
  topology behavior, 466
  well-configured, 90
ipmap
  described, 543
  managing objects, 255
  propagation of events from, 605
IPv6 Network command, 574
IPv6 Node Detail view, 574
IPv6 Prefix Groups view, 574
IPX
  described, 23
  discovery, 56, 57
  interaction with IP, 58
  layout, 57
  polling, 179, 180, 184
  requirements for discovery, 57
  transport software, 100
IPX discovery
  duplicate IP Address, 159
  failure, 154
  hop count
    expanding, 123
    limiting, 130
  incorrect node names, 157
  IP Network 0.0.0.0, 156
  missing routers, 156
  no vendor translation, 159
  node discoverd as two nodes, 159
  partial, 157

J

Java
  errors, 617
  parameters, modifying, 499
jumpstart

netmon, 152

K

keyboard, 474

L

latency time
for WANs, 182
in polling, 182
Launcher
accessing, 571
blank window, 616
CGI error, 616
configuring, 494
error log, 498, 653
features, 492
Information and Reports tab, 575
Java error, 617
Java parameters, 499
Object Views tab, 575
registration file. See WLRF
starting, 492
tabs, 575
Tasks tab, 575
Tools tab, 575
troubleshooting, 616
user interface, 492
user login error, 615
WLRF error, 617
Layer 1
hardware used in, 25, 26
in OSI model, 21
Layer 2
hardware used in, 26
in OSI model, 21
protocols, 23
Layer 3
hardware used in, 26
in OSI model, 22
protocols, 23
Layer 4
in OSI model, 22
protocols, 23
Layer 5
in OSI model, 22
Layer 6
in OSI model, 22
Layer 7
hardware used in, 26
in OSI model, 22
protocols, 22, 23
layers, in OSI model, 21
layout, 242
automatic, 56
bus, 242
description of, 56
point to point, 242
ring, 242
row/column, 242
layout algorithm
default, 241
level 2
discovery, 56, 59, 185
polling, 180, 184
license
checking number of nodes, 533
OVLicenseMgr, 599
limitations, known in loading MIBs, 634
line
attributes, 475
configuration, 475
Graph, All Data, 472
Graph, Select Data, 473
list block, in WLRF, 495
Load/Unload MIBs operation, 633
loaded MIB database, modifying, 633
loadhost program
expand management domain, 122
limit management domain, 127
loading MIBs, 413
limitations of, 634
operation, 633
problems with, 633
unique object label, 634
local host file
quick check, 92
well-configured, 91, 133
Local Registration File (LRF)
customizing for performance, 535
customizing for startup, 535
locating objects
see find
log files
audit, 491
error, 498, 653
Launcher error, 653
logging
common options, 640
correlations, 380

ECT 2199 CPL-AC

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1229
Doc: 3740



description of, 639
example, 645
explained, 643
log files, 648
output, 649
recommendations, 580
Web Launcher errors, 616, 653
with netfmt, 643
with nettl, 644
lp, 475
LRF. See Local Registration File

M

MAC address, using to discover devices, 59
magicpacket command, 570
maintenance
audit log file, 491
daily, 527
error log file, 498, 653
monthly, 533
weekly, 531
managed object, defined, 53
Management Information Base. See MIB
Management Information Framework. See MIF
management region
expanding, 108, 117, 119
IPX hop count, 123
loadhost program, 122
seed file, 120
limiting, 117, 124
Discovery filter, 128
IPX hop count, 130
loadhost program, 127
netmon.noDiscover file, 125
oid_to_type file, 129
troubleshooting, 131
management station
interaction with Network Presenter, 505
receiving traps, 565
web components installed on, 485
Management Web Page, accessing on remote node, 572
manager
defined, 51
manager-agent
communication through SNMP, 52
ManageX Server-Down correlation
behavior, 369
setting parameters, 370
managing
polling, 193
manpages
acessing, 72
printing, 73
viewing, 636
MANPATH statement
setting, 101
manuals, accessing online, 69
map database, described, 62
maps
access rights, 292
adding features, 278
automatic discovery and layout, 56
background graphics, 260
changes, 286
child submap, 245
compound status, 275
containment realm, 252
context, 296
copying, 215
creating symbols, 263
defined, 199
expanding, 247
file permissions, 292
filters for objects, 232
geometry, 266
hiding objects, 233
independent submap, 245
initial appearance, 103
layout
auto, 241
do-it-yourself, 242
limiting menu choices, 299
maintaining the containment realm, 255
menu control, 299
metaconnections submaps, 245
network symbol names, 221
new object holding area, 244
no access, 293
open map, 199, 215, 221
overlay, 267
partitioned internet submaps, 248
permissions, 292
persistance, 229
preferences, 287
problems with, 654
propagate most critical status, 276
propagate status at threshold value, 276

Quick Navigator, 288
read-only access, 292
read-write access, 292
remote viewing, 317
removing old snapshots, 555
See also expanding maps
See also Partitioned Internet submap
size and placement, 266
snapshot, 555
start over, 161
startup options, 289
switch/bridge display, 217
troubleshooting
IP, 131
IPX, 153
user preferences, 287
marginal status, 275
MAU MIB
described, 28
for topology polling, 184
memory
clearing from browser, 613
conservation tips, 657
not enough, 657
performance impact, 656
problems affecting ovwdb, 604
related problems, 579
memory requirements
for maps, 229
menu items
adding to Network Presenter, 505
adding to NNM, 299
greyed, 206
meshing
definition of, 59
example, 227
specifying in NNM, 228
meta-connection
submap, 246
symbol, 245
MIB, 43
accessing information, 52
Application Builder operation, 443, 628, 629
bridge, 28
for topology polling, 184
Browse operation, 46
building new applications, 43
collecting historical information, 45
data, 472
data collection
effects of, 453, 654
operation, 608
defined, 27
defining thresholds, 44
operation for, 453
DMI conversion from MIF, 95, 419
enterprise-specific objects, 43
graphing data, 45
instance, 29
loading (adding), 413
prerequisites, 414
MAU
described, 28
for topology polling, 184
numeric values, 447, 455
object, 28, 43
object identifier, 28
object label, unique, 634
obtaining MIB files, 94
organization, 28
private, 28
querying, 412
repeater, 28
for topology polling, 184
RFC (technical details), 33
RMON, 27
See Also data collection
setting MIB values, 412
setting values, 412
SNMP traps, 44
storing data for trend analysis, 45
tree, 28
troubleshooting, 572
variable bindings, 404
vendor-specific, 413
viewing, 412, 572
viewing MIB values, 412
MIB Application Builder
and DMI device, 628, 631
using, 443
MIB applications
executing, 629
problems building, 628, 629
troubleshooting, 629
MIB Browser. See SNMP MIB Browser
MIB event thresholds,defining, 44
mib.coerce file, 464
mibExpr.conf file, 463

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1230
Doc: 3740

MIB-II
described, 27
Microsoft Terminal Services, 317, 318
MIF, 54, 327
configuring for NNM, 95, 419
described, 29
loading (adding), 95, 419
with translation to MIB, 420
without translation to MIB, 420
mapping to MIB, 328
vendor-specific, 420
modifying
events, 423
Java parameters, 499
line attributes, 475
ovsuf, 536
monitoring
CPU load, 559
devices, 326
disk space, 559
Ethernet statistics, 558
Ethernet traffic, 558
Frame Relay circuit average frame size, 558
Frame Relay circuit congestion, 558
Frame Relay circuit errors, 558
Frame Relay circuit traffic data rate, 558
Frame Relay circuit traffic frame rate, 558
Frame Relay Circuits, 569
Frame Relay Data Link errors, 569
Frame Relay data link errors, 559
SNMP authentication failures, 560
SNMP errors, 561
SNMP operations, 560
SNMP traffic, 560
TCP connections, 557
mouse and keyboard
grapher, 474
moving
symbols, 257
multi-homed node, discovery of, 103

N

name resolution, 91, 92, 133
naming network symbols, 221
Neighbor command, 572
neighbor view, 518
NetBios
quick check, 92
well-configured, 91, 133
netfmt, 643
described, 643
examples of, 649
filtering options, 649
netmon, 466
address table poll operations, 179
configuration check operations, 179
configuring, 193
dependencies, 586
described, 541, 587
disabling, 195
discovery behavior, 541
enabling, 195
event generation conditions, 604
frequency of discovery values, 178
instance restrictions, 589
IP discovery, 56
IPX discovery, 57
jumpstart(-J), 152
monitoring, 194
netmon.noDiscover file, 125
performance check, 193
permissions, 623
poll operations, 179
problems with, 154
proxies, 179
queue (-q, -Q), 193
requirements for discovery, 56, 57
seed file, 119
timeout intervals, 179
trace masks, 641
tracing, 641
tracing example, 641
troubleshooting, 587
tools, 589
netmon.cmstr, 147
testing community names, 93
netmon.equivPorts, 60, 226, 228
netmon.lock file, 589
netmon.lrf, 193
described, 536
segRedux, 217
netmon.noDiscover file
effect on discovery, 126
example, 126
HSRP virtual IP address, 126
procedure, 126
netmon.snmpStatus, 274
netnmrc script
execution sequence, 625

nettl
described, 643
examples of, 645
generating log files, 648
generating trace files, 648
log file output, 649
options
-log, 645
-start, 644
-status, 644
-stop, 648
-traceoff, 647
-traceon, 646
pathnames for, 643
subsystems used with, 643
Network Activity menu, described, 556, 568
Network Configuration
ARP Cache command, 562
ATM Properties command, 565
Cisco VLAN MembershipTable command, 563
DS1/E1 Serial Line Properties command, 565
DS3/E3 Serial Line Properties command, 565
Interface Properties command, 562
IP Addresses command, 562
IP Routing Table command, 562
IP Services command, 562
SONET/SDH Properties command, 565
Network Connectivity
Locate Route via SNMP command, 567
Show Path command, 567
Trace Route command, 567
network hardware
bridge, 26
gateway, 26
hub, 26
repeater, 25
router, 26
switch, 26
network layer
hardware used in, 26
in OSI model, 22
protocols, 23
network level, 230
network management
benefits, 42
defined, 42
functions, 42
proactive, 40
network management operation
problems with, 626
remote node support for, 626
network map
using a seed file, 119
network object, 111
Network Presenter
components, 502
connecting to an NNM session, 502
features, 501
features vs. NNM, 503
interaction with management station, 505
permissions, 618
problems starting, 618
registration file. See NPRF
specifying map to open, 502
starting, 501
symbol registration file, 506
troubleshooting, 618
URL for, 501
network traffic
control, 178
viewing, 560
NetworkAdmin user role, 488
NetworkOper user role, 488
networks
naming symbols, 221
new node discovery
polling, 185
NIS
quick check, 92
well-configured, 91, 133
NNM
configuration files, changing permissions, 295
options for starting, 289
starting, 106, 121, 122, 195
status check, 106
NNM Extended Topology, 44
no access, 293
node
deleting unwanted, 658
discovery of IP, 57
discovery of IPX, 57
information obtainable from, 582
information storage, 57
listing information about, 565
multi-homed, 103

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1231
3740
Doc:

non-SNMP, 582, 626
object, 112
obtaining status, 566
polling, 566
represented as a symbol, 105, 679
testing remote, 570
turning on remote, 570
Node command, 573
node view, 520
description, 520
normal status, 275
notification, 325
defined, 52
NPRF
adding menus, 505
adding toolbar buttons, 505
format, 505
location, 505
troubleshooting, 619
NTAdmin user role, 488
NTOper user role, 488
numeric MIB values, 447, 455

O

object database
and ovwdb, 542
described, 62
object manager
ovstatus cannot find, 585
objects
adding attributes, 238
attribute

setting parameters, 393
OV_HSRP_(group) correlator, 394
behavior, 395
parameter settings, 396
OV_MultipleReboots correlator, 388
behavior, 388
parameter settings, 389
OV_NodeIf_(group) correlator, 390
behavior, 390
disabling, 392
important node filter, 390
setting parameters, 391
ovactiond
dependencies, 586
described, 541
troubleshooting, 590
trusted commands, 433
trustedCmds.conf directory, 433, 434
ovactiond.lrf, described, 536
ovaddobj command
described, 541
netmon, configuring seed file, 125
OVAdmin user role, 489
ovalarmadm, 347
ovalarmsrv
dependencies, 586
described, 542
troubleshooting, 590
ovas
described, 542
ovbackup.ovpl, 167, 170
ovcapsd, 54, 327, 420
dependencies, 586
described, 542, 591
troubleshooting, 591
ovcapsd.lrf, described, 537
overlay of submaps, 267
overview
Alarm Browser, 329
Event Configuration, 422
ovhtpasswd command, 487
ovrepld
dependencies, 586
described, 542
troubleshooting, 594
ovrepld.lrf, described, 537
ovrequestd, 542
ovrequestd background service, 607
ovrestore.ovpl, 172, 173
ovspmd
described, 541
determining problems, 592
recreating sockets directory, 593
troubleshooting, 592
ovstart command
described, 541
in starting background services, 584
ovstatus command
failure to find object manager, 585
verifying daemon services, 585
ovsuf
described, 541
modifying, 536
ovtopmd
dependencies, 586
described, 542, 594
troubleshooting, 594, 595
ovtopmd.lrf, described, 537
ovtopodump
description of, 597
troubleshooting, 597
ovtopofix command, 217
ovtrapd
dependencies, 586
described, 542, 599
operation of, 599
troubleshooting, 599
ovtrapd.lrf, described, 537
ovuispmd
dependencies, 586
described, 542, 600
troubleshooting, 600
ovuispmd.lrf, described, 537
ovw command
described, 543
options, 289
-mapcount, 289
-verify, 289, 302
ovw.auth file, location, 506
ovwchgrp, 295, 624
ovwchmod, 295, 624
ovwchown, 295, 624
ovwdb
corrupted OVW object database, 604
dependencies, 586
described, 542, 602
insufficient memory, 603
insufficient performance, 603
troubleshooting, 602
ovwdb.auth file
location, 506

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1232
3740
Doc:

ovwdb.lrf, described, 537
ovwls, 295, 624
ovwperms, 295

P

paging automatically. See automatic actions
Pair-Wise correlation
  behavior, 372
  setting parameters, 373
palette, 207
Partitioned Internet submap
  creating, 251
  example of, 255
  how it is managed, 255
  overview of, 248
  See Also containment realm
password
  in user authentication file, 487
  modifying, 487
pasting symbols, 257
patch releases, verifying, 533
Path command, 573
PATH statement
  modifying, 101
path view, 519
pause NNM services
  for back up
    analytical, 166, 168
    operational, 168
Performance
  Graph Data, 472
performance, 473
  customizing startup, 535
  diagnosing problems, 44, 45
  improving NNM, 658
  increasing, 656
  limiting factors, 656
  polling, 531
  problems with, 656
performance management
  components, 42
  reports, 45
  tools, 45
performance problems, diagnosing, 556, 557, 559, 568
Perl (HP's version)
  backup/archive/restore, 176
permissions
  change for configuration files, 295
  change for database files, 295
  changing, 624
  default, 623
  no access, 293
  read-only, 292
  read-write, 292
  restoring default, 624
persistance of submaps, 229
persistence filter, 231
physical layer
  hardware used in, 25, 26
  in OSI model, 21
ping
  remote node, 570
  using to determine connection, 567
planning, 80
  assuming responsibility, 82
  changes to the map, 286
  how to configure NNM, 83
  which devices to manage, 87
pmd, 323
  alarm gathering, 324
  dependencies, 586
  described, 542, 604
  operation of, 604
  permissions, 623
  troubleshooting, 381, 397, 591, 604
pmd.lrf, described, 537
point to point layout, 242
Poll Node command, 566
poll operations, in netmon, 179
polling
  adjusting intervals, 531
    from a remote computer, 182
  behavior, 589
  causing problems, 580
  configuration check, 180, 183
  controls, 178, 588
  delays in, 589
  disabling, 195
  during map generation, 178
  effects of reducing, 178, 179, 654
  file, 588
  initial process, 56
  latency time, 182
  new node discovery, 178, 180, 185
  non-IP devices, 59
  non-IPX devices, 59
  performance
    checking, 531
  problems with, 589

secondary failures, 180, 192
secondary IP addresses, 137
status, 178, 179, 181
to conserve memory, 657
topology check, 180, 184
traffic generated by, 654
troubleshooting
IP, 131
jumpstart netmon, 152
SNMP, 93, 145
subnet masks, 91, 149
tuning, 193, 194
values storage, 178, 543, 588
Port Address Mapping command, 522
description, 522
port number, used to start HP OpenView Web, 485
port trunking
definition of, 59
example, 225
specifying in NNM, 226
Port-Address Mapping command, 571
ports, connection problem, 596, 603
predefined symbols, 208
preferences, 287
preferences, setting a user default map, 287
presentation layer, in OSI model, 22
print command, 475
configuration, 475
printing
graph, 475
online help, 68
private MIB, 28
proactive network management, 40
problem management
components, 42
tools, 43
problems, 131
additional sources of information, 579
address resolution, 579
analyzing symptoms, 582
background services, 584
Browse MIB operation, 628
characterization, 582
diagnosing network faults, 44, 45
diagnosing performance, 44, 45
event correlation, 381, 397
failure to discover IPX nodes, 154
Launcher won't start, 616
launching applications, 637
limitations on loading MIBs, 634
loading MIBs, 633
map, 654
netmon, 154, 589
network management operation, 626
network operation, 623
ovtopmd, 595
ovtopodump, 597
ovwdb, 603
performance, 656
pmd, 606
polling, 589
resource exhaustion, 579
runtime, 623, 625
starting Launcher, 613
starting Network Presenter, 618
subnet mask, 149
unmanaging a network, 589
user logins, 615
X Windows, 635
product support
contacting, 77
propagating symbol status, 271
most critical status, 276
status at threshold value, 276
protocols, and OSI model, 24

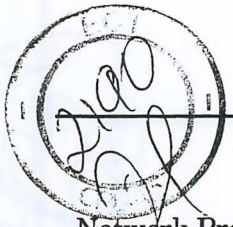
Q

quick check
name resolution, 92
Quick Navigator, 288
creating, 287

R

read-only
access, 292
read-write
access, 292
real-time data, 473
real-time data graphing, stopping, 474
recreating map and topology databases, 161
reference pages
acessing, 72
printing, 72
viewing, 636
registering an application, 278
registration files
field, 667
Launcher. See WLRF

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1233
3740
Doc:



Network Presenter. See NPRF
symbol, 664
update/verify, 668
regverify command, 494
release notes, accessing, 71
remote access to NNM, 317
remote nodes
testing, 570
turning on, 570
Remote Ping
described, 567
problems with, 626
remoteConfAllow.conf file, 182
removing, old snapshots, 555
Repeated-Events correlation
behavior, 376
setting parameters, 376
repeater
discovery of, 103
repeater MIB
for topology polling, 184
repeater MIB, described, 28
repeaters, 25
report
configuration interface, 45
general availability, 45
general inventory, 45
inventory, 107
modification, 45
Reporting interface, 516
troubleshooting, 614
reports
removing, 529
restarting automatic map generation, 161
restore
adding scripts, 176
all NNM data, 171
some NNM data, 173
RFC documents
list of, 33
ring layout, 242
RMON
Host Table Command, 560
Segment Errors command, 559
Segment Octets command, 559
Segment Packet Sizes command, 560
Segment Packet Types command, 560
Segment Utilization command, 559
RMON menu, described, 559
RMON MIB, 27
root submap, 202
routers, 26
routes, locating IP, 567
routing tables
in IP discovery, 144
viewing, 562
row/column layout, 242
running services, checking, 527
runtime components on network
problems with, 623

S

SAM, accessing, 565
Scheduled-Maintenance correlation
behavior, 379
setting parameters, 379
searching online help, 68
secondary failures
Connector-Down correlation, 363
OV_NodeIf_(group) correlator, 390
polling, 192
security
audit log file, 491
for HP OpenView Web, 486
ovw.auth file, 506
ovwdb.auth file, 506
session configuration file, 490
user authentication file, 487
user roles file, 488
security management
components, 43
seed file
description of, 120
effect, 122
example, 120
format, 126
location, 126
name, 126
networks implied by, 126
when to use, 119
segment
object, 112
segment level, 230
Selected Nodes, 473
Selected Nodes command, 561
selecting
sources that correspond with alarms, 339
selection name, locate object by, 113
Server Web Page
accessing on remote node, 572
service provider

See DMI
services
at start-up time, 547
checking running, 527
dependencies on other services, 585
during operation, 548
logging and tracing, 639
netmon, 466
pmd, 323
starting with ovstart, 584
troubleshooting background, 584
verifying with ovstatus, 585
viewing configured, 562
web interface, 545
session configuration file, 490
defaults, 490
format, 490
location, 490
session layer, in OSI model, 22
set operation, 52
set request, 53
setting
community names, 145
filters, 335
home submap, 287
MIB values, directly, 412
MIB values, using query, 412
user default map, 287
setting your path, 101
settling time
event correlation, 354
Simple Network Management Protocol. See SNMP
Snapshot Recover operation, 135
snapshots
map, 555
removing old, 555
SNMP, 473
agents required, 134
Authentication Failures command, 560
community names, 146
configuration, 145, 146
data graph, 472
data graphing, 473
Errors command, 561
event configuration, 423
event correlation, 352
graphing data on all nodes, 561
graphing data on selected nodes, 561
nodes without, 59, 582, 626
Operations command, 560
operations for accessing MIB information, 52
polling, 178, 474
port, 146
proxie for agent, 146
RFC (technical details), 33
services, listing supported, 562
SetRequests in a Browse MIB operation, 628
Traffic command, 560
traps, 44
variable bindings, 404
version 1, described, 22
version 2
described, 23
SNMP agent
changing, 678
defined, 52
management operations exclusive to, 626
non-HP, 626
propagation of events from, 599
required for SNMP, 134
setting attribute, 676
unknown, 148
well-configured
community names, 93
MIB files, 93
trap forwarding, 93
SNMP Data Presenter
configuring, 511
features, 509
starting, 510
SNMP MIB Browser
accessing, 572
querying, 412
setting values, 412
troubleshooting SNMP, 136, 140, 147
viewing, 412
snmp notify, 325
SNMP services, 53
get request, 53
get response, 53
getBulk, 53
getNext, 53
set request, 53
SNMP Trap Recipients command, 565
SNMP traps, 326
forwarding from NNM, 326

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1234
Doc:
3740

forwarding to NNM, 325
snmpCol.trace file, 609
snmpColDump, 608
snmpCollect
dependencies, 586
described, 543
tracing, 610
troubleshooting, 608
snmpCollect.lrf, described, 538
snmpd
errors, 635
propagation of events from, 599
SNMPv1
traps, 325
SNMPv1, described, 22
SNMPv2c, 325
described, 23
traps, 325
sockets
recreating ovsmpd sockets directory, 593
SOLID database
discreet backup, 175
sources that correspond with alarms, 339
sparse files (UNIX only)
backup, 171, 172, 173
special variables, 436
SRF, 664
staging area for backups, 165
standard deviation, 453
star
layout, 242
starting NNM, 106, 121, 122, 161, 173, 174, 195
redo initial discovery, 161
startup
automatic
disabling, 535
enabling, 535
customizing for performance, 535
state file
configuration, 344
static correlation parameters, 355
Station command, 573
station view
description, 522
status
categories, 271
colors, 271
compound source, 273
compound, explained, 275
conditions, 271
devices outside firewall, 184
marginal, 275
object source, 273
polling, 181
polling by object class, 182
polling with SNMP, 183, 273
propagate most critical, 276
symbol status, 271
stopping
all NNM sessions, 319
NNM to redo discovery, 161
real-time data graphing, 474
storing, MIB data for trend analysis, 45
streams and event correlation, 356, 380
subclass, symbol, 207
submaps, 245
background graphic, 202, 260, 262
creating, 244, 245
defined, 200
geometry, 266
home, 202
independent, creating, 245
layout algorithm, 241
meta-connection, 246
Node, 259
overlay, 267
Partitioned Internet, 248
persistence, 229
Quick Navigator, 288
regular vs. meta-connection, 246
root, 202
Segment, 259
setting, 287
subnet masks, 150
hierarchial, 91, 149
non-contiguous, 91, 149
problems with, 149
troubleshooting, 91, 149
subsystems used with nettl command, 643
support
obtaining, 77
programs provided, 74
swap space related problems, 579
switch centric view, 574
switches, 26
display of, 217
symbol
See node
symbol registration file, 664
for Network Presenter, 506

symbols
adding, 258
behavior, 279
changing, 662
characteristics, 209
class, 207
color
propagate, 274
status, 270
connection, 208, 246
context, 296
copying, 257
creating, 263, 662
cutting and pasting, 257
defined, 207
executable, 279
explodable, 279
hiding on map, 233
icon, 207
meta-connection, 245
moving, 257
multiple connections between, 245
naming networks, 221
predefined, 208
See node
status, 113, 271
subclass, 207
type, 114, 207
varieties, 207
synchronized data
restore all NNM data, 171
sysObjectID, 676
definition, 465
describing an SNMP agent's source, 466
determining IP topology behavior, 466
determining symbol type, 466
event reduction, 352
identifying an event's source, 466
netmon, 466
System Administration Manager, accessing, 565
System Information command, 565
system registry, 268
map access, 303
map appearance, 268

T

tab block, WLRF, 495
TCP
described, 23
viewing connections, 557
TCP Connections command, 557
TCP/IP
described, 23
telnet
accessing hpterm, 570
accessing terminal emulator, 570
accessing xterm, 571
terminal emulator, accessing, 570
terminal window, accessing, 570
thresholds
file, 588
operation for defining, 453
time intervals, 473
timeout intervals, 179
Tip of the Day
behavior, 69
toolbar buttons
adding to Network Presenter, 505
Tools
HP OpenView Launcher command, 571
Port-Address Mapping command, 571
Remote Power On command, 570
Report Presenter command, 569
Telnet (hpterm) command, 570
Telnet (xterm) command, 571
Terminal Connect command, 570
Unused IP Addresses command, 571
Views
All HSRP Groups command, 574
All VLANs command, 574
CDP command, 573
Internet command, 573
IPv6 Network command, 574
Neighbor command, 572
Node command, 573
OSPF Backbone command, 573
Path command, 573
Station command, 573
topology
polling, 184
topology database
and ovtopmd, 542
described, 63
total restore of NNM data, 171
trace file
trimming, 529
tracing
cautions for using, 639

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1235
Doc: 3740

common options, 640
data collection, 610
description of, 639
netmon, 641
recommendations, 580
trace files, 648
trimming file, 529
turning on, 647
with nettl, 646
traffic generation
measurement of polling, 654
regulation of polling, 178, 654
training
HP Education, 77
Transmission Control Protocol. See TCP
transport layer
in OSI model, 22
protocols, 23
trapd.conf, 422, 432
file, 631
trapd.log, 343
traps, 325, 422
defined, 52, 325
forwarding from NNM, 326
forwarding to NNM, 93, 325, 565
recipients, 326
SNMP, 44
trend database, described, 63
trimming
trace file, 529
troubleshooting, 131
additional sources of information, 579
Alarm Browser, 619
analyzing problems, 582
archive, 171, 174
background services, 584
backup, 171, 174
collecting too much data, 580
defaults modifications, 581
DMI communication, 628
IP, 131
Launcher, 616
Launcher error log file, 498, 653
name resolution scheme, 91, 92, 133
network operation, 623
Network Presenter, 618
OVLicenseMgr, 599
polling too much, 580
recommended practices, 579
restart initial discovery, 161
SNMP agents, 146
symptoms, 582
trustedCmds.conf directory, 433, 434

U

UDP, described, 23
universal pathnames
setting up, 101
universal pathnames for UNIX, 100
UNIXAdmin user role, 489
UNIXOper user role, 489
unknown status, 275
unmanage objects, 117
automatically, 129, 193, 669
defined, 53
effects of, 193, 654
uses of, 193, 654
Unused IP Addresses command, 571
user authentication file, 487
location, 487
modifying, 487
User Datagram Protocol. See UDP
user default map
setting, 287
user preferences, 287
user roles
described, 488
NetworkAdmin, 488
NetworkOper, 488
NTAdmin, 488
NTOper, 488
OVAdmin, 489
UNIXAdmin, 489
UNIXOper, 489
user roles file, 488
format, 489
location, 489

V

values
MIB, 412
variable binding
event reduction, 352
how to find and use, 404
variables, 436
vendor attribute, 676
viewing
connection labels, 223
events, 330
MIB values, 412

Example

The following example takes you through all the required steps in greater detail.

oid_to_type

NNM identifies each device by referencing the information contained in two configuration files:

- *Windows:*

  install_dir\conf\oid_to_type

  install_dir\conf\HPoid2type (Do *not* edit this one.)

- *UNIX:*

  $OV_CONF/oid_to_type

  $OV_CONF/HPoid2type (Do *not* edit this one.)

Although the entries in these files are already extensive, you may encounter a situation where you want to make additions or changes to the oid_to_type file.

See the instructions at the beginning of the oid_to_type ASCII file. See also the *oid_to_type* reference page in NNM's online help (or the UNIX manpage) for more information.

For this example, the sysObjectID is: 1.3.6.1.4.1.99.1.1

In the oid_to_type file, use an ASCII editor to add the following entry:

1.3.6.1.4.1.99.1.1:NewVendor:New SNMP Agent:B

ovw_fields and snmp_fields

The field registration files contain valid values for the object fields. The ovw_fields files contain the valid values for the vendor field. The snmp_fields files contains the valid values for the SNMP agent field.

ovw_fields For this example, modify the following ASCII file to add the new vendor information:

- *Windows:*
  install_dir\fields\c\ovw_fields
- *UNIX:*
  $OV_FIELDS/$LANG/ovw_fields

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1236
3740
Doc:

$LANG refers to the setting of the $LANG language shell environment variable. To check the value of $LANG on your system, from the command prompt, enter:

```
echo $LANG
```

Use the value returned. If no value is returned, then use the default, which is C.

The following example illustrates how the ovw_fields file could be modified. Note the new entry in the file.

NOTE These entries are case-sensitive and must exactly match the field in the oid_to_type file.

```
 Field "vendor" {

Type      Enumeration;
  Flags   capability, general, locate;
  Enumeration "Unset",
  "Hewlett-Packard",
  "HP/Apollo",
  "ACC",
  "Cayman",
  "cisco Systems",
    :
  "NetWare",
  "NewVendor",              <-- new entry
  "Novell",
  "NRC",
  "SGI",
  "SynOptics",
  "Ungermann-Bass",
  "Wellfleet",
  "Xyplex",
   ;
 }
```

snmp_fields For this example, modify the following ASCII file to add the new SNMP agent information:

- *Windows:*
  install_dir\fields\c\snmp_fields

- *UNIX:*
  `$OV_FIELDS/$LANG/snmp_fields`

  `$LANG` refers to the setting of the `$LANG` language shell environment variable. To check the value of `$LANG` on your system, from the command prompt, enter:

  `echo $LANG`

  Use the value returned. If no value is returned, then use the default, which is `C`.

The following example illustrates how an `snmp_fields` file could be modified. Note the new entry in the file.

NOTE These entries are case-sensitive and must exactly match the field in the `oid_to_type` file.

```
Field "SNMPAgent" {
  Type      Enumeration;
  Flags     capability, general, locate;
  Enumeration "Unset",
  "HP 3000/XL",
  "HP 386",
  "HP 700/[R]X X-Terminal",
  "HP 9000/HP-UX",
    :
  "cisco Terminal Server",
  "cisco T-Router",
  "cisco Protocal Translator",
  :
  "Netware 386 TCP/IP",
  "New SNMP Agent",       <-- new entry
  "Novell Lantern",
  "NRC Fusion Xenix agent",
  "Process Software Corp. VMS agent",
    :
  "Xyplex Remote Ethernet Bridge",
  "4BSD ISODE";
  }
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1237
3740
Doc:

Configure the Database

It is not necessary to shut down the NNM services or to exit NNM when performing this step.

It is necessary to reinitialize the fields so that the new ones in the `snmp_fields` and `ovw_fields` files are loaded into the object database.

To reinitialize the fields, at the command prompt, type:

```
ovw -fields
```

Updating Field Values

It is not necessary to shut down the NNM services or to exit NNM when performing this step.

To force the `netmon` service to reread the `oid_to_type` file, at the command prompt type:

```
xnmpolling -event
```

Updating the Map

To update the map to reflect the changes, close and then reopen the map.

If the device has already been discovered, the vendor and SNMP agent changes will be detected during the next regularly scheduled configuration check. Those fields will be updated at that time to reflect the new values. You can set the intervals between configuration checks using `xnmpolling` or using the `Options:Network Polling Configuration->IP` menu item.

Alternately, you can delete the device's symbol from the map and let it be rediscovered. When the device is rediscovered, the new values will be used.

Backing Up Your Efforts

The following *analytical data* directories are *not* included in NNM's backup scripts:

- *Windows:*

  install_dir\backgrounds
  install_dir\bitmaps
  install_dir\fields
  install_dir\symbols

- *UNIX operating system:*

```
$OV_BACKGROUNDS
$OV_BITMAPS
$OV_FIELDS
$OV_SYMBOLS
```

When you make changes or additions to map backgrounds, bitmap files, field registration files, or symbol registration files ensure that your new files are properly backed up. See "Backup/Restore to Protect Your Investment of Time" on page 165 for more information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1238
3740
Doc:



Changing an Object's Vendor and SNMP Agent

Procedure

Symbols

.login file
  modifying, 101
.profile file
  modifying, 101
.vueprofile file
  modifying, 101

A

access
  no access, 293
  read-only, 292
  read-write, 292
  to maps, 292
accessing
  alarm information from the map, 339
  map information from alarms, 338
  MIB information, 52
accounting management
  components, 43
acknowledging alarms, 334
action block, WLRF, 496
adding
  background graphic, 262
  features to NNM, 278
  IP interface object, 260
  new symbols, 263, 662
  node object, 259
  segment object, 258
additional actions
  alarms, 339
  configuring, 339, 441
  See also Alarm Browser
additional views
  cdp view, 521
  internet view, 522
  neighbor view, 518
  node view, 520
  path view, 519
  Port-Address mapping command, 522
  station view, 522
address
  resolution, 579
  table poll operations in netmon, 179
  well-configured, 90
Address Resolution Protocol. See ARP/RARP
administrative symbol status, 271
agent. See SNMP agent
Alarm Browser
  acknowledging alarms, 334
  All Alarms category, 331
  assign category, 348
  configuring, 342
    automatic delete, 345
    event database, 343
    state file, 344
  correlated alarms, 352
  de-duplicated alarms, 352
  deleting alarms, 337
  features, 512
  filtering alarms, 335
  overview, 329
  starting, 513
  troubleshooting, 619
  window, 330, 332, 337
alarm categories
  configuring, 349
  window, 329, 331
alarm to map connection, 338
alarms, 323, 330, 338, 423
  accessing information, 338
  acknowledging, 334
  adding, 423
  additional actions, 339
  automatic actions, 433
  automatic delete configuration, 345
  categories, 348
  categories, new, 349
  configuration
    sources, 432
  configuring, 423
  copying, 423
  correlated
    see event reduction capabilities
  de-duplicated
    see event reduction capabilities
  definition, 323
  deleting, 337, 423
  deleting automatically, 345
  displaying, 329
  filtering, 335
  highlighting, 339
  monitoring devices, 326
  moving to a different category, 348
  using to diagnose problems, 566
  using to filter events, 566
  using to launch specific URLs, 340
  zoom to highlighted object, 338
Alarms command, 566

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1239
3740
Doc:

aliases, for web server, 485
All command, 561
All HSRP Groups command, 574
All VLANs command, 574
analytical data backup, 166
app-default files, 269
Application Builder. See MIB Application Builder
application layer
  hardware used in, 26
  in OSI model, 22
  protocols, 22
application registration files (ARF)
  control menu choices, 299
archive
  implement your plan, 170
  importance of, 165
ARF files for menu control, 299
ARP cache, viewing, 562
ARP/RARP, described, 23
attributes
  changing, 235
  locating objects by, 113
  object, 205
audit log file, 491
  format, 491
  location, 491
automatic actions, 433
  using trusted commands, 433
automatic discovery, 56
automatic thresholds, 453

B

background graphic
  adding, 262
  formats, 260
background processes
  See services
backup
  adding scripts, 176
  archive
    implement your plan, 170
    importance of, 165
  directory (staging area), 166
  disk space requirements, 168
  frequency, 167
  how it works, 166
  procedure, 167
  SOLID database, 175
  troubleshooting, 171, 174
backup routers
  missing from map, 136
Berkeley Internet Name Domain (BIND) Service, 579
Bridge MIB
  Base Port Table command, 564
  Base Table command, 563
  Spanning Tree Port Table command, 564
  Spanning Tree Table command, 564
  Static Table command, 564
  Transparent Forwarding Table command, 564
  Transparent PortTable command, 564
bridge MIB
  described, 28
  for topology polling, 184
bridges, 26
  discovery of, 103
  display of, 217
Browse MIB operation, SNMP Set requests, 628
browser
  DMI, 417
  MIB, 412
  See Alarm Browser
browsing
  alarms, 335
browsing MIBs
  problems with, 628
  See also SNMP MIB Browser
browsing MIFs. See DMI Browser
building new MIB applications, 43
bundled
  correlations, 360
  correlators, 386
bus layout, 242

C

cache, clearing from browser, 613
capabilities, 206
categories for alarms
  assigning, 348
  changing default, 348
  creating new, 349
  moving an alarm, 348
CDP command, 573
cdp view
  description, 521
CGI errors, 616
CGI programs, described, 545

change management
tools, 46
characteristics, symbol, 209
checking disk space, 527
checkpoint phases for backup, 166
child submaps
creating, 245
Cisco Discovery Protocol
Cache Table command, 563
Global Table command, 563
Interface Table command, 563
class, symbol, 207
client station, web components installed on, 485
collecting
historical MIB information, 45
MIB information, problems, 608
collecting data
See data collection
collecting SNMP data. See data collection
colors, status, 271
command
xnmevents, 341
communications problems diagnosing, 566
community names
configuring NNM, 93, 146
configuring SNMP agents, 93, 146
defined, 52
GET/SET, 93, 146
problems with, 626
requests for information, 52
testing with netmon.cmstr, 93, 147
Community-based SNMP version 2, 52
Composer, 386
compound status propagation, 275
configuration check
operations in netmon, 179
polling, 183
configuration management
components, 42
tools, 46
configuring
additional actions, 441
alarm categories, 349
alarms, 423
automatic actions, 433
correlations, 352
correlators, 352
de-duplications, 352
events, 422, 423
polling, 178, 194
print command, 475
problems with events, 631
SNMP events, 423
connection labels
defined, 223
connection symbol, 208
connections, multiple connections between symbols, 245
connectivity problems, diagnosing, 556, 557, 562, 567, 568
connector topology
polling, 184
Connector-Down correlation
behavior, 361
setting parameters, 362
important node filter, 192, 362
secondary failures, 192, 363
conserving memory, 657
container object, 248, 251
containment realm
editing guidelines, 253
example of Internet submap, 253
example of Partitioned Internet submap, 255
maintaining, 255
overview of, 252
context for menu items, 296
contrib programs
accessing, 74
controlling management traffic, 178
copying
events, 423
symbols, 257
correlating events, 352
correlation
background information, 354
command line control, 380
ConnectorDown, 361
files, 381
FrameRelay, 365
MgXServerDown, 369
new, 382
PairWise, 371
RepeatedEvent, 375
ScheduledMaintenance, 379
troubleshooting, 381
Correlation Composer, 386
correlator
background information, 354
files, 397

ECT 220 CPI-AC
RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1240
Doc. 3740



new, 398
OV_Chassis_Cisco, 387
OV_Connector_IntermittentStatus, 393
OV_HSRP_(group), 394
OV_MultipleReboots, 388
OV_NodeIf_(group), 390
troubleshooting, 397
CPU
load operation, problems with, 626
speed, performance impact, 656
viewing load, 559
CPU Load command, 559
CRC errors, viewing, 558
creating
child submaps, 245
correlations, 383
correlators, 398
de-duplication configurations, 358
executable symbols, 280
independent submaps, 245
Quick Navigator, 287
submaps, 244
critical status, 275
customizing
background graphic, 262
setting a user default map, 287
setting the home submap, 287
startup files, 535
cutting symbols, 257

D

data collection
configuring, 450
disk space usage, 168
graph, 472
graphing, 472, 473
reducing file size with ovdwtrend, 529
scheduling, 451
setting thresholds, 456
storing results, 448
using the data collector, 447
viewing results, 453
Data Collector, 473
data graphing, 473
data link layer
discovery of devices, 59
hardware used in, 26
in OSI model, 21
protocols, 23
Data Warehouse
Export Events command, 571
Export Topology command, 571
Export Trend Data command, 571
data warehouse, described, 63
database files
changing permissions, 295
databases
corrupted OVW object database, 604
event, 63
map, 62
NNM, 62
object, 62
topology, 63
trend, 63
de-duplicated, 358
deleting, 423
alarms, 337
nodes, 658
old snapshots, 555
description
Composer correlators, 386
de-duplication, 358
ECS correlations, 360
object, 236
Desktop Management Interface. See DMI
destination
SNMP trap, 325, 326
developing
additional actions, 441
automatic actions, 433
de-duplication configurations, 358
new correlations, 383
new correlators, 398
devices
discovery of, 104
supporting SNMP, 43
DHCP
described, 24
filter, 183
polling, 179, 181, 183
well-configured, 91
dialog boxes
General Attributes, 205
discovery, 103
automatic, 56
description of, 56
DIscover Level-2 Objects check box, 185
duplicate IP Address, 159
expanding, 117, 119

incorrect IPX node names, 157
IP and IPX, 58
IP Network 0.0.0.0, 156
IPX failure, 154
IPX node discoverd as two nodes, 159
Level 2, 59, 185
limiting, 117, 124
MAC address, 59
missing IPX routers, 156
netmon -k options, 185
no vendor translation, 159
non-IP devices, 59
non-IPX devices, 59
partial IPX, 157
problems with, 154
recommendations, 134, 153
requirements for IP, 56
requirements for IPX, 58
routing tables, 144
start again, 161
unmanaging a network, 589
verify accuracy, 109
discovery filter
procedure, 128
to improve performance, 531
disk space
checking, 527
regaining, 527, 529
viewing usage, 559
Disk Space command, 559
displaying alarms, 330
distributed event correlation, 357
DMI
configuring, 95, 417
described, 30
event, 54, 327
features, 30
MIF, 54, 327
See MIF
service provider, 54, 327
viewing status, 574
DMI Browser
accessing, 574
querying DMI values, 417
DMI devices
can't communicate with, 628
problems querying, 611, 628, 631
DNS
caching-only name server, 91
quick check, 92
secondary name server, 91
well-configured, 91, 133
documenting a map, 555
dynamic correlation parameters, 355
Dynamic Host Configuration Protocol. See DHCP

E

ECS, 360
e-mail message generation. See automatic actions
Enterprise Identification, 423
Enterprise MIB
adding, 423
correlating, 352
deleting, 423
environment variables
setting up, 101
error log file
contents, 498
Launcher, 653
using for troubleshooting, 498
Web Launcher, 616, 653
errors
monitoring SNMP, 561
viewing Ethernet, 558
Ethernet
statistics, monitoring, 558
traffic, monitoring, 558
Ethernet Errors command, 558
Ethernet Traffic command, 558
Event Browser
See Alarm Browser
Event Configuration
operation, 631
overview, 422
event correlation
bundled edition
Connector-Down, 192, 361
Frame-Relay, 365
ManageX Server-Down, 369
Pair-Wise, 371
Repeated-Event, 375
Scheduled-Maintenance, 379
developing your own, 383, 398
disabling, 354
distributed, 357
enabling, 354
settling time, 354
files, 381

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1241
Doc: 3740

general recommendations, 356
introduction, 353
parameters
dynamic, 355
static, 355
See event reduction capabilities
sources for more, 382
streams, 356, 380
event database
configuration, 343
event database, described, 63
Event Identification, 423
event log, browsing, 566
event reduction capabilities
Correlation Composer, 386
de-duplication, 358
described, 61, 352
ECS, 360
web based, 515
event storm prevention
Composer correlators, 386
Connector-Down correlation, 361
de-duplication, 358
ManageX Server-Down correlation, 369
Pair-Wise correlation, 371
Repeated-Event correlation, 375
Scheduled-Maintenance correlation, 379
events, 423
actions, 441
adding, 423
automatic actions, 433
configuration, 631
sources, 432
configuring, 423
correlating, 352
de-duplication, 358
definition, 323
deleting, 423
listing, 566
management stations receiving, 565
processes that generate, 591
propagation of, 591, 604
services that generate, 604
exact match, 114
executable symbols
adding, 280
described, 279
executing MIB applications, problems, 628
expanding maps
containment realm, 252
creating Partitioned Internet submap, 251
higher level maps, 247
IP interface object, adding, 260
node object, adding, 259
See Also containment realm
segment object, adding, 258
explodable symbols
defined, 279
export map, 256
Extended Topology, 44

F

fault management
components, 42
event reduction capabilities, 352
HP OpenView IT/Operations, 44
tools, 43
faults on network, diagnosing, 44, 45
field definitions, problems with, 595
field registration files, 667
file
backing up originals, 580
modifying default X resources, 581
original product, 580
permissions, 623
filters
alarms, 335
DHCP, 183
discovery, 128, 183
important node, 192
Connector-Down correlation, 362
OV_NodeIf_(group) correlator, 390
map, 232
persistence, 231
find
attributes, 235
entering text for exact match, 114
entering text for pattern match, 114
entering text for regular expressions, 114
objects, 113, 114
forwarding
SNMP trap from NNM, 326
SNMP trap to NNM, 325
Frame Relay
Circuit Congestion command, 558
Circuit Errors command, 558
Circuit Traffic Avg. Frame Size command, 558
Circuit Traffic Data Rate command, 558

Circuit Traffic Frame Rate command, 558
correlation of health, 365
Data Link Errors command, 559
Properties command, 564
Virtual Circuits command, 564
frequency of discovery value, in netmon, 179
FRF, 667
full restore of NNM data, 171

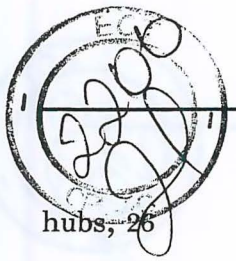
G

gateways
described, 26
discovery of, 103
General Attributes dialog box, 205
generating
alarms, 323
geometry of submaps, 266
get request, 53
get response, 53
getBulk request, 53
getNext request, 53
GIF graphics format, 260
graph
CPU load, 559
Ethernet errors, 558
Ethernet traffic, 558
Frame Relay circuit congestion, 558
Frame Relay circuit errors, 558
Frame Relay circuit traffic data rate, 558
Frame Relay circuit traffic frame rate, 558
interface discard percentage, 557, 569
interface discard rate, 556, 568
interface error percentage, 556, 568
interface error rate, 556, 568
interface statistics, 556, 568
interface traffic avg. packet size, 557
interface traffic data rate, 557
interface traffic packet rate, 557
interface traffic throughput, 557
interface traffic utilization, 557
printing, 475
selected data, 473
SNMP data, 561
SNMP errors, 561
SNMP operations, 560
SNMP traffic, 560
Graph All Data, 472
Graph SNMP Data command, 561
graphics
backgrounds for maps, 260
graphing
data, 472
historical data, 473
MIB data, 45
real-time data, 473
with xnmgraph, 544
greyed menu items, 206

H

help system, 67
files, viewing, 636
overview, 67
printing, 68
searching, 68
using separately from NNM, 69
using to create manuals, 68
hiding objects on map, 233
highlighting
alarms, 339
sources, 338
historical data, 473
holding area, 244
home submap
defined, 202
setting, 287
hotlist
creating, 287
HP Agent
trap recipients, 326
HP Education, 77
HP OpenView Grapher, 472
HP OpenView IT/Operations, for fault management, 44
HP OpenView Launcher. See Launcher
HP OpenView Web
applications, 484
Correlation Composer, 386
event correlation, 515
features, 484
requirements, 485
security, 486
setting up, 485
web browser, 485
web server, 485
HP-RDMI service provider, 417
hpterm, accessing, 570
HP-UX SAM command, 565
HSRP Group Detail view, 574
HSRP Node Detail view, 574
httpd service, troubleshooting, 586

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1242
3740
Doc:



hubs, 26

I

ICMP
  polling, 179, 181
ICMP, described, 23
icon symbols
  described, 207
import map, 256
important node filter
  Connector-Down correlation, 362
  OV_NodeIf_(group) correlator, 390
  setting, 192
independent submaps, creating, 245
initial discovery
  process, 107
  start again, 161
  troubleshooting
    IP, 131
  verify information, 109
instance
  query for, in MIB Browser, 412
instance, MIB, 29
interface
  status of interface, 556, 568
  status of node, 556, 568
Interface Avg. Packet Size command, 557
Interface Error Percentage command, 556, 568
Interface Error Rate command, 556, 568
Interface Errors
  Data Link Errors command, 569
  Discard Percentage command, 557, 569
  Discard Rate command, 556, 568
  Frame Relay Circuits command, 569
interface object, 112
Interface Status command, 556, 568
Interface Traffic
  Data Rate command, 557
  Throughput command, 557
  Utilization command, 557
Interface Traffic command
  uses of, 654
Interface Traffic Packet Rate command, 557
Internet command, 573
Internet Control Message Protocol. See ICMP
Internet level, 230
Internet Packet Exchange. See IPX
internet view
  description, 522
inventory network objects
  internet object properties, 111
inventory report, 107
IP
  addressing, 579
  described, 23
  discovery, 56
  forwarding, 140
  interaction with IPX, 58
  internet object, 111
  objects, discovery of, 103
  requirements for discovery, 56
  routes, locating, 567
  secondary addresses, 137
  topology behavior, 466
  well-configured, 90
ipmap
  described, 543
  managing objects, 255
  propagation of events from, 605
IPv6 Network command, 574
IPv6 Node Detail view, 574
IPv6 Prefix Groups view, 574
IPX
  described, 23
  discovery, 56, 57
  interaction with IP, 58
  layout, 57
  polling, 179, 180, 184
  requirements for discovery, 57
  transport software, 100
IPX discovery
  duplicate IP Address, 159
  failure, 154
  hop count
    expanding, 123
    limiting, 130
  incorrect node names, 157
  IP Network 0.0.0.0, 156
  missing routers, 156
  no vendor translation, 159
  node discoverd as two nodes, 159
  partial, 157

J

Java
  errors, 617
  parameters, modifying, 499
jumpstart

netmon, 152

K

keyboard, 474

L

latency time
for WANs, 182
in polling, 182
Launcher
accessing, 571
blank window, 616
CGI error, 616
configuring, 494
error log, 498, 653
features, 492
Information and Reports tab, 575
Java error, 617
Java parameters, 499
Object Views tab, 575
registration file. See WLRF
starting, 492
tabs, 575
Tasks tab, 575
Tools tab, 575
troubleshooting, 616
user interface, 492
user login error, 615
WLRF error, 617
Layer 1
hardware used in, 25, 26
in OSI model, 21
Layer 2
hardware used in, 26
in OSI model, 21
protocols, 23
Layer 3
hardware used in, 26
in OSI model, 22
protocols, 23
Layer 4
in OSI model, 22
protocols, 23
Layer 5
in OSI model, 22
Layer 6
in OSI model, 22
Layer 7
hardware used in, 26
in OSI model, 22
protocols, 22, 23
layers, in OSI model, 21
layout, 242
automatic, 56
bus, 242
description of, 56
point to point, 242
ring, 242
row/column, 242
layout algorithm
default, 241
level 2
discovery, 56, 59, 185
polling, 180, 184
license
checking number of nodes, 533
OVLicenseMgr, 599
limitations, known in loading MIBs, 634
line
attributes, 475
configuration, 475
Graph, All Data, 472
Graph, Select Data, 473
list block, in WLRF, 495
Load/Unload MIBs operation, 633
loaded MIB database, modifying, 633
loadhost program
expand management domain, 122
limit management domain, 127
loading MIBs, 413
limitations of, 634
operation, 633
problems with, 633
unique object label, 634
local host file
quick check, 92
well-configured, 91, 133
Local Registration File (LRF)
customizing for performance, 535
customizing for startup, 535
locating objects
see find
log files
audit, 491
error, 498, 653
Launcher error, 653
logging
common options, 640
correlations, 380

ECT 2190 CPL-AC

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1243
3740
Doc:

description of, 639
example, 645
explained, 643
log files, 648
output, 649
recommendations, 580
Web Launcher errors, 616, 653
with netfmt, 643
with nettl, 644
lp, 475
LRF. See Local Registration File

M

MAC address, using to discover devices, 59
magicpacket command, 570
maintenance
audit log file, 491
daily, 527
error log file, 498, 653
monthly, 533
weekly, 531
managed object, defined, 53
Management Information Base. See MIB
Management Information Framework. See MIF
management region
expanding, 108, 117, 119
IPX hop count, 123
loadhost program, 122
seed file, 120
limiting, 117, 124
Discovery filter, 128
IPX hop count, 130
loadhost program, 127
netmon.noDiscover file, 125
oid_to_type file, 129
troubleshooting, 131
management station
interaction with Network Presenter, 505
receiving traps, 565
web components installed on, 485
Management Web Page, accessing on remote node, 572
manager
defined, 51
manager-agent
communication through SNMP, 52
ManageX Server-Down correlation
behavior, 369
setting parameters, 370
managing
polling, 193
manpages
acessing, 72
printing, 73
viewing, 636
MANPATH statement
setting, 101
manuals, accessing online, 69
map database, described, 62
maps
access rights, 292
adding features, 278
automatic discovery and layout, 56
background graphics, 260
changes, 286
child submap, 245
compound status, 275
containment realm, 252
context, 296
copying, 215
creating symbols, 263
defined, 199
expanding, 247
file permissions, 292
filters for objects, 232
geometry, 266
hiding objects, 233
independent submap, 245
initial appearance, 103
layout
auto, 241
do-it-yourself, 242
limiting menu choices, 299
maintaining the containment realm, 255
menu control, 299
metaconnections submaps, 245
network symbol names, 221
new object holding area, 244
no access, 293
open map, 199, 215, 221
overlay, 267
partitioned internet submaps, 248
permissions, 292
persistance, 229
preferences, 287
problems with, 654
propagate most critical status, 276
propagate status at threshold value, 276

Quick Navigator, 288
read-only access, 292
read-write access, 292
remote viewing, 317
removing old snapshots, 555
See also expanding maps
See also Partitioned Internet submap
size and placement, 266
snapshot, 555
start over, 161
startup options, 289
switch/bridge display, 217
troubleshooting
IP, 131
IPX, 153
user preferences, 287
marginal status, 275
MAU MIB
described, 28
for topology polling, 184
memory
clearing from browser, 613
conservation tips, 657
not enough, 657
performance impact, 656
problems affecting ovwdb, 604
related problems, 579
memory requirements
for maps, 229
menu items
adding to Network Presenter, 505
adding to NNM, 299
greyed, 206
meshing
definition of, 59
example, 227
specifying in NNM, 228
meta-connection
submap, 246
symbol, 245
MIB, 43
accessing information, 52
Application Builder operation, 443, 628, 629
bridge, 28
for topology polling, 184
Browse operation, 46
building new applications, 43
collecting historical information, 45
data, 472
data collection
effects of, 453, 654
operation, 608
defined, 27
defining thresholds, 44
operation for, 453
DMI conversion from MIF, 95, 419
enterprise-specific objects, 43
graphing data, 45
instance, 29
loading (adding), 413
prerequisites, 414
MAU
described, 28
for topology polling, 184
numeric values, 447, 455
object, 28, 43
object identifier, 28
object label, unique, 634
obtaining MIB files, 94
organization, 28
private, 28
querying, 412
repeater, 28
for topology polling, 184
RFC (technical details), 33
RMON, 27
See Also data collection
setting MIB values, 412
setting values, 412
SNMP traps, 44
storing data for trend analysis, 45
tree, 28
troubleshooting, 572
variable bindings, 404
vendor-specific, 413
viewing, 412, 572
viewing MIB values, 412
MIB Application Builder
and DMI device, 628, 631
using, 443
MIB applications
executing, 629
problems building, 628, 629
troubleshooting, 629
MIB Browser. See SNMP MIB Browser
MIB event thresholds,defining, 44
mib.coerce file, 464
mibExpr.conf file, 463

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1244
3740
Doc:



MIB-II
  described, 27
Microsoft Terminal Services, 317, 318
MIF, 54, 327
  configuring for NNM, 95, 419
  described, 29
  loading (adding), 95, 419
    with translation to MIB, 420
    without translation to MIB, 420
  mapping to MIB, 328
  vendor-specific, 420
modifying
  events, 423
  Java parameters, 499
  line attributes, 475
  ovsuf, 536
monitoring
  CPU load, 559
  devices, 326
  disk space, 559
  Ethernet statistics, 558
  Ethernet traffic, 558
  Frame Relay circuit average frame size, 558
  Frame Relay circuit congestion, 558
  Frame Relay circuit errors, 558
  Frame Relay circuit traffic data rate, 558
  Frame Relay circuit traffic frame rate, 558
  Frame Relay Circuits, 569
  Frame Relay Data Link errors, 569
  Frame Relay data link errors, 559
  SNMP authentication failures, 560
  SNMP errors, 561
  SNMP operations, 560
  SNMP traffic, 560
  TCP connections, 557
mouse and keyboard
  grapher, 474
moving
  symbols, 257
multi-homed node, discovery of, 103

N

name resolution, 91, 92, 133
naming network symbols, 221
Neighbor command, 572
neighbor view, 518
NetBios
  quick check, 92
  well-configured, 91, 133
netfmt, 643
  described, 643
  examples of, 649
  filtering options, 649
netmon, 466
  address table poll operations, 179
  configuration check operations, 179
  configuring, 193
  dependencies, 586
  described, 541, 587
  disabling, 195
  discovery behavior, 541
  enabling, 195
  event generation conditions, 604
  frequency of discovery values, 178
  instance restrictions, 589
  IP discovery, 56
  IPX discovery, 57
  jumpstart(-J), 152
  monitoring, 194
  netmon.noDiscover file, 125
  performance check, 193
  permissions, 623
  poll operations, 179
  problems with, 154
  proxies, 179
  queue (-q, -Q), 193
  requirements for discovery, 56, 57
  seed file, 119
  timeout intervals, 179
  trace masks, 641
  tracing, 641
  tracing example, 641
  troubleshooting, 587
    tools, 589
netmon.cmstr, 147
  testing community names, 93
netmon.equivPorts, 60, 226, 228
netmon.lock file, 589
netmon.lrf, 193
  described, 536
  segRedux, 217
netmon.noDiscover file
  effect on discovery, 126
  example, 126
  HSRP virtual IP address, 126
  procedure, 126
netmon.snmpStatus, 274
netnmrc script
  execution sequence, 625

nettl
described, 643
examples of, 645
generating log files, 648
generating trace files, 648
log file output, 649
options
-log, 645
-start, 644
-status, 644
-stop, 648
-traceoff, 647
-traceon, 646
pathnames for, 643
subsystems used with, 643
Network Activity menu, described, 556, 568
Network Configuration
ARP Cache command, 562
ATM Properties command, 565
Cisco VLAN MembershipTable command, 563
DS1/E1 Serial Line Properties command, 565
DS3/E3 Serial Line Properties command, 565
Interface Properties command, 562
IP Addresses command, 562
IP Routing Table command, 562
IP Services command, 562
SONET/SDH Properties command, 565
Network Connectivity
Locate Route via SNMP command, 567
Show Path command, 567
Trace Route command, 567
network hardware
bridge, 26
gateway, 26
hub, 26
repeater, 25
router, 26
switch, 26
network layer
hardware used in, 26
in OSI model, 22
protocols, 23
network level, 230
network management
benefits, 42
defined, 42
functions, 42
proactive, 40
network management operation
problems with, 626
remote node support for, 626
network map
using a seed file, 119
network object, 111
Network Presenter
components, 502
connecting to an NNM session, 502
features, 501
features vs. NNM, 503
interaction with management station, 505
permissions, 618
problems starting, 618
registration file. See NPRF
specifying map to open, 502
starting, 501
symbol registration file, 506
troubleshooting, 618
URL for, 501
network traffic
control, 178
viewing, 560
NetworkAdmin user role, 488
NetworkOper user role, 488
networks
naming symbols, 221
new node discovery
polling, 185
NIS
quick check, 92
well-configured, 91, 133
NNM
configuration files, changing permissions, 295
options for starting, 289
starting, 106, 121, 122, 195
status check, 106
NNM Extended Topology, 44
no access, 293
node
deleting unwanted, 658
discovery of IP, 57
discovery of IPX, 57
information obtainable from, 582
information storage, 57
listing information about, 565
multi-homed, 103

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1245
3740
Doc:

non-SNMP, 582, 626
object, 112
obtaining status, 566
polling, 566
represented as a symbol, 105, 679
testing remote, 570
turning on remote, 570
Node command, 573
node view, 520
description, 520
normal status, 275
notification, 325
defined, 52
NPRF
adding menus, 505
adding toolbar buttons, 505
format, 505
location, 505
troubleshooting, 619
NTAdmin user role, 488
NTOper user role, 488
numeric MIB values, 447, 455

O

object database
and ovwdb, 542
described, 62
object manager
ovstatus cannot find, 585
objects
adding attributes, 238
attribute

setting parameters, 393
OV_HSRP_(group) correlator, 394
behavior, 395
parameter settings, 396
OV_MultipleReboots correlator, 388
behavior, 388
parameter settings, 389
OV_NodeIf_(group) correlator, 390
behavior, 390
disabling, 392
important node filter, 390
setting parameters, 391
ovactiond
dependencies, 586
described, 541
troubleshooting, 590
trusted commands, 433
trustedCmds.conf directory, 433, 434
ovactiond.lrf, described, 536
ovaddobj command
described, 541
netmon, configuring seed file, 125
OVAdmin user role, 489
ovalarmadm, 347
ovalarmsrv
dependencies, 586
described, 542
troubleshooting, 590
ovas
described, 542
ovbackup.ovpl, 167, 170
ovcapsd, 54, 327, 420
dependencies, 586
described, 542, 591
troubleshooting, 591
ovcapsd.lrf, described, 537
overlay of submaps, 267
overview
Alarm Browser, 329
Event Configuration, 422
ovhtpasswd command, 487
ovrepld
dependencies, 586
described, 542
troubleshooting, 594
ovrepld.lrf, described, 537
ovrequestd, 542
ovrequestd background service, 607
ovrestore.ovpl, 172, 173
ovspmd
described, 541
determining problems, 592
recreating sockets directory, 593
troubleshooting, 592
ovstart command
described, 541
in starting background services, 584
ovstatus command
failure to find object manager, 585
verifying daemon services, 585
ovsuf
described, 541
modifying, 536
ovtopmd
dependencies, 586
described, 542, 594
troubleshooting, 594, 595
ovtopmd.lrf, described, 537
ovtopodump
description of, 597
troubleshooting, 597
ovtopofix command, 217
ovtrapd
dependencies, 586
described, 542, 599
operation of, 599
troubleshooting, 599
ovtrapd.lrf, described, 537
ovuispmd
dependencies, 586
described, 542, 600
troubleshooting, 600
ovuispmd.lrf, described, 537
ovw command
described, 543
options, 289
-mapcount, 289
-verify, 289, 302
ovw.auth file, location, 506
ovwchgrp, 295, 624
ovwchmod, 295, 624
ovwchown, 295, 624
ovwdb
corrupted OVW object database, 604
dependencies, 586
described, 542, 602
insufficient memory, 603
insufficient performance, 603
troubleshooting, 602
ovwdb.auth file
location, 506

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1246
3740
Doc:



ovwdb.lrf, described, 537
ovwls, 295, 624
ovwperms, 295

P

paging automatically. See automatic actions
Pair-Wise correlation
  behavior, 372
  setting parameters, 373
palette, 207
Partitioned Internet submap
  creating, 251
  example of, 255
  how it is managed, 255
  overview of, 248
  See Also containment realm
password
  in user authentication file, 487
  modifying, 487
pasting symbols, 257
patch releases, verifying, 533
Path command, 573
PATH statement
  modifying, 101
path view, 519
pause NNM services
  for back up
    analytical, 166, 168
    operational, 168
Performance
  Graph Data, 472
performance, 473
  customizing startup, 535
  diagnosing problems, 44, 45
  improving NNM, 658
  increasing, 656
  limiting factors, 656
  polling, 531
  problems with, 656
performance management
  components, 42
  reports, 45
  tools, 45
performance problems, diagnosing, 556, 557, 559, 568
Perl (HP's version)
  backup/archive/restore, 176
permissions
  change for configuration files, 295
  change for database files, 295
  changing, 624
  default, 623
  no access, 293
  read-only, 292
  read-write, 292
  restoring default, 624
persistance of submaps, 229
persistence filter, 231
physical layer
  hardware used in, 25, 26
  in OSI model, 21
ping
  remote node, 570
  using to determine connection, 567
planning, 80
  assuming responsibility, 82
  changes to the map, 286
  how to configure NNM, 83
  which devices to manage, 87
pmd, 323
  alarm gathering, 324
  dependencies, 586
  described, 542, 604
  operation of, 604
  permissions, 623
  troubleshooting, 381, 397, 591, 604
pmd.lrf, described, 537
point to point layout, 242
Poll Node command, 566
poll operations, in netmon, 179
polling
  adjusting intervals, 531
    from a remote computer, 182
  behavior, 589
  causing problems, 580
  configuration check, 180, 183
  controls, 178, 588
  delays in, 589
  disabling, 195
  during map generation, 178
  effects of reducing, 178, 179, 654
  file, 588
  initial process, 56
  latency time, 182
  new node discovery, 178, 180, 185
  non-IP devices, 59
  non-IPX devices, 59
  performance
    checking, 531
  problems with, 589

secondary failures, 180, 192
secondary IP addresses, 137
status, 178, 179, 181
to conserve memory, 657
topology check, 180, 184
traffic generated by, 654
troubleshooting
IP, 131
jumpstart netmon, 152
SNMP, 93, 145
subnet masks, 91, 149
tuning, 193, 194
values storage, 178, 543, 588
Port Address Mapping command, 522
description, 522
port number, used to start HP OpenView Web, 485
port trunking
definition of, 59
example, 225
specifying in NNM, 226
Port-Address Mapping command, 571
ports, connection problem, 596, 603
predefined symbols, 208
preferences, 287
preferences, setting a user default map, 287
presentation layer, in OSI model, 22
print command, 475
configuration, 475
printing
graph, 475
online help, 68
private MIB, 28
proactive network management, 40
problem management
components, 42
tools, 43
problems, 131
additional sources of information, 579
address resolution, 579
analyzing symptoms, 582
background services, 584
Browse MIB operation, 628
characterization, 582
diagnosing network faults, 44, 45
diagnosing performance, 44, 45
event correlation, 381, 397
failure to discover IPX nodes, 154
Launcher won't start, 616
launching applications, 637
limitations on loading MIBs, 634
loading MIBs, 633
map, 654
netmon, 154, 589
network management operation, 626
network operation, 623
ovtopmd, 595
ovtopodump, 597
ovwdb, 603
performance, 656
pmd, 606
polling, 589
resource exhaustion, 579
runtime, 623, 625
starting Launcher, 613
starting Network Presenter, 618
subnet mask, 149
unmanaging a network, 589
user logins, 615
X Windows, 635
product support
contacting, 77
propagating symbol status, 271
most critical status, 276
status at threshold value, 276
protocols, and OSI model, 24

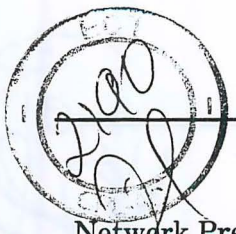
Q

quick check
name resolution, 92
Quick Navigator, 288
creating, 287

R

read-only
access, 292
read-write
access, 292
real-time data, 473
real-time data graphing, stopping, 474
recreating map and topology databases, 161
reference pages
acessing, 72
printing, 72
viewing, 636
registering an application, 278
registration files
field, 667
Launcher. See WLRF

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1247
Doc 3740



Network Presenter. See NPRF
symbol, 664
update/verify, 668
regverify command, 494
release notes, accessing, 71
remote access to NNM, 317
remote nodes
testing, 570
turning on, 570
Remote Ping
described, 567
problems with, 626
remoteConfAllow.conf file, 182
removing, old snapshots, 555
Repeated-Events correlation
behavior, 376
setting parameters, 376
repeater
discovery of, 103
repeater MIB
for topology polling, 184
repeater MIB, described, 28
repeaters, 25
report
configuration interface, 45
general availability, 45
general inventory, 45
inventory, 107
modification, 45
Reporting interface, 516
troubleshooting, 614
reports
removing, 529
restarting automatic map generation, 161
restore
adding scripts, 176
all NNM data, 171
some NNM data, 173
RFC documents
list of, 33
ring layout, 242
RMON
Host Table Command, 560
Segment Errors command, 559
Segment Octets command, 559
Segment Packet Sizes command, 560
Segment Packet Types command, 560
Segment Utilization command, 559
RMON menu, described, 559
RMON MIB, 27
root submap, 202
routers, 26
routes, locating IP, 567
routing tables
in IP discovery, 144
viewing, 562
row/column layout, 242
running services, checking, 527
runtime components on network
problems with, 623

S

SAM, accessing, 565
Scheduled-Maintenance correlation
behavior, 379
setting parameters, 379
searching online help, 68
secondary failures
Connector-Down correlation, 363
OV_NodeIf_(group) correlator, 390
polling, 192
security
audit log file, 491
for HP OpenView Web, 486
ovw.auth file, 506
ovwdb.auth file, 506
session configuration file, 490
user authentication file, 487
user roles file, 488
security management
components, 43
seed file
description of, 120
effect, 122
example, 120
format, 126
location, 126
name, 126
networks implied by, 126
when to use, 119
segment
object, 112
segment level, 230
Selected Nodes, 473
Selected Nodes command, 561
selecting
sources that correspond with alarms, 339
selection name, locate object by, 113
Server Web Page
accessing on remote node, 572
service provider



See DMI
services
at start-up time, 547
checking running, 527
dependencies on other services, 585
during operation, 548
logging and tracing, 639
netmon, 466
pmd, 323
starting with ovstart, 584
troubleshooting background, 584
verifying with ovstatus, 585
viewing configured, 562
web interface, 545
session configuration file, 490
defaults, 490
format, 490
location, 490
session layer, in OSI model, 22
set operation, 52
set request, 53
setting
community names, 145
filters, 335
home submap, 287
MIB values, directly, 412
MIB values, using query, 412
user default map, 287
setting your path, 101
settling time
event correlation, 354
Simple Network Management Protocol. See SNMP
Snapshot Recover operation, 135
snapshots
map, 555
removing old, 555
SNMP, 473
agents required, 134
Authentication Failures command, 560
community names, 146
configuration, 145, 146
data graph, 472
data graphing, 473
Errors command, 561
event configuration, 423
event correlation, 352
graphing data on all nodes, 561
graphing data on selected nodes, 561
nodes without, 59, 582, 626
Operations command, 560
operations for accessing MIB information, 52
polling, 178, 474
port, 146
proxie for agent, 146
RFC (technical details), 33
services, listing supported, 562
SetRequests in a Browse MIB operation, 628
Traffic command, 560
traps, 44
variable bindings, 404
version 1, described, 22
version 2
described, 23
SNMP agent
changing, 678
defined, 52
management operations exclusive to, 626
non-HP, 626
propagation of events from, 599
required for SNMP, 134
setting attribute, 676
unknown, 148
well-configured
community names, 93
MIB files, 93
trap forwarding, 93
SNMP Data Presenter
configuring, 511
features, 509
starting, 510
SNMP MIB Browser
accessing, 572
querying, 412
setting values, 412
troubleshooting SNMP, 136, 140, 147
viewing, 412
snmp notify, 325
SNMP services, 53
get request, 53
get response, 53
getBulk, 53
getNext, 53
set request, 53
SNMP Trap Recipients command, 565
SNMP traps, 326
forwarding from NNM, 326

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1248
Doc. 3740

forwarding to NNM, 325
snmpCol.trace file, 609
snmpColDump, 608
snmpCollect
dependencies, 586
described, 543
tracing, 610
troubleshooting, 608
snmpCollect.lrf, described, 538
snmpd
errors, 635
propagation of events from, 599
SNMPv1
traps, 325
SNMPv1, described, 22
SNMPv2c, 325
described, 23
traps, 325
sockets
recreating ovsmpd sockets directory, 593
SOLID database
discreet backup, 175
sources that correspond with alarms, 339
sparse files (UNIX only)
backup, 171, 172, 173
special variables, 436
SRF, 664
staging area for backups, 165
standard deviation, 453
star
layout, 242
starting NNM, 106, 121, 122, 161, 173, 174, 195
redo initial discovery, 161
startup
automatic
disabling, 535
enabling, 535
customizing for performance, 535
state file
configuration, 344
static correlation parameters, 355
Station command, 573
station view
description, 522
status
categories, 271
colors, 271
compound source, 273
compound, explained, 275
conditions, 271
devices outside firewall, 184
marginal, 275
object source, 273
polling, 181
polling by object class, 182
polling with SNMP, 183, 273
propagate most critical, 276
symbol status, 271
stopping
all NNM sessions, 319
NNM to redo discovery, 161
real-time data graphing, 474
storing, MIB data for trend analysis, 45
streams and event correlation, 356, 380
subclass, symbol, 207
submaps, 245
background graphic, 202, 260, 262
creating, 244, 245
defined, 200
geometry, 266
home, 202
independent, creating, 245
layout algorithm, 241
meta-connection, 246
Node, 259
overlay, 267
Partitioned Internet, 248
persistence, 229
Quick Navigator, 288
regular vs. meta-connection, 246
root, 202
Segment, 259
setting, 287
subnet masks, 150
hierarchial, 91, 149
non-contiguous, 91, 149
problems with, 149
troubleshooting, 91, 149
subsystems used with nettl command, 643
support
obtaining, 77
programs provided, 74
swap space related problems, 579
switch centric view, 574
switches, 26
display of, 217
symbol
See node
symbol registration file, 664
for Network Presenter, 506

symbols
adding, 258
behavior, 279
changing, 662
characteristics, 209
class, 207
color
propagate, 274
status, 270
connection, 208, 246
context, 296
copying, 257
creating, 263, 662
cutting and pasting, 257
defined, 207
executable, 279
explodable, 279
hiding on map, 233
icon, 207
meta-connection, 245
moving, 257
multiple connections between, 245
naming networks, 221
predefined, 208
See node
status, 113, 271
subclass, 207
type, 114, 207
varieties, 207
synchronized data
restore all NNM data, 171
sysObjectID, 676
definition, 465
describing an SNMP agent's source, 466
determining IP topology behavior, 466
determining symbol type, 466
event reduction, 352
identifying an event's source, 466
netmon, 466
System Administration Manager, accessing, 565
System Information command, 565
system registry, 268
map access, 303
map appearance, 268

T

tab block, WLRF, 495
TCP
described, 23
viewing connections, 557
TCP Connections command, 557
TCP/IP
described, 23
telnet
accessing hpterm, 570
accessing terminal emulator, 570
accessing xterm, 571
terminal emulator, accessing, 570
terminal window, accessing, 570
thresholds
file, 588
operation for defining, 453
time intervals, 473
timeout intervals, 179
Tip of the Day
behavior, 69
toolbar buttons
adding to Network Presenter, 505
Tools
HP OpenView Launcher command, 571
Port-Address Mapping command, 571
Remote Power On command, 570
Report Presenter command, 569
Telnet (hpterm) command, 570
Telnet (xterm) command, 571
Terminal Connect command, 570
Unused IP Addresses command, 571
Views
All HSRP Groups command, 574
All VLANs command, 574
CDP command, 573
Internet command, 573
IPv6 Network command, 574
Neighbor command, 572
Node command, 573
OSPF Backbone command, 573
Path command, 573
Station command, 573
topology
polling, 184
topology database
and ovtopmd, 542
described, 63
total restore of NNM data, 171
trace file
trimming, 529
tracing
cautions for using, 639

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1249
3740
Doc:

common options, 640
data collection, 610
description of, 639
netmon, 641
recommendations, 580
trace files, 648
trimming file, 529
turning on, 647
with nettl, 646
traffic generation
measurement of polling, 654
regulation of polling, 178, 654
training
HP Education, 77
Transmission Control Protocol. See TCP
transport layer
in OSI model, 22
protocols, 23
trapd.conf, 422, 432
file, 631
trapd.log, 343
traps, 325, 422
defined, 52, 325
forwarding from NNM, 326
forwarding to NNM, 93, 325, 565
recipients, 326
SNMP, 44
trend database, described, 63
trimming
trace file, 529
troubleshooting, 131
additional sources of information, 579
Alarm Browser, 619
analyzing problems, 582
archive, 171, 174
background services, 584
backup, 171, 174
collecting too much data, 580
defaults modifications, 581
DMI communication, 628
IP, 131
Launcher, 616
Launcher error log file, 498, 653
name resolution scheme, 91, 92, 133
network operation, 623
Network Presenter, 618
OVLicenseMgr, 599
polling too much, 580
recommended practices, 579
restart initial discovery, 161
SNMP agents, 146
symptoms, 582
trustedCmds.conf directory, 433, 434

U

UDP, described, 23
universal pathnames
setting up, 101
universal pathnames for UNIX, 100
UNIXAdmin user role, 489
UNIXOper user role, 489
unknown status, 275
unmanage objects, 117
automatically, 129, 193, 669
defined, 53
effects of, 193, 654
uses of, 193, 654
Unused IP Addresses command, 571
user authentication file, 487
location, 487
modifying, 487
User Datagram Protocol. See UDP
user default map
setting, 287
user preferences, 287
user roles
described, 488
NetworkAdmin, 488
NetworkOper, 488
NTAdmin, 488
NTOper, 488
OVAdmin, 489
UNIXAdmin, 489
UNIXOper, 489
user roles file, 488
format, 489
location, 489

V

values
MIB, 412
variable binding
event reduction, 352
how to find and use, 404
variables, 436
vendor attribute, 676
viewing
connection labels, 223
events, 330
MIB values, 412

network services, 562
object descriptions, 111, 112
see find
traffic route, 562
VLAN membership view, 574

W

WANs
latency time for, 182
web browser
launching on remote node, 572
requirement on client station, 485
web interface services, 545, 550
web server
aliases, 485
included in NNM, 485
web sites
for NNM manuals, 76
HP OpenView, 78
HP Openview, 76
network management, 35
OpenView Forum, 77
product support, 77
WebWindow, 496
well-configured network
community names, 93
DHCP, 91
DMI service providers, 95
MIB files obtained, 94
name resolution, 91, 133, 141, 143
SNMP, 145
subnet masks, 91, 149
trap forwarding, 93
troubleshooting, 131
white papers,accessing, 75
wildcards
event sources, 432
netmon.noDiscover file, 126
threshold monitoring, 452
window, 331, 332
Alarm Browser, 329
Alarm Categories, 329
window geometry, 266
Windows
Diagnostics, 569
Event Viewer, 569
Performance Monitor, 561
Registry Editor, 565
system registry, 268
WLRF, 494
action block, 496
components, 494
list block, 495
location, 494
problem reading, 617
tab block, 495
verifying, 494
Web Launcher Registration File, 494
WebWindow, 496
www access, 318

X

X Windows
.Xdefaults file, 581
performance impact, 656
problems with, 635
resources, 581, 635
restoring default resources, 635
X11 monochrome bitmap format, 260
xnm program
operations started by, 626
permissions, 623
xnmappmon
described, 543
operations started by, 627
xnmbrowser, described, 543
xnmbuilder, described, 543
xnmcollect, described, 543
xnmevents
command, 341
xnmeventsExt.conf file, 340
launching views and URLs, 340
modifying, 340
xnmgraph, described, 544
xnmloadmib, described, 544
xnmpolling, 194
xnmpolling, described, 544
xnmsnmpconf, described, 544
xnmtrap, 422
xnmtrap, described, 544
xpr, 475
xterm, accessing, 571
xwd, 475

Z

zoom, 474

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1250
3740
Doc:

2184

São Paulo, 16 de dezembro de 2003

Aos
CORREIOS

Pregão nº 118/2003 – CPL/AC

Prezados Senhores,

A TM Solutions está honrada em responder sua solicitação. Estamos encaminhando para apreciação nossa proposta para Pregão nº 118/2003 - CPL/AC.

Estamos confiantes que a nossa proposta atenderá suas necessidades atuais e futuras. Para maiores esclarecimentos e informações, não hesite em contatar-nos.

A TM Solutions possui pessoal, tecnologia, experiência e comprometimento que resultarão em uma parceria perfeita com vocês.

Atenciosamente,

Roberto Florentino da Silva Junior

Representante Legal

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1251
Doc. 3740

1. Proposta Econômica

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1252
Doc: 3740

2187

PROPOSTA ECONÔMICA

PREGÃO Nº 118/2003.

1. Razão Social da Empresa: .TM Solutions – Tecnologia da Informação Ltda.
2. CNPJ Nº: 67.726.505/0001-09
3. Inscrição Estadual: 206.073.934.112
4. Inscrição Municipal: 5.16276-7
5. Endereço Completo: .Rua Ceará, 193 – Conjunto 3 – Alphaville – Barueri – SP – cep: 06465-120
6. Telefone: (011).4166-6999 Fax: ..(011) 4166-6999 E-mail: .tmsolution@tmsolution.com.br
7. Validade da Proposta: ..60. *(sessenta)* dias
8. Prazo de Pagamento: Em parcela única, mediante entrega das ferramentas, no prazo de 15 (quinze) dias após a emissão do Termo de Aceitação Final – TAF.
9. Banco: Real Agência: 0822 Conta Corrente: 7723347-1
10. Representante da Empresa: .Roberto Florentino da Silva Junior
11. Cargo: .Representante de Vendas . RG: .5.150.005-9 (SSP-PR). CPF: .005.539.839-11
12. Unidade da Federação de emissão da Nota Fiscal: .São Paulo

Apresentamos nossa Proposta para fornecimento do material do objeto do Pregão nº /2003, acatando todas as estipulações consignadas no Edital, conforme abaixo:

ITEM	DESCRIÇÃO	UNID.	QTDE.	PREÇO UNITÁRIO (R$)	PREÇO TOTAL (R$)
01	Licença do Software HP OPEN VIEW NETWORK NODE MANAGER ENTERPRISE VERSÃO 6.2 OU SUPERIOR.	UM.	05	99.000,00	495.000,00 X 494.000,00

PREÇO UNITÁRIO (R$ 99.000,00) NOVENTA E NOVE MIL REAIS
PREÇO TOTAL (R$ 494.000,00) QUATROCENTOS E NOVENTA E QUATRO MIL REAIS

Garantia do objeto: (01 ano)

Solicito desconsiderar valor acima e considerar valor correto - Quatrocentos e noventa e cinco mil X

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1253
3740
Doc:

2181

tmX Solutions

MODELO DE PLANILHA DE CUSTOS DE FORMAÇÃO DO PREÇO

ITEM	PERCENTUAL
1. MATÉRIA PRIMA/INSUMOS:	
	80%
Subtotal	80%
2. TRIBUTOS	
	5%
Subtotal	5%
3. TRASPORTES	
	2.5%
Subtotal	2.5%
4. DESPESAS ADMINISTRATIVAS	
	2.5%
Subtotal	2.5%
5. LUCRO	
	5%
Subtotal	5%
6. OUTROS	
	0% 5%
Subtotal	0% 5%
TOTAL	100%

Declaramos que tomamos conhecimento de todas as informações e condições para o cumprimento das obrigações objeto desta licitação e que atendemos todas as condições do Edital.

Data: .16./ 12./ .2003

Roberto Florentino da Silva Junior
Representante Legal

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1254
3740

2. Características Técnicas

2180

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1255
Doc: 3740

CORREIOS EMPRESA BRASILEIRA DE CORREIOS E TELÉGRAFOS

Especificação Técnica
Licenças de Software para Gerenciamento

	Características Mínimas
1. Descrição	Software HPOpenView Network Node Manager Enterprise v. 6.20 ou superior
2. Quantidade de Licenças	5 (cinco)
3. Garantia	- 12 (doze) meses a contar do Termo de Aceite Final -A garantia deve compreender a correção de falhas no produto, independentemente de correções tornadas públicas, desde que tenham sido detectadas e formalmente comunicadas à contratada. - Caso seja detectado bugs ou falhas no software, a empresa contratada deverá fornecer atualizações necessárias à correção do problema. Os produtos devem ser isentos de back doors. - A versão deve ser a última disponível no mercado na data de entrega do produto.
4. Compatibilidade	O produto deve ser compatível com o sistema operacional SUN SOLARIS e HP-UX.
5. Documentação Técnica	O produto deve ser entregue com documentação técnica do fabricante. Deverá ser fornecida documentação: – das parametrizações (customizações) realizadas nas ferramentas no processo de instalação e configuração; e – de instalação, configuração e operação.
6. Outros	O produto deve: – Ser fornecido em CD/ROM; – Ser fornecido, instalado, configurado e integrado às ferramentas HP OpenView NNM e VP/O já existentes no ambiente de gerência da ECT, mantendo a padronização existente; – A instalação compreende, dentre outros, a preparação dos servidores SUN e/ou HP, instalação e parametrização dos respectivos Sistemas Operacionais (Solaris e/ou HP UX). Os servidores e sistemas operacionais serão fornecidos pela ECT. – A instalação compreende, dentre outros, a implementação de alarmes definidos segundo padronização da ECT, integração com as consoles do HP-VP/O e descoberta (discovery) dos elementos a serem gerenciados.
7. Prazos	Entrega: até 10 (dez) dias, após a assinatura do contrato; Instalação e Configuração Final: até 40 (quarenta) dias após a Entrega; Termo de Aceite Final: até 5 (cinco) dias após a Instalação e Configuração Final; Pagamento: até 15 (quinze) dias após o Termo de Aceite Final.

RQS nº 03/2005 - CN - CPMI - CORREIOS
1
Fls. Nº 1256
3740
Doc:

Especificação Técnica
Licenças de Software para Gerenciamento

8. Atendimento e Suporte	- Deve ser fornecido a referência completa do canal de atendimento e suporte técnico do produto ofertado, com a nomeação e o telefone do(s) responsável(eis) técnicos que possa(m) responder questionamentos sobre todas as características do produto em pauta. - O atendimento e suporte ao produto deve compreender o acesso a help-desk para atendimento e abertura de chamados em língua portuguesa (durante horário comercial), incluindo o atendimento telefônico e o atendimento via e-mail. - Na descrição dos requisitos técnicos constantes de proposta referente ao produto devem ser apresentadas as demais modalidades de suporte técnico disponibilizadas, com detalhamento dos seus meios de acesso, quando existentes. -O atendimento a chamadas deve ocorrer, se necessário, nos dias úteis da semana no horário comercial, no esquema 8 x 5, até 4 (quatro) horas da abertura dos chamados por uma central de atendimento 0800 do fabricante. - O prazo de Atendimento e Suporte é de 12 (doze) meses a contar do Termo de Aceite Final.
9. Garantia Contratual	5% (cinco porcento) do valor global do contrato. Vigência: até o prazo final do Atendimento e Suporte.
10. Atualização	-A contratada deverá prover toda e qualquer atualização pertinente ao produto pelo período mínimo de um ano. -Em caso de upgrades, quando a aplicação da nova versão resultar em perda de dados, incapacidade de abertura ou gravação de arquivos ou qualquer outra incompatibilidade relativamente às versões anteriores, tais restrições deverão estar claramente relatadas na descrição dos requisitos de natureza técnica das propostas -Para fins desta especificação técnica, entende-se como atualização o provimento de toda e qualquer evolução do produto, incluindo: - patches, fixes, correções, updates e service packs; - novas releases, builds e funcionalidades; - o provimento de upgrades para novas versões de mercado ou lançamentos (tal como ocorre, por exemplo, na migração de *Produto* 6 para *Produto* 7 e similares); e, - o provimento de upgrades englobando, inclusive, versões não sucessivas, caso a disponibilização de tais versões ocorra durante o período da garantia (como exemplo, a migração de *Produto* 5 para *Produto* 7, 8 ou posterior). -A contratada deverá fornecer tais atualizações independentemente de solicitação expressa da contratante.

(X) Atende ( ) Não atende

RQS nº 03/2005 - CN - CPMI - CORREIOS
2
FLS. Nº 1257
3740
Doc:

3. Documentação

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1258
Doc: 3740

declaração

Hewlett Packard Brasil Ltda.
Alameda Rio Negro, 750 - Alphaville
06454-000 - Barueri - SP
CNPJ: 61.797.924/0001-55
Fone: (11) 4197 8000
Fax: (11) 4197 8432

www.hp.com.br

690469-BR

ANEXO 3

(MODELO VI)

DECLARAÇÃO DE SOLIDARIEDADE

EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS - ECT

SBN, Quadra 01 – Bloco "A" – 4º andar – Ala Norte – Ed. Sede/ECT – CEP 70002-900 – Brasília/DF

Fax.: 61. 426.2759

REF.: PREGÃO Nº 118/2003 – CPL/AC

Hewlett-Packard Brasil Ltda., CNPJ nº 61.797.924/0001-55, situada na Al. Rio Negro, 750 – Alphaville – Barueri/SP, na condição de fabricante, declara ser responsável solidária com a TM Solutions – Tecnologia de Informação Ltda, CNPJ 67.726.505/0001-09, situada à Rua Ceará, 193 – Alphaville – Barueri/SP, no atendimento ao Edital em epígrafe, no que diz respeito ao prazo de fornecimento, atendimento e suporte técnico e prestação de garantia, relativos aos produtos indicados em sua Proposta Econômica.

Barueri, 15 de dezembro de 2003.

Ieda T. Viana Batista
Representante Legal
Tel. 11.4197.8749
Hewlett Packard Brasil Ltda.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1259
3740
Doc:

690469-BR

DECLARAÇÃO DE ATENDIMENTO DE CERTIFICAÇÃO TÉCNICA

À

EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS - ECT

SBN, Quadra 01 – Bloco "A" – 4º andar – Ala Norte – Ed. Sede/ECT – CEP 70002-900 – Brasília/DF

Fax.: 61. 426.2759

REF.: PREGÃO Nº 118/2003 – CPL/AC

TM Solutions Tecnologia da Informação Ltda., CNPJ nº CNPJ nº 67.726.505/0001-09, por intermédio de seu representante legal o Sr. ROBERTO FLORENTINO DA SILVA JUNIOR,, portador da Carteira de Identidade nº 5.150.005-9 (SSP/PR) e do CPF nº 005.539.839-11, DECLARA, para os devidos fins que, possui Certificação Técnica para prestação de suporte, manutenção e garantia.

Barueri, 15 de dezembro de 2003.

Roberto Florentino da Silva Junior
Representante Legal
TM Solutions Tecnologia da Informação Ltda
CNPJ Nº 67.726.505/0001-09

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1260
3740
Doc:

ANEXO 6

TERMO DE GARANTIA TECNICA

Inicio de Vigência:

As empresas abaixo descritas, firmam entre si o presente Instrumento, doravante denominado simplesmente de TERMO DE GARANTIA TECNICA.

DESIGNAÇÃO DAS PARTES DORAVANTE NO TERMO	ECT	FORNECEDORA
Razão Social	EMPRESA BRASILEIRA DE CORREIOS E TELEGRAFOS	TM SOLUTIONS TECNOLOGIA DA INFORMAÇÃO LTDA
Endereço	SBN, Qd. 01 – Bloco "A" – 4º andar – Ala Norte – Ed.Sede/ECT	Rua Ceará, 193 – Alphaville – Barueri/SP
CEP	70002-900	06465-120
Cidade	Brasília	Barueri
Estado	DF	SP
CNPJ		67.726.505/0001-09
I.E.		206.073.934.112

1. **OBJETO**: Garantia Técnica do software HPOpen View Network Node Manager Enterprise v.6.20 ou superior, englobando o atendimento e suporte.
2. **PRAZO DE GARANTIA:** a partir da data de emissão do Termo de Aceite Final, encerrando-se 12 (doze) meses após a emissão deste Termo de aceite final.
3. RESPONSABILIDADE DA FORNECEDORA:

3.1 – Corrigir falhas no produto, independentemente de correções tornadas públicas, desde que tenham sido detectadas e formalmente comunicadas à FORNECEDORA.

3.2 – Fornecer atualizações necessárias à correção de problemas como bugs ou falhas no software. Os produtos devem ser isentos de back doors.

3.3 – entregar a última versão disponível no mercado na data de entrega do produto.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1261
3740
Doc:

3.4 – Comprometemo-nos a fornecer à ECT todas as atualizações de versões do software adquirido durante a vigência deste TERMO.

3.5 Forneceremos a referência completa do canal de atendimento e suporte técnico do produto ofertado, com a nomeação e o telefone dos responsáveis técnicos que possam responder questionamentos sobre todas as características do produto em pauta.

3.6 Prestar atendimento de suporte técnico a ECT, pelo período de 1(um) ano, visando sanar eventuais problemas, observando-se os seguintes prazos:
a) atendimento: no prazo de 04(quatro) horas corridas; e
b) solução do problema: 12(doze) horas corridas.

3.6.1. Define-se como tempo de atendimento o período compreendido entre o horário de comunicação do chamado feito pela ECT e o horário de chegada ao local de atendimento.

3.6.2. Define-se como tempo de solução do problema, o período compreendido entre o horário de comunicação do chamado feito pela ECT e o horário de término da solução, deixando o software em condições normais de operação.

3.7. o atendimento e suporte ao produto devem compreender o acesso a help-desk para atendimento e abertura de chamados em língua portuguesa(durante horário comercial), incluindo o atendimento telefônico e o atendimento via e-mail.

3.8 – Na descrição dos requisitos técnicos constantes da proposta referente ao produto serão apresentadas as demais modalidades de suporte técnico disponibilizadas, com detalhamento dos seus meios de acesso, quando existentes.

3.9. o atendimento a chamados deve ocorrer, se necessário, nos dias úteis da semana no horário comercial, no esquema 8 x 5, até (quatro) horas da abertura dos chamados por uma central de atendimento nº 0800.130999.

3.10. o prazo de atendimento e suporte é de 12(doze) meses a contar da data de emissão do termo de aceite final – TAF, pela ECT.

3.11. a TM SOLUTIONS proverá toda e qualquer atualização pertinente ao produto pelo período mínimo de um ano.

3.12. em caso de upgrades, quando a aplicação da nova versão resultar em perda de dados, incapacidade de abertura ou gravação de arquivos ou qualquer outra incompatibilidade relativamente às versões anteriores, tais restrições estarão claramente relatadas na descrição dos requisitos de natureza técnica das palavras.

CORREIOS
Fls. Nº 1262
3740
Doc:

3.13. – Para fins da especificação técnica constante neste contrato, entende-se como atualização o provimento de toda e qualquer evolução do produto, incluindo:

- patches, fixes, correções, updates e serviços packs
- novas releases, builds e funcionalidades;
- o provimento de upgrades para novas versões de mercado ou lançamentos (tal como ocorre, por exemplo, na migração de produto 6 para Produto 7 e similares); e
- o provimento de upgrades englobando, inclusive, versões não sucessivas, caso a disponibilização de tais versões ocorra durante o período da garantia(como exemplo, a migração de Produto 5 para Produto 7, 8 ou posterior).

3.14. A TM SOLUTIONS fornecerá tais atualizações independentemente de solicitação expressa da ECT.

4. – DAS PENALIDADES:

4.1. 0 não atendimento do suporte técnico e solução de problemas à ECT, dentro dos prazos estabelecidos no subitem 3.4. deste Termo: 1% (um por cento) sobre o valor unitário da ferramenta, cujo atendimento foi reclamado, por hora de atraso.

4.2. – o não atendimento de qualquer item descrito neste Termo de Garantia Técnica : 1% (um por cento) sobre o valor unitário da ferramenta.

Barueri, 15 de dezembro de 2003.

CONTRATADA:

Representante Legal.: Roberto F. da Silva Junior

Testemunha:

CONTRATANTE:

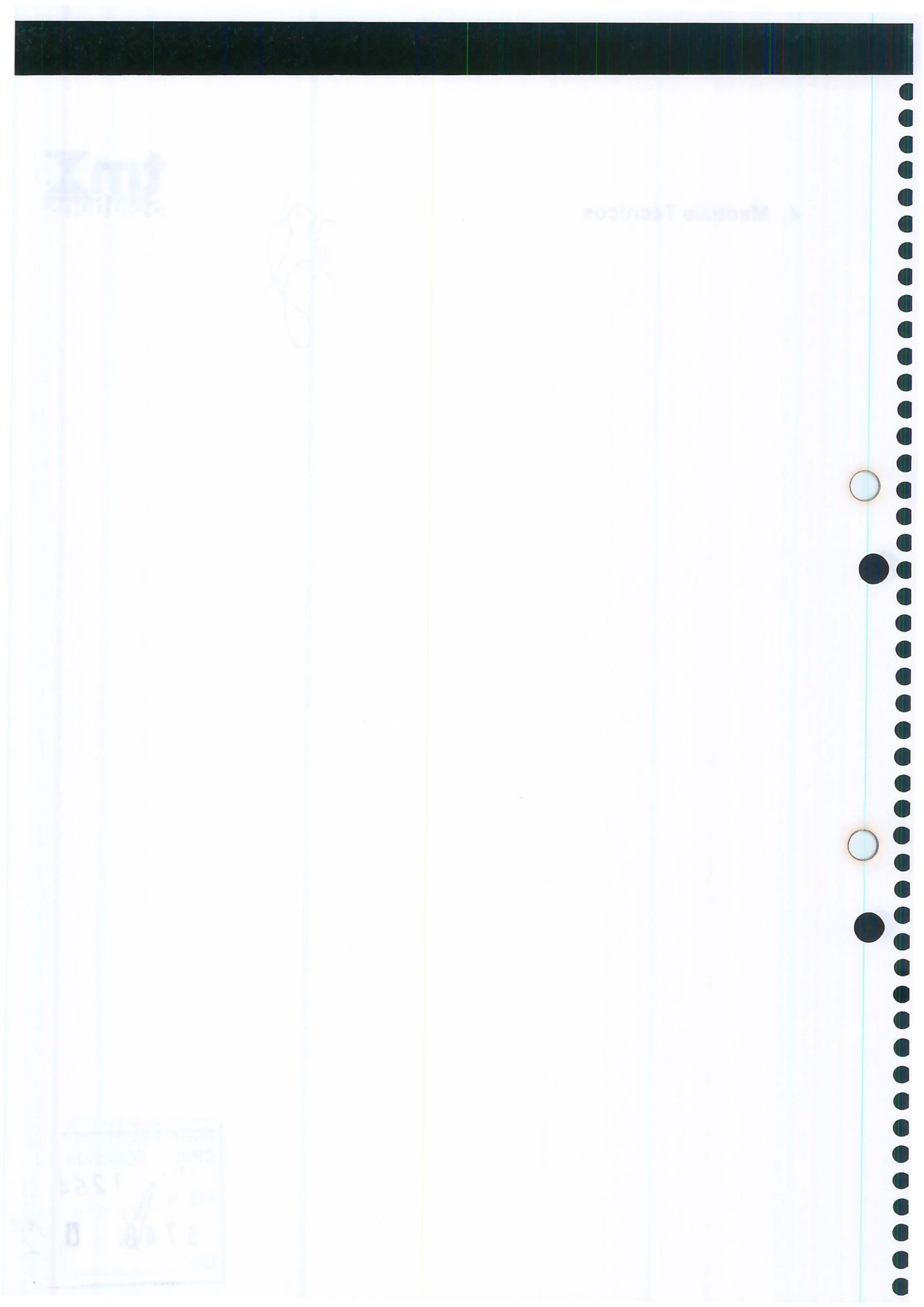
Representante Legal

Testemunha:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1263
3740
Doc:

4. Manuais Técnicos

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1264
3740
Doc:



2170

HP OpenView Network Node Manager

A Guide to Scalability and Distribution

HP-UX, Solaris, and Windows operating systems



Manufacturing Part Number: J5323-90001

January, 2003

© Copyright 2003 Hewlett-Packard Company.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1265
3740
Doc:

Manual - I

Legal Notices

Warranty.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices.

©Copyright 1983-2003 Hewlett-Packard Company.

No part of this document may be copied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

Contains software from AirMedia, Inc.

© Copyright 1996 AirMedia, Inc.

Trademark Notices

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

Windows® and MS Windows® are U.S. registered trademarks of Microsoft Corporation.

2167

Windows® 2000 is a U.S. registered trademark of Microsoft Corporation.

Windows NT® is a U.S. registered trademark of Microsoft Corporation.

Netscape and Netscape Navigator are U.S. trademarks of Netscape Communications Corporation

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

Oracle7TM is a trademark of Oracle Corporation, Redwood City, California.

OSF/Motif® and Open Software Foundation® are trademarks of the Open Software Foundation, Inc. in the U.S. and other countries.

Pentium® is a U.S. registered trademark of Intel Corporation.

UNIX® is a registered trademark of The Open Group.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1266
3740
Doc:

2166

2165

Support

1. Overview of Scalability and Distribution in NNM

Scalability and Distribution in NNM 15
Benefits of Scalability 15
What Makes NNM a Scalable Solution for Network Management? 16
Network, System, and Operator Efficiency via Filtering 19
Distributed Internet Discovery and Monitoring 20
Capacity Planning 21
About Management Stations and Collection Stations 22
Management Consoles 24
On-Demand Submaps 26
Distributed Threshold Monitoring and Event Forwarding 27
General Events 27
Threshold Events 28
Trend Data Collection in a Distributed NNM Solution 28
Large-Map Viewing Support 29
The Panner 30
The Quick Navigator 30

2. The Scalable Architecture of Network Node Manager

The Distribution Model for Network Node Manager 33
Network Connections between Distributed Components 36
Filters 37
Discovery Filtering 40
Topology Filtering 41
Map Filtering 42
Defining New Filters 43
Filter Utilities 45
Distributed Internet Discovery and Monitoring 46
About Collection Domains 46
Distributed Services Architecture 48
High Availability Management Information 50
Overlapping Collection Domains 52
Configuration Concepts 56
Distributed Threshold Monitoring and Event Forwarding 59

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 126797
3740
Doc:

Event Correlation for "Connector Down" 60
Data Collection for Distributed Threshold Monitoring 62
On-Demand Submaps 64
Transient Submaps and the Submap List Dialog 67
Persistence Filtering 68
Comparing Map Filters and Persistence Filters 69
Management Consoles 70
Management Consoles and On-Demand Submaps 72
Customized Views of the Network 72
Management Consoles and X-Terminals 73
Interface Managed-state Automation 74
Microsoft Terminal Server Access 75
Accessing a Single NNM Station From Multiple Terminal Server Clients 75
Accessing Multiple NNM Stations From a Single Terminal Server Client 77
Accessing Multiple NNM Stations From Multiple Terminal Server Clients 78

3. Strategies for Deploying Network Node Manager

Planning the Right Approach 83
General Considerations about Scalability and Distribution 84
General Strategies for Deployment 87
Deployment Strategies for NNM 89
Use of Scalability Features in NNM Deployment 89
Fully Centralized Management 92
Implementation Tactics 93
Implications of Using the Fully Centralized Management Model 94
Centralized-Hierarchical Management 95
Implementation Tactics 96
Implications of Using Centralized-Hierarchical Management 97
Hierarchical Management 98
Implementation Tactics 100
Implications of Using the Hierarchical Management Model 101
Cooperative Independent Management 103
Implementation Tactics 104
Implications of Using the Cooperative Independent Model 105

4. Procedures for Scaling NNM

Configuring Management Consoles 109
Configuring a Windows System Console Server 111
Installing a Management Console on Windows for an NNM Server on Windows . 111
UNIX System Server Configuration 112
Installing Management Consoles on Windows for UNIX System Management Servers 115
UNIX System Console Configuration 117
Increasing Security for Management Consoles 119
Undoing a Management Console 120
Configuring On-Demand Submaps 121
Configuring Demand Level 121
Specifying a Persistence Filter 124
Integrating Applications With On-Demand Submaps 125
Configuring a Map Filter 127
Configuring Data Collection for a Station 128
Configuring a Discovery Filter 128
Managing and Unmanaging Locally Monitored Objects 132
Configuring Collection Stations 133
Configuring Security for a Collection Station 133
Configuring a Topology Filter for a Collection Station 134
Changing the Topology Filter for a Collection Station 135
Configuring IPX on a Collection Station under Windows 136
Configuring Management Stations 137
Determining if a Node is a Collection Station 137
Determining All Objects Monitored by a Collection Station 138
Configuring for a Specific Collection Station 138
Unmanaging a Collection Station 140
Removing a Collection Station from a Management Station 141
Configuring a Remote Communication Timeout and Retry Count 141
Performing a Full Topology Synchronization 144
Identifying Collection Station Communication Problems 145
Troubleshooting Collection Station Communication 147
Configuring Domain Overlaps and Failover 150
Determining the Primary Collection Station for an Object 150
Changing the Primary Collection Station for an Object 151
Changing the Overlap Mode 152

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1268
3740
Doc:

Collection Station Failover 153
Configuring Event Forwarding and Correlation 154
Forwarding an Event 154
Using Distributed Data Collection 159

5. Dynamic Views and Distributed Management

Dynamic Views and Distributed Management 163
NNM Neighbor View 164
NNM Path View 165

A. The Filter Definition Language

The Filter Definition File 169
Filters and Filter-Expressions 170
Sets 171
Attribute Value Assertions 172
Valid Operators for AVAs 173
Boolean AVAs 174
Integer AVAs 175
Enumerated (Enum) AVAs 175
String AVAs 175
Excluding a Node 180
Relationships Between Nodes and Interfaces 180
Valid Operators for Logical Combinations of AVAs or Filters 180
Filterable Objects and Attributes 181
Filter File Grammar 187
Filter File Example 189
Setting Up Collection Domains 190
Excluding Nodes 192
Failover Filters 193
Important Node Filters 193
Topology Filters 194
Map Filters 195
Using the Network Presenter 195
Default Filter File 197

B. Using NNM Under a Mixed Codeset Environment

2161

Glossary **209**

Index **213**

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1269
Doc 3740

Support

Please visit the HP OpenView web site at:

`http://openview.hp.com/`

There you will find contact information and details about the products, services, and support that HP OpenView offers.

The support area of the HP OpenView web site includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1270
3740
Doc:

1 Overview of Scalability and Distribution in NNM

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1271
3740
Doc.

Scalability and Distribution in NNM

You can configure NNM to perform well for a wide range of network sizes and degrees of complexity. This attribute is commonly referred to as the **scalability** of NNM. Scalability gives NNM the potential to handle almost any size network, in both local and wide-area environments.

One approach to making a product like NNM scalable, and an important feature of NNM, is to distribute the network management workload to multiple, usually remote, systems. NNM makes **distribution** possible, so you can monitor and manage much larger networks while minimizing the management resources required.

In summary, the scalability and distribution of NNM optimizes the use of two key resources:

- First, NNM includes features that help you use the *system resources* at the management station very efficiently.
- Second, other features of NNM, especially distribution, reduce the amount of management traffic over your *network*, most importantly, over congested or expensive links.

Benefits of Scalability

Having a scalable network management platform, implemented in part through distribution, provides you with many benefits in your application of NNM as a network management solution.

First, scalability gives your network management solution the ability to evolve with your organization. Networks are dynamic entities that reflect the changing structures and needs of the organizations they serve. As your network changes and grows, the scalable features of NNM make it easier to adapt your network management to handle new networking landscapes.

Second, a distributed network management solution can dramatically reduce the traffic overhead that network management can impose on congested or expensive network links. Most large (enterprise) networks include serial or wide-area (WAN) links. Such links are both relatively slow and expensive. Without a distributed network management solution, it is simply impractical to monitor tens of thousands of nodes from a single workstation; the networking load emanating from the

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 272
3740

management station becomes a bottle neck. Distribution minimizes the amount of network management traffic on these links, freeing bandwidth for business purposes.

Third, a distributed solution makes it possible to share network management responsibility and resource requirements among multiple sites. By spreading the resources and responsibilities out, you reduce the risk of losing all network management in the event of an unexpected shutdown of your management station. Distribution also makes it easier to perform maintenance shutdowns without losing your overall network management.

Fourth, a scalable network management solution, sensibly deployed and properly configured, results in faster response times and better performance. You spend less time waiting for data and more time acting on it. Furthermore, it improves network reliability by allowing local management actions even when contact is lost with a remote central management site.

Finally, deploying a scalable network management platform means everyone in your organization can share a single customizable tool. This naturally leads to a common vocabulary, common experiences, sharable expertise, and the ability to more easily articulate and implement standard processes and procedures in your organization.

All together, NNM's scalability and distribution gives you the power to manage the large and geographically dispersed enterprise networks that are critical to key business or organizational processes. You can use common applications at every level to create a more integrated, consistent solution to the complex problems in these environments.

What Makes NNM a Scalable Solution for Network Management?

The idea of "scalability" is abstract, but HP OpenView Network Node Manager has several broad categories of features that make scalability a concrete reality.

Distributed Internet Discovery and Monitoring

Distributed Internet Discovery and Monitoring lets remote collection stations monitor their part of the network and inform the central management station about it. This reduces network traffic, and also reduces the load on the central station.

Management Consoles

Management consoles off-load display processing from the management station to a display station. With management consoles, you can have more operators monitoring and managing your network without loss of performance; these operators can handle larger environments.

Web Browser Interface

Accessing network management functions from your web browser lets you monitor your network from any location with a web browser installed, even if it is not a management console. See *Managing Your Network with HP OpenView Network Node Manager* for more information.

Large-Map Viewing Support

NNM gives you two essential features for examining large maps:

- The panner, which makes it easy to navigate submaps with hundreds of symbols.
- The quick navigator, which gives you instant access to your most critical or frequently visited submaps.

On-Demand Submaps

The on-demand submap feature provides a very significant boost in the performance of NNM, allowing it to manage many more objects (up to ten times) than with persistent submaps. Enabling the on-demand submap feature lets your management station use less memory to perform the same tasks.

Filtering

Filters let you reduce the amount of extraneous data being handled by the system, or presented to the operator. This provides improved performance, and reduces visual clutter for the operator.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1273
3740
Doc:

Event Forwarding

You can configure your remote stations so that events from managed nodes, or from non-NNM applications on the collection station, get forwarded to interested management stations. This can be set up to occur whether or not the event triggers local actions, or has already been correlated.

Important events generated internally to NNM, such as topology or status change events, are automatically forwarded from a collection station to the interested management stations, without additional configuration steps.

Distributed Threshold Monitoring

Distributed threshold monitoring reduces management traffic on the network by allowing remote stations, instead of the management station, to collect SNMP trend data and trigger threshold events based on that data.

Interface Managed-state Automation

NNM lets you automatically manage or unmanage interfaces based on filters. Interface managed-state automation makes it easier to manage large environments, where frequently many discovered interfaces do not require active status polling.

High Availability and Fault Tolerance

NNM stations can be run on HP Service Guard clusters to provide continuous availability. Also, if a collection station fails, you can configure its status polling duties to transfer over to a management station. You can also perform backup of your network management data without losing incoming information during that time.

Your practical limits in using all the above depend on the size of your network environment, your management strategy, and the resources available on the management and collection stations. For the most current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide*, available at `http://openview.hp.com/`.

NOTE The upper limits of operators and managed devices depends very heavily on the level of monitoring and data collection you require. In general, increasing the polling intervals on noncritical nodes increases the number of nodes that can be handled.

Network, System, and Operator Efficiency via Filtering

For NNM to manage very large environments, all resources (network, system, and human) must be used as efficiently as possible. To maximize the efficient use of these resources, NNM employs a strategy of data reduction via filters.

A **filter** is essentially just a way to remove unneeded data from consideration for further processing. The result of less data in the system is higher performance for NNM, and improved usability for the operators.

For example, you may have an operator whose only concern is the routers and hubs in your environment. For that operator, any other objects on his map are merely clutter. With NNM, you can apply a filter to the map, so that only routers and hubs appear.

See "Filters" on page 37 for more details about filtering in NNM.

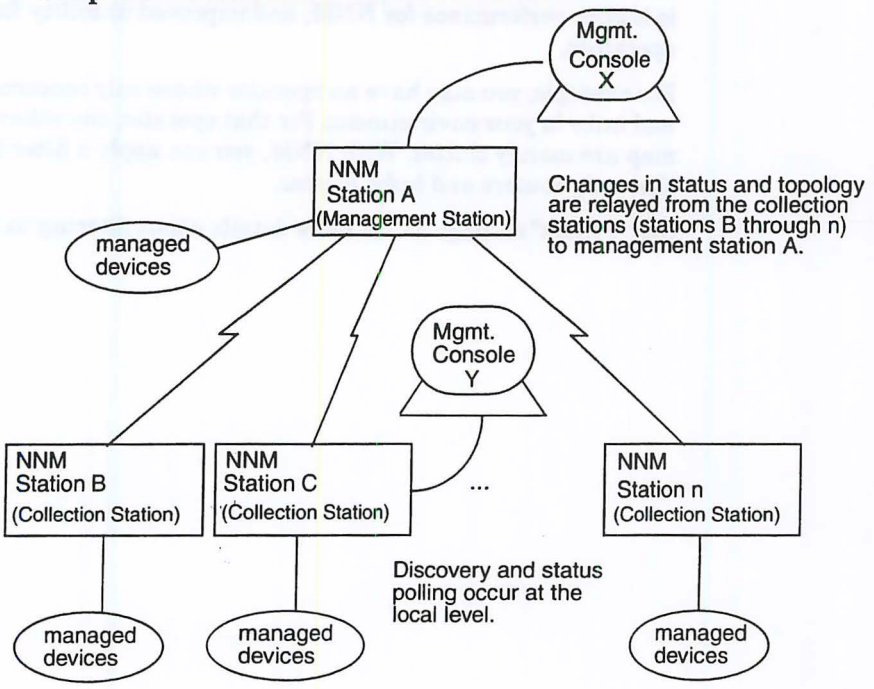
RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1274
Doc: 3740

Distributed Internet Discovery and Monitoring

A network management system can consume significant resources while performing discovery, topology monitoring, and status polling. One feature of HP OpenView Network Node Manager is the ability to move much of this load from the management station to one or more remote machines.

This capability is called **Distributed Internet Discovery and Monitoring**, and is illustrated in Figure 1-1. The device count for this model assumes one interface per device, on average. Note that the management console at Station C indicates that it also serves as a management station for the objects it monitors; this is the usual configuration of NNM.

Figure 1-1 Simplified Distribution Model for NNM



To use distributed internet discovery and monitoring, you designate one or more remote machines as **collection station**s. Each collection station takes over the task of monitoring some portion of the network, while informing all interested management stations of any changes in the status or topology of the network it monitors.

Capacity Planning

Because distributed management partitions the work of discovery and status polling, it also dramatically reduces traffic on the network, most importantly on expensive or congested links.

When considering performance and configuration issues, you must distinguish between nodes and objects. There is a one to many relationship between the number of nodes and the number of objects in the object database. Even though a network model is typically described in terms of the number of nodes the application manages, it is the number and type of managed objects that is the most important parameter when predicting how the application will scale and perform.

Determining the exact number of managed objects is especially critical when predicting, for example, the size of a database, the load on `netmon`'s polling cycle, or the load imposed on a management station when synchronizing with a collection station. You'll want to determine the appropriate node to object multiplier for your environment.

Not all network environments conform to the typical environment described above. In some environments, the ratio of objects to nodes is higher because enterprise routers tend to have more than two physical interfaces. For example a network center responsible for monitoring only backbone routers would have a higher ratio. In some cases nodes may have additional virtual interfaces. Secondary addresses, for example, increase the number of objects associated with that particular managed node.

There is no concrete limit to the number of objects or devices you can manage, or to the management stations you can deploy. Your practical limits depend on the size of your network environment, your management strategy, and the resources available on the management and collection stations. For the most current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide*, available at `http://openview.hp.com/`.

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls Nº 1275
3740
Doc:

About Management Stations and Collection Stations

In the previous section (including Figure 1-1), two terms were introduced:

- Management station
- Collection station

It is important to recognize that these labels state the *roles* of the machines involved, and do not refer to different software on them. In this vein, you should note that a single NNM station can perform either role, or both at once. Regardless of the role it is playing (as a collection or management station, or both), every NNM station has the full capabilities of NNM[1]. HP Service Guard clusters for UNIX systems may be used for any type of management station to ensure constant availability.

The role of a management station is to make the network management functionality available to users, either directly or via one or more management consoles.[2]

The role of a collection station is to be a collection point in the overall network management system. A collection station typically performs topology and IP status monitoring, threshold data collection, local event correlation, and event forwarding or handling on behalf of one or more management stations.

When changes occur in topology or status, or when a configured threshold is crossed, the necessary information is forwarded from the collection station to any interested management stations, so that the end-user at a management console is informed. The set of objects for which topology and status information is forwarded can be controlled via filtering.[3]

---

1. Only NNM Enterprise nodes (unlimited license) can receive information from collection stations.
2. See "Management Consoles" on page 24.
3. See "Use of Scalability Features in NNM Deployment" on page 89 for introductory information, and "Filters" on page 37 for more details about filtering.

Management and collection stations alike have all components of the HP OpenView NNM software running on them. The only difference is that a collection station has been designated and configured to serve one role, and a management station has been designated and configured to serve another.

Stated another way, every NNM station (regardless of operating system or license limit) is inherently a management station, but it must be configured to use the management resources of a remote collection station. Likewise, every NNM station is *also* inherently a collection station, but it must be configured to provide its data to a remote management station.

In Network Node Manager, a computer acting as a collection station is generally also a management station in its own right, with local users performing network monitoring and management, either independently or in cooperation with the users at a remote management station.

This is illustrated in Figure 1-1. In that illustration, the operator at Management Console Y can see only the nodes directly managed by NNM Station C. On the other hand, the operator at Management Console X can (depending on how the collection stations are configured) see all the objects in the entire scope of management for NNM Station A.

NNM Station View

The NNM Station view is useful in a distributed management environment. It shows you a graphical representation of the collection stations and management stations in your topology. You can use this view to troubleshoot communications between collection stations and management stations. See "Identifying Collection Station Communication Problems" on page 145 for detailed information.

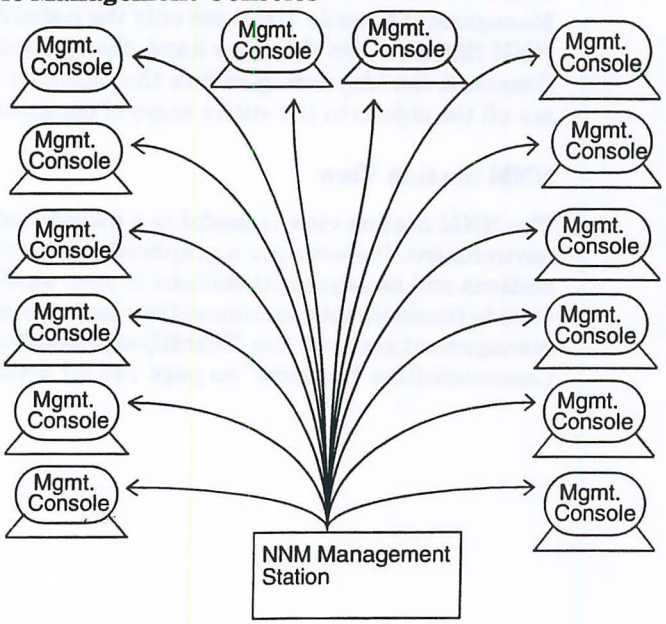
RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1276
3740
Doc:

Management Consoles

One of the main problems associated with managing large networks is providing access to enough operators to handle all the objects in the map.

With HP OpenView Network Node Manager, you can have many operators simultaneously monitoring your network, as shown in Figure 1-2, operating from the same topology database and sharing common discovery and monitoring processes at the management station. Operators can share one map, or have individual maps. The limit on how many again depends on the size of your environment and the resources available to the management solution. For the most current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide*, available at `http://openview.hp.com/`.

Figure 1-2 Multiple Management Consoles



Consoles run on UNIX[4] or Windows[5] operating systems work with management stations on a UNIX system. These management consoles communicate with the UNIX system management station via NFS and socket connections on a LAN link. Management stations on the Windows operating system only support consoles run on Windows, not consoles run on UNIX. This is because a management station on a Windows operating system uses Windows file sharing, not NFS.

Web browsers using Network Presenter may reside on any system, including the same system as a management console. However, the web server must reside on a full management station, not a console.

4. In this manual, the term UNIX, when used without other qualifications, refers to the supported UNIX operating systems, as described in the Release Notes.
5. in this manual, the term Windows, when used without other qualifications, refers to the supported Windows operating systems, as described in the Release Notes.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1277
3740
Doc:

On-Demand Submaps

One of the potential problems with having maps that contain thousands of nodes involves the use of available memory.

The `ipmap` application[6] typically creates a hierarchy of several levels of submaps (root, Internet, segment, node). An interesting and important point is that many of these submaps are rarely, if ever, visited by an operator.

Imagine if NNM kept every submap in the map in memory at all times. In a large map, with literally thousands of submaps, this approach would create a substantial requirement for memory.

However, NNM makes it possible to specify that only *some* of the submaps be kept persistently in memory; any *other* submap is created if and only if a user requests it. This means that for a management station with a given amount of memory, you can manage maps with many more submaps containing many more objects.

The main benefit of the on-demand submap feature is a dramatic improvement in performance, especially during synchronization. Meanwhile, the features and functionality of NNM are essentially identical whether or not on-demand submaps are enabled. Whenever you double-click on an explodable object in `ipmap`, the submap opens promptly (though submaps with many objects may take several seconds to open). Furthermore, all features of NNM, including "find" and IP status propagation, work as usual.

Some applications that were created before this feature was part of NNM may not be compatible with the on-demand submap feature. They may expect certain objects to be available in memory at all times. In this case, you can use **persistence filtering** to make those objects persistent.[7] Persistence filtering provides per-object exceptions to the on-demand feature, so that certain objects and their submaps are always present in memory even if on-demand submaps are enabled.

6. See *Managing Your Network with HP OpenView Network Node Manager* for information about this and other key NNM processes.
7. See "Persistence Filtering" on page 68 for details.

Distributed Threshold Monitoring and Event Forwarding

In an NNM distributed environment, it is necessary that operators at the management console be aware of critical events wherever they occur. This is commonly called "management by exception." For this reason, NNM has the ability to forward events, typically from collection stations to management stations.

Using the graphical `Event Configuration` window, you can configure any event, on a case-by-case basis, to be forwarded to any or all of the following:

- All managers currently using the NNM station as a collection station.
- Particular hosts, identified by hostname or IP address.
- Hosts listed (by hostname or IP address) in a specific file.

All configurable events, including threshold events, can be configured for forwarding. Internal NNM events are automatically forwarded to management stations as needed.

When defining new events, we recommend that you use multiple varbinds with individual pieces of data rather than using a full string. This allows the receiving machine to specify the formatting. Refer to the reference page in NNM online help (or the UNIX system manpage) for *trapd.conf* more information.

General Events

You can forward any or all events from collection stations to management stations. This is most useful when a collection station receives little or no local attention, or when you have applications that issue events which you want to have forwarded to the management station.

For example, suppose you have a collection station that monitors an agent that generates an event called `FuseIsLit`. At the collection station, you can configure that event to be forwarded to the management station, and thereby alert the operator that the device is not functioning properly.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1278
Doc 3740

Threshold Events

Threshold events give you a way to be notified of traffic patterns that are outside normal expectations. For example, you could set a threshold to monitor disk utilization on a server. If the amount of free disk falls below the threshold you set, NNM can notify an operator, or take other predetermined actions (such as mailing a message). Threshold events help operators detect and isolate problems as they arise, before users experience difficulty.

In the context of a distributed network management solution, the ability to forward threshold events means that the management station does not itself have to perform data-collection on all the objects that need thresholds monitored. That effort, and the associated network traffic, is delegated to the various collection stations that the manager uses.

Trend Data Collection in a Distributed NNM Solution

Some users may be interested in having trend data collected at remote locations and forwarded back to a central point, such as an NNM management station, for trend analysis.

Distributed data collection doesn't reduce the load on a management station if the data is sent back to the management station in real time. Therefore, in NNM the remote station stores any trend data in its own database. Data can then be transferred to a relational database if that is available.[8]

NNM does not provide a way to automatically synchronize data back to the management station. It does, however, offer some basic tools that you can use to create custom solutions. For example, you can transfer NNM's data files from the collection stations to the management station (via FTP or a similar utility) during off-peak periods. Then you can use NNM's data-merging tool (see the *ovcoltosql* reference page in NNM online help (or the UNIX system manpage)) to merge the data into an SQL database. Then you can use database tools to create reports on the data.

8. See *Reporting and Data Analysis with HP OpenView Network Node Manager* for information on supported database.

Large-Map Viewing Support

When a submap contains hundreds of nodes, the symbols and connections get smaller, and it becomes difficult to make sense of the graphical picture. Also, changes in status are not as noticeable.

HP OpenView Network Node Manager has two features that make it easy to use maps that contain hundreds, even thousands, of nodes:

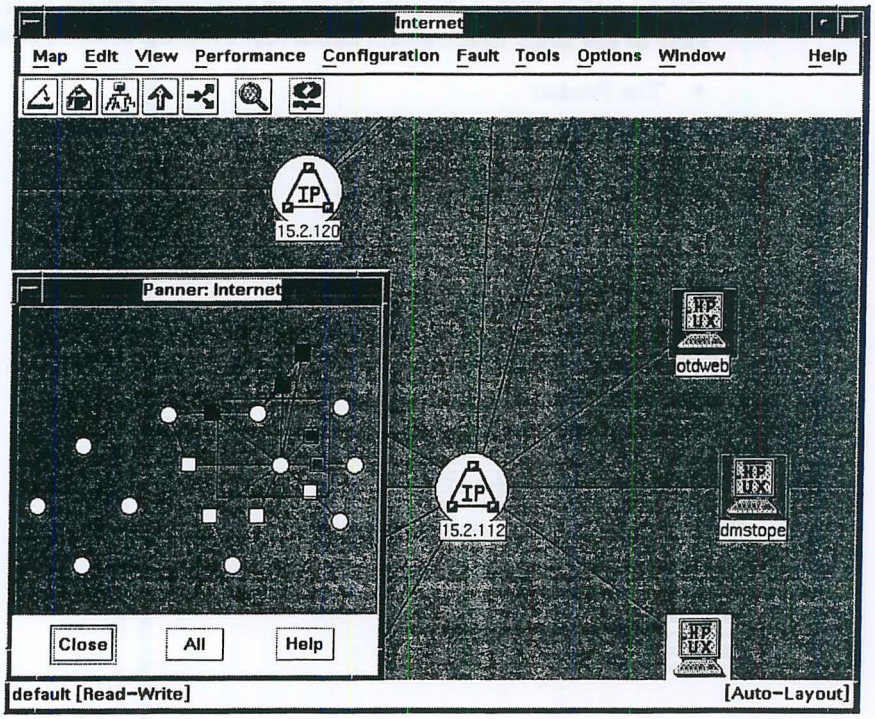
- The Panner
- The Quick Navigator

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº
1279
Doc: 3740

The Panner

The panner, shown in Figure 1-3, provides a way to zoom in on regions of a submap, and drag the zoomed region around. See *Managing Your Network with HP OpenView Network Node Manager*, or NNM's online help, for details.

Figure 1-3 The Panner



The Quick Navigator

The Quick Navigator is a special window that you can customize easily for quick access to your most frequently visited submaps. Your tool bar has a Quick Navigator button, which is described in the online help.

Each operator can customize their own Quick Navigator window by following the simple directions in the online help.

2 The Scalable Architecture of Network Node Manager

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1280
3740
Doc:

This chapter contains more detailed information about the distribution and scalability features of HP OpenView Network Node Manager (NNM). It includes diagrams and descriptions of the major elements of the distributed, scalable NNM architecture, and shows how data moves through the system.

NOTE

The information in this chapter is not introductory; readers are assumed to have read the previous chapter. Readers are also assumed to be conversant with NNM's key features for network monitoring, data collection, event handling, and so on. This includes a functional understanding of some key services (background processes on UNIX systems) in non-distributed NNM, including `ovw`, `ipmap`, `snmpCollect`, `ovtopmd`, and `netmon`. See *Managing Your Network with HP OpenView Network Node Manager* for details about the key services in Network Node Manager.

Later chapters contain guidelines on how to deploy NNM effectively in your organization, and specific configuration procedures to use with the scaling and distribution features of NNM.

The Distribution Model for Network Node Manager

Figure 2-1 illustrates the key components of the distribution scheme implemented by NNM. This diagram is fairly complex, and much of the remainder of this chapter is devoted to explaining many of the concepts it illustrates.

The diagram shows several components that can, and often do, run on different systems. These include full NNM management stations, NNM 250 management stations, NNM stations in the role of collection stations, and management consoles. These components can be run in any combination of supported operating systems (except for management consoles: Windows operating system servers can only serve Windows operating system clients).

NOTE The Windows operating system workstation provides status and topology information on IP and IPX devices. The IPX information exported by the Windows operating system collection station is passed to the UNIX system management station, thus providing a graphical representation of the IPX network topology and status of the individual devices.

In Figure 2-1, stations with no local management console are labeled as collection stations; stations that do have a local management console are labeled as management stations.

NOTE The labelling of management and collection stations in Figure 2-1 is for illustrative purposes only; most (if not all) collection stations also serve as management stations. See "About Management Stations and Collection Stations" on page 22.

Again, whether a particular system is a management station or collection station may be a matter of whose point of view one has at the moment. From the point of view of an operator at Management Console

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1281
3740
Doc:

1, it appears that NNM Station C is a collection station (just like NNM Station D). But from the point of view of an operator at Management Console 4, NNM Station C is the management station he is using.

Each management station can support approximately 15 management consoles via a LAN connection. The management consoles run the per-operator services, freeing up resources on the management station. A later section of this chapter covers this in more detail.[1] As shown in Figure 2-1 at NNM station A, it is still possible to run the per-operator services on the management station, routing the display to an X terminal, or, for NNM on a Windows operating system, a Windows operating system console connected to a Windows operating system collection station.[2]

The number of devices that a full NNM management station can manage in a distributed configuration varies with several different factors:

- The management station's resources (CPU, memory, and disk storage)
- Network performance
- Status and discovery polling intervals
- The level of data collection and threshold monitoring you have configured
- The number of collection stations being managed
- The number of nodes being managed by each collection station

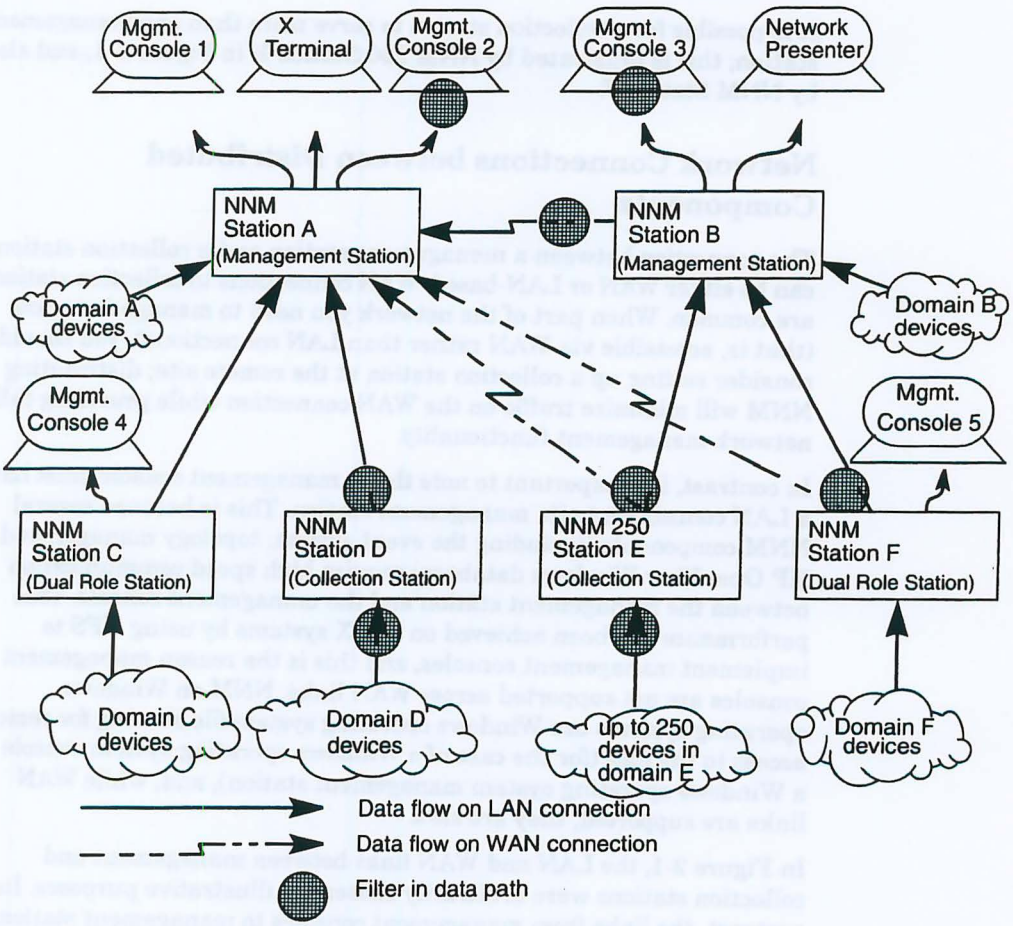
For more information on selecting and sizing the correct computer system for your NNM management station, see the latest version of the *NNM Performance and Configuration Guide*.

To attain your desired IP monitoring response times, you need to maximize the management station resources and set polling intervals to the maximums you can tolerate.

The only differences between a full NNM management station and an NNM 250 management station are that the NNM 250 management stations can manage only up to 250 nodes per license and cannot manage collection stations.

1. See "Management Consoles" on page 70
2. See also "Management Consoles and X-Terminals" on page 73

Figure 2-1 The Distribution Model for Network Node Manager



With NNM, it is also possible to obtain management information from one or more NNM stations acting as collection stations. In Figure 2-1, most of the NNM stations (Stations B, C, D, E, and F) are operating in the role of collection stations.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1282
3740
Doc:

Stations C and F illustrate how an NNM station can have the role of a management station (possibly making use of collection stations), a collection station (serving one or more management stations), or both roles at once.[3]

It is possible for a collection station to serve more than one management station; this is illustrated by NNM 250 Station E in Figure 2-1, and also by NNM Station F.

Network Connections between Distributed Components

The connection between a management station and a collection station can be either WAN or LAN-based. WAN connections to collection stations are common. When part of the network you need to manage is remote (that is, accessible via WAN rather than LAN connections), you should consider setting up a collection station at the remote site; distributing NNM will minimize traffic on the WAN connection while providing full network management functionality.

In contrast, it is important to note that a management console must have a LAN connection to its management station. This is because several NNM components (including the event system, topology manager, and HP OpenView Windows database) require high speed communication between the management station and the management console. This performance has been achieved on UNIX systems by using NFS to implement management consoles, and this is the reason management consoles are not supported across WAN links. NNM on Windows operating systems use Windows operating system file sharing for remote access to the files (for the case of a Windows operating system console to a Windows operating system management station), and, while WAN links are supported, they are slow.

In Figure 2-1, the LAN and WAN links between management and collection stations were arbitrarily chosen for illustrative purposes. In contrast, the links from management consoles to management stations are necessarily LAN connections.

3. See "About Management Stations and Collection Stations" on page 22.

Filters

The function of most filters is to select network management data that is of sufficient value to be kept, and to eliminate other data.[4] Data that is useful at one point (say, a site management station) can be filtered out before it gets sent to another (say, regional management station) where it is unneeded.

NNM uses two basic types of filters:

- A **data-stream filter** acts as a sieve through which objects flow. This type of filter contains criteria that permit some objects to proceed, and blocks other objects. Downstream from a data-stream filter, the data stream includes only those objects that the filter passed; other objects are blocked, and thus eliminated from the data at the point of the filter.

  Note that once an object has passed a data-stream filter, later changes to the filter have no effect on it. It remains in the data stream.

- A **set-defining filter** is applied to a pool of candidate objects, and determines which objects belong in the final set based on the criteria contained in the filter. Before a new object can be added to the set, it is tested by the set-defining filter to determine if it is a valid member or not.

  If a set-defining filter is changed, all candidate objects are reevaluated to determine which ones belong in the new set and which do not. Then the set is reconstituted out of valid members.

The difference may seem abstract at first. As an analogy, you can compare a data-stream filter to a wire-mesh sieve, of the kind used to sort stones. Once a large stone has passed through the sieve, it is in the sorted pile beneath regardless of whether you later switch to a finer mesh in the sieve.

Imagine, on the other hand, that your sieve behaved like a set-defining filter. In that case, changing to a finer mesh in the sieve would cause all the source material to be refiltered, yielding a sorted pile of uniformly smaller stones.

4. See "Persistence Filtering" on page 68 for an important exception.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1283
3740
Doc:

In either case, remember that a filter specifies or describes the objects you want it to pass, *not* the objects you want it to reject. When the filter is applied, it passes the selected objects through, eliminating the rest from the data stream. As a user, you can apply filters only to object data; however, applications can filter events also.[5]

Filtering is based on the information contained in a subset of the fields of the object database (ovwdb).[6] These fields are candidates to be all or part of the criteria by which objects are assessed in a filter.

Filters can eliminate unnecessary data at different points in the system:

- Discovery filtering at any NNM station.
- Exported topology filtering at the collection station.
- Map filtering at the management station.
- Failover filtering on the management station.

Table 2-1, Comparing Types of Filters, compares the types of filters. See "Filter File Example" on page 189 for more information.

Table 2-1 Comparing Types of Filters

Filter Type	Apply on Incoming Data	Reevaluate If Filter Changes	Purpose	Applied So Data Is	Reference
Discovery	X		Limit scope of objects added to database.	Excluded	page 40
Topology	X	X	Limit information forwarded from collection station to management station.	Excluded	page 41

5. Interested application developers should see the *HP OpenView Integration Series: SNMP Developer's Guide*.
6. See "Filterable Objects and Attributes" on page 181 for specifics.

Table 2-1 Comparing Types of Filters (Continued)

Filter Type	Apply on Incoming Data	Reevaluate If Filter Changes	Purpose	Applied So Data Is	Reference
Map	X	X	Show only items of interest to operator on map.	Excluded	page 42
Persistence	X	X	Disable on-demand submaps for third party applications.	Included	page 68
Failover	X	X	Limit nodes polled by management station when collection station fails.	Included	page 52
Important Nodes	X	X	List unreachable important nodes as primary alarms in the Alarm Browser rather than children of a connector down event.	Included	*Managing Your Network with HP OpenView Network Node Manager*
DHCP Range	X		Identify DHCP (shared or floating) IP addresses	Included	*Managing Your Network with HP OpenView Network Node Manager*

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1284
3740
Doc:

Discovery Filtering

Discovery filters specify which devices an NNM station is actively discovering and monitoring. The purpose of discovery filtering is to reduce the discovery and monitoring effort of the station. Different stations have independent (though possibly identical) discovery filters.

Discovery filtering limits the scope of objects that `netmon` adds to the collection station topology database. To unmanage objects and limit the set of nodes that are polled at all, refer to *Managing Your Network with HP OpenView Network Node Manager*. The filter may be set to pass, for example:[6]

- Gateways.
- Bridges, routers, and hubs.
- All devices.
- Nodes based on their `sysObjectID`.
- Objects inside or outside of a particular range of IP addresses.

By default, Segments and Networks pass the discovery filter.

Discovery filtering is achieved by configuring the `netmon` service[7]; the filter is then applied to all newly discovered objects. Objects that are rejected by the discovery filter never appear in any topology or object database.

Discovery filters are data-stream filters; changes to a discovery filter affect new data *only*. All objects that previously passed the filter remain in the data stream, regardless of whether they would currently pass or not, and polling is still done on all previously discovered objects whether or not they would now pass the filter. You can, however, use the `ovtopofix` command to change the set of previously discovered objects.[8]

7. See "Configuring a Discovery Filter" on page 128, for details, *netmon* and *xnmpolling* reference pages in NNM online help (or the manpages on UNIX systems), the NNM online help, and "Distributed Services Architecture" on page 48.
8. See the *ovtopofix* reference page in NNM online help (or the UNIX system manpage) for details.

Implement any discovery filtering on an NNM station before you begin using it as a collection station; this will improve overall performance, by reducing the amount of synchronization effort.

Topology Filtering

Topology filters specify which topology data gets forwarded to a management station. The result is less management traffic on the network and lower data storage requirements at the management station. By default, the topology filter does not pass Networks and Segments.

A topology filter at a collection station defines the subset of topology data that management stations can see. The idea is to have the topology filter at the collection station pass information about only those objects in which the manager is interested. Data about objects outside the manager's interest doesn't clog up the link to the management station.

Objects rejected by a topology filter remain in the collection station's topology database. They are not, however, provided to a higher-level management station. Each collection station has only one topology filter in place. Note that this means the topology filter of a collection station must meet the needs of all management stations.Through topology filtering, you can choose to provide the following kinds of topology data to interested managers (many other choices exist):[9]

- All topology data, by using no filter at all.
- Nodes with (or specifically without) a certain `sysObjectID`.
- Objects inside or outside of a particular range of IP addresses.
- Nodes from a particular vendor.
- Objects with particular physical address.
- All token ring segments.

Topology filtering is achieved by configuring the `ovtopmd` service.[10] You should test topology filters at the collection station before the station goes into service.[11]

9. See "Filterable Objects and Attributes" on page 181 for specifics.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1285
3740
Doc.

Topology filters are, technically, data-stream filters. However, in effect, any change to a topology filter affects new and old data *alike*. When a topology filter is changed, the topology database of the management station is resynchronized with the filtered collection station topology database. Some objects may be deleted from the management station topology (if they do not pass the new topology filter), and some objects may be added (if they were previously rejected, but now pass the topology filter). As a result, the database of the management station ends up reflecting the topology being passed by the new topology filter, so the effect is that of a set-defining filter.

NOTE Topology filters do not affect the events that are passed from collection stations to management stations. This means that any events that you have configured to be forwarded are in fact forwarded from the collection station to the management stations, regardless of whether the objects to which the events refer pass the topology filter or not. Listing particular event sources in the event configuration at the management station can reduce the likelihood of operator confusion.

Map Filtering

The purpose of map filtering is to give the operator visibility of only those objects in which he or she has interest. By default, Networks and Segments do not pass the map filter.

Map filtering occurs on a per-map basis, not a per-display basis. All operators who use a particular map have the same filtered view. Additional maps can be created and separately filtered for specific purposes.

10. See "Distributed Internet Discovery and Monitoring" on page 46, Chapter 4, Procedures for Scaling NNM, and the *ovtopmd* reference page in NNM online help (or the UNIX system manpage), for further details.
11. See the reference page in NNM online help (or the UNIX system manpage) for *ovtopodump*, especially the `-f` option, for instructions on testing topology filters.

9130

Objects that are rejected by a map filter remain in the management station's topology database, and are still subject to status polling. Events from these objects pass through and are visible in the event subsystem, but this can be changed to show only events from objects on the operator's current map.[12]

Like the previously discussed types of filtering, map filtering can be configured so that (regardless of how much other topology data exists in the database) the map seen by the operator displays only the objects of interest to that operator. In general, this means objects that match some combination of attributes and attribute values; among the many choices, this can include:[13]

- All objects, by using no filter at all.
- Connectors, networks, and segments only.
- Nodes with specific `sysObjectIDs`.
- Bridges, hubs, and their segments.
- Objects inside or outside of a particular range of IP addresses.
- Only nodes that support SNMP.

Map filtering is generally configured in the NNM interface.[14]

Map filters are set-defining filters. When you change a map filter, all the objects currently in the map are reevaluated to see if they pass the new filter; new objects must also pass the filter before being added to the map.

Defining New Filters

All filters, discovery, topology, map, and persistence, are configured by creating a text file in which you use a special filter definition language to define filters that pass and reject objects in the ways you want.[15]

---

12. See the *xnmevents* reference page for details on the "filter by map" feature.
13. See "Filterable Objects and Attributes" on page 181 for specifics.
14. See the online help and Chapter 4, Procedures for Scaling NNM, for further details.
15. See Appendix A, The Filter Definition Language, for details on the syntax, semantics, and mechanics of filter definition.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1286
3740
Doc:

NOTE While you can create multiple filter definition files, you can use only one at any given time. Hence, only the filters defined in the currently in-use filter definition file are available.

You can give each filter you define a sensible name. For example, a map filter that would pass only routers might be named `Routers`.

Effective use of filtering lets you monitor a broader domain with a given management station. For example, suppose you have a site with 5000 workstations and PCs connected by 300 hubs and routers.

If you are only interested in the connecting devices, you might be able to use a single collection station with filters configured to discover and monitor only the 300 hubs and routers. Without such filtering, monitoring all 5300 nodes might require three or more collection stations to maintain equivalent performance.

NOTE As a rule, the sooner you can filter out a particular object, the better overall performance of the network management solution will be. For example, by using discovery filtering to discover and monitor exactly and only those objects of interest, you can dramatically reduce the amount of data that all other parts of the system have to handle. The next-best type of filter, to reduce the data load on the distributed management system, is a topology filter. While a local collection station may need broader discovery for its own management domain, the management stations that use the collection station frequently do not require a full copy of the topology at the collection station; topology filtering is the way to prevent unnecessary data from being exported to the management station.

Filter Utilities

NNM provides the utilities shown in Table 2-2, Filter Utilities, to help you build filters that do what you want and expect.

Table 2-2 Filter Utilities

Utility Name	Description
On Windows operating systems: *install_dir*\bin\ovfiltercheck On UNIX systems: $OV_BIN/ovfiltercheck	Provides syntax validation for a filter file. Can also be used to check individual Set, Filter, and Filter-Expression statements for correct syntax.
On Windows operating systems: *install_dir*\bin\ovfiltertest On UNIX systems: $OV_BIN/ovfiltertest	Tests all or part of a specific object database (ovwdb) against a filter. Objects that pass the filter are reported to the output. Use the -c option to specify a collection station to determine which objects the management station polls on failover.
On Windows operating systems: *install_dir*\bin\ovtopodump On UNIX systems: $OV_BIN/ovtopodump	Use the -f option to compare a filter against the current topology database.

See the reference pages in NNM's online help (or the UNIX system manpages) for these commands to obtain details on their syntax and use.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1287
3740
Doc:

Distributed Internet Discovery and Monitoring

Distributed Internet Discovery and Monitoring is one of NNM's keys to providing a scalable network management solution. The purpose of this section is to give you a picture of exactly which parts of NNM are distributed, and how data flows through the distributed solution. With this knowledge, you will be able to better understand what is occurring as you deploy NNM.

About Collection Domains

Within the NNM model of distribution outlined in "The Distribution Model for Network Node Manager" on page 33, it is useful to distinguish these two sets of objects:

Management domain

This is the set of all objects that are of interest to the user. In Figure 2-1, the management domain of the operator at Management Console 1 contains all the objects in the whole network (except objects that are removed by intervening filters). On the other hand, the management domain of the operator at Management Console 6 consists of only the objects directly monitored by Station F; no other objects are visible from that station.

Keep in mind that the management domain is an attribute of the management station, not the operator. Different operators might deal with different subsets of the management domain, based on map definitions and map filters.

Collection domain

This is the set of objects that are directly discovered and monitored by an NNM station. This typically includes any objects on which data collection (for trends or thresholds) is occurring.

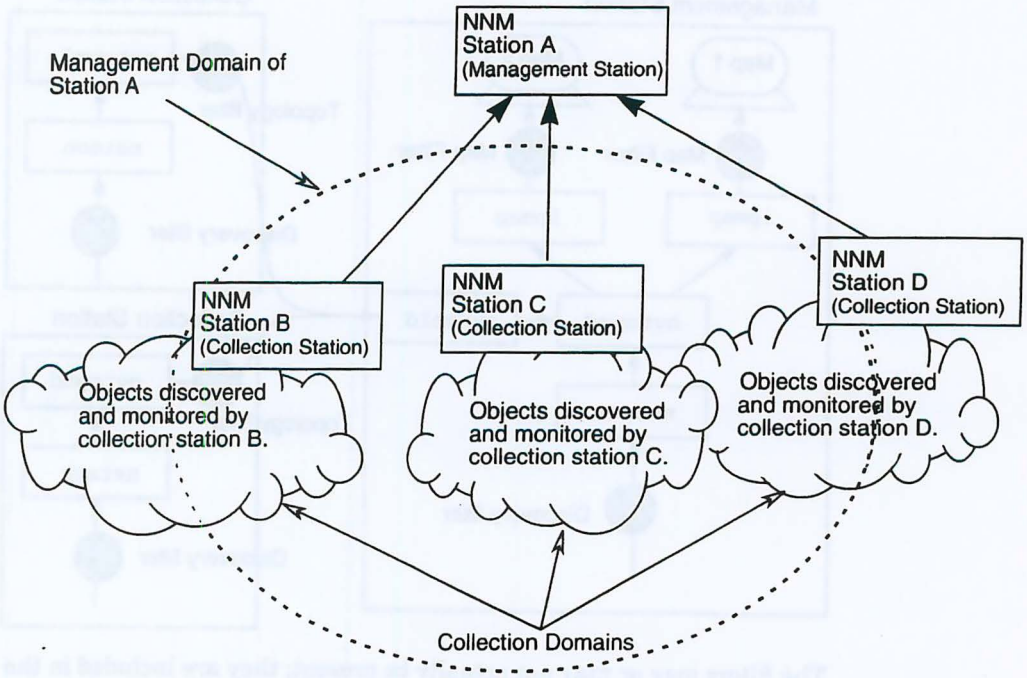
At a high level, these definitions can be depicted as in Figure 2-2.

In the diagram, the management domain of station A does not include all the objects in the collection domains of all the collection stations. Remember, the collection stations are probably management stations too. For each of these, the management domain is coincident with the collection domain.

However, the administrator of the overall network, working from Management Station A, is quite possibly very selective about which objects within the various collection domains of the collection stations are of interest to operators at the management station.

You can use filtering to select exactly those objects, and thus constrain your management domain to those objects that make the most sense for you.

Figure 2-2 Management and Collection Domains



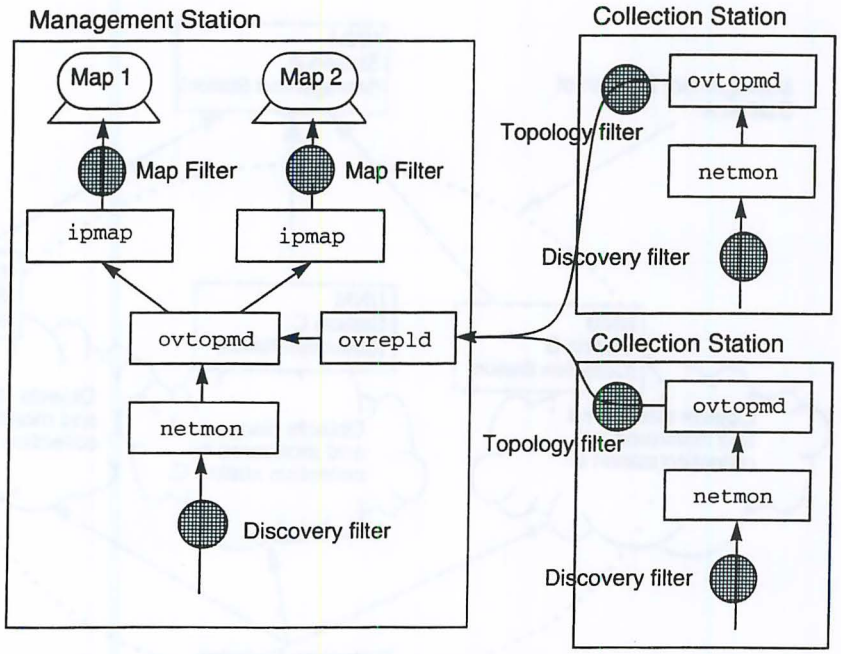
RG nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1288
3740

Distributed Services Architecture

Network Node Manager relies on the complex interplay of several different services (background processes on UNIX systems) to provide the level of functionality and performance you need. In making NNM a scalable solution, several of these services appear in locations remote from the management station.

Figure 2-3 is a diagram of the key services involved in a distributed deployment of NNM. Of these, the `ovrepld` service is central to the distribution of network topology; the others have other, stand-alone functionality. The `ovrepld` service is the "replicator" of the topology, responsible for integrating topology data from multiple collection stations into the management station's topology database.

Figure 2-3 Service Components in Distributed Internet Monitoring



The filters may or may not actually be present; they are included in the illustration at all the points where they would potentially exist. Note also that when a collection station is also fulfilling a local management

role, it runs local `ipmap` and `ovw` services too. And finally, understand that in the interest of simplicity, Figure 2-3 omits the role of the event system, which is illustrated in Figure 2-4.

How Distributed Internet Discovery and Monitoring Works

Figure 2-3, shows two collection stations working on behalf of the management station. Each collection station has its own collection domain, which is the responsibility of the local `netmon` service. You can set discovery filters to minimize unnecessary discovery and monitoring.

Having a station take the role of a collection station, or make use of collection stations, requires several other configuration steps. "Configuration Concepts" on page 56 introduces these configurations steps, and "Configuring Collection Stations" on page 133 gives complete details.

After the stations have been configured correctly, start the collection station as usual. The `netmon` service begins IP and level-2 discovery, and (along with the `ovtopmd` service) populates the local topology database.[16] It takes time for this process to finish, but to minimize management traffic on the network, you should allow NNM to finish (or nearly finish) discovery before you begin to use it as a collection station. The `Performance:Network Polling Statistics` tool can help you determine when the collection station has reached a steady state.[17]

After waiting for the collection station to build its topology database and reach a steady state, the management station administrator uses the `xnmtopoconf` command to begin using the discovery and monitoring services of the collection station.[18]

At this point, the management station obtains access to the topology data at the collection station. It requests the collection station to send the objects in the collection station's topology database across the network. If the collection station has a topology filter configured, only those objects that pass the filter are provided to the management station.

---

16. See *Managing Your Network with HP OpenView Network Node Manager* for details about these and other services (background processes on UNIX systems) in Network Node Manager.
17. See the online help about this tool for more information about the procedure.
18. See the reference page in NNM online help (or the UNIX system manpage) for *xnmtopoconf*.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1289
3740
Doc:

Topology data that is not derived from a local `netmon` service is not sent to the management station. This precludes the possibility of cycles (where station "A" discovers and reports "B," which discovers and reports "C," which again discovers and reports "A," ...). It also precludes indirect multiple-level hierarchical management.[19]

The `ovrepld` service on the management station replicates the topology data from the collection station in the local topology database. "Replication" does not imply a 100% mirroring of the collection station topology database at the management station. Remember that topology filtering at the collection station means that some of the objects present in the collection station's topology database may *not* be present at the management station. The topology data that *does* pass the topology filter is kept synchronized between the collection station and the management station.

NOTE

The `ovrepld` service provides synchronization of the topology data *only*. It does not affect any other databases (such as `ovwdb`, `snmpCollect`, or `ovw`).

Once the topology merging is done, the `ovtopmd` service treats the new objects just like objects obtained from the local `netmon` service.

After the synchronization phase is complete, only *changes* in status and topology get sent to the management station. The `ovrepld` service updates the topology database of the management station to reflect the changes.

High Availability Management Information

One way to ensure your network management information is always available is to run your management stations on HP Service Guard clusters. If the primary processor goes down, processing automatically and transparently rolls over to another processor in the cluster. Configure Service Guard NNM stations using the `ov.conf` configuration file parameter `HOSTNAME=`. See the *ov.conf* reference page in NNM online help (or the UNIX system manpage) for more information.

19. See "Hierarchical Management" on page 98, especially Figure 3-4 and Figure 3-5, for more information on multilevel hierarchical management.

As part of the Service Guard interface, NNM offers `ovwrs` (self-restarting `ovw`). This interface runs `ovw` while monitoring the status of the console server process on the management station. If the connection to the server is lost, the it informs the user and re-establishes its connection to the server. See the reference page in NNM online help (or the UNIX system manpage) for *ovwrs* for more information.

Collection Station Failover

NNM also provides capability to continue data collection when a collection station goes down. The management station's `ovrepld` service performs periodic status checks to verify the status and state of the currently managed collections stations. When a status check fails, the status of the collection station is downgraded one level. The default interval between checks is five minutes (but this can be reconfigured via the `xnmtopoconf` command). Thus, it will take 20 minutes before a "Collection Station Critical" event is generated; an event confirmation popup dialog is presented to the operator. The nodes affected by the failure are left with the status they had at the time the collection station stopped responding.

Collection Station failover enables a management station to take over status polling responsibilities for a collection station which is temporarily unreachable. When the collection station returns to normal, the management station returns to its previous state, delegating discovery and monitoring of those objects to the collection station. This feature is not intended to provide support for collection stations which will be down for a long time or which have been permanently removed from service.

In order to prevent `netmon` from being overloaded, failover only takes over status polling, not the full responsibilities of the collection station. Discovery and SNMP configuration polling are not picked up.

When the collection station returns to normal operation, the management station removes the failed over topology list from its polling queue and resynchronizes with the collection station. The status from the collection station is considered to be current, which means it takes priority and overwrites the status for the objects where were stored in the management station database.

IP and IPX (Windows operating systems) collection stations can failover to a management station. IPX interfaces from a Windows operating system collection station are not polled by a UNIX system management station.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1290
3740
Doc:

You control failover operations through the management station's `Options:Network Polling Configuration:IP` menu selection, "`Status Polling`" tab; or through the `xnmtopoconf` flags "`failover`," "`nofailover`," and "`failoverFilter`." Refer to the reference page in NNM online help (or the UNIX system manpage) for more information.

Failover Filtering

The default operation is for the management station to pick up status polling responsibility for all nodes loaded in the management station's topology from that collection station. However, you can control the load on the management station by providing a failover filter that lists specifically which nodes should be polled. The failover filter behaves like a discovery filter which loads networks and segments, and then filters on nodes and interfaces before the data is given to `netmon`. The interfaces and the node to which they are attached are considered a unit. If one interface on the node passes the filter, then the entire node and all of its interfaces that the collection station polls pass the filter as well. You determine which objects are picked up on failover on a collection station by collection station basis.

Failover Considerations

The management station must have access to the interfaces which are to be picked up in a failover situation. A route needs to exist to the interface to be polled.

The possibility of overloading the management station is a consideration when configuring failover. The devices for which continuous status polling is especially important, such as routers and gateways, are good candidates for inclusion in a failover filter. The management station needs information about connection devices in order to detect secondary failures.

Overlapping Collection Domains

Reexamine Figure 2-2, and notice that sometimes the objects in the collection domain of one collection station are *also* within the collection domain of a different collection station.

For example, in Figure 2-2 the collection domain of Station C overlaps that of Station D, and both serve as collection stations for Station A. Such instances are not uncommon in practice. It is easy to imagine a

router that Stations C and D both care about and monitor. At Station A, that one router will appear in the topology data arriving from both collection stations.

When a management station receives multiple versions of the same object from different collection stations, it uses the rules described in the next section to automatically choose one version as the "primary" version; it then treats all other versions as "secondary."

The station that provides the primary version of an object's data is called the **primary collection station** for the object; any other station that provides information about that object is a **secondary collection station** for the object.

Note that a collection station can be a primary for one object, and a secondary for another object. In other words, the choice of primary vs. secondary is on a per object basis, not a per station basis. Furthermore, a collection station does not know or care whether it is the primary or secondary station for a given object.

Only the primary version of data is displayed in the operator's map. Unless you specifically request information from a secondary version, all topology queries return information from the primary version.

Overlapping collection domains cause redundancy and can therefore waste memory, processing and network resources. In order to reduce the overlap, set the DeleteSecondary mode via `xnmtopoconf` on the management station.

The Selection of Primary and Secondary Collection Stations

NNM uses several rules to decide which of several versions of an object is primary (and by implication, which collection station is the primary collection station). The rules are evaluated in order, and the first rule that distinguishes a primary collection station is applied and the process terminates; remaining rules are ignored.

The rules NNM uses to establish the primary collection station for an object are as follows:

1. If only one station is reporting the object, that station is the primary collection station for the object.
2. If the object is an interface (`isInterface == TRUE`), skip to rule 7.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1291
3740
Doc:

3. If only one station reporting the object is *a.)* managed (meaning currently in active use as a collection station), and *b.)* has noncritical status or has failed over, that station is the primary collection station for the object.
4. If the user has expressed a preferred primary collection station for the object[20], that station is the primary collection station for the object.
5. If only one station reporting the object is managing the object (meaning actively managing it, either by default or via `Edit:Manage/Unmanage Objects`, that station is the primary collection station for the object.
6. If one station reporting the object is a gateway, that station is the primary collection station for the object. (A gateway is a node with multiple interfaces performing IP routing functions.)
7. If the object (A) is completely contained in another object (B), the collection station for the container object (B) is the primary collection station for the object (A). For example, a non-gateway node should have the same primary collection station as the network that contains it.
8. If one of only two stations reporting the object is non-local, the non-local station is the primary collection station for the object.
9. The first station to report the object is the primary collection station for it.

You can express a preferred primary collection station for an object.[21] However, you should be aware that if conditions force NNM to reevaluate the primary collection station, your preference may be temporarily overridden, according to the preceding rules.

---

20. See the *xnmtopoconf* reference page in NNM online help (or the UNIX system manpage), especially the `-preferred` and `-clearPreferred` options.
21. See the *xnmtopoconf* reference page in NNM online help (or the UNIX system manpage).

For example, suppose the preferred primary collection station you selected for an object goes down and you have configured `nofailover`. If a secondary collection station can pick up reporting for that object, that station becomes the primary collection station for the object until the preferred primary station is again available.

If the down primary collection station has failed over to the management station, the management station does not make its local version of the object the primary. Where failed over objects were in overlapping domains with the management station, `netmon` handles the duplicate objects by only polling the device once and updating all of the objects with the status.

A management station will not pick up status polling on secondary objects during failover. There is already a primary collection station still providing information for those objects.

Overlaps with the Collection Domain of the Management Station

In some cases, particularly when an existing large collection domain is partitioned by collection stations, the collection domain of the management station overlaps the collection domain of a collection station. The question then arises, what should be done with the secondary (local) version of information about objects in the overlap?

You have three choices:

1. "`Allow Overlap`", which means that the `netmon` running on the management station should continue polling the node even though a collection station is also polling the node. This would also accept the associated resource consumption caused by duplicate monitoring (potentially over an expensive link) and duplicate information in the topology database.
2. "`Unmanage Secondary`", which unmanages the local version of objects (networks, segments, and nodes) in the overlap region, but keeps them in the database. (The local unmanaged version of the object will not be shown on any maps.) This eliminates the duplicate polling, but still incurs the data storage overhead. If the collection station should fail, the management station can be made the primary collection station to quickly restore management to the affected objects. This will not happen automatically. Refer to "Changing the Primary Collection Station for an Object" on page 151 or to the *xnmtopoconf* reference page in NNM online help (or the UNIX system manpage) for information on configuring failover.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1292
3740
Doc:

3. "`Delete Secondary`" deletes the local version of overlapping objects from the topology database. This eliminates the overhead of both duplicate monitoring and duplicate objects in the database. You then rely on the collection station to provide all information about the objects in the overlap.

   When this is the mode, a local version of any overlapping networks is retained in an unmanaged state. The `netmon` on the management station will not discover nodes that belong to an unmanaged network. If a collection station fails, you will have to delete the collection station, then manage the networks and wait for `netmon` to discover the nodes that have been deleted unless you have failover configured.

The third option is the default behavior of an NNM management station. However, only non-connector nodes are deleted; NNM does not delete networks, segments or routers that overlap with the collection station's collection domain. This maintains visibility to the boundary of the collection domain of the collection station even in the event of collection station failure. The local versions of connector objects are put in the "unmanaged" state. If the normal primary collection station for these objects becomes unavailable, the local versions can become the primary version.

You can choose which behavior you prefer by using `xnmtopoconf`.[22]

Configuration Concepts

For a station to either be, or make use of, a collection station requires additional configuration steps.

This section provides only a brief summary of configuration to acquaint you with the general concepts, and gain a better understanding of what is required when deploying distributed IP discovery and monitoring. Detailed steps for configuring management and collection stations are provided in "Configuring Collection Stations" on page 133.

NOTE NNM does not provide remote configuration utilities. Therefore, the configuration steps used to set up a collection station have to be made from the collection station itself. You can, of course, use `telnet` to log in

22. See the *xnmtopoconf* reference page in NNM online help (or the UNIX system manpage).

Distributed Threshold Monitoring and Event Forwarding

The event subsystem for NNM allows forwarding of events (including topology changes, correlated events, and threshold events) from collection stations to management stations.

The services (background processes on UNIX systems) that NNM uses in basic event forwarding are:

- The trap service (`ovtrapd`).
- The postmaster service (`pmd`).

Figure 2-4 illustrates these services, and their relationship to other key NNM files and services.

The `ovtrapd` service is responsible for receiving SNMP traps and inform-requests on port 162 via UDP, the protocol of the SNMP standard. It buffers them, and passes them to the postmaster (pmd) service.

The `ovtrapd` service automatically provides an inform-reply to inbound SNMPv2C inform-requests.

The postmaster service routes the traps it receives from `ovtrapd` to the appropriate subsystem. Moreover, the postmaster service is the central dispatcher that all management applications (both NNM and third-party) use to communicate with each other. It uses the TCP protocol to route events between them so messages are not dropped, even over noisy or congested links.

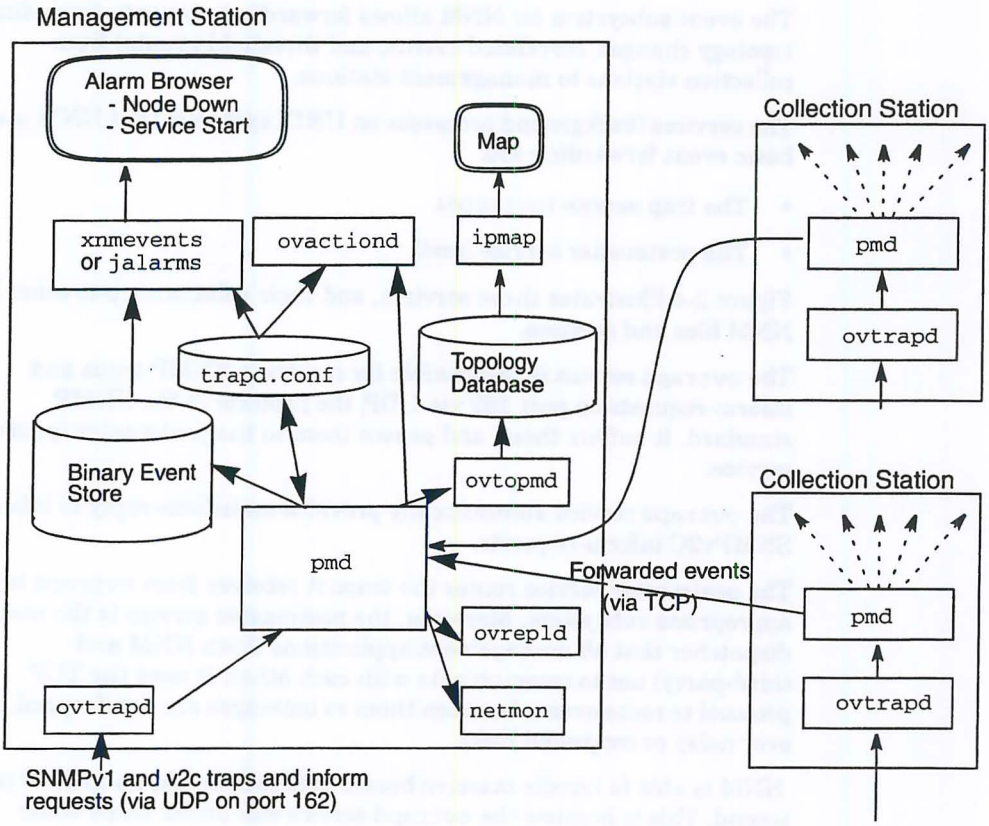
NNM is able to handle massive bursts of SNMP traps, up to 2000 per second. This is because the `ovtrapd` service can buffer traps while forwarding them to the postmaster for routing. This buffering reduces the likelihood that traps in a burst will be dropped.

The `Event Configuration` window supports event forwarding. It also supports an event-identifier naming convention, where SNMP version 1 traps, SNMP version 2C traps, and SNMP version 2C inform requests

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1293
Doc: 3740

use the same naming conventions for event IDs. See the online help and the *trapd.conf* reference page in NNM online help (or the UNIX system manpage) for details.

Figure 2-4 The Basic Event System in NNM



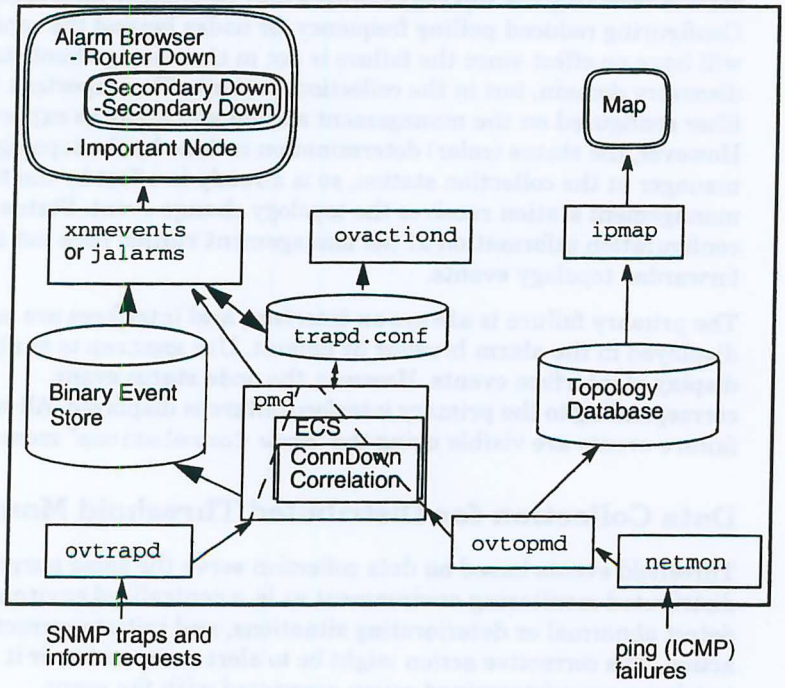
Event Correlation for "Connector Down"

One of NNM's key features is its ability to correlate incoming event information. See *Managing Your Network with HP OpenView Network Node Manager* for a complete description. The most useful correlation

rules for a distributed environment clarify information coming in when a connector (router, gateway, etc.) goes down and all the nodes beyond the connector become unreachable.

Since these events originate from `netmon` polling rather than from SNMP traps coming in through `ovtrapd`, the internal handling and forwarding is somewhat different from basic events. This is shown in Figure 2-5.

Figure 2-5 The Correlated Event System for "Connector Down"



When `netmon` recognizes a ping failure, which in the case of interest happens to be a connector failure, it notifies `ovtopmd` to update the topology database. `ovtopmd` notifies `pmd` that it has done so, and `pmd` runs the event through the Event Correlation System while `ipmap` updates the map. The correlated event then appears with a "children" indicator in the Alarm Browser.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
1294
Fls. Nº
3740
Doc:

In a distributed environment, pmd forwards the topology change for the nodes to the management station. At the management station, the pmd informs ovrepld to update the topology database. When ovtopmd makes that change, it informs pmd of the topology change. pmd then handles that topology change notice just like a local topology change notice, and routes it through the ECS correlation for "Connector Down." Note that the "Connector Down" event itself was not forwarded. The management station automatically derives that event from the topology change notification.

Operation of the "Connector Down" correlation on the management station receiving the topology changes may be slightly unexpected. Configuring reduced polling frequency for nodes beyond the connector will have no effect since the failure is not in the management station's discovery domain, but in the collection station's. The important node filter configured on the management station will apply as expected. However, the status (color) determination is done by the topology manager at the collection station, so is already in effect by the time the management station receives the topology change event. Status (color) configuration information at the management station does not apply to forwarded topology events.

The primary failure is always an interface, and interfaces are not displayed in the alarm browser by default. Use xnmtrap to enable display of interface events. However, the node status event corresponding to the primary interface failure is displayed. All secondary failure events are visible using the "Show Correlations" menu.

Data Collection for Distributed Threshold Monitoring

Threshold events based on data collection serve the same purpose in a distributed monitoring environment as in a centralized environment: to detect abnormal or deteriorating situations, and initiate corrective action. The corrective action might be to alert an operator, or it might be to trigger a predetermined action associated with the event.

A collection station can independently collect data (from the objects that it monitors) for threshold monitoring. When a threshold event is triggered, it can be automatically forwarded to a management station.

At the management station, it doesn't matter whether a threshold event was triggered by local data collection (done at the management station), or forwarded from a collection station. Forwarded threshold events are

automatically consolidated with local threshold events. Whether forwarded or locally triggered, the threshold event looks the same to the management station, and receives the same treatment.

NOTE Topology filters do not affect the events that are passed from collection stations to management stations. This means that any events that you have configured to be forwarded are in fact forwarded from the collection station to the management stations, regardless of whether the objects to which the events refer pass the topology filter or not. Listing particular event sources in the event configuration at the management station can reduce the likelihood of operator confusion. Also, this note does not apply to events internal to NNM.

See "Configuring Event Forwarding and Correlation" on page 154 for details about configuring event forwarding, including threshold event forwarding.

Remote Thresholds with Remote Actions

For some threshold events on collections stations, you may want to consider creating actions at the collection station. Where this is a reasonable tactic, it has the advantage that the action will be invoked even if contact is lost with the central site.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1295
3740
Doc.

On-Demand Submaps

As described in "On-Demand Submaps" on page 26, the reason for enabling the on-demand submap feature is to improve NNM's performance and reduce it's use of memory and disk space. Rather than keep all the submaps in memory (which, for a large map, can require large amounts of memory), you can specify that many of the submaps only be created at the moment you need them.

A **persistent submap** is created and maintained for the life of the map. In contrast, a **transient submap** is created (and removed) only as necessary; that is, "on-demand." Transient submaps are created and maintained by the `ipmap` service, and removed by the `ovw` service.

Figure 2-6, A Typical Hierarchy of Persistent Submaps, and Figure 2-7, A Typical Hierarchy of Transient Submaps, show the difference between persistent submaps and transient submaps.

All the submaps in Figure 2-6 are persistent; this is the default when you first install NNM on UNIX systems. On Windows operating system management stations, the default is `Internet Level`. In contrast, in Figure 2-7 only the "Root" and "Internet" submap levels are persistent. Submaps from the "Network" level down are transient submaps. These are created only as they are needed. The `ipmap` service does not allocate memory for them, nor does it maintain topology changes in them. This saves both memory and execution time. Note that status from transient submaps is propagated up in the usual way.

The visible submaps (when on the same levels as the crossed-out ones) are also transient submaps, but the operator has navigated into that part of the submap hierarchy, and so these submaps are currently resident in memory.

You use the `IP Map Configuration` dialog box to set submaps to be persistent down to whatever level of the submap hierarchy you select. On Windows operating systems, the initial configuration for demand level is `Internet Level`.

Most users of this feature will start with submaps set to be persistent at the `Internet Level` (as in Figure 2-7), and set it to lower levels only to improve submap-opening performance. This is typically necessary only when the higher-level submaps are densely populated.[27]

If you want to reset the on-demand submap feature to its default, use the `IP Map Configuration` dialog box in NNM to set submap persistence to `Unset`. On Windows operating systems, `Unset` sets the persistence level to `Internet Level`. On UNIX systems, `Unset` sets the persistence level to `All Levels`.

With on-demand submaps enabled at any level, most NNM features and operations work as they always have. Locate operations and IP status propagation, in particular, are not limited to what is currently in memory. Both functions work across all submaps, regardless of whether they are persistent or transient.

In cases where a located item is not yet in memory, the necessary submap is created, on-demand, if and when the user opens that submap from the locate dialog box.

Transient Submaps and the Submap List Dialog

The only feature that changes its behavior when the on-demand feature is enabled, is the `Submaps in Map` dialog box. Only submaps that are currently in memory (that is, either persistent, or transient but currently in memory) can appear in the `Submaps in Map` dialog box.[28]

In other words, when the on-demand submap feature is enabled, submaps that are not presently in memory are not present in the `Submaps in Map` list. This behavior may alter the usefulness of the `Submaps in Map` dialog box, depending on the expectations of the operator.

To reduce the possibility of operator confusion when the on-demand submap feature is enabled, you may wish to remove the following menu item (which opens the `Submaps in Map` dialog box):

```
Map:Submap->Open
```

27. See also the "Caution" block on "Configuring Management Consoles" on page 109.
28. See the online help for more information about this dialog box.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1296
3740
Doc:

See *Managing Your Network with HP OpenView Network Node Manager* for information about how to remove a menu item.

Persistence Filtering

Unlike the filters described earlier, the purpose of persistence filtering is not to reduce the amount of unnecessary management data in the data stream. Instead, the purpose of persistence filtering is to let some older applications that are not inherently compatible with the on-demand submap feature operate normally when the on-demand submap feature is enabled.

NOTE This is probably not an issue on Windows operating systems, since there are few "older" applications. However, some third-party developers may port their older UNIX system applications without changes.

Suppose an application has been created with the implicit assumption that the object or objects it is interested in are always available in memory. Such an application may fail or exhibit unstable behavior if the object it needs resides in a transient submap, and is thus not in memory at all times.

For example, a vendor you use may have developed an application that adds statistics component symbols under the router symbols created by the `ipmap` service. Such an application may assume that routers are part of the map (that is, present in memory) as soon as they are discovered. The on-demand feature, when enabled, invalidates that assumption.

A persistence filter can provide backwards compatibility for this type of application. The necessary persistence filter for the example application passes all routers. Then any submap that contains a router is made persistent, so that the expectation of the application is met.

A persistence filter tells the `ipmap` service that any submap containing an object that passes the filter should be made into a persistent submap. The object will then be in memory, as the application expects.

Persistence filters are set-defining type filters. A persistence filter is automatically applied to existing map and object data to determine which submaps must be persistent. When you change a persistence filter, all the objects currently in the topology database are reevaluated to see if

2104

they pass the new filter. Submaps containing objects that pass the new filter are made persistent. Submaps that do not contain such objects are made transient if they are below the current persistence level. [29]

Comparing Map Filters and Persistence Filters

A persistence filter is different from a map filter. A map filter specifies a subset of the topology data that is allowed on the map. The persistence filter states which objects should be made persistent in memory; those objects are made persistent by making the submaps they reside on persistent.

You can think of this as a two step process. First, the map filter passes a set of objects that are allowed to be present on the map. Then the persistence filter tests these objects to see which, if any, must be persistent in memory.

No matter what the persistence filter specifies, the user still has access to all of the objects that passed through the map filter.

When an object is found to meet the criteria in the persistence filter, all submaps containing that object are made persistent. That is, a submap is made persistent if it contains even one persistent object; it might also contain objects that do not meet the persistence specification criteria. In addition, the child submap of the persistent object is also made persistent.

Because persistence and map filters are both set-defining filters, if you change either for a given map (via the `IP Map Configuration` dialog box; see the online help for details), the `ipmap` service recalculates which submaps should be persistent. This might take a long time for larger databases.[30]

29. See "On-Demand Submaps" on page 64 for more details on persistence filtering. See "Specifying a Persistence Filter" on page 124 for configuration information.
30. See also "Map Filtering" on page 42.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1297
3740
Doc:

Management Consoles

Distribution of management consoles is done via NFS (or Windows operating system file sharing) mounting of the map database and the appropriate configuration files, and by then using the distributed RPC capability of the object database service, ovwdb, the topology database, and the event system.

Figure 2-8 is a diagram of the resulting services, and where they are located. As shown, each management console actually runs the user-specific ovw-related services. The management station keeps the common databases, and runs the services (background processes on UNIX systems) common to all users.

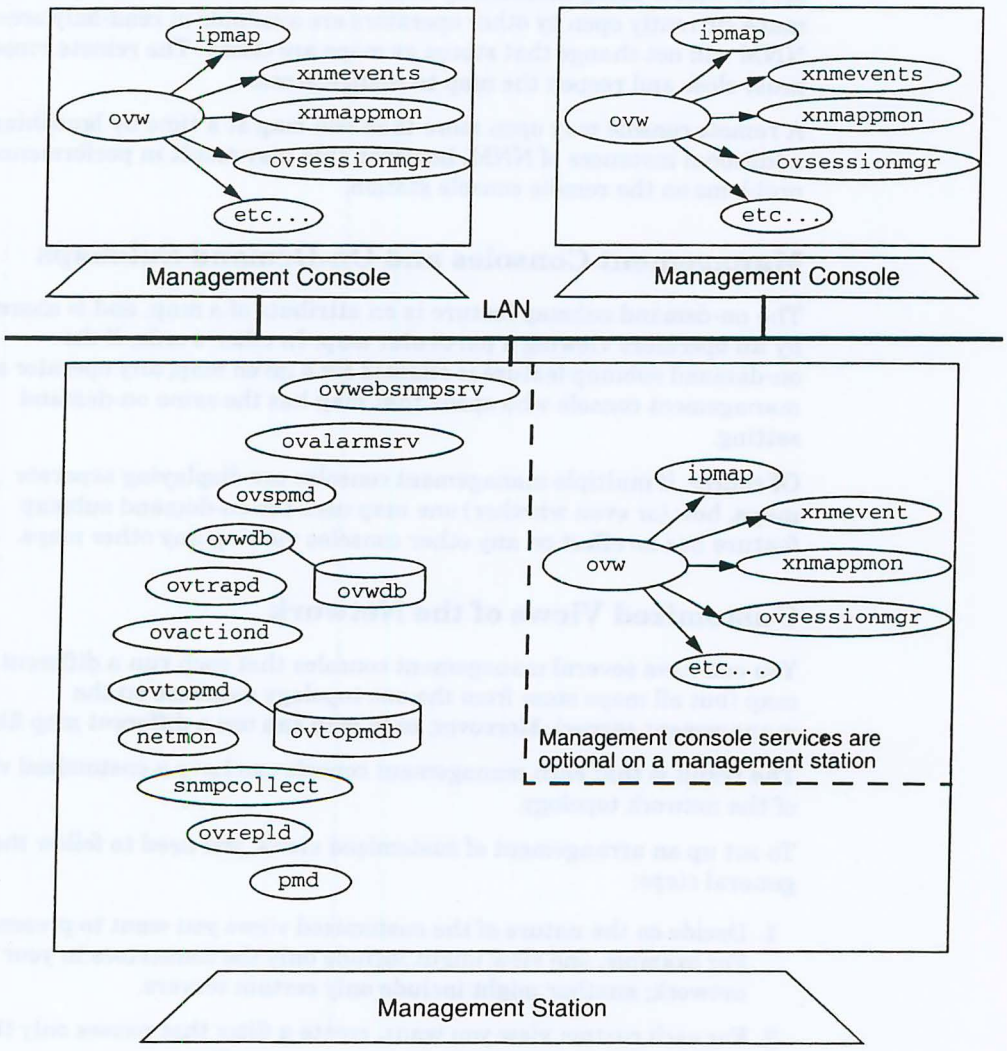
This relieves the management station of a significant demand for its resources (memory and CPU), since otherwise each operator would have independent copies of these services executing on the management station.

Relocating the ovw-related services allows the management station to apply more of its resources to network management and monitoring activities, and less to supporting the operators.

The object database remains centrally located on the management station, and is accessed by the management consoles over the network sockets. In addition to the various ovw-related services that communicate with the NNM services via socket connections, the map database and configuration files use NFS (or Windows operating system) file sharing.

NOTE Management consoles are *not* the same as NFS diskless clients. NFS diskless is an operating system concept. As described above, the distribution mechanism for management consoles uses NFS and sockets.

Figure 2-8 Management Consoles



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1298
Doc: 3740

Operators can each have their own maps. If, on the other hand, they share a map, only the first operator to open the map can edit it; others have read-only access. When using remote console into a management server that is being accessed by other remote or local console operators, maps currently open by other operators are available in read-only access. NNM will not change that status as maps are closed. The remote console must close and reopen the map to change access.

A remote console may open more than one map at a time by launching additional instances of NNM, however, this may result in performance problems on the remote console station.

Management Consoles and On-Demand Submaps

The on-demand submap feature is an attribute of a map, and is shared by all operators viewing a particular map. In other words, if the on-demand submap feature is enabled for a given map, any operator at a management console who opens that map has the same on-demand setting.

Of course, if multiple management consoles are displaying separate maps, how (or even whether) one map uses the on-demand submap feature has no effect on any other consoles viewing any other maps.

Customized Views of the Network

You can have several management consoles that each run a different map (but all maps stem from the one topology database on the management server). Moreover, each map can use a different map filter.

The result is that each management console can have a customized view of the network topology.

To set up an arrangement of customized views, you need to follow these general steps:

1. Decide on the nature of the customized views you want to present. For example, one view might include only the connectors in your network; another might include only certain servers.
2. For each custom view you want, create a filter that passes only the objects you want visible in that custom view.[31]
3. At each management console, create a new map (`Map:New`), and apply the appropriate map filter for the operator at that console.

Management Consoles and X-Terminals

In principle, it is possible to run several X-terminal sessions from a management console, or directly from the management station. You might speculate that this would allow NNM to support more operators.

However, due to internal constraints, this approach *does not* allow the management server to support more operators. You should limit the number of operators per management station to avoid degrading the performance of the interface.

Attaching X-terminals to a management console might nevertheless have cost savings, if the management console host has sufficient CPU, memory, and disk space to support the X-sessions, and low cost X-terminals are available and suitable for the operators. The key services described earlier are still off-loaded from the management station to the management console.

31. See "Filters" on page 37 and Appendix A, The Filter Definition Language, for more information on creating filters.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1299
3740
Doc:

Interface Managed-state Automation

As you probably know, NNM lets you "unmanage" interfaces. NNM does not do status polling on unmanged interfaces, so setting interfaces to the Unmanaged state significantly lightens the load on the management station.

NNM lets you automatically manage or unmanage interfaces based on filters. Interface managed-state automation makes it easier to manage large environments, where frequently many discovered interfaces do not require active status polling.

Interface managed-state automation relys on a command (`ovautoifmgr`) that periodically sweeps through the topology and sets the managed state of interface objects according to rules in the managed-state configuration file (`ovautoifmgr.conf`).

Based on the rules in the configuration file, interfaces that do not need to be managed are put into the Unmanaged state. Interfaces which do need to be managed (and are not already) are put into the Managed state with their status set to `UNKNOWN`. Then `netmon` begins to monitor the interface's operational status and generate events.

The the `ovautoifmgr` command is not a continuously-running process. Instead, it is designed to be run periodically by a scheduling mechanism. It requires that `ovtopmd` be running.

For further information and instructions on using interface managed-state automation, refer to the `ovautoifmgr(1m)` and `ovautoifmgr.conf(4)` reference (man) pages.

Microsoft Terminal Server Access

You can connect to Network Node Manager (on a Microsoft Terminal Server) from a remote workstation through a Terminal Server Client. You can do any of the following:

- Install or upgrade NNM on the remote server.
- Perform administrative NNM functions such as backup/restore of NNM database.
- Open NNM and display the network map onto the local workstation.
- Start multiple Terminal Server Client sessions to the same remote NNM management station, open NNM in each session and display the network maps onto the local workstation.
- Start multiple Terminal Server Client sessions to different remote NNM management stations, open NNM on each NNM management station and display the network maps onto the local workstation.

The following examples provide a few of the possible implementation strategies available to network managers when running the NNM application on servers with the Microsoft Terminal Server features enabled.

Accessing a Single NNM Station From Multiple Terminal Server Clients

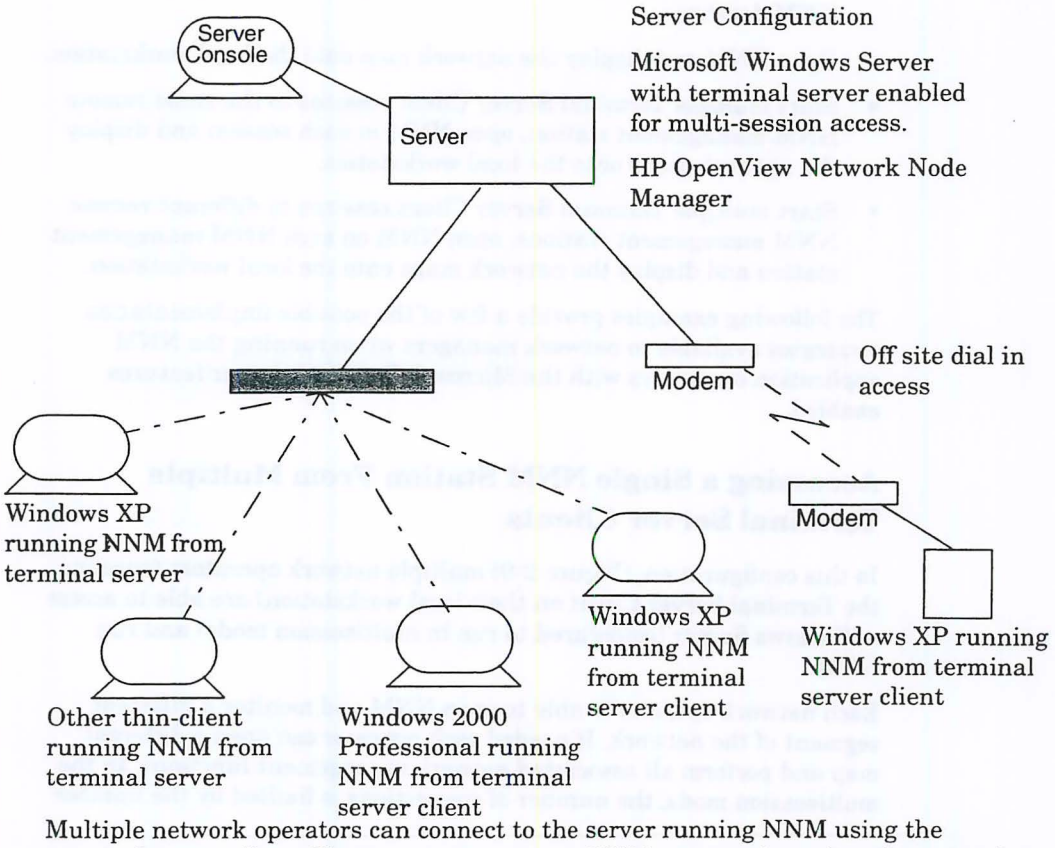
In this configuration, (Figure 2-9) multiple network operators (running the Terminal Server Client on their local workstation) are able to access a Windows Server (configured to run in multisession mode) and run NNM.

Each network operator is able to open NNM and monitor a different segment of the network. If needed each operator can open a different map and perform all associated network management functions. In the multisession mode, the number of connections is limited by the number

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1300
3740
Doc:

of client licenses available. Accounts with administrator privileges can be used to start and stop NNM processes, run NNM database backups, and install NNM patches.

Figure 2-9 Multiple Terminal Server Clients Accessing a Single NNM Station



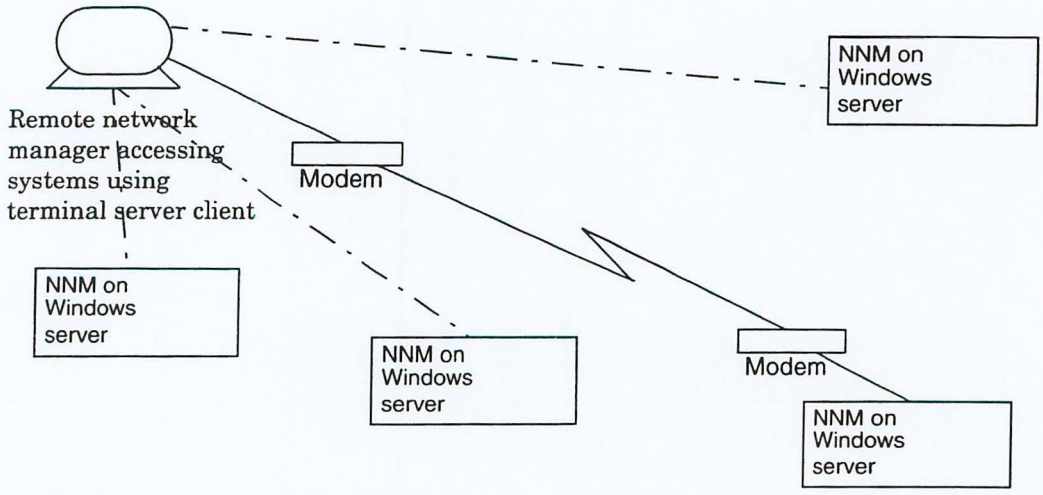
Multiple network operators can connect to the server running NNM using the terminal server client. The operators can open NNM maps and monitor the network segment from their local workstation.

Accessing Multiple NNM Stations From a Single Terminal Server Client

In this configuration, (Figure 2-10) a single network manager is able to access multiple Windows servers configured to run under Remote Administrator mode. The NNM application is installed on each Windows server. The remote network manager, using the Terminal Server Client, is able to connect to each remote system, monitor the network, and perform all network management functions. With this configuration a network manager has the ability to access and display multiple NNM sessions on their local workstation.

The remote administration mode limits the number of connections to the server (maximum of two) and only grants connections to accounts that have administrator privileges.

Figure 2-10 Accessing Multiple NNM Stations



Server Configuration

Microsoft Windows Server with terminal server enabled and installed as Remote Administrator mode.

HP OpenView Network Node Manager running on each server to manage the local network

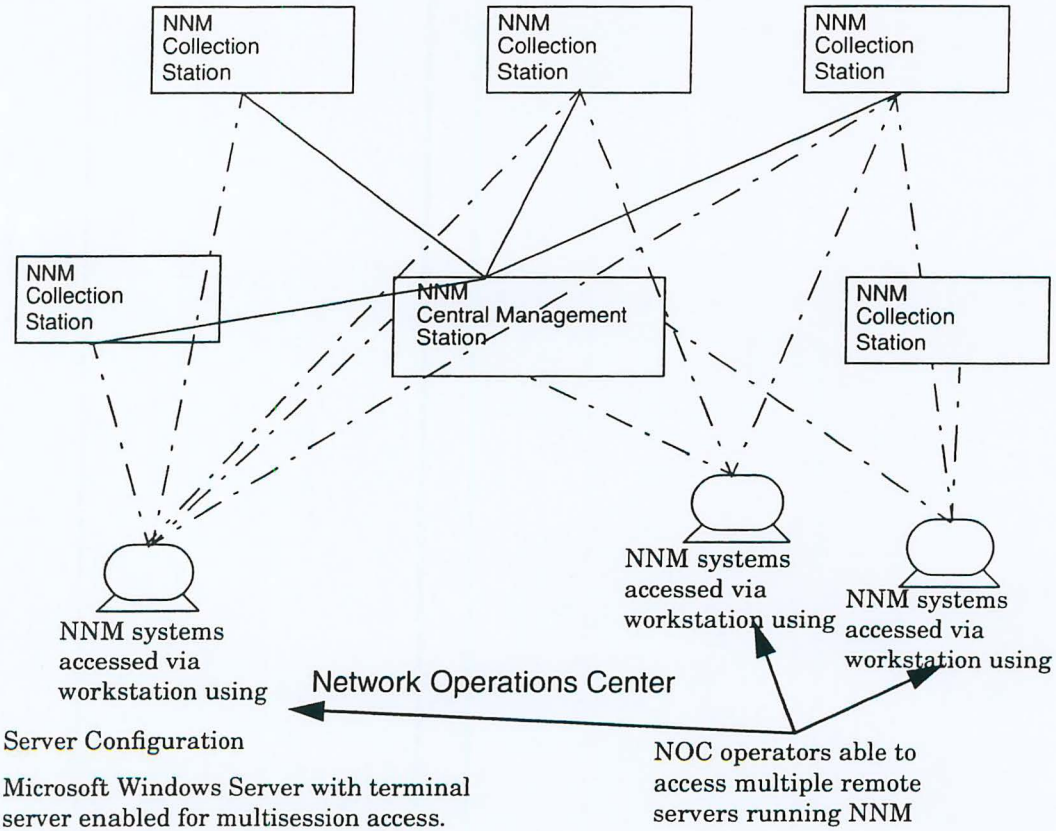
RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1301
3740
Doc:

Accessing Multiple NNM Stations From Multiple Terminal Server Clients

In this configuration, (Figure 2-11) a central Network Operations Center (NOC) is responsible for monitoring the entire network. The network management architecture is constructed of multiple Windows servers running NNM configured as collection stations, each collection station forwards information to a central NNM management station. The NOC operators are responsible for monitoring the health of the network.

The Terminal Server Client enables operators to access multiple NNM stations and to monitor different segments of the entire network from a single workstation. Operators can open multiple NNM sessions on each NNM station to view more than one map. Operators with administrator privileges can remotely start and stop NNM processes, run NNM database backups, and install NNM patches.

Figure 2-11 **Multiple NNM Stations Accessed by Multiple Terminal Server Clients**



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1302
3740
Doc:

3 Strategies for Deploying Network Node Manager

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1303
3740
Doc:

This chapter contains guidelines and ideas for deploying an HP OpenView Network Node Manager (NNM) solution that meets your goals and fits well with your organization.

The purpose of this chapter is to help you understand some of the reasonable models you can use as you plan your network management solution, and some criteria you can use to select a model.

It includes general approaches and general tips to help you succeed. With this knowledge, you will be able to better plan and implement your distributed, scalable network management solution.

NOTE

The information in this chapter is not introductory; readers are assumed to have read the previous chapters. Readers are also assumed to be conversant with NNM's key features for network monitoring, data collection, event handling, and so on. This includes a functional understanding of some key elements in non-distributed NNM, including `ovw`, `ipmap`, `ovtopmd`, and `netmon`. See *Managing Your Network with HP OpenView Network Node Manager* for details about these key services (background processes on UNIX systems) in Network Node Manager.

The remaining chapters and appendices contain specific configuration procedures to use with the scaling and distribution features of NNM.

Planning the Right Approach

Now that you understand Network Node Manager's scalable and distributable features, your questions naturally turn to issues like:

- "What should I *do* with all this?"
- "Can I just ignore NNM's scalability features for now? Should I?"
- "How would I employ distribution and scalability on a massive scale?"
- "What makes sense in my organization?"

You have a wide range of choices in your deployment of NNM. The simplest choice, and one that will make sense to some, is to use none of the scalability features at all. Others, who manage large, dispersed networks, will elect to scale up their use of NNM to deal with that large environment. Still others will find that a mix of some scalability features meets their requirements.

You can combine several different models as you plan your strategy. Each fits well with a particular set of goals. Your choice of approach will be driven, in large measure, by the nature of your organization and the problems you are solving with your network management solution.

Remember as you plan that you are never "locked-in" to one strategy; as your organization changes, you can adapt your use of NNM to keep up with those changes.

Organizations differ in many ways. Organizational variables to consider as you begin planning your deployment of NNM include:

Size The needs of a small organization, with perhaps a few hundred nodes, are very different from the needs of a corporate campus where you may have thousands or tens of thousands of networked objects. The networks in larger organizations are inevitably larger and more complex than in small organizations. Consequently, the larger the organization, the stronger are the reasons to use more of the scalability features of NNM.

Structure Some organizations, like the military, have clear hierarchies of authority and reporting. Others, like universities, may consist of looser affiliations between

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1304
Doc: 3740

cooperating but largely autonomous groups. These structural differences will have a significant effect on how network management is conducted.

Geography Some organizations, like a hospital, are geographically compact but require reliable network management. Within the confines of the hospital, NNM may have few requirements for scaling. But suppose that hospital is part of a medical services company; the central site, located thousands of miles away, may want to perform network management functions in *all* their many hospitals. Then issues of distribution and scalability are very important.

Trends The network that supports an organization is in a constant state of change. Yet it is important to understand general trends in how a network is evolving: is it stable? is it becoming more geographically dispersed? bigger? more expensive to manage? You will want your network management plans to account, as best you can, for the trends in your network.

General Considerations about Scalability and Distribution

The following general points are useful when planning your deployment of NNM. Margin notes summarize key concepts from the adjoining text.

Limits to netmon affect the maximum number of nodes you can monitor.

Due to the nature of ICMP pings, the `netmon` service (background process on UNIX systems) has limits to the amount of polling it can perform in a given period of time. You can maximize the number of nodes the `netmon` service can handle (while maintaining a consistent five-minute status polling cycle) by increasing the polling interval, especially for less important nodes. See "Configuring SNMP" in *Managing Your Network with HP OpenView Network Node Manager* for details on how to set special polling intervals. For more current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide.*

You may also want to take advantage of interface managed-state automation, as described in "Interface Managed-state Automation" on page 74.

2088
21

If the environment you want to manage has more nodes than you can monitor efficiently with a single netmon service, you will want to have another netmon service, in the form of another collection station, to off-load some of the polling work from the management station.

WAN performance also limits remote monitoring.

A WAN link introduces propagation delays that compound the above issue. That means that if your environment is split, with part of it accessible via LAN and the rest via WAN, the actual limit of managed nodes for a netmon service will be less than the limit stated above. How much less depends on the proportion of nodes on the LAN link vs. on the WAN link. In general, you will want to avoid monitoring nodes over a WAN link, unless you have only a few nodes at the remote site, or the node there are unimportant, and can receive infrequent polling.

In some circumstances, however, remote monitoring is necessary. As a rule-of-thumb, if a netmon service is monitoring remote sites, reduce the number of nodes it handles by one-tenth for each remote site. Thus, if a collection station is monitoring, say, 3 remote sites, you would expect it to handle up to 1400 nodes, rather than 2000.[1] The calculation for this estimate is as follows: 2000 - ((0.1 x 2000) x 3) = 1400.

In addition, remote monitoring via a WAN has very high operating costs in network traffic compared to the operating cost of monitoring via a remote collection station. Each status and configuration poll and response would have to cross the link, rather than simply any topology changes.

Take advantage of NNM wherever you can.

Given the low performance of WAN links, you can always achieve higher NNM performance by using a collection station for remote (WAN) nodes.

Since scalability is part of every NNM station (including NNM 250), it makes excellent sense to take advantage of NNM wherever it exists in your network. For example, you might have a "hidden" NNM station at a remote site, running NNM as the basis for another application like HP OpenView Operations. Consider using it as a collection station.

If your remote site has no NNM installation, you may want to install a collection station if you have perhaps fifty or more nodes to be monitored; NNM 250 might be a good choice for a small remote site. As an alternative, you could have a collection station located at one remote site, and monitoring multiple other remote sites.

1. Again, this estimate assumes that reliable 5-minute polling of all nodes is required.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1305
3740
Doc:



The final layout of your solution will depend at least in part on an analysis of the costs involved with each alternative you consider.

Ensure that you can always contact your collection stations.

Relying on a remote station for network management carries certain risks, but that risk can be driven down or eliminated.

As an example, suppose some collection station is your sole source of information for a part of your network, and the main gateway between the management station and that collection station goes down. By default, it takes up to twenty minutes before a "Collection Station Critical" event is generated, and an event confirmation popup dialog is presented to the operator. The nodes affected by the failure are *not* marked "Unknown".[2]

You can diminish the likelihood and effect of such a situation in three ways.

- First, arrange to have overlapping management domains or failover coverage, particularly for key connection nodes between the management station and collection stations.
- Second, make contingency arrangements that allow alternative communication paths to the collection station. You can establish redundant routes to the collection station via multiple gateways, or by adding a direct link from the manager to the collection station if that is possible. Consider lower-cost approaches that may have lower (but still acceptable) performance in an emergency.

  Third, use HP Service Guard for your management and/or collection stations.

Use as many collection stations as you can efficiently manage.

The more collection stations you have, the smaller the impact of temporarily losing any one of them, and the easier it is to roll management of that region to a different collection station. Within the limits of your ability to configure and manage collection stations, use as many collection stations as possible to ensure redundancy and off-load polling. For more current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide.*

2. See the note about `ovrepld`'s periodic status checks in "How Distributed Internet Discovery and Monitoring Works" on page 49.

Consider the flexibility of NNM 250

The NNM 250 product is limited to managing 250 nodes per license, but you can purchase multiple licenses to increase that number incrementally. Check current pricing to decide if multiple NNM 250 licenses are preferable to a full NNM product in your situation. NNM 250 can act as a collection station for multiple management stations, but cannot receive data from other collection stations.

Partition your Internet submap to reduce the visual complexity

Because it is feasible to manage many thousands of nodes, your internet submap may become densely populated, and difficult to work with. You can solve this problem by creating Partitioned Internet submaps to create reasonable groups of nodes. See "Partitioned Internet submap" in the index of *Managing Your Network with HP OpenView Network Node Manager* for details.

NOTE Be sure to consult the latest version of the *HP OpenView Network Node Manager Performance and Configuration Guide* for more information about configuring NNM in large environments.

General Strategies for Deployment

This section gives a few general pointers on how to deploy a distributed network management solution in your organization.

Plan ahead

Create a master plan for your organization that substantially outlines your goals for network management distribution and scaling. Keep in mind that your plan will continue to evolve along with your network.

Network planners, operations managers, and HP OpenView administrators need to collaborate in the planning process. They each bring a unique perspective, and getting early and continuing consensus important to the success of the project.

Describe and diagram the current state of your network management solution. Do the same for the final state you intend to achieve. Work together to identify each step that will be needed to migrate to the new arrangement.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1306
Doc: 3740

Start small You don't have to implement every aspect of your final plan all at once. Begin by setting up just one piece of the final picture.

You might choose to implement on-demand submaps on a management console. Or, you might decide to set up one collection station to see how that goes. Choose something that makes sense in your final plan, implement it, and then test it thoroughly before you proceed.

Go slowly Add more small pieces of your final plan one at a time. As you go, keep testing and rechecking your implementation to ensure that you are obtaining the results you want.

Be particularly attentive to your filters. Carefully designed and implemented filtering can be central to the effectiveness of your solution, and the set of filters provided in the default filter file will be useful to many people. Those who need to design other filters should be aware that creating filters can be complicated, and requires considerable attention to detail.

Also, review your polling intervals (under the menu item `Options:SNMP Configuration`). Poll your most important nodes more often (for example, every 3 minutes) than your less important nodes (for example, every 15 or 30 minutes). This will help you maximize the benefits of scalability.

Keep records Maintaining a large network management solution is not trivial. Along with the planning documents, keep records of what steps have been taken and when. Note any issues that came up with a step, and, more importantly, the resolution of those issues. This "paper trail" can be useful in the event that you want to roll back to an earlier configuration for troubleshooting or re-engineering your distribution scheme.

Backup your system NNM pauses all services yet queues information coming in from collection stations, so you can backup your database without missing any information. Refer to *Managing Your Network with HP OpenView Network Node Manager* for more information.

2084
21

Deployment Strategies for NNM

You have a number of choices about which of the scalability features of NNM you want to use, and to what degree you want to use them. This section describes several models of deployment to help you understand some alternatives to consider as you put scalable NNM into operation.

The following models are considered in this chapter:

- Fully centralized
- Centralized hierarchical
- Hierarchical
- Cooperative independent

NOTE

This chapter uses the above models to show how different organizational structures can be reflected in the deployment of network management within the organization. The deployment models in this chapter are not, by any means, the only way to convey the ideas presented here. This can not be overemphasized. Few organizations, if any, will use one of these models in a pure form. As you read this section, you are encouraged to look for ideas and approaches that can be applied in some part of your own organization. It can be helpful to imagine that the strategies in this section apply to very small parts of your overall network management solution. For example, a management station that has a hierarchical relationship to one collection station might simultaneously have a cooperative relationship with another management station.

Use of Scalability Features in NNM Deployment

All of these features are available to you in any way you choose to deploy NNM. The following table shows the most common scalable features used in each type of NNM scenario.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls: Nº 1307
3740
Doc:

Table 3-1 Scalability Features in Use Models

Scalability Feature	Centralized page 92	Centralized/ Hierarchical page 95	Hierarchical page 98	Cooperative page 103
Scalable Product Structure	X	X	X	X
Distributed Collection Stations, page 48		X	X	X
Management Consoles, page 70	X	X	X	X
Network Presenter web GUI, *Managing Your Network with HP OpenView Network Node Manager*,	X	X	X	X
On-Demand Submaps, page 64	X	X	X	X
Discovery Filtering, page 40	X	X	X	X
Topology Filtering from Collection Station to Management Station, page 41			X	X
Map Filtering for Operators, page 42	X	X	X	X
Event Forwarding, page 59		X	X	X
Threshold Event Forwarding, page 59		X	X	X
High Availability - Service Guard, page 50	X	X	X	X

2087

Table 3-1 Scalability Features in Use Models (Continued)

Scalability Feature	Centralized page 92	Centralized/ Hierarchical page 95	Hierarchical page 98	Cooperative page 103
High Availability - Failover with Failover Filtering, page 52		X	X	X
High Availability - Overlapping Domains, page 55			X	X

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1308
3740
Doc:

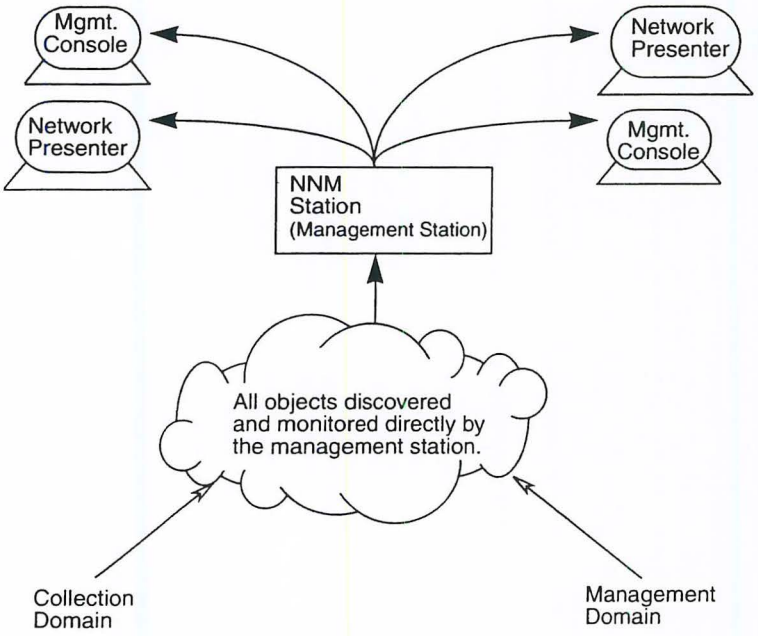
Fully Centralized Management

In a fully centralized network management scheme, one management station performs all monitoring and data collection functions for a whole management domain. There is little or no remote network management hardware or personnel. The primary focus is probably network management, with primary attention to the main connectors, like bridges, hubs, and routers.

Users of non-distributed network management products (including early versions of Network Node Manager) naturally use this model, since it is the only strongly supported model available. In fact, for many situations, a fully centralized usage of NNM is a highly functional and reasonable choice. Even in this model, scalability can be very useful.

Figure 3-1 illustrates a fully centralized network management scheme.

Figure 3-1 Fully Centralized Management Model



Most users of this feature will start with submaps set to be persistent at the `Internet Level` (as in Figure 2-7), and set it to lower levels only to improve submap-opening performance. This is typically necessary only when the higher-level submaps are densely populated.[27]

If you want to reset the on-demand submap feature to its default, use the `IP Map Configuration` dialog box in NNM to set submap persistence to `Unset`. On Windows operating systems, `Unset` sets the persistence level to `Internet Level`. On UNIX systems, `Unset` sets the persistence level to `All Levels`.

With on-demand submaps enabled at any level, most NNM features and operations work as they always have. Locate operations and IP status propagation, in particular, are not limited to what is currently in memory. Both functions work across all submaps, regardless of whether they are persistent or transient.

In cases where a located item is not yet in memory, the necessary submap is created, on-demand, if and when the user opens that submap from the locate dialog box.

Transient Submaps and the Submap List Dialog

The only feature that changes its behavior when the on-demand feature is enabled, is the `Submaps in Map` dialog box. Only submaps that are currently in memory (that is, either persistent, or transient but currently in memory) can appear in the `Submaps in Map` dialog box.[28]

In other words, when the on-demand submap feature is enabled, submaps that are not presently in memory are not present in the `Submaps in Map` list. This behavior may alter the usefulness of the `Submaps in Map` dialog box, depending on the expectations of the operator.

To reduce the possibility of operator confusion when the on-demand submap feature is enabled, you may wish to remove the following menu item (which opens the `Submaps in Map` dialog box):

```
Map:Submap->Open
```

27. See also the "Caution" block on "Configuring Management Consoles" on page 109.
28. See the online help for more information about this dialog box.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1309
Doc: 3740

See *Managing Your Network with HP OpenView Network Node Manager* for information about how to remove a menu item.

Persistence Filtering

Unlike the filters described earlier, the purpose of persistence filtering is not to reduce the amount of unnecessary management data in the data stream. Instead, the purpose of persistence filtering is to let some older applications that are not inherently compatible with the on-demand submap feature operate normally when the on-demand submap feature is enabled.

NOTE This is probably not an issue on Windows operating systems, since there are few "older" applications. However, some third-party developers may port their older UNIX system applications without changes.

Suppose an application has been created with the implicit assumption that the object or objects it is interested in are always available in memory. Such an application may fail or exhibit unstable behavior if the object it needs resides in a transient submap, and is thus not in memory at all times.

For example, a vendor you use may have developed an application that adds statistics component symbols under the router symbols created by the `ipmap` service. Such an application may assume that routers are part of the map (that is, present in memory) as soon as they are discovered. The on-demand feature, when enabled, invalidates that assumption.

A persistence filter can provide backwards compatibility for this type of application. The necessary persistence filter for the example application passes all routers. Then any submap that contains a router is made persistent, so that the expectation of the application is met.

A persistence filter tells the `ipmap` service that any submap containing an object that passes the filter should be made into a persistent submap. The object will then be in memory, as the application expects.

Persistence filters are set-defining type filters. A persistence filter is automatically applied to existing map and object data to determine which submaps must be persistent. When you change a persistence filter, all the objects currently in the topology database are reevaluated to see if

2104

they pass the new filter. Submaps containing objects that pass the new filter are made persistent. Submaps that do not contain such objects are made transient if they are below the current persistence level. [29]

Comparing Map Filters and Persistence Filters

A persistence filter is different from a map filter. A map filter specifies a subset of the topology data that is allowed on the map. The persistence filter states which objects should be made persistent in memory; those objects are made persistent by making the submaps they reside on persistent.

You can think of this as a two step process. First, the map filter passes a set of objects that are allowed to be present on the map. Then the persistence filter tests these objects to see which, if any, must be persistent in memory.

No matter what the persistence filter specifies, the user still has access to all of the objects that passed through the map filter.

When an object is found to meet the criteria in the persistence filter, all submaps containing that object are made persistent. That is, a submap is made persistent if it contains even one persistent object; it might also contain objects that do not meet the persistence specification criteria. In addition, the child submap of the persistent object is also made persistent.

Because persistence and map filters are both set-defining filters, if you change either for a given map (via the `IP Map Configuration` dialog box; see the online help for details), the `ipmap` service recalculates which submaps should be persistent. This might take a long time for larger databases.[30]

29. See "On-Demand Submaps" on page 64 for more details on persistence filtering. See "Specifying a Persistence Filter" on page 124 for configuration information.
30. See also "Map Filtering" on page 42.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 1310
Doc: 3740

Management Consoles

Distribution of management consoles is done via NFS (or Windows operating system file sharing) mounting of the map database and the appropriate configuration files, and by then using the distributed RPC capability of the object database service, ovwdb, the topology database, and the event system.

Figure 2-8 is a diagram of the resulting services, and where they are located. As shown, each management console actually runs the user-specific ovw-related services. The management station keeps the common databases, and runs the services (background processes on UNIX systems) common to all users.

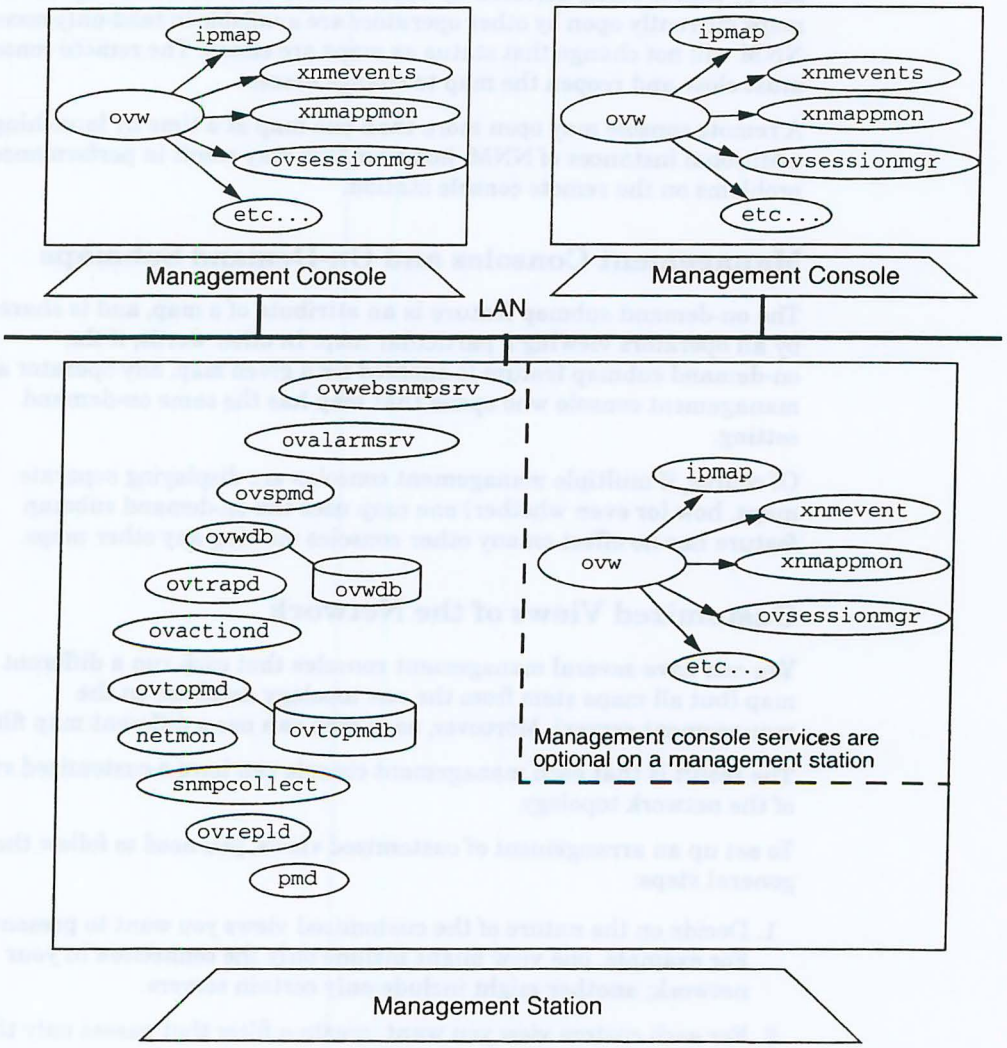
This relieves the management station of a significant demand for its resources (memory and CPU), since otherwise each operator would have independent copies of these services executing on the management station.

Relocating the ovw-related services allows the management station to apply more of its resources to network management and monitoring activities, and less to supporting the operators.

The object database remains centrally located on the management station, and is accessed by the management consoles over the network sockets. In addition to the various ovw-related services that communicate with the NNM services via socket connections, the map database and configuration files use NFS (or Windows operating system) file sharing.

NOTE Management consoles are *not* the same as NFS diskless clients. NFS diskless is an operating system concept. As described above, the distribution mechanism for management consoles uses NFS and sockets.

Figure 2-8 Management Consoles



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1311
3740
Doc:

Operators can each have their own maps. If, on the other hand, they share a map, only the first operator to open the map can edit it; others have read-only access. When using remote console into a management server that is being accessed by other remote or local console operators, maps currently open by other operators are available in read-only access. NNM will not change that status as maps are closed. The remote console must close and reopen the map to change access.

A remote console may open more than one map at a time by launching additional instances of NNM, however, this may result in performance problems on the remote console station.

Management Consoles and On-Demand Submaps

The on-demand submap feature is an attribute of a map, and is shared by all operators viewing a particular map. In other words, if the on-demand submap feature is enabled for a given map, any operator at a management console who opens that map has the same on-demand setting.

Of course, if multiple management consoles are displaying separate maps, how (or even whether) one map uses the on-demand submap feature has no effect on any other consoles viewing any other maps.

Customized Views of the Network

You can have several management consoles that each run a different map (but all maps stem from the one topology database on the management server). Moreover, each map can use a different map filter.

The result is that each management console can have a customized view of the network topology.

To set up an arrangement of customized views, you need to follow these general steps:

1. Decide on the nature of the customized views you want to present. For example, one view might include only the connectors in your network; another might include only certain servers.
2. For each custom view you want, create a filter that passes only the objects you want visible in that custom view.[31]
3. At each management console, create a new map (`Map:New`), and apply the appropriate map filter for the operator at that console.

Management Consoles and X-Terminals

In principle, it is possible to run several X-terminal sessions from a management console, or directly from the management station. You might speculate that this would allow NNM to support more operators.

However, due to internal constraints, this approach *does not* allow the management server to support more operators. You should limit the number of operators per management station to avoid degrading the performance of the interface.

Attaching X-terminals to a management console might nevertheless have cost savings, if the management console host has sufficient CPU, memory, and disk space to support the X-sessions, and low cost X-terminals are available and suitable for the operators. The key services described earlier are still off-loaded from the management station to the management console.

31. See "Filters" on page 37 and Appendix A, The Filter Definition Language, for more information on creating filters.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1312
3740
Doc:

Interface Managed-state Automation

As you probably know, NNM lets you "unmanage" interfaces. NNM does not do status polling on unmanged interfaces, so setting interfaces to the Unmanaged state significantly lightens the load on the management station.

NNM lets you automatically manage or unmanage interfaces based on filters. Interface managed-state automation makes it easier to manage large environments, where frequently many discovered interfaces do not require active status polling.

Interface managed-state automation relys on a command (`ovautoifmgr`) that periodically sweeps through the topology and sets the managed state of interface objects according to rules in the managed-state configuration file (`ovautoifmgr.conf`).

Based on the rules in the configuration file, interfaces that do not need to be managed are put into the Unmanaged state. Interfaces which do need to be managed (and are not already) are put into the Managed state with their status set to `UNKNOWN`. Then `netmon` begins to monitor the interface's operational status and generate events.

The the `ovautoifmgr` command is not a continuously-running process. Instead, it is designed to be run periodically by a scheduling mechanism. It requires that `ovtopmd` be running.

For further information and instructions on using interface managed-state automation, refer to the `ovautoifmgr(1m)` and `ovautoifmgr.conf(4)` reference (man) pages.

Microsoft Terminal Server Access

You can connect to Network Node Manager (on a Microsoft Terminal Server) from a remote workstation through a Terminal Server Client. You can do any of the following:

- Install or upgrade NNM on the remote server.
- Perform administrative NNM functions such as backup/restore of NNM database.
- Open NNM and display the network map onto the local workstation.
- Start multiple Terminal Server Client sessions to the same remote NNM management station, open NNM in each session and display the network maps onto the local workstation.
- Start multiple Terminal Server Client sessions to different remote NNM management stations, open NNM on each NNM management station and display the network maps onto the local workstation.

The following examples provide a few of the possible implementation strategies available to network managers when running the NNM application on servers with the Microsoft Terminal Server features enabled.

Accessing a Single NNM Station From Multiple Terminal Server Clients

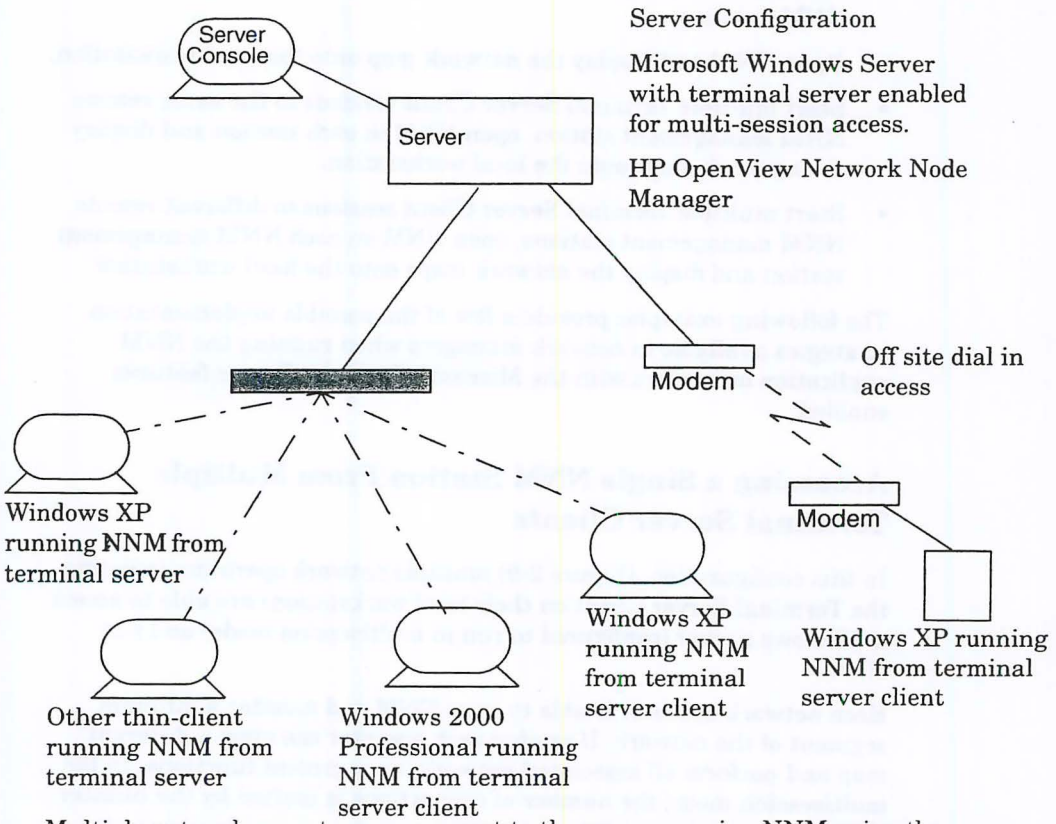
In this configuration, (Figure 2-9) multiple network operators (running the Terminal Server Client on their local workstation) are able to access a Windows Server (configured to run in multisession mode) and run NNM.

Each network operator is able to open NNM and monitor a different segment of the network. If needed each operator can open a different map and perform all associated network management functions. In the multisession mode, the number of connections is limited by the number

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1313
3740
Doc:

of client licenses available. Accounts with administrator privileges can be used to start and stop NNM processes, run NNM database backups, and install NNM patches.

Figure 2-9 Multiple Terminal Server Clients Accessing a Single NNM Station



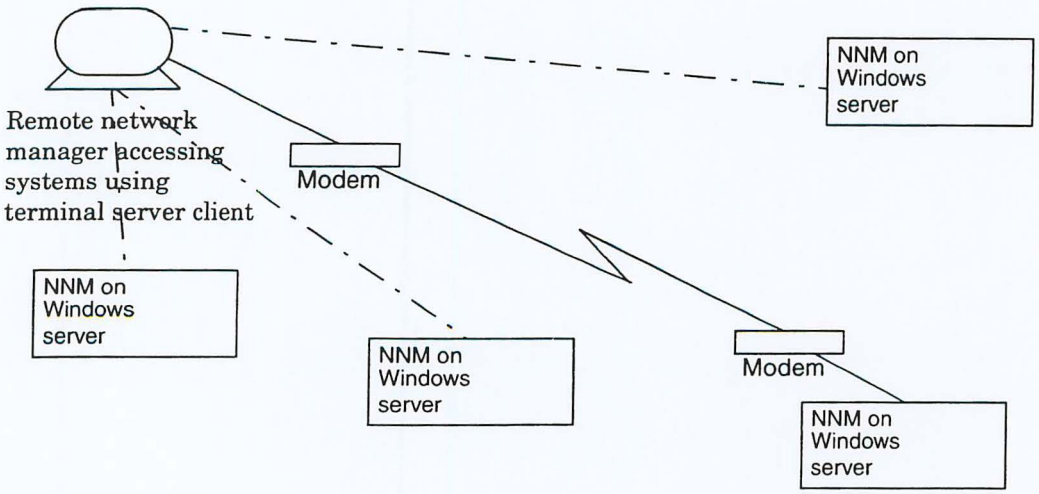
Multiple network operators can connect to the server running NNM using the terminal server client. The operators can open NNM maps and monitor the network segment from their local workstation.

Accessing Multiple NNM Stations From a Single Terminal Server Client

In this configuration, (Figure 2-10) a single network manager is able to access multiple Windows servers configured to run under Remote Administrator mode. The NNM application is installed on each Windows server. The remote network manager, using the Terminal Server Client, is able to connect to each remote system, monitor the network, and perform all network management functions. With this configuration a network manager has the ability to access and display multiple NNM sessions on their local workstation.

The remote administration mode limits the number of connections to the server (maximum of two) and only grants connections to accounts that have administrator privileges.

Figure 2-10 Accessing Multiple NNM Stations



Server Configuration

Microsoft Windows Server with terminal server enabled and installed as Remote Administrator mode.

HP OpenView Network Node Manager running on each server to manage the local network

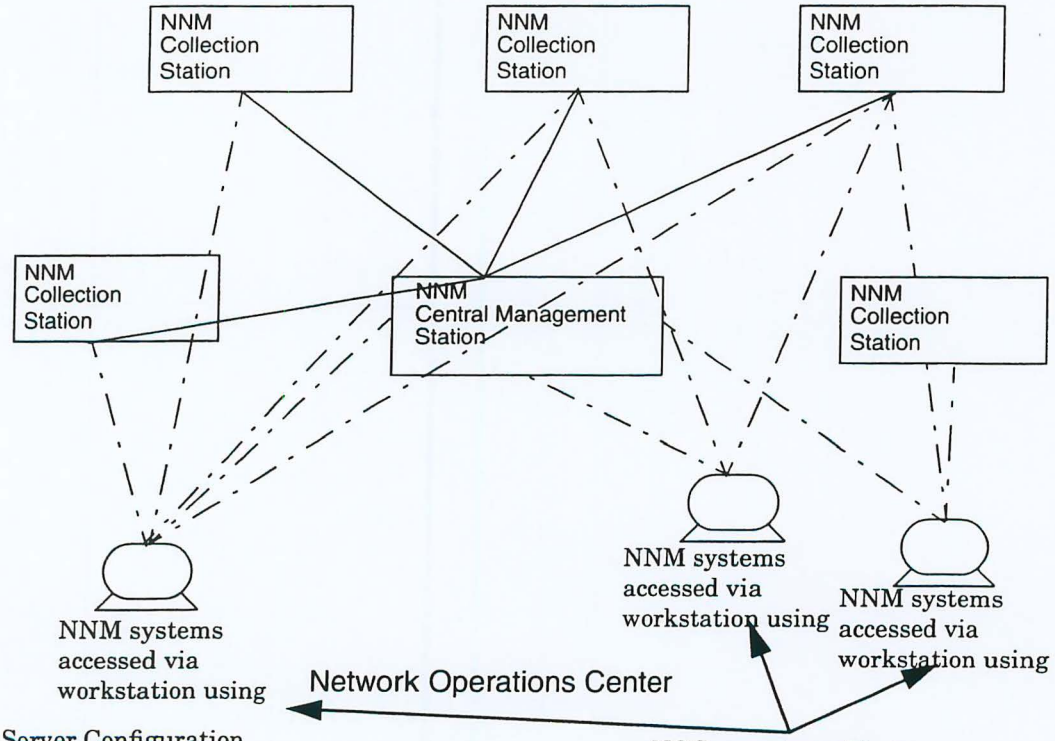
RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1314
3740
Doc:

Accessing Multiple NNM Stations From Multiple Terminal Server Clients

In this configuration, (Figure 2-11) a central Network Operations Center (NOC) is responsible for monitoring the entire network. The network management architecture is constructed of multiple Windows servers running NNM configured as collection stations, each collection station forwards information to a central NNM management station. The NOC operators are responsible for monitoring the health of the network.

The Terminal Server Client enables operators to access multiple NNM stations and to monitor different segments of the entire network from a single workstation. Operators can open multiple NNM sessions on each NNM station to view more than one map. Operators with administrator privileges can remotely start and stop NNM processes, run NNM database backups, and install NNM patches.

Figure 2-11 **Multiple NNM Stations Accessed by Multiple Terminal Server Clients**



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1315
3740
Doc:

3 Strategies for Deploying Network Node Manager

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1316
3740
Doc:



Strategies for Deploying Network Node Manager

This chapter contains guidelines and ideas for deploying an HP OpenView Network Node Manager (NNM) solution that meets your goals and fits well with your organization.

The purpose of this chapter is to help you understand some of the reasonable models you can use as you plan your network management solution, and some criteria you can use to select a model.

It includes general approaches and general tips to help you succeed. With this knowledge, you will be able to better plan and implement your distributed, scalable network management solution.

NOTE

The information in this chapter is not introductory; readers are assumed to have read the previous chapters. Readers are also assumed to be conversant with NNM's key features for network monitoring, data collection, event handling, and so on. This includes a functional understanding of some key elements in non-distributed NNM, including `ovw`, `ipmap`, `ovtopmd`, and `netmon`. See *Managing Your Network with HP OpenView Network Node Manager* for details about these key services (background processes on UNIX systems) in Network Node Manager.

The remaining chapters and appendices contain specific configuration procedures to use with the scaling and distribution features of NNM.

Planning the Right Approach

Now that you understand Network Node Manager's scalable and distributable features, your questions naturally turn to issues like:

- "What should I *do* with all this?"
- "Can I just ignore NNM's scalability features for now? Should I?"
- "How would I employ distribution and scalability on a massive scale?"
- "What makes sense in my organization?"

You have a wide range of choices in your deployment of NNM. The simplest choice, and one that will make sense to some, is to use none of the scalability features at all. Others, who manage large, dispersed networks, will elect to scale up their use of NNM to deal with that large environment. Still others will find that a mix of some scalability features meets their requirements.

You can combine several different models as you plan your strategy. Each fits well with a particular set of goals. Your choice of approach will be driven, in large measure, by the nature of your organization and the problems you are solving with your network management solution.

Remember as you plan that you are never "locked-in" to one strategy; as your organization changes, you can adapt your use of NNM to keep up with those changes.

Organizations differ in many ways. Organizational variables to consider as you begin planning your deployment of NNM include:

Size The needs of a small organization, with perhaps a few hundred nodes, are very different from the needs of a corporate campus where you may have thousands or tens of thousands of networked objects. The networks in larger organizations are inevitably larger and more complex than in small organizations. Consequently, the larger the organization, the stronger are the reasons to use more of the scalability features of NNM.

Structure Some organizations, like the military, have clear hierarchies of authority and reporting. Others, like universities, may consist of looser affiliations between

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1317
3740
Doc:

cooperating but largely autonomous groups. These structural differences will have a significant effect on how network management is conducted.

Geography Some organizations, like a hospital, are geographically compact but require reliable network management. Within the confines of the hospital, NNM may have few requirements for scaling. But suppose that hospital is part of a medical services company; the central site, located thousands of miles away, may want to perform network management functions in *all* their many hospitals. Then issues of distribution and scalability are very important.

Trends The network that supports an organization is in a constant state of change. Yet it is important to understand general trends in how a network is evolving: is it stable? is it becoming more geographically dispersed? bigger? more expensive to manage? You will want your network management plans to account, as best you can, for the trends in your network.

General Considerations about Scalability and Distribution

The following general points are useful when planning your deployment of NNM. Margin notes summarize key concepts from the adjoining text.

Limits to netmon affect the maximum number of nodes you can monitor.

Due to the nature of ICMP pings, the `netmon` service (background process on UNIX systems) has limits to the amount of polling it can perform in a given period of time. You can maximize the number of nodes the `netmon` service can handle (while maintaining a consistent five-minute status polling cycle) by increasing the polling interval, especially for less important nodes. See "Configuring SNMP" in *Managing Your Network with HP OpenView Network Node Manager* for details on how to set special polling intervals. For more current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide.*

You may also want to take advantage of interface managed-state automation, as described in "Interface Managed-state Automation" on page 74.

2088
21

If the environment you want to manage has more nodes than you can monitor efficiently with a single `netmon` service, you will want to have another `netmon` service, in the form of another collection station, to off-load some of the polling work from the management station.

WAN performance also limits remote monitoring.

A WAN link introduces propagation delays that compound the above issue. That means that if your environment is split, with part of it accessible via LAN and the rest via WAN, the actual limit of managed nodes for a `netmon` service will be less than the limit stated above. How much less depends on the proportion of nodes on the LAN link vs. on the WAN link. In general, you will want to avoid monitoring nodes over a WAN link, unless you have only a few nodes at the remote site, or the node there are unimportant, and can receive infrequent polling.

In some circumstances, however, remote monitoring is necessary. As a rule-of-thumb, if a `netmon` service is monitoring remote sites, reduce the number of nodes it handles by one-tenth for each remote site. Thus, if a collection station is monitoring, say, 3 remote sites, you would expect it to handle up to 1400 nodes, rather than 2000.[1] The calculation for this estimate is as follows: 2000 - ((0.1 x 2000) x 3) = 1400.

In addition, remote monitoring via a WAN has very high operating costs in network traffic compared to the operating cost of monitoring via a remote collection station. Each status and configuration poll and response would have to cross the link, rather than simply any topology changes.

Take advantage of NNM wherever you can.

Given the low performance of WAN links, you can always achieve higher NNM performance by using a collection station for remote (WAN) nodes.

Since scalability is part of every NNM station (including NNM 250), it makes excellent sense to take advantage of NNM wherever it exists in your network. For example, you might have a "hidden" NNM station at a remote site, running NNM as the basis for another application like HP OpenView Operations. Consider using it as a collection station.

If your remote site has no NNM installation, you may want to install a collection station if you have perhaps fifty or more nodes to be monitored; NNM 250 might be a good choice for a small remote site. As an alternative, you could have a collection station located at one remote site, and monitoring multiple other remote sites.

1. Again, this estimate assumes that reliable 5-minute polling of all nodes is required.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1318
3740
Doc:



The final layout of your solution will depend at least in part on an analysis of the costs involved with each alternative you consider.

Ensure that you can always contact your collection stations.

Relying on a remote station for network management carries certain risks, but that risk can be driven down or eliminated.

As an example, suppose some collection station is your sole source of information for a part of your network, and the main gateway between the management station and that collection station goes down. By default, it takes up to twenty minutes before a "Collection Station Critical" event is generated, and an event confirmation popup dialog is presented to the operator. The nodes affected by the failure are *not* marked "Unknown".[2]

You can diminish the likelihood and effect of such a situation in three ways.

- First, arrange to have overlapping management domains or failover coverage, particularly for key connection nodes between the management station and collection stations.
- Second, make contingency arrangements that allow alternative communication paths to the collection station. You can establish redundant routes to the collection station via multiple gateways, or by adding a direct link from the manager to the collection station if that is possible. Consider lower-cost approaches that may have lower (but still acceptable) performance in an emergency.

  Third, use HP Service Guard for your management and/or collection stations.

Use as many collection stations as you can efficiently manage.

The more collection stations you have, the smaller the impact of temporarily losing any one of them, and the easier it is to roll management of that region to a different collection station. Within the limits of your ability to configure and manage collection stations, use as many collection stations as possible to ensure redundancy and off-load polling. For more current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide.*

2. See the note about `ovrepld`'s periodic status checks in "How Distributed Internet Discovery and Monitoring Works" on page 49.

2086

Consider the flexibility of NNM 250

The NNM 250 product is limited to managing 250 nodes per license, but you can purchase multiple licenses to increase that number incrementally. Check current pricing to decide if multiple NNM 250 licenses are preferable to a full NNM product in your situation. NNM 250 can act as a collection station for multiple management stations, but cannot receive data from other collection stations.

Partition your Internet submap to reduce the visual complexity

Because it is feasible to manage many thousands of nodes, your internet submap may become densely populated, and difficult to work with. You can solve this problem by creating Partitioned Internet submaps to create reasonable groups of nodes. See "Partitioned Internet submap" in the index of *Managing Your Network with HP OpenView Network Node Manager* for details.

NOTE Be sure to consult the latest version of the *HP OpenView Network Node Manager Performance and Configuration Guide* for more information about configuring NNM in large environments.

General Strategies for Deployment

This section gives a few general pointers on how to deploy a distributed network management solution in your organization.

Plan ahead

Create a master plan for your organization that substantially outlines your goals for network management distribution and scaling. Keep in mind that your plan will continue to evolve along with your network.

Network planners, operations managers, and HP OpenView administrators need to collaborate in the planning process. They each bring a unique perspective, and getting early and continuing consensus important to the success of the project.

Describe and diagram the current state of your network management solution. Do the same for the final state you intend to achieve. Work together to identify each step that will be needed to migrate to the new arrangement.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1319
Doc 3740

Start small You don't have to implement every aspect of your final plan all at once. Begin by setting up just one piece of the final picture.

You might choose to implement on-demand submaps on a management console. Or, you might decide to set up one collection station to see how that goes. Choose something that makes sense in your final plan, implement it, and then test it thoroughly before you proceed.

Go slowly Add more small pieces of your final plan one at a time. As you go, keep testing and rechecking your implementation to ensure that you are obtaining the results you want.

Be particularly attentive to your filters. Carefully designed and implemented filtering can be central to the effectiveness of your solution, and the set of filters provided in the default filter file will be useful to many people. Those who need to design other filters should be aware that creating filters can be complicated, and requires considerable attention to detail.

Also, review your polling intervals (under the menu item `Options:SNMP Configuration`). Poll your most important nodes more often (for example, every 3 minutes) than your less important nodes (for example, every 15 or 30 minutes). This will help you maximize the benefits of scalability.

Keep records Maintaining a large network management solution is not trivial. Along with the planning documents, keep records of what steps have been taken and when. Note any issues that came up with a step, and, more importantly, the resolution of those issues. This "paper trail" can be useful in the event that you want to roll back to an earlier configuration for troubleshooting or re-engineering your distribution scheme.

Backup your system NNM pauses all services yet queues information coming in from collection stations, so you can backup your database without missing any information. Refer to *Managing Your Network with HP OpenView Network Node Manager* for more information.

2084
21

Deployment Strategies for NNM

You have a number of choices about which of the scalability features of NNM you want to use, and to what degree you want to use them. This section describes several models of deployment to help you understand some alternatives to consider as you put scalable NNM into operation.

The following models are considered in this chapter:

- Fully centralized
- Centralized hierarchical
- Hierarchical
- Cooperative independent

NOTE

This chapter uses the above models to show how different organizational structures can be reflected in the deployment of network management within the organization. The deployment models in this chapter are not, by any means, the only way to convey the ideas presented here. This can not be overemphasized. Few organizations, if any, will use one of these models in a pure form. As you read this section, you are encouraged to look for ideas and approaches that can be applied in some part of your own organization. It can be helpful to imagine that the strategies in this section apply to very small parts of your overall network management solution. For example, a management station that has a hierarchical relationship to one collection station might simultaneously have a cooperative relationship with another management station.

Use of Scalability Features in NNM Deployment

All of these features are available to you in any way you choose to deploy NNM. The following table shows the most common scalable features used in each type of NNM scenario.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1320
Doc: 3740

Table 3-1 Scalability Features in Use Models

Scalability Feature	Centralized page 92	Centralized/ Hierarchical page 95	Hierarchical page 98	Cooperative page 103
Scalable Product Structure	X	X	X	X
Distributed Collection Stations, page 48		X	X	X
Management Consoles, page 70	X	X	X	X
Network Presenter web GUI, *Managing Your Network with HP OpenView Network Node Manager*,	X	X	X	X
On-Demand Submaps, page 64	X	X	X	X
Discovery Filtering, page 40	X	X	X	X
Topology Filtering from Collection Station to Management Station, page 41			X	X
Map Filtering for Operators, page 42	X	X	X	X
Event Forwarding, page 59		X	X	X
Threshold Event Forwarding, page 59		X	X	X
High Availability - Service Guard, page 50	X	X	X	X

2087

Table 3-1 Scalability Features in Use Models (Continued)

Scalability Feature	Centralized page 92	Centralized/ Hierarchical page 95	Hierarchical page 98	Cooperative page 103
High Availability - Failover with Failover Filtering, page 52		X	X	X
High Availability - Overlapping Domains, page 55			X	X

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1321
3740
Doc:

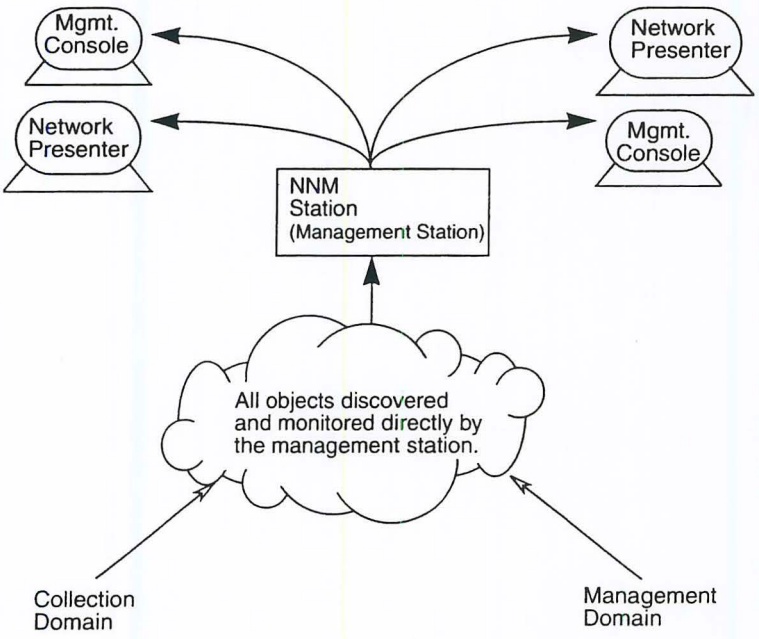
Fully Centralized Management

In a fully centralized network management scheme, one management station performs all monitoring and data collection functions for a whole management domain. There is little or no remote network management hardware or personnel. The primary focus is probably network management, with primary attention to the main connectors, like bridges, hubs, and routers.

Users of non-distributed network management products (including early versions of Network Node Manager) naturally use this model, since it is the only strongly supported model available. In fact, for many situations, a fully centralized usage of NNM is a highly functional and reasonable choice. Even in this model, scalability can be very useful.

Figure 3-1 illustrates a fully centralized network management scheme.

Figure 3-1 Fully Centralized Management Model

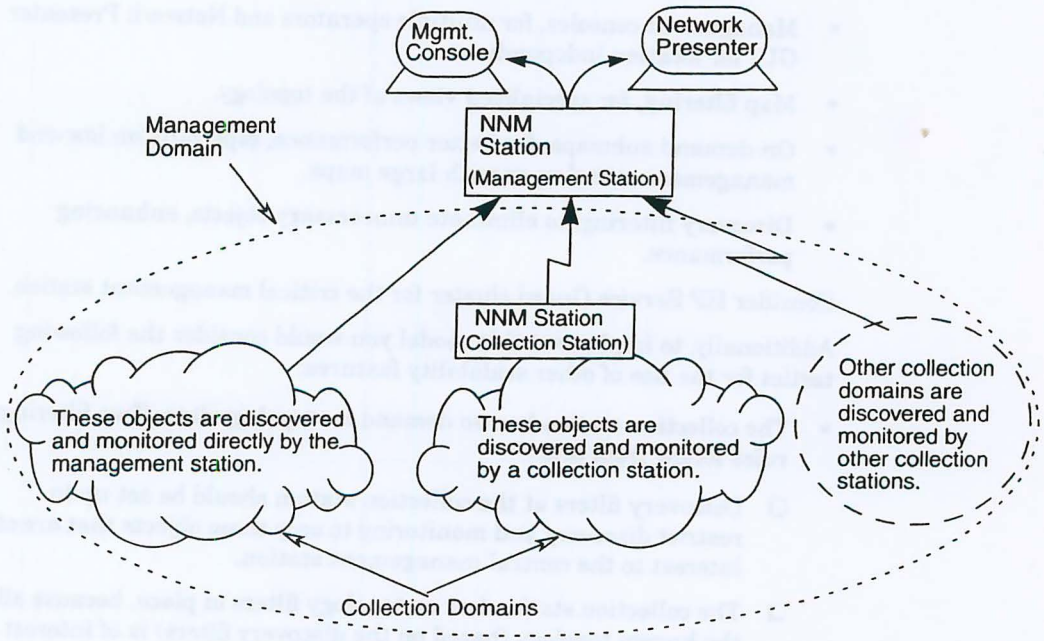


Centralized-Hierarchical Management

Sometimes, one primary group has responsibility for a large network management environment. The centralized-hierarchical model involves a network that for some reason is not suitable for monitoring by a fully centralized model. The environment may be too large,[5] or you may have sizeable remote sites where network management support is minimal.

In Figure 3-2, all operators are located at the management station; this is the main characteristic of a centralized-hierarchical situation.

Figure 3-2 Centralized-Hierarchical Management Model



5. See "General Considerations about Scalability and Distribution" on page 84.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1322
3740
Doc:

While the management station in the diagram has its own collection domain, it keeps a hierarchy of several remote collection stations that provide distributed network management services. Human support for network management at the remote sites is minimal and probably does not extend to operating NNM from a console.

Implementation Tactics

Implementing a centralized-hierarchical management model is, like all distributed models, more complex than a simple centralized approach.

All of the scalability features mentioned for the fully centralized model are still applicable in exactly the same way, and for the same purposes, as for the centralized-hierarchical model:[6]

- Management consoles, for multiple operators and Network Presenter GUI for location independence.
- Map filtering, for specialized views of the topology.
- On-demand submaps, for better performance, especially on low-end management consoles, or with large maps.
- Discovery filtering, to eliminate unnecessary objects, enhancing performance.

Consider HP Service Guard cluster for the critical management station.

Additionally, to implement this model you would consider the following tactics for the use of other scalability features:

- The collection station has no demand for topology data. Two filtering rules follow from this:
  - Discovery filters at the collection station should be set up to restrict discovery and monitoring to only those objects that are of interest to the central management station.
  - The collection station has no topology filters in place, because all the known topology (based on the discovery filters) is of interest to the central management station.
- Configure collection station failover so that the management station can pick up for critical collection stations.

6. See "Filters" on page 37, "On-Demand Submaps" on page 64, and "Management Consoles" on page 70.

- You will probably want to forward all threshold events that you configure for the collection station. The most likely forwarding would be to the %REMOTE_MANAGERS_LIST%, so that any interested manager would receive the events.

  One potential exception to this rule would occur if you only want a local action performed for a particular threshold event, and no higher level attention to the matter.

- If you are dealing with a large environment and using the centralized-hierarchical model, you may want the collection stations (even though essentially unmanned) to perform remote trend data collection. You would then plan to pull that data to the central management station for merging, report generation, and analysis.[7]

Implications of Using Centralized-Hierarchical Management

The centralized-hierarchical model is somewhat more complex to deploy and maintain than the fully centralized model, because each collection station requires special configuration. However, it has many advantages for environments that are either geographically dispersed, or too large to monitor from a single station.

You can manage networks with up to about 25,000 devices (assuming one interface per device, on average), and roughly fifteen operators. Performance of the map in a large environment can be improved by using map filtering and on-demand submaps.

A centralized-hierarchical model (like a fully centralized approach) puts the management responsibilities (and expertise) in one location, which works well in some organizations.

If you have to monitor remote nodes over a WAN, and still want centralized network management, a centralized-hierarchical approach can reduce traffic on expensive WAN links. The risk is slightly higher, since you are relying on the remote collection stations for data.

Finally, in a large network, the overall performance of your network management solution is probably better, because you are not performing polling over the lower performance WAN links.

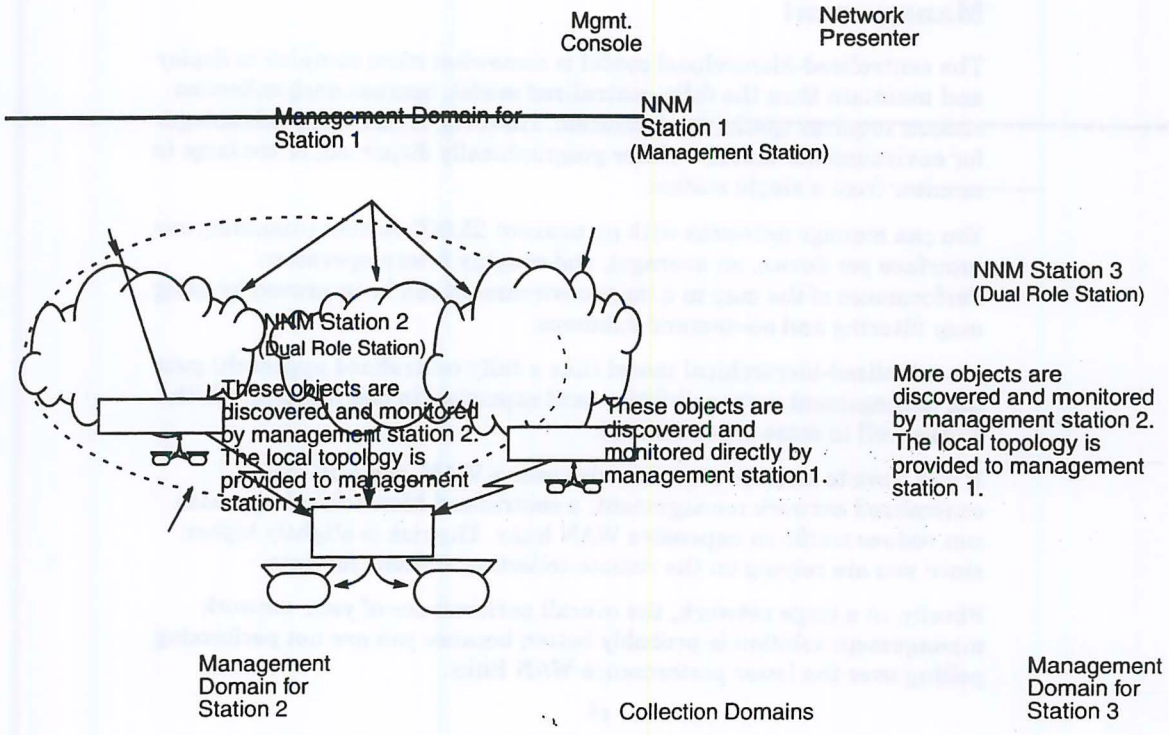
7. See the reference page in NNM online help (or the UNIX system manpage) for *ovcoltosql*.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1323
3740

Hierarchical Management

In many large organizations, a central group has broad responsibility for the network resources of the organization, usually for the major gateways and connecting infrastructure of the network (commonly called the network "backbone"). In the outlying sites, local network managers control the local configuration, usually including local connectivity, server availability, etc. This hierarchy of responsibility is reflected in the scheme illustrated in Figure 3-3, where NNM Stations are 2 and 3 are independent management stations, while also acting as collection stations for NNM Station 1.

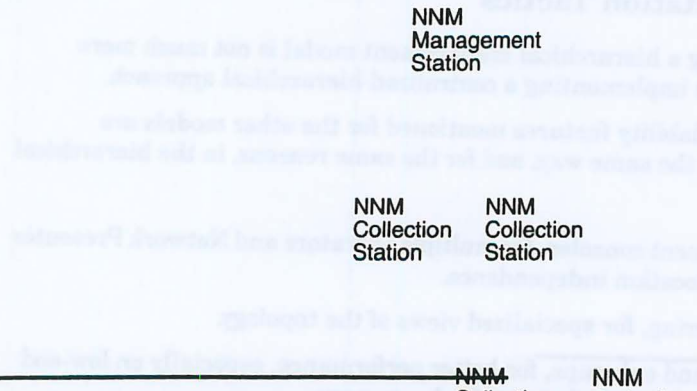
Figure 3-3 Hierarchical Management Model



While the management station in the diagram has its own collection domain, it keeps a hierarchy of several remote collection stations that provide distributed network management services. Human support for network management at the remote sites is minimal and probably does not extend to operating NNM from a console.

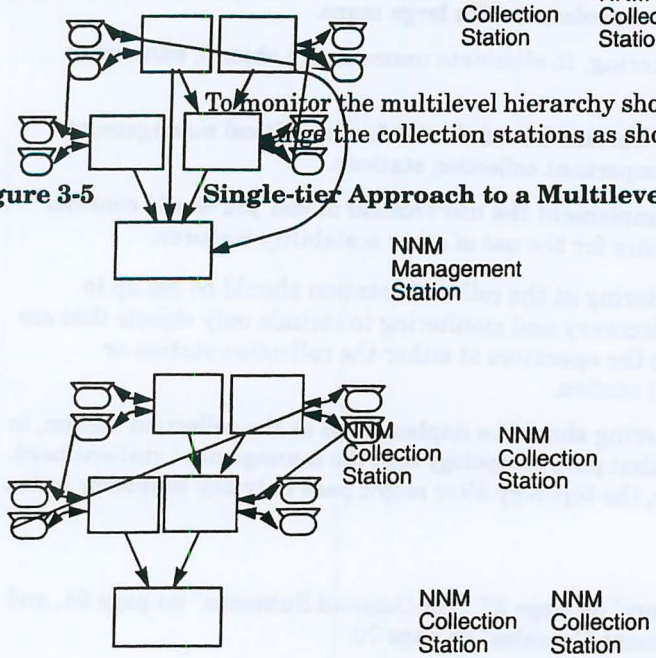
While multiple levels are possible in a hierarchical environment, Network Node Manager passes topology and status data only one level. That is, topology data received from a collection station can not be forwarded again. Only topology and status data that is derived from a local `netmon` service can be forwarded to remote managers.

Figure 3-4 Unsupported Multilevel Hierarchical Management



To monitor the multilevel hierarchy shown in Figure 3-4, you would have to change the collection stations as shown in Figure 3-5.

Figure 3-5 Single-tier Approach to a Multilevel Hierarchy



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1324
3740

In Figure 3-5, the top-level management station uses both the first- *and* second-tier collection stations directly, to obtain all the information it needs.

Topology filters at the second-tier must pass all the objects needed by either first-tier or top-level management stations, but the same would be true even if multiple-level management were possible.

Implementation Tactics

Implementing a hierarchical management model is not much more complex than implementing a centralized-hierarchical approach.

All of the scalability features mentioned for the other models are applicable in the same way, and for the same reasons, in the hierarchical model:[8]

- Management consoles, for multiple operators and Network Presenter GUI for location independence.
- Map filtering, for specialized views of the topology.
- On-demand submaps, for better performance, especially on low-end management consoles, or with large maps.
- Discovery filtering, to eliminate unnecessary objects, enhancing performance.

  Consider HP Service Guard cluster for the critical management station and important collection stations.

Additionally, to implement the hierarchical model you would consider the following tactics for the use of other scalability features:

- Discovery filtering at the collection station should be set up to restrict IP discovery and monitoring to include only objects that are of interest to the operators at either the collection station or management station.
- Topology filtering should be implemented at the collection station, to expose only that part of topology that the management stations need. For example, the topology filter might pass only key connector nodes.

8. See "Filters" on page 37, "On-Demand Submaps" on page 64, and "Management Consoles" on page 70.

- The interests of operators at the management stations and the collection stations may overlap on some objects. Map filtering can be cooperatively designed and implemented between the management stations and the collection stations, so that any overlap is considered and deliberate.
- Configure collection station failover so that the management station can pick up for critical collection stations.
- You might want to forward some threshold events that you configure on the collection station, most probably to the `%REMOTE_MANAGERS_LIST%`, so that all interested managers receive those events.

  Or, you might want to duplicate a MIB variable via a MIB expression. This lets you set two different thresholds on the value, one that triggers local action and one that triggers attention at the management station.

  Of course, some thresholds might be of local interest only, and not be forwarded to the managers.
- If you are dealing with a large environment and using the hierarchical model, you may want collection stations to perform remote trend data collection.

  You would then plan to pull that data to the central management station for merging, report generation, and analysis. The administrators at the remote site may also have local use for the same trend data, or a subset of it.[9]

Implications of Using the Hierarchical Management Model

The hierarchical management model takes full advantage of the benefits that scalability offers. On the other hand, it can be complex to deploy and maintain in a large environment.

9. See "Trend Data Collection in a Distributed NNM Solution" on page 28 for more information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1325
Doc: 3740

Implementing a fully hierarchical management scheme makes it possible to manage larger environments than any other approach. Such environments are often geographically dispersed, too large to monitor effectively from a single site, and staffed, at least some of the time, with network management personnel at the remote sites.

Performance of the maps at any management station can always be improved through map filtering and using on-demand submaps. Your experiences will depend on the resources you have available, and the performance tuning you implement.[10] For the most current test results and product performance information see the latest version of the HP OpenView NNM *Performance and Configuration Guide*.

A hierarchical model (unlike any centralized approach) disperses the management responsibilities and expertise across the organization. Failures at any point in the system are less likely to have wide ranging consequences.

A hierarchical approach can significantly cut traffic on costly WAN links.

Finally, in a large network, the overall performance of your network management solution is probably better this way than with any other approach, in part because situations that develop in the collection domain of the collection stations can be generally handled by the local operators.

10. See "General Considerations about Scalability and Distribution" on page 84 for ideas.

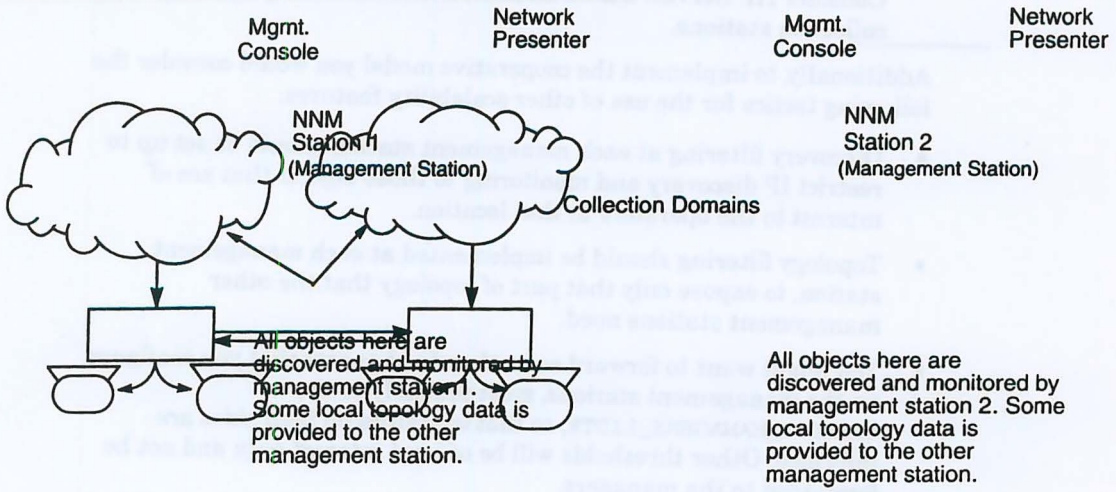
Cooperative Independent Management

In some situations, two largely independent sites need to share information at the boundaries of their management domains. Administrators at each site have primary responsibility for their part of the overall managed domain. This is shown in Figure 3-6.

In addition, these administrators are likely to have a strong interest in the major connecting nodes they share with other sites, in the primary servers at other sites, or in other key nodes or resources that reside in the domains of other sites.

This peer relationship may or may not reflect the organizational structure. You might choose this model because of the need for tight cooperation, even though one site is actually "higher" in the organizational hierarchy.

Figure 3-6 Cooperative Independent Management Model



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1326
3740
Doc:

Implementation Tactics

Implementing a cooperative management model is similar to implementing a hierarchical approach. In fact, cooperative management could be viewed as simply a variant of the hierarchical model, where each management station is, from the perspective of the other, just a subordinate collection station.

Again, all of the scalability features useful in the centralized model are still applicable in exactly the same way, and for exactly the same reasons, in the cooperative model:[11]

- Management consoles, for multiple operators and Network Presenter GUI for location independence.
- Map filtering, for specialized views of the topology.
- On-demand submaps, for better performance, especially on low-end management consoles, or with large maps.
- Discovery filtering at each management station can eliminate unnecessary objects, enhancing performance.
- Consider HP Service Guard cluster for critical management or collection stations.

Additionally, to implement the cooperative model you would consider the following tactics for the use of other scalability features:

- Discovery filtering at each management station should be set up to restrict IP discovery and monitoring to those objects that are of interest to the operators at that location.
- Topology filtering should be implemented at each management station, to expose only that part of topology that the other management stations need.
- You might want to forward some threshold events that you configure on the management stations, most probably to the `%REMOTE_MANAGERS_LIST%`, so that operators on both sides are informed. Other thresholds will be of local interest only, and not be forwarded to the managers.

11. See "Filters" on page 37, "On-Demand Submaps" on page 64, and "Management Consoles" on page 70.

- When using the cooperative independent model, you may want to collect trend data on the shared resources. Depending on the actual configuration of the resources, you may want one or all management stations to perform trend data collection. If multiple stations are collecting trend data, you might want to choose one to act as the central location for merging the data, report generation, and analysis. The administrators at each management site may also have local use for the same trend data.

Implications of Using the Cooperative Independent Model

The cooperative independent management model is very similar in technical complexity to a more purely hierarchical approach, and likewise requires that the sites cooperate in nontechnical ways as well. For example, scheduled downtime of critical or shared resources at one site should not come as a surprise to the other sites.

In implementing a cooperative independent management scheme, you can assume that each site has complete responsibility for local management of non-shared resources and objects.

A management station with a cooperative relationship to another management station can, at the same time, have a hierarchical relationship with one or more other collection stations.

The cooperative model acknowledges that management responsibilities and expertise are not centralized in the organization, and that unique skills and requirements exist at different sites. While a failure at one point in the system is unlikely to have wide ranging consequences, a local problem may get little attention from a remote site.

Finally, the overall performance of your network management solution is good, in part because situations that develop in the collection domains are generally handled locally.[12] Thus, a cooperative approach provides benefits without creating significant traffic on costly WAN links.

12. See "Filters" on page 37, "On-Demand Submaps" on page 64, and "Management Consoles" on page 70.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1327
3740
Doc:

2066
21

4 Procedures for Scaling NNM

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1328
Doc. 3740

This chapter is not an introduction to NNM procedures. Readers are assumed to be conversant with NNM's key features for network monitoring, data collection, event handling, and so on. Readers who are looking for that information should turn to *Managing Your Network with HP OpenView Network Node Manager* instead. That manual also covers basic configuration of NNM station options that are not exclusive to distributed management.

This chapter covers procedures for scaling NNM. These procedures are:

- Configuring management consoles.
- Configuring on-demand submaps.
- Configuring distributed internet monitoring.
  - — Data collection
  - — Collection station
  - — Management station
  - — Domain overlap and failover
- Configuring event forwarding.
- Using distributed data collection.

Display

Mgmt. Station

Domain

Collection Station

Domain

Filter

The accompanying diagram serves as your roadmap through this chapter. As new areas of configuration are introduced, they are circled on the diagram.

All of the documentation for HP OpenView Windows and Network Node Manager is written with the assumption that you have activated environment variables on UNIX systems. For information about environment variables, see the reference page in NNM online help (manpage on UNIX systems) for *ov.envvars*.



NOTE This chapter refers to operating systems in the form OS Version.X (for example, HP-UX 11.X). Refer to the Release Notes, Supported Configurations topic for the operating systems that are supported with this release.

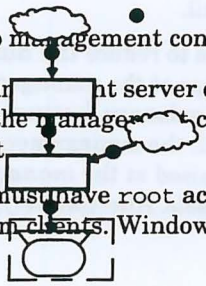
Configuring Management Consoles

Distribution of the HP OpenView Windows Graphical User Interface (GUI) is done via NFS mounting (Windows operating system file sharing for Windows operating system servers) of the map database and the appropriate configuration files, and by using the distributed RPC capability of the object database service (or background process on UNIX systems), ovwdb.

This section has five components:

- Configuring an NNM server on a machine running the Windows operating system (Windows operating system file sharing).
- Configuring a client on a Windows system for server on a Windows system (Windows operating system file sharing).
- Configuring a server on a UNIX operating system.
- Configuring a client on a Windows system to use a server on a UNIX
- Configuring a client on a UNIX system.

NOTE The management console (client) and the server must run the same revision of NNM. Refer to the Release Notes, Supported Configurations topic for the operating systems that are supported with this release.



To set up management consoles, the following must be true:

- A management server on UNIX must be configured as an NFS server and the management console (client) must be configured as an NFS client.
- You must have root access on UNIX system servers and UNIX system clients. Windows systems require Administrator rights.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1329
Doc 3740

- The client must have read-write access to a UNIX system server's file system via NFS.
- User and group IDs must be synchronized between the client and server.

The basic steps in installing management consoles are:

1. Install NNM on the server system, following the instructions in the *HP OpenView Network Node Manager Installation Quick Start*. (You do not need an additional license for the client.)
2. Mount the server's HP OpenView data directories on the client system.
3. Install NNM on the client system.
4. For UNIX system clients, run the `ovwsetupclient` configuration script on the client to have it use the mounted databases for maps and objects.
5. Run `ovstart` on the server system.
6. Run `ovw` on the client system.

CAUTION If a "lightweight" system (for example, a HP9000/715 with 64 Mbytes of RAM) is configured as a management console client for a server with a large database, it is possible that the resulting performance of the client system will be unacceptably slow, or that one or more of the background processes that run on the management console will run out of memory.

This is because `ipmap` and the `ovw` process sizes grow in proportion to the number of objects that are associated with persistent maps. For example, suppose that management station has 40,000 objects in its default map and the on-demand submap feature is disabled. If a lightweight management console tries to open this map, the synchronization process on the management console will cause `ovw` and `ipmap` to grow so large that either performance will be exceedingly slow, or one of the processes will run out of memory and fail.

The solution to this problem is to reduce the number of objects that are associated with persistent maps at the management console. This can be done by using the on-demand submaps feature, or map filters, or both. If the map is to be shared by both the management station and the console, the demand level should be raised at the *management* station *prior* to starting the management console. Alternatively, a copy of the map can be

created at the management station, and that copy can be configured with a higher demand level and/or filters. This new map can then be started up by the management console. For the best performance at the management console, set the demand level to Internet.

Configuring a Windows System Console Server

1. Share the *install_dir* directory from the NNM management server as *ShareName*. You may use Windows Explorer using a right mouse click. Give the users `Full Control` access.
2. Start the NNM services from the Control Panel at the NNM management server. These services must run during installation, or installation will fail.

Installing a Management Console on Windows for an NNM Server on Windows

First, install NNM on the Windows operating system machine that will be the management server, then follow these steps. You will need to know the name of the server to which the console will connect and the *ShareName* on the server.

1. On the NNM remote console, verify that you can connect to the *ShareName* share. You may use Windows Explorer.

NOTE During installation, the *install_dir*`\conf\*.auth` files are edited to give the remote console access to the manager's database and services. If you experience problems connecting to a management server, you may want to verify the rights granted in these files. You may also edit these files to customize rights for remote console operators.

2. On the NNM remote console system, insert the CD-ROM and run `setup.exe`. When installing, pick the `[Remote Console Installation]`. This removes any databases or local configuration files (these files might be in place if you had previously installed the full NNM management server). Supply the machine name of the NNM management server and share name *ShareName*.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1330
3740

3. You can now run NNM from this remote console as if you were at a full management server. The remote console has no icons for `[ovstop]` and `[ovstart]`, since to use these from a remote console, you must explicitly name what to start-up or shutdown. However, you can run these services from the command line.

Remote console operator rights to view maps are controlled the same way as operators viewing maps directly on the management server. Use NTFS file system access assignments to the *`install_dir`*`\databases\openview\mapdb` directory and subdirectories. Refer to *Managing Your Network with HP OpenView Network Node Manager* for details.

UNIX System Server Configuration

The server system is the management station on which you installed NNM and whose map and object database you want to export to the client system. You must be `root` to perform these steps. In the following steps, replace *`client_name`* with the hostname of the client from which you want to use these databases.

The following steps allow all users, including `root`, to run `ovw` sessions

1. Install NNM on the server as described in the *HP OpenView Network Node Manager Installation Quick Start* for the system.
2. If management consoles are connecting to this server from a Windows system, verify that the `pcnfsd` process is running on the server. This process lets your Windows operating system consoles know the name of the management station and that the station is running the `pcnfsd` daemons.

NOTE This step explains how to configure the `pcnfsd` process to authenticate NFS access requests from Windows clients. Although the `pcnfsd` process is commonly used for authentication, third-party providers of Windows NFS client products offer alternative methods, such as NIS authentication. If you prefer to use the `pcnfsd` process, complete this step. If you skip this step and use a third-party authentication procedure, it must be configured to allow access to user IDs in the range of 0-60002.

a. Create the file `/etc/pcnfsd.conf`. It will contain one line that reads:

   `uidrange 0-60002`

   Save and close this file.

b. Start PCNFS.

- On HP-UX:

  Edit the `/etc/rc.config.d/nfsconf` file. In it, change the PCNFS_SERVER= line to look like this:

  `PCNFS_SERVER=1`

  Save and close this file. To start the service, run the command:

  `/sbin/init.d/nfs.server start`

- On Solaris:

  Verify that the PCNFS product is installed on the management station and that `pcnfsd` is running:

  `ps -ef | grep pcnfsd`

  If it is not running, start it with `/opt/SUNW/pcnfs/scripts/pcnfs start`.

3. Ensure that NFS is running on the server.

- **On HP-UX:**

  a. Run this command:

  `ps -ef | grep nfsd`

  b. If the `nfsd` process is not running, edit the file `/etc/rc.config.d/nfsconf` and change `NFS_SERVER=0` to `NFS_SERVER=1` and run the following command:

  `/sbin/init.d/nfs.server start`

- **On Solaris 2.X systems** (NFS must already be installed):

  a. Run this command:

  `ps -ef | grep nfsd`

  b. If the `nfsd` process is not running, execute:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1331
Doc 3740

```
/etc/init.d/nfs.server start
```

4. Configure the exportation of the HP OpenView file system to the client as follows:

   - For an HP-UX server, edit the `/etc/exports` file. You will either modify two existing lines or add new ones, depending on the contents of this file.

     -- If the line `/etc/opt/OV/share -root=` is present, add your console system's name after the equal sign. If there is already a system name after the equal sign, then add a colon (:) followed by your console system's name after the first system name.

     -- If the line `/etc/opt/OV/share -root=` is not present, add it and include your console system's name.

     -- Do the same for the line `/var/opt/OV/share -root=`.

     When you have finished editing, the file should look like this:

     ```
     /etc/opt/OV/share root=First_System:Console_System
     /var/opt/OV/share -root=First_System:Console_System
     ```

     or

     ```
     /etc/opt/OV/share -root=Console_System
     /var/opt/OV/share -root=Console_System
     ```

     Save and close the `/etc/exports` file.

   - For a Solaris server, edit the `/etc/dfs/dfstab` file by adding the following two lines to it:

     ```
     share -F nfs -o root=Console_System /etc/opt/OV/share
     share -F nfs -o root=Console_System /var/opt/OV/share
     ```

     Save and close the `/etc/dfs/dfstab` file.

5. Run the following two commands to unexport and re-export the directories from the server:

   On HP-UX:

   ```
   /usr/sbin/exportfs  -au
   /usr/sbin/exportfs  -av
   ```

   On Solaris 2.X:

   ```
   share -F nfs -o root=client_name /var/opt/OV/share
   share -F nfs -o root=client_name /etc/opt/OV/share
   ```

Use the fully qualified domain name when specifying the *client_name*.

6. Verify that NNM is running on the management station. Type

   /opt/OV/bin/ovstatus | more

   You should see a list of processes that are currently running. Check the list to verify that the ovwdb process is running. If ovwdb is not, type

   /opt/OV/bin/ovstart ovwdb

   Then, type **/opt/OV/bin/ovstatus | more** again to verify that ovwdb is now running.

Installing Management Consoles on Windows for UNIX System Management Servers

To set up a remote management console on a Windows operating system to use a UNIX management station server, first satisfy the following prerequisites:

- Make sure that the management station server is not already mapped as a network drive on your Windows operating system console. If it is, remove the network drive connection.
- Verify that you have a compatible NFS client product installed on your Windows operating system console. (See the NNM Release Notes for a list of NFS client products that have been tested with NNM.)
- You will need to know the name of the server to which the console will connect and the two directories exported in step 4 and 5 of "UNIX System Server Configuration" on page 112.

Once the prerequisites are satisfied, perform the following steps:

1. Verify or configure the following settings in the NFS client software on the system running Windows that will be a management console.
   - The name of the management station you are connecting your management console to. Indicate the station by name, not by IP address.
   - The root login name and password for connecting to the management station.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1332
3740
Doc:

5. Once installation is completed, it is recommended that you change the configuration of your PCNFS server product so that the authentication is that of the user using NNM on the Windows operating system console, instead of `root`. For example, if a user called `ovuser` is running NNM on both the management station and the Windows operating system station, the configured PCNFS authentication should be `ovuser` instead of `root`. By changing the authentication, you ensure that any files generated during an NNM session will be accessible from both the station and the Windows operating system console.

UNIX System Console Configuration

Before you begin, you will need to know the name of the server to which the console will connect. Perform the following steps on each client machine:

1. Install NNM on the console as described in the *HP OpenView Network Node Manager Installation Quick Start* for the system.
2. Ensure that the console is running as an NFS client.

- **On HP-UX:**
  a. Run this command:

     `ps -ef | grep biod`

  b. If the `biod` process is not running, edit the file `/etc/rc.config.d/nfsconf` and change `NFS_CLIENT=0` to `NFS_CLIENT=1` and run the following command:

     `/sbin/init.d/nfs.client start`

- **On Solaris 2.X:**
  a. Run this command:

     `ps -ef | grep -e "statd|lockd"`

  b. If you do not see both the `/usr/lib/nfs/statd` and the `/usr/lib/nfs/lockd` processes running, execute:

     `/etc/init.d/nfs.client start`

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1333
3740
Doc:

3. Choose a mount point for the server's HP OpenView file systems. To make sure this file system is mounted at boot time, you must modify the appropriate file shown below. You must be `root` to modify these files. Replace *server_name* with the name of the server whose databases you want to use on this client.

NOTE As an alternative to these steps, NFS access may be provided via the NFS automounter. Consult your operating system's manual for details.

- On **HP-UX:**
  a. Run these commands:

     mkdir -p /opt/OV/nfs/*server***/var/opt/OV/share**

     mkdir -p /opt/OV/nfs/*server***/etc/opt/OV/share**

  b. Add these lines to the `/etc/fstab` file:

```
server:/var/opt/OV/share /opt/OV/nfs/server/var/opt/OV/share nfs rw 0 0
server:/etc/opt/OV/share /opt/OV/nfs/server/etc/opt/OV/share nfs rw 0 0
```

  c. Run these commands:

     /etc/mount *server*:**/etc/opt/OV/share**

     /etc/mount *server*:**/var/opt/OV/share**

- **On Solaris 2.X:**
  a. Run these commands:

     mkdir -p /opt/OV/nfs/*server***/var/opt/OV/share**

     mkdir -p /opt/OV/nfs/*server***/etc/opt/OV/share**

  b. Add these lines to the `/etc/vfstab` file:

```
server:/var/opt/OV/share - /opt/OV/nfs/server/var/opt/OV/share/ nfs - yes rw
server:/etc/opt/OV/share - /opt/OV/nfs/server/etc/opt/OV/share/ nfs - yes rw
```

  c. Run these commands:

     /etc/mount *server*:**/etc/opt/OV/share**

     /etc/mount *server*:**/var/opt/OV/share**

4. Set up the client by running the following script:

   $OV_BIN/ovwsetupclient /opt/OV/nfs/*server*

NOTE If you have used the NFS automounter, the path may be different.

5. To verify that the configuration is correct, run the following command:

   ovw -server

   Look at the return value from the `ovw -server` command on your display. It should look similar to:

   ```
   %ovw -server

   your server name shows up here
   ```

6. Run **ovw** on the management console.

   If you are running on an HP Service Guard cluster, you may run **ovwrs** rather than **ovw**, if NNM is configured as a package. Refer to the *ovwrs* man page for more information about restartable **ovw**.

Increasing Security for Management Consoles

Authorization files on the server allow you to limit which consoles may access the information on the server. If you have modified default authorizations, add the server hostname and each client hostname to the authorization file for `ovwdb` and `ovw`. Be sure to add the line *client_name* + for each client you are giving access to the server. The files `ovwdb.auth` and `ovw.auth` are located in `$OV_CONF`.

server_name +

client_name_1 +

client_name_2 +

where *server_name* is the name of the system where your map database resides. The addition of these lines enables any user from *client_name_1* or *client_name_2* to use the database on *server_name*.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1334
3740
Doc.

NOTE A third authorization file also exists, `ovspmd.auth`. This file limits which consoles have permission to run `ovstop` and `ovstart`. **You should be careful about giving too many users this permission.**

Undoing a Management Console

If you want to undo the management console setup and run NNM in a normal manner, you must follow these steps in the order listed.

CAUTION Failure to follow these steps could result in damage to your databases.

- On UNIX systems:
  1. Run the following command on the console:

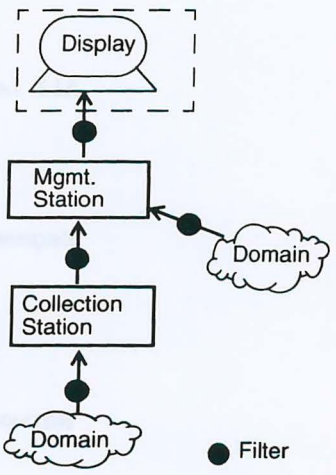
     ```
     $OV_BIN/ovwsetupclient -u
     ```

  2. Remove the lines that were added to the `/etc` files in the previous Server Configuration and Client Configuration sections.
- On Windows systems:
  1. Reinstall NNM from the installation CD.

Configuring On-Demand Submaps

This section discusses how to:

- Configure on-demand submaps.
- Specify a persistence filter.
- Integrate applications with on-demand submaps.



Configuring Demand Level

You can set the demand level of maps as you create them or after you have already created the map. You can set the submap demand level using the `-D` option on the `ipmap` command or using the `IP Map Configuration` dialog box. See the reference page in NNM online help (or manpage on UNIX systems) for *ipmap* for information setting the demand level using the command line.

To set the demand level as you are creating the map, use the following procedure:

1. Select `Map:New...` from the menu bar; the `New Map` wizard (dialog box on UNIX systems) appears.
2. Select `IP Map` from the `Configurable Applications` list. Figure 4-1 illustrates the list under the Windows operating system.
3. Click `[Configure For This Map...]`; the `IP Map Configuration` dialog box differs according to the operating system, as shown in Figure 4-2 and Figure 4-3.
4. On UNIX systems, in the `IP Map Configuration` dialog box, use the scroll bar in the top pane to scroll down to the `------ On-Demand Specification -----` section of the pane.
5. Use the option button under the question "`To what level should submaps be persistent?`" to specify the demand level. You can specify one of the following:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1335
3740
Doc:

`Unset`

Resets the demand level to the platform default. On systems running the Windows operating system, this is `Internet Level`. On UNIX systems, it is `All Levels`.

`All Levels`

Specifies all submaps as persistent. This is the same as specifying level 1 when using the `ipmap -D` command.

`Segment Level and Higher`

Specifies that segment, network, and Internet level submaps are persistent. This is the same as specifying level 2 when using the `ipmap -D` command.

`Network Level and Higher`

Specifies that network and Internet level submaps are persistent. This is the same as specifying level 3 when using the `ipmap -D` command.

`Internet Level`

Specifies that Internet level submaps are persistent. This is the same as specifying level 4 when using the `ipmap -D` command.

6. Click `[Verify]` to verify that the values are valid.
7. Click `[OK]` to close the `IP Map Configuration` dialog box.
8. On systems running the Windows operating system, click `[Next]` to continue filling in the wizard windows. On UNIX systems, click `[OK]` from the `New Map` dialog box after you have completed the required fields.

You can use the `Map:Properties` menu from the menu bar to change the demand level after the map has already been created.

Click the `[Applications]` tab in the `Map:Properties` dialog box on systems running the Windows operating system. Using the `Map Properties` dialog box, follow the above procedure for setting the demand level of a new map. You must have read-write access to the map in order to change its demand level.

Refer to "On-Demand Submaps" on page 64 for more information about the on-demand submap feature.

Figure 4-1 Windows Map Properties Property Sheet, Applications Tab

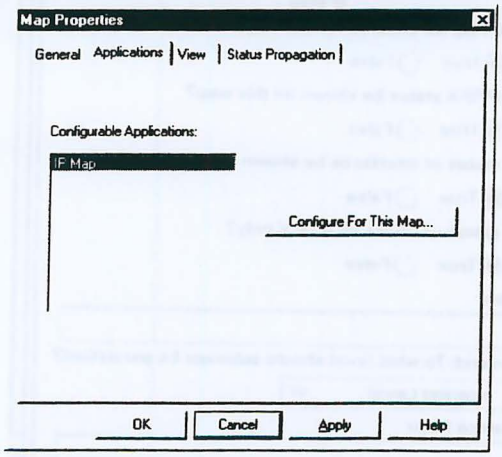
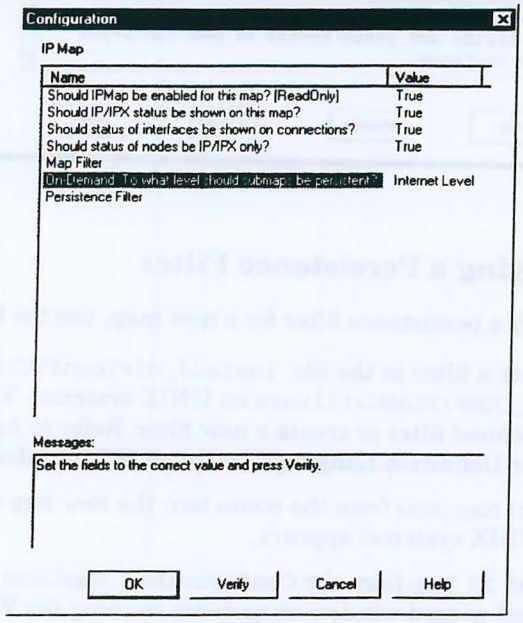
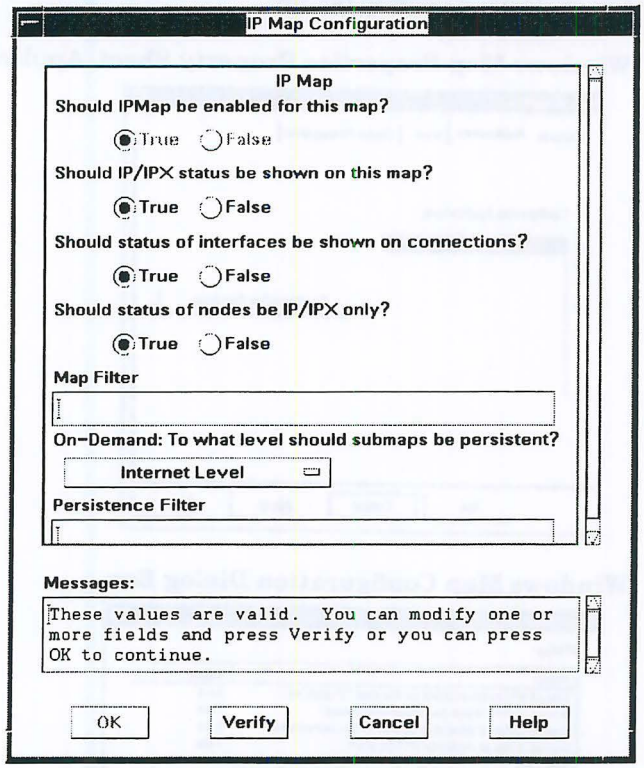


Figure 4-2 Windows Map Configuration Dialog Box



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1336
3740
Doc:

Figure 4-3 IP Map Configuration Dialog Box on UNIX Systems



Specifying a Persistence Filter

To specify a persistence filter for a new map, use the following procedure:

1. Create a filter in the file *install_dir*\conf\C\filters (`$OV_CONF/$LANG/filters` on UNIX systems). You can either use a predefined filter or create a new filter. Refer to Appendix A, "The Filter Definition Language," on page 167 for information on filters.
2. Select `Map:New` from the menu bar; the `New Map` wizard (dialog box on UNIX systems) appears.
3. Select `IP Map` from the `Configurable Applications` list (in the second wizard window on systems running the Windows operating system, as shown in Figure 4-1).

4. Click [Configure For This Map...]; the IP Map Configuration dialog box appears, as shown in Figure 4-2 and Figure 4-3.
5. On Windows systems, select Persistence Filter. The Persistence Filter dialog box opens.

   On UNIX systems, in the IP Map Configuration dialog box, use the scroll bar in the top pane to scroll down to the ------ On-Demand Specification----- section of the pane.
6. In the Persistence Filter text field, enter a filter name or expression.
7. Click [Verify] to verify that the values are valid.
8. Click [OK] to close the IP Map Configuration dialog box.
9. On Windows systems, click [Next] to continue filling in the wizard windows.

   On UNIX systems, click [OK] from the New Map dialog box after you have completed the required fields.

You can use Map:Properties from the menu bar to change the persistence filter after the map has already been created.

Using [Applications] tab in the Map:Properties dialog box, as shown in Figure 4-1 on page 123, (or the Map Description dialog box on UNIX systems), follow the above procedure for setting the persistence filter of a new map. You must have read-write access to the map in order to specify a persistence filter.

Refer to "Persistence Filtering" on page 68 for more information about persistence filters.

Integrating Applications With On-Demand Submaps

Before integrating a new application with NNM, you should have a good understanding of how your application works so your application can produce the same results whether you are using the on-demand submap feature of NNM or not. This may require a persistence filter to use when on-demand submaps are enabled.

For example, if your application adds a hub symbol to a segment submap and needs the status of the hubs to propagate up the submap hierarchy, then you need to specify a persistence filter.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1337
3740
Doc:

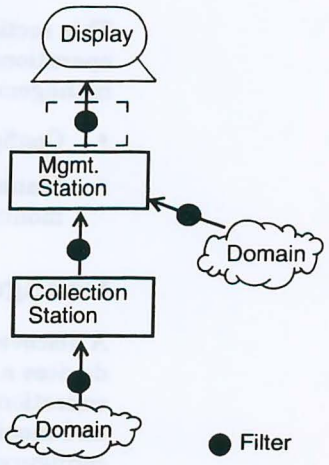
Another example of when a persistence filter is needed is if your application, at start-up, queries the map for all objects of a certain type and performs an operation for each of those objects found. Your application needs to ensure that the objects of this type are on the map by including a persistence filter that specifies this object type.

Use the following procedure to create and specify a persistence filter.

1. Determine what objects your application requires in the map.
2. Start your application running on NNM.
3. Select an object that your application has added and that you want to remain persistent in the submap.
4. Select `Edit:Object Properties` from the menu bar.
5. From the `Object Description` dialog box, view the object attributes for `Capabilities`.
6. Determine which capabilities are unique to that object type, for example, which are set to true.
7. With this information you can create a filter that will allow this object type to pass through.
8. Follow the steps for configuring the demand level and specifying a persistence filter.

Configuring a Map Filter

A map filter allows the operator to display only the objects of interest to that operator. Objects that are rejected by a map filter remain in the management station's topology database and are still subject to status polling. Use the following procedure to configure a map filter on a management station:



1. Create a filter in the file *install_dir*\conf\C\filters ($OV_CONF/$LANG/filters on UNIX systems). You can either use a predefined filter or create a new filter. Refer to Appendix A, "The Filter Definition Language," on page 167 for information on filters.
2. On systems running the Windows operating system, select the Applications tab in the Map:Properties dialog box.

   On UNIX systems, select Map:Properties from the menu bar. The Map Description dialog box appears.
3. Select IP Map from the Configurable Applications list and click [Configure For This Map]. The IP Map Configuration dialog box appears, as shown in Figure 4-2 on page 123 (Figure 4-3 for UNIX systems).
4. You must have read/write rights to the current map.

   On systems running the Windows operating system, select Map Filter, and enter the filter name.

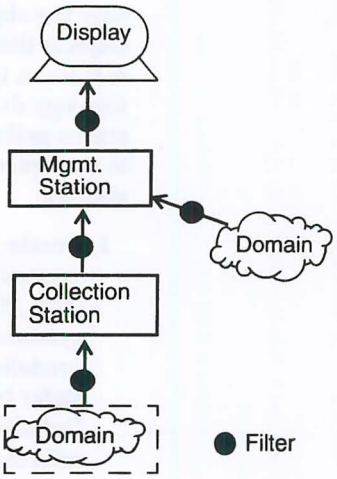
   On UNIX systems, enter the filter name that you created in the text box under Map Filter.
5. Click [Verify] to make sure the filter name or expression you specified is a valid filter.
6. Click [OK] to save the changes and close the dialog box.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1338
3740
Doc:

Configuring Data Collection for a Station

This section describes how to perform operations required on all collection and management stations:

- Configure a discovery filter.
- Manage and unmanage a locally monitored object.



Configuring a Discovery Filter

A discovery filter reduces the number of devices a management station or collection station is actively discovering and monitoring. A discovery filter can be configured on a management station or a collection station. Use the following procedure to configure a discovery filter:

1. Create a filter in the file *install_dir*\conf\C\filters (`$OV_CONF/$LANG/filters` on UNIX systems). You can either use a predefined filter or create a new filter. Refer to Appendix A, "The Filter Definition Language," on page 167 for information on filters.
2. Select `Options:Network Polling Configuration:IP/IPX` (`Options:Network Polling Configuration:IP` on UNIX systems) from the menu bar. The dialog box tabs under the Windows operating system are shown in Figure 4-4, Figure 4-5, and Figure 4-6. The `Network Polling Configuration` dialog box for UNIX systems appears as shown in Figure 4-7.
3. Make sure the `Discover New Nodes` option button is on in the IP and IPX tabs, as needed. (There is no IPX on UNIX systems.)
4. On Windows systems, click the `[Use Filter]` option button on the `[General]` tab and choose a filter from the list box.

   On UNIX systems, click the `Use Discovery Filter` option button to the on position. The corresponding text box will ungray.
5. Enter the filter name as defined in the filters file into this text box.

6. Click [OK] to save the changes and close the dialog box.

The discovery filter will be applied to all newly discovered objects. Polling is still done on all previously discovered objects whether or not they would have passed the filter.

To apply the filter to previously discovered objects you need to perform the following steps (from a command window on the Windows operating system):

1. Stop netmon by typing

   ovstop netmon

2. Once netmon is stopped, execute the following command:

   ovtopofix -f *filtername*

3. Then start netmon by typing:

   ovstart netmon

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1339
3740
Doc:

Figure 4-4 **Windows Network Polling Configuration, General Tab**

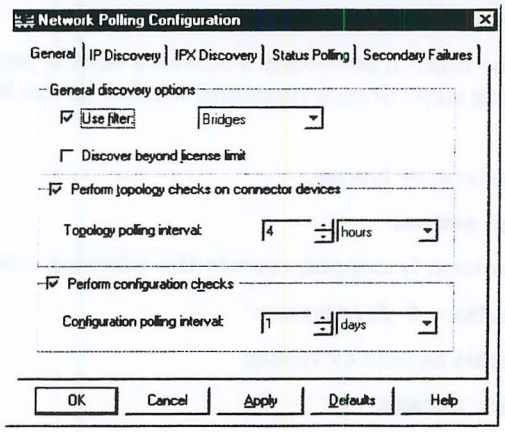


Figure 4-5 **Windows Network Polling Configuration, IP Discovery Tab**

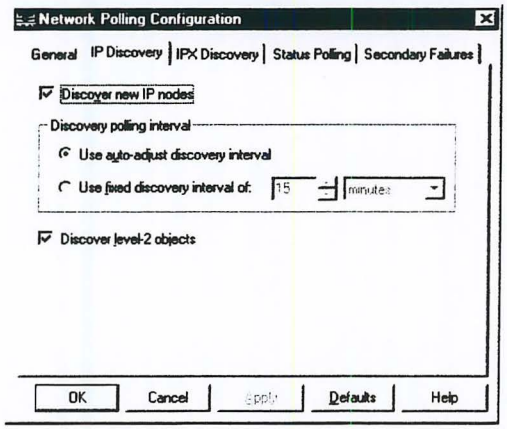


Figure 4-6 Windows Network Polling Configuration, IPX Discovery Tab

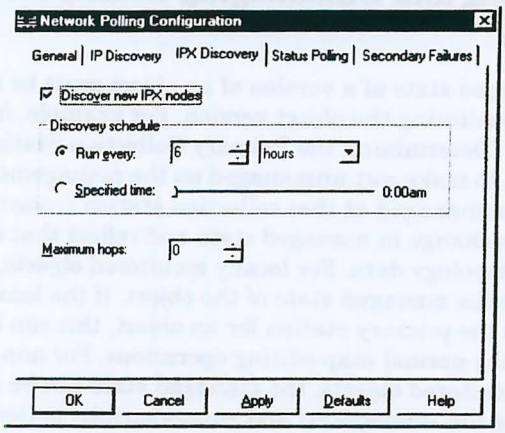
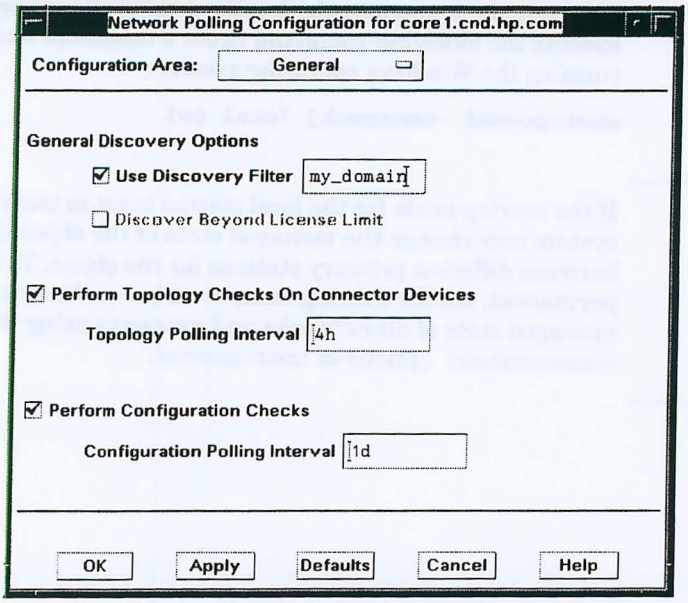


Figure 4-7 UNIX System Network Polling Configuration Dialog Box



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1340
3740
Doc:

Managing and Unmanaging Locally Monitored Objects

The managed state of a version of an object must be set on the collection station monitoring the object version. For example, in the examples shown in "Determining the Primary Collection Station for an Object" on page 150, to make `gw1` unmanaged on the management station, the node must be unmanaged at that collection station (`remstn1`). `remstn1` will detect the change in managed state and reflect that in the management station's topology data. For locally monitored objects, it may be desirable to change the managed state of the object. If the local management station is the primary station for an object, this can be accomplished through the normal map editing operations. For non-primary versions of locally monitored objects, the managed state can be changed by specifying the `-manageobj` and `-unmanageobj` options of `xnmtopoconf`:

`xnmtopoconf [-manageobj | -unmanageobj]` *`station object`*

For example, to manage the locally monitored version of node `gw1` execute the following command (from a command window on systems running the Windows operating system):

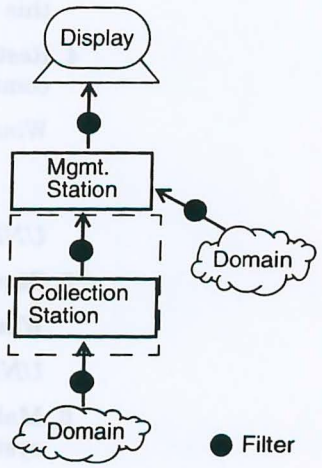
```
xnmtopoconf -manageobj local gw1
```

NOTE If the overlap mode for the local station is set to `Unmanage` or `Delete`, the system may change the managed state of the object during a transition between different primary stations for the object. To make your changes permanent, set the overlap mode to `Allow` and manually set the managed state of all networks and gateways using the `-manageobj` and `-unmanageobj` options of `xnmtopoconf`.

Configuring Collection Stations

This section describes how to:

- Configure security for a collection station.
- Configure a topology filter for a collection station.
- Change the topology filter a collection station.
- Configure a Windowsoperating system IPX collection station.



Configuring Security for a Collection Station

On the collection station, you need to configure SNMP security to allow the exporting of topology information. Use the following procedure to do this (on UNIX systems, you must be `root` to execute this procedure).

1. Make sure NNM is not running. If NNM is running,

   Windows Stop all NNM services by clicking the `NNM Services - Stop` icon.

   UNIX Exit all sessions and issue the command **`ovstop`**

2. Make sure the SNMP master agent is not running by executing the following command:

   Windows Stop `SNMP EMANATE Adapter for Windows` and `SNMP EMANATE Master Agent` using the `Control Panel Services` applet.

   UNIX **`/usr/sbin/snmpd -k`**

3. Edit the set community name line in the *`install_dir`*`\conf\SnmpAgent\snmpd.conf` (`/etc/SnmpAgent.d/snmpd.conf` on UNIX systems) file to read as follows:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1341
Doc. 3740

```
set-community-name: name #enter community name
```

where, *name* is the community name of your choice. By default, NNM does not install a default set community name. You must set this value before attempting to manage a station.

4. Restart the SNMP master agent by executing the following commands:

Windows	Restart `SNMP Emanate Adaptor` and `SNMP Emanate Master Agent` using the `Control Panel Services` applet.
UNIX	**`/usr/sbin/snmpd`**

5. Start NNM by executing the following command:

Windows	Click the `NNM Services - Start` icon.
UNIX	**`ovstart -v`**

6. Make sure the `ovtopmd` service (background process on UNIX systems) is running by executing the following command:

Windows	Click the `NNM Status` icon.
UNIX	**`ovstatus ovtopmd`**

Configuring a Topology Filter for a Collection Station

A topology filter at a collection station defines the subset of topology data that management stations can access. For more information, see "Topology Filtering" on page 41. Use the following procedure to configure a topology filter on a collection station:

1. Create a filter for the *install_dir*`\conf\C\filters` (`$OV_CONF/$LANG/filters` on UNIX systems) file. You can either use a predefined filter or create a new filter. Refer to Appendix A, "The Filter Definition Language," on page 167 for information on filters.
2. Make sure NNM is not running. If NNM is running, exit all sessions and issue the following command:

Windows	Click the `NNM Services - Stop` icon.
UNIX	**`ovstop`**

3. Edit the `vtopmd.lrf` file to include the `-f` option followed by the desired filter name or filter expression name. For example,

```
ovtopmd:ovtopmd:
OVs_YES_START:pmd,ovwdb:0 -f Routers: OVs_WELL_BEHAVED:15:
```

   where, `Routers` is a predefined filter contained in the standard filter definition file.

4. Reconfigure `ovtopmd` by executing the following command (from a command window on systems running the Windows operating system):

   `ovaddobj ovtopmd.lrf`

5. Start the NNM services by executing the following command:

   Windows Click the `NNM Services - Start` icon.

   UNIX **`ovstart -v`**

   The start-up of NNM may take a little longer the first time, to adjust for `ovtopmd` to apply the filter to the existing topology database.

Only information that passes the topology filter is passed on to the management station. Existing information on the management station that does not pass the newly-configured filter will be removed from the management station's topology database.

Changing the Topology Filter for a Collection Station

You can change the topology filter for a collection without stopping NNM using the following procedure.

1. Create a filter for the *`install_dir`*`\conf\C\filters` (`$OV_CONF/$LANG/filters` on UNIX systems) file. You can either use a predefined filter or create a new filter. Refer to Appendix A, "The Filter Definition Language," on page 167 for information on filters.
2. Execute the following command (from a command window on systems running Windows):

   `ovtopmd -f` *`filtername`*

   where filtername is the new filter that you want to apply to the database. This command sends an event that tells `ovtopmd` to apply the new filter to the topology database.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1342
3740
Doc:

To remove the topology filter, execute the following command (from a command window on systems running Windows):

```
ovtopmd -f ""
```

NOTE To make the filter application permanent, perform steps 3 and 4 from the "Configuring a Topology Filter for a Collection Station" on page 134.

Configuring IPX on a Collection Station under Windows

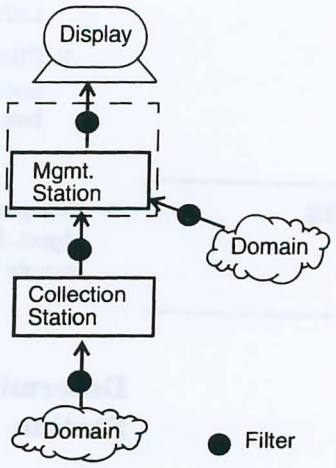
If you want to prevent IPX information from being passed to the NNM management station, do one of the following:

- During installation of the NNM collection station, disable IPX discovery. The following procedure prevents IPX discovery from occurring on the collection station.
  1. Choose the `Custom Installation` option, and disable the automatic starting of network discovery.
  2. Once installation is complete, start the NNM user interface.
  3. Select the `Options:Network Polling Configuration:IP/IPX` menu item.
  4. From the `[IPX Discovery]` tab, click on the `[Discover New Nodes]` button to disable IPX discovery.
  5. Start the IP discovery services using the `NNM Services - Start` icon in the `HP OpenView` program group.
- If you want IPX discovery enabled on the NNM collection station, proceed with a normal installation. After the system is installed, configure the `IPOnlyObjects` filter as a topology filter. Refer to "Configuring a Topology Filter for a Collection Station" on page 134 for this information. This prevents any IPX networks or IPX-only objects from being propagated to the management station. However, nodes that are discovered to support both IP and IPX will still contain IPX interfaces, with only a physical address and no IP address.

Configuring Management Stations

This section describes how to:

- Determine if a node is a collection station.
- Determine all objects monitored by a specific collection station.
- Configure a management station to use a specific collection station.
- Unmanage a collection station from a management station.
- Remove a collection station from a management station.
- Configure a remote communication timeout and retry count.
- Perform a full synchronization.



Determining if a Node is a Collection Station

There are several ways to determine what nodes are collection stations.

- The easiest is to use the Station view available from the `Tools:Views->Station` menu, or at this URL: `http://`*`nodename`*`:7510/topology/stationView`, where *nodename* is an NNM management station.
- Alternatively, you can execute the following command (from a command window on systems running a Windows operating system):

  `xnmtopoconf -print`

  This will give you a list of current collection stations and tell you if they are managed or unmanaged. The nodes with a managed status are currently acting as collection stations.
- Finally, you can also use ovw to determine which nodes are acting as collection stations. Use the following procedure:

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1343
3740
Doc:

1. From the menu bar select `Edit:Find->Object By Attribute`. The `Find by Attribute` dialog box appears.
2. In the `Objects Attributes` list, select `isCollectionStationNode`.
3. Click `[Apply]`. The known collection stations will be in the `Located and Highlighted` list in the `Locate Attribute` dialog box.

NOTE It is possible for collection stations to exist without having a node object. For example, when a collection station is being used from a remote location and it is not part of the locally discovered topology.

Determining All Objects Monitored by a Collection Station

You can see all the objects monitored by a given collection station by specifying the `ovtopodump` command with the `-r` and `-C` options together. For example, (from a command window on systems running a Windows operating system)

```
ovtopodump -rRISC stn2
```

If there is both a node and a collection station with the same name, it may be necessary to use the object ID to distinguish the two objects with the `-r` option. Another option is to print all objects and use the `grep` command to find the objects from that collection station. For example,

```
ovtopodump -RISC | grep stn2
```

Configuring for a Specific Collection Station

You can configure a management station to connect to a collection station. Use the following procedure to do this (you must be `Administrator` on systems running a Windows operating system or `root` on UNIX systems to execute this procedure):

1. Make sure the NNM services (background processes on UNIX systems) are running:

- On Windows , use the `Control Panel Services` applet to check status. If the NNM services are not running, use the `Control Panel Services` applet to start the services.
- On UNIX, execute the following command:

  `ovstatus`

  If the NNM services are not running, execute the following command:

  `ovstart`

2. Determine what collection stations already exist as described in "Determining if a Node is a Collection Station" on page 137to get a list of current collection stations and see if they are managed or unmanaged. If the collection station you want does not appear, continue to the next step. If the collection station *does* appear, continue with step 4.
3. Add the collection station to the topology by executing the following command:

   `xnmtopoconf -add -unmanage` *`collectionstation`*

TIP When NNM is first started, all the collection stations attempt to report to the management station at the same time, slowing down the system. Unmanage them and bring them on one at a time.

   This same command is used for the floating host name of a Service Guard cluster on UNIX systems. As part of your Service Guard configuration process, you updated the `ov.conf` configuration file `HOSTNAME= parameter`. Refer to the *ov.conf* reference page in NNM online help (or manpage on UNIX systems) for more information.

4. Configure the `set` community name to be used when communicating with the collection station by selecting `Options:SNMP Configuration` from the menu bar. This displays the `SNMP Configuration` dialog box.
5. In the "`Specific Nodes`" tab (`SNMP Parameters` pane of the dialog box on UNIX systems), specify in the `Set Community` text field the same set community name that you configured on the collection station.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1344
3740
Doc:

6. Click [OK] to close the SNMP Configuration dialog box.
7. To make sure the collection station is configured correctly, execute the following command (from a command window on systems running a Windows operating system):

   xnmtopoconf -test *collectionstation*

   If you see SNMP errors or timeouts reported, refer to "Troubleshooting Collection Station Communication" on page 147 for more information.
8. Manage the collection station by executing the following command:

   xnmtopoconf -manage *collectionstation*

   This causes the management station to start monitoring and synchronizing with the remote collection station. As part of this, the management station will be added to the collection station's internal list of interested managers. This internal list is referred to as %REMOTE_MANAGERS_LIST% in various places in the interface, such as the event configuration system, when forwarding is being configured.

Unmanaging a Collection Station

To unmanage a collection station from a management station, execute the following command (as Administrator on systems running a Windows operating system or root on UNIX systems) from the management station (from a command window on systems running a Windows operating system):

xnmtopoconf -unmanage *collectionstation*

This removes the management station from the list of active management stations (%REMOTE_MANAGERS_LIST%) for this collection station. The collection station however remains in the management station's database. This command may take a few minutes to complete. All objects for which the collection station is the primary collection station are either assigned a new primary collection station or have their status set to unknown.

Since new primary collection stations are being assigned, this command may take some time to complete.

Removing a Collection Station from a Management Station

Determine what collection stations already exist as described in "Determining if a Node is a Collection Station" on page 137to get a list of current collection stations and see if they are managed or unmanaged.

To remove a collection station from the management station's database, execute the following command (as `Administrator` on systems running a Windows operating system or `root` on UNIX systems) from the management station (from a command window on systems running a Windows operating system):

xnmtopoconf -delete *collectionstation*

This will remove all the symbols representing the collection station objects from the maps on the management station. When a collection station is deleted, a new primary is picked automatically. If none exists, the node is deleted from the management station.

This command may take some time to complete since all data reported from that collection station is removed. If you will be using this data in the future, you may want to unmanage the collection station instead of removing it.

Configuring a Remote Communication Timeout and Retry Count

A WAN link connecting a management station and a collection station will likely have a slow response time and a larger packet loss rate due to congestion. The following procedure will determine the appropriate set of timeouts to use for remote communication.

1. Ping the remote collection station by executing the following command (from a command window on systems running a Windows operating system):

   ping *collectionstation*

   For Solaris, use **ping -s** *collectionstation*.

   After a period of time, stop the ping and note the average round trip time and the packet loss rate.

2. Configure the timeouts and retry count for the remote collection station, based on the behavior received from the ping.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1345
3740
Doc:

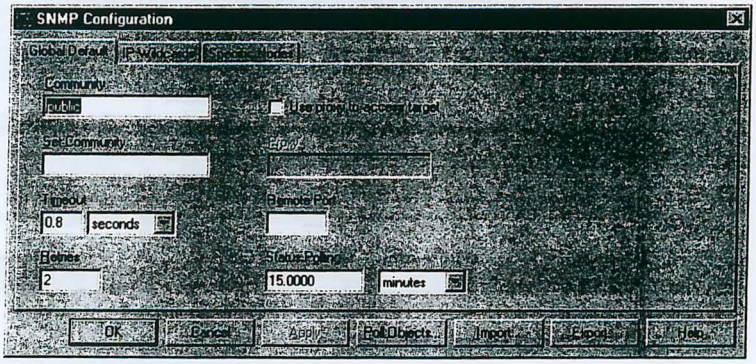
For example, for a reasonable timeout configuration, take the average ping round-trip time, double it, and add a little. For a retry count, the higher the packet loss rate, the more retransmissions you should specify to occur before a failed SNMP request. You should keep a retry count of at least 3.

3. Select `Options:SNMP Configuration` from the menu bar; the `SNMP Configuration` dialog box appears, as shown in Figure 4-8 (Figure 4-9 for UNIX systems).
4. In the `SNMP Parameters` section of the dialog box, specify the timeout configuration in the `Timeout` text box and the retry count in the `Retry Count` text box.
5. Click `[OK]` to save the changes and close the dialog box.
6. Verify communication with the remote collection station by executing the following command (from a command window on systems running a Windows operating system):

   xnmtopoconf -test *collectionstation*

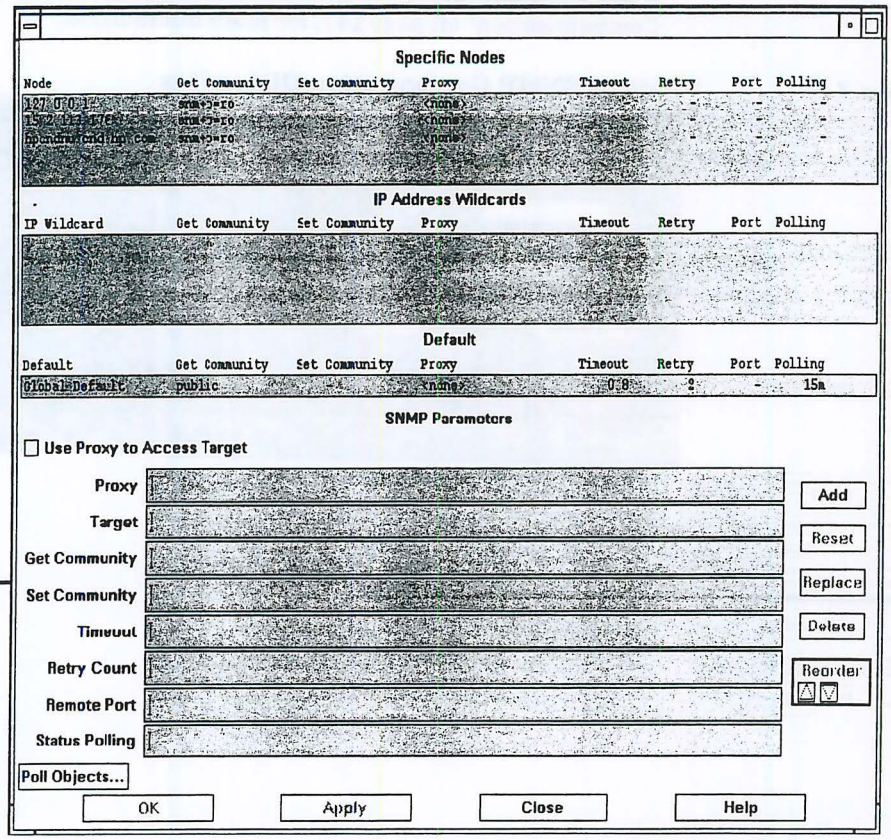
If the test fails, refer to "Troubleshooting Collection Station Communication" on page 147, for more information.

Figure 4-8 Windows SNMP Configuration Dialog Box



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1346
Doc. 3740

Figure 4-9 **UNIX System SNMP Configuration Dialog Box**



Performing a Full Topology Synchronization

A full topology synchronization causes a complete check of every attribute of every object reported by the remote collection station. This includes adding objects that are unknown and deleting objects that are not known at the remote collection station.

Perform a full synchronization by executing the command (from a command window on aWindows operating system):

nmdemandpoll -s *collectionstation*

All results and actions taken are reported to the command line. The output consists of the following:

- General processing status. There will be output noting the general flow of the synchronization process as well as general information related to the remote collection station (for example, hostname, port, version).
- Detailed output concerning the processing of all objects, regardless of whether any changes were detected.
- Warnings about objects that have conflicts or other errors in updating the objects in the database.
- Information about objects that no longer exist in the remote site's database and that are being removed from the local topology database.

TIP When resynchronizing peer-to-peer management stations, the simultaneous resynchronization can cause NNM to slow down and fail. Unmanage one until the other has resynchronized, then remanage it to synchronize it.

Identifying Collection Station Communication Problems

You can check the status of a collection station or management station using the NNM Station view.

One way to open an NNM Station view is by using the NNM `Tools:Views->Station` command. For other ways of opening an NNM Station view, see the *Interacting with Views* section of the HP OpenView web online help.

The status color of the local management station indicates whether or not it is responding to NNM status polls. The status color of a collection station indicates whether or not the local management station is receiving data from that remote collection station:

- Tan color: The collection station is unmanaged.
- Green color (management station): The management station operational status is normal.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1347
Doc: 3740

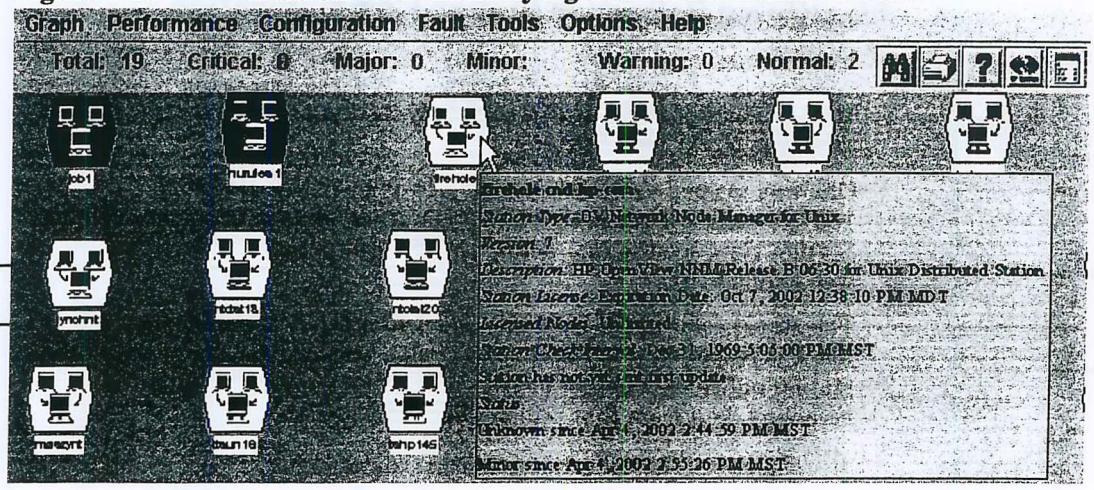
- Other color (management station): The management station operational status is abnormal.
- Green color (collection station): The collection station to management station communication status is normal.
- Other color (collection station): The collection station to management station communication status is abnormal.

In Figure 4-10 on page 146, the NNM Station view shows you that management station `job1` is managing `nurules1`. The status of both collection station `nurules1` and management station `job1` is normal.

However, the communication status of collection station `firehole` recently changed, as shown by the exclamation point, and is now showing an abnormal status color. You need to troubleshoot the communication from collection station `firehole` to management station `nurules1`. See "Troubleshooting Collection Station Communication" on page 147for troubleshooting techniques.

NOTE By resting your mouse pointer over collection station `firehole`, NNM displays some additional information.

Figure 4-10 Station View: Identifying Communication Problems



Troubleshooting Collection Station Communication

To troubleshoot the communication between a management station and a collection station use `xnmtopoconf`, as shown in the following procedure.

1. To determine the status of the managed collection stations, execute the command (from a command window on systems running a Windows operating system):

   `xnmtopoconf -print`

   This will produce a list of managed collection stations and their status as follows:

```
STATION          STATUS     INTERVAL OVERLAP MODE     FAILOVER   FAILOVER FILTER
ab.cnd.hp.com    Unmanaged  5m       AllowOverlap     off        <none>
be.cnd.hp.com    Critical   2m       AllowOverlap     ON         Routers
cat.cnd.hp.com   Unmanaged  5m       AllowOverlap     off        <none>
dog.cnd.hp.com   Normal     5m       AllowOverlap     configured <none>
emu.cnd.hp.com   Critical   5m       AllowOverlap     off        <none>
local            Normal     5m       DeleteSecondary  off        <none>
yak.cnd.hp.com   Unmanaged  5m       AllowOverlap     off        <none>
```

   The `STATUS` is determined by the status checks, which are performed, by default, at 5 minute intervals. The `STATUS` can be one of the following values:

`Unmanaged`	The collection station is currently not being monitored.
`Unknown`	The collection station has not yet had a status check. The initial synchronization may be in progress.
`Normal`	The collection station has responded to the most recent status check.
`Warning`	The collection station has not responded to the most recent status check, but it did respond to the status check before that.
`Minor`	The collection station has not responded to two consecutive status checks.
`Major`	The collection station has not responded to three consecutive status checks.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 1348
3740
Doc:

`Critical` The collection station has not responded to four consecutive status checks.

2. If the results of this command produce any collection stations with a status other than unmanaged, unknown, or normal, execute the following command to help determine the problem with this Windows operating system):

   xnmtopoconf -test *collectionstation*

   For example, executing this command on `hobbes.msr.hp.com` produces output similar to the following:

```
Testing station hobbes.msr.hp.com.
ICMP round trip time = 120 ms.
  Ping test to hobbes.msr.hp.com (15.31.16.141) succeeded.
  Get sysObjectID test failed:
    Error in SNMP reply: No response arrived before timeout
Test for station hobbes.msr.hp.com failed
```

   In this example, the get `sysObjectID` test failed. (Refer to the information below for potential causes.)

   Executing `xnmtopoconf -test` on a collection station with a status other than unmanaged, unknown, or normal can produce one of the following results:

   - `Ping test to the` *`collection station`* `failed:`

     This could be because the node is down or that the SNMP timeout or retry count needs to be increased.

   - `Get sysObjectID test to the` *`collection station`* `failed:`

     This could be because

     — the SNMP agent on the collection station is down.

     — the SNMP timeout or retry count needs to be increased.

     — the get community name is incorrectly configured.

   - `Get topology info test to the` *`collection station`* `failed:`

This could be because

— one or more of the services (background processes on UNIX systems) are not running on the collection station. Run `ovstatus` on the collection station to determine which services are not running. If necessary, run `ovstart` to start the services.

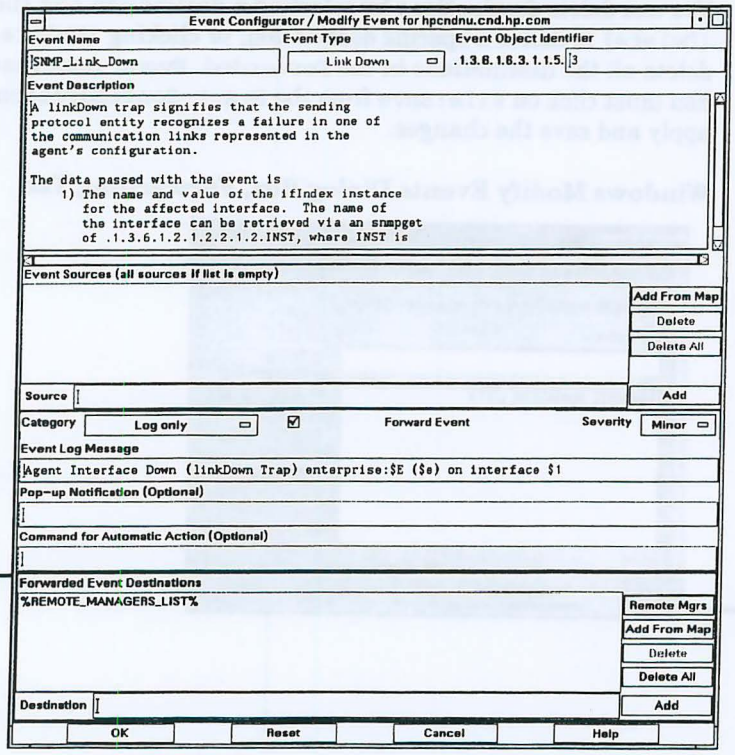
— the get community name is incorrectly configured.

- `Set event forwarding test to the` *`collection station`* `failed:`

  This could be because the set community name is incorrectly configured on either the collection station or the management station.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1349
Doc: 3740

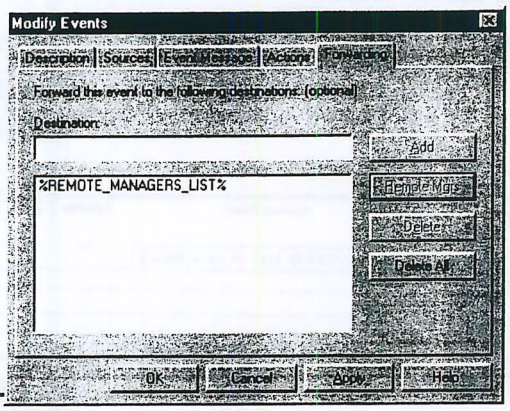
Figure 4-12 UNIX System Event Configuration/Modify Event Dialog Box



RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1350
3740
Doc.

You can delete destinations by selecting a destination and clicking `[Delete]` to delete a specific destination, or clicking `[Delete All]` to delete all the destinations in the `Forwarded Event Destinations` list. You must click on `File:Save` from the `Event Configuration` window to apply and save the changes.

Figure 4-11 Windows Modify Events Dialog Box, Forwarding Tab



7. Click `[OK]` from the `Modify Events` dialog box.
8. Click `File:Save` from the `Event Configuration` window to save the changes.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1351
Doc 3740

2. Select an enterprise from the `Enterprise list` (the `Enterprise Identification` pane on UNIX systems).
3. Select an event that you want to forward from the `Event Identification` pane.
4. On Windows systems, select `Edit:Events->Modify Event` from the menu bar in the `Event Configuration` window; the `Modify Events` dialog box appears. See Figure 4-11.

   On UNIX systems, select `Edit:Modify Event` from the menu bar in the `Event Configuration` window; the `Event Configurator/Modify Event` dialog box appears. Figure 4-12 shows the `Event Configurator/Modify Event` dialog box.
5. On Windows systems, click the `[Forwarding]` tab.

   On UNIX systems, click on the `Forward Event` check box to expand the dialog box to display the `Forwarded Event Destinations` pane.
6. Complete the `Forwarded Event Destinations` pane (`[Forwarding]` tab) by specifying the destinations to forward the events to.

   You can add destinations in the following ways:

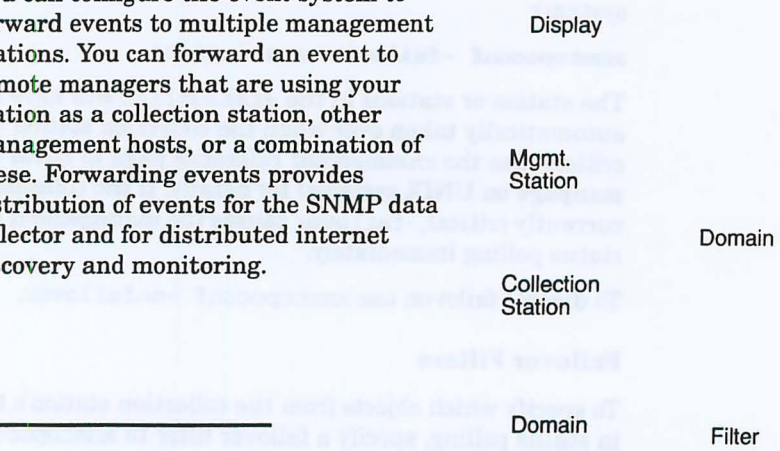
   - Clicking `[Remote Mgrs]` to add all remote management stations to the `Forwarded Event Destinations` list. The remote ons are specified in a list indicated by the special string `%REMOTE_MANAGERS_LIST%`. This list is created automatically as systems are defined to be collection stations.
   - Clicking `[Add From Map]` to add the destinations that are p.

   NOTE Even though the `%REMOTE_MANAGERS_LIST%` string exists, the actual file (*`install_dir`*`\bin\databases\remoteMgrs` on stations running a Windows operating system, `$OV_DB/remoteMgrs` on UNIX systems) may not exist, or may not contain the remote management stations you expect. You can verify the contents of the `remoteMgrs` file using a text editor.

   - Typing the destination in the `Destination` text box and clicking `[Add]`. The destination you specify can be a file containing a list of destinations, a hostname, or an Internet address.

Configuring Event Forwarding and Correlation

You can configure the event system to forward events to multiple management stations. You can forward an event to remote managers that are using your station as a collection station, other management hosts, or a combination of these. Forwarding events provides distribution of events for the SNMP data collector and for distributed internet discovery and monitoring.



NOTE When forwarding threshold events, be sure that you forward the corresponding rearm event. See the *Managing Your Network with HP OpenView Network Node Manager* manual for information on configuring threshold and rearm events.

Forwarding an Event

You can modify events to have them forwarded to multiple management stations. When you create a new event, you can specify to have that event forwarded. HP recommends that you use multiple varbinds with individual pieces of data rather than using a full string. This allows the receiving application to specify the formatting. This procedure explains how to modify an event.

1. Select Actions:`Event Configuration` from the menu bar; the `Event Configuration` window appears. From the command line, you may run `xnmtrap`.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1352
Doc 3740

Collection Station Failover

Collection station failover allows a management station to pick up status polling responsibility for a collection station that fails. To enable failover (from a command window on systems running a Windows operating system):

xnmtopoconf -failover *stationlist*

The station or stations in the *stationlist* will have status polling automatically taken over when the collection station is downgraded to critical. See the *xnmtopoconf* reference page in NNM online help (or manpage on UNIX systems) for details. If the collection station is currently critical, `-failover` causes the management station to take over status polling immediately.

To disable failover, use `xnmtopoconf -nofailover`.

Failover Filters

To specify which objects from the collection station's topology to include in status polling, specify a failover filter to `xnmtopoconf` (from a command window on systems running the Windows operating system):

xnmtopoconf -failoverFilter *filter stationlist*

A new or changed filter is applied to the objects associated with the collection stations in the *stationlist*. If the collection station is not failed over, the filter will be applied the next time it fails. However if the objects from a station are already failed over, `netmon` on the management station releases the objects associated with the collection station(s) and then reloads the collection station topology and applies the new filter as it loads the topology.

This temporarily overrides the system's choice of primary. If something changes to affect the choice of primary according to the described rules, the system will change to a new primary. The choice can be made stronger by specifying the `-preferred` option of `xnmtopoconf`. For example, execute the following command (from a command window on systems running a Windows operating system):

```
xnmtopoconf -preferred -primary stn2 gw1
```

to mark the version from `stn2` as the preferred choice for the primary collection station for this object. So long as `stn2` is managed and in a noncritical state it will be the primary collection station for `gw1`. You can clear the preference by specifying the `-clearPreferred` option (from a command window on systems running a Windows operating system):

```
xnmtopoconf -clearPreferred stn2 gw1
```

Changing the Overlap Mode

The overlap mode determines how the system behaves when an overlap is detected between the local management station and a remote collection station. The overlap mode applies to the collection station from the management station's perspective. The overlap mode is applied when an object is made a secondary to another remotely monitored version of the object. (See "Overlaps with the Collection Domain of the Management Station" on page 55 for a complete description.) To change the overlap mode use the `-overlap` option of `xnmtopoconf` (from a command window on systems running a Windows operating system):

```
xnmtopoconf -overlap mode local
```

where *mode* can be one of the following:

- `Allow Secondary Local Objects`
- `Unmanage Secondary Local Objects`
- `Delete Secondary Local Objects` (default)

The mode applies to all monitored objects for the local management station that are made secondaries for other remotely monitored objects. The mode cannot be changed on an individual object basis.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1353
Doc 3740

produces the following output:

```
OBJECT ID(S)    OBJECT      STATUS      IP ADDRESS       STATION
146              gw1        Normal      10.2.104.1       remstn1
146/145          gw1        Normal      10.2.112.1       remstn1
146/595          gw1        Normal      10.2.104.1       remstn1
146/1158         gw1        Normal      10.2.120.1       remstn1
146             &gw1        Unmanaged   10.2.104.1       local
146/145         &gw1        Unmanaged   10.2.112.1       local
146/595         &gw1        Unmanaged   10.2.104.1       local
146/1158        &gw1        Unmanaged   10.2.120.1       local
146             &gw1        Unknown     10.2.104.1       stn2
146/145         &gw1        Unknown     10.2.112.1       stn2
146/595         &gw1        Unknown     10.2.104.1       stn2
146/1158        &gw1        Unknown     10.2.120.1       stn2
```

In the second example, the node `gw1` has the collection station `remstn1` as its primary station, but is also known to be monitored by `stn2` and by the local management station. (The special station name `local` is used to represent locally monitored objects.) The "`&`" symbol designates the secondary versions of the objects. (Meanings of other symbols in this location are documented in the *ovtopodump* reference page in NNM online help (or manpage on UNIX systems)).

Changing the Primary Collection Station for an Object

The system will choose a primary collection station for an object, based on the rules as described in "The Selection of Primary and Secondary Collection Stations" on page 53. This choice should be adequate for most purposes. However, you can explicitly override the choice of primary by specifying the `-primary` option to the `xnmtopoconf` command. For example, executing the following command makes the designated collection station the primary for the listed objects. This requires `root` access on UNIX systems or `Administrator` privileges on systems running a Windows operating system.

`xnmtopoconf -primary` *`collectionstation object`*

For example, if it was desired that `stn2` be the primary for `gw1`, the following command could be executed (from a command window on systems running a Windows operating system):

```
xnmtopoconf -primary stn2 gw1
```

Using Distributed Data Collection

This section discusses how to export data from collection stations into a single Relational Database Management System (RDBMS) for report generation. For each collection station, use the following procedure:

1. Use the Network Node Manager data collector tool to collect MIB data. Refer to the *Managing Your Network with HP OpenView Network Node Manager* manual for information on data collection.
2. Determine which data collector files you want to merge into the RDBMS. These files are located in *install_dir*\databases\snmpCollect (`$OV_DB/snmpCollect` on UNIX systems).
3. Use `ftp` or `rcp` to copy the files from the collection station to a temporary data directory on the management station. You should also copy each data file's corresponding description file. The description file is named identically to the data file, except that an exclamation mark (`!`) is appended to the end of the filename. For example,

   ```
   rcp $OV_DB/snmpCollect/ifInOctets.1 clifford:/tmp/collsta5
   rcp $OV_DB/snmpCollect/ifInOctets.1! clifford:/tmp/collsta5
   ```

   copies the data and description files for instance 1 of MIB variable `ifInOctets` to the management station `clifford`.

   Alternately, if the network link between the management station and collection station is of sufficient capacity, you may make the files accessible via NFS.
4. If the file *install_dir*\conf\collectProxyMap (`$OV_CONF/collectProxyMap` on UNIX systems) exists on the collection station, copy it to the management station as well, either in the temporary data directory or another directory.
5. Make sure the temporary directory on the management station has `drwxrwxrwx` permission and that each data file has `-rw-rw-rw` permission.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1354
3740
Doc:

6. On the management station, run the `ovcoltosql` command as `root`, to export the data into the RDBMS. Specify the temporary data directory as the data source by using the `-s` option. For example, (from a command window on systems running a Windows operating system):

   `ovcoltosql -Ro -s /tmp/collsta5`

   This example exports data from the directory `/tmp/collsta5` into an Oracle database.

   If there is a `collectProxyMap` file for the collection station, use the `-p` option of `ovcoltosql` to specify the proxy map file location.

   Refer to the *ovcoltosql* reference page in NNM online help (or manpage on UNIX systems), and to the *Reporting and Data Analysis with HP OpenView Network Node Manager* manual for options that you can specify with this command.

If two or more collection stations collect on the same instance of the same MIB variable on the same node, they are said to have an overlapping collection. If data from an overlapping collection is merged into a single RDBMS, some of the data will not be entered into the RDBMS. `ovcoltosql` exports the data that is more recent than that already in the RDBMS. The collection station from which data is exported first will have data from its overlapping collection entered into the RDBMS, while most, if not all of the overlapping data from the second collection station

NOTE

You can execute `ovcoltosql` on the collection stations themselves to a common RDBMS server, but it is not recommended. This can cause potential performance problems when slow network links are traversed. Also, this approach results in the `topo_id` column of the `snmp_trend_dataset` table, which consists of topology IDs, to be assigned by different collection stations. Hence, the column will be useless for performing SQL joins across topology and trend tables.

Refer to the *Reporting and Data Analysis with HP OpenView Network Node Manager* online manual for information on RDBMS querying and administering operations.

5 Dynamic Views and Distributed Management

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1355
3740
Doc:

This chapter discusses how several NNM dynamic views function when you use them with DIDM. Readers are assumed to have read previous chapters and understand how to configure collection station to management station communication.

Dynamic Views and Distributed Management

Numerous dynamic views are available from NNM. These views present a graphical (or tabular) representation of your network infrastructure.

Management station views of the Neighbor view and Path view will display links to views from collection stations or provide additional information in the following situation:

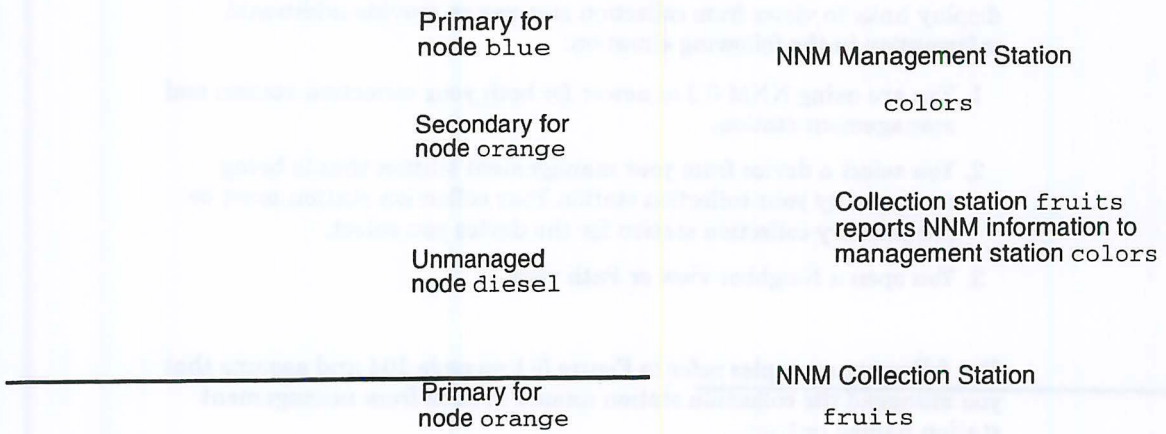
1. You are using NNM 6.3 or newer for both your collection station and management station.
2. You select a device from your management station that is being managed by your collection station.Your collection station must be the primary collection station for the device you select.
3. You open a Neighbor view or Path view.

NOTE The following examples refer to Figure 5-1 on page 164 and assume that you managed the collection station named `fruits` from management station named `colors`.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1356
3740
Doc:

Figure 5-1 shows node `colors` acting as a management station that manages node `blue` and collection station `fruits` within an NNM distributed environment. In this example, collection station `fruits` forwards NNM information to management station `colors`.

Figure 5-1 NNM Dynamic Views: Collection Station to Management Station Communication



NNM Neighbor View

The Neighbor view shows you a graphical representation of the selected device and the connector devices related to it, within a specified number of hops of the selected device.

To open a Neighbor view from NNM, use the `Tools:Views->Neighbor` me wser to htt 0/topology/neighborView.

NOTE Replace *hostname* in the examples with the actual hostname or the IP address of the system NNM is installed on.

A N des the following information in the environment shown in Figure 5-1:

- The management station `colors` is primary for `blue`. If you open a Neighbor view from `colors` with `blue` selected, it does not show nodes that are managed remotely. In this example, `orange` is not in the view, even if it is within the hop distance, because it is remotely managed by `fruits`. The Neighbor view includes a graphical representation of `blue` and other locally managed nodes of `colors`.
- Assume `colors` has a secondary copy of `orange` in its topology database, but that `fruits` is primary for `orange`. If you open a Neighbor view from `colors` with `orange` selected, it does not show nodes that are managed locally. In this example, `blue` is not in the view, even if it is within the hop distance, because it is locally managed by `colors`. The Neighbor view includes a graphical representation of `orange` and other locally managed nodes of `fruits`. This view also provides a link to a Neighbor view from `fruits`.
- If you try to open a Neighbor view of `diesel`, the Neighbor view tells you that `diesel` does not exist in the topology.

NNM Path View

The Path view presents a graphical representation of the path between two nodes and a table of interface information about the devices contained in the path.

To open a Path view from NNM with Extended Topology, use the `Tools:Views->Path` menu or point your browser to `http://`*`hostname`*`:7510/topology/pathView`.

Refer to Figure 5-1 on page 164. If you open a Path view from `colors` with `blue` as the source node and `orange` as the destination node, NNM displays the Path view, a table of interface information about the devices contained in the path, and tells you that `orange` is managed by `fruits`.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1357
Doc: 3740

Dynamic Views and Distributed Management

A The Filter Definition Language

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1358
Doc: 3740



The Filter Definition Language

This appendix discusses in detail the language used to define filters in the filter definition file, giving you the information you need to modify existing filters, or define new ones.

This appendix is a reference to the contents of the filter definition file, and to the grammar of the filter definition language.

NOTE This appendix assumes that you are familiar with two topics normally covered in the study of computer science: Boolean expressions and Backus-Naur Form (BNF) grammars. This appendix makes no attempt to teach the fundamentals of either Boolean expressions or BNF grammars. If you are unfamiliar with these topics, you may find it helpful to review these ideas in a computer science text book before you feel entirely comfortable defining new filters.

The Filter Definition File

Filters are defined in an editable file of ASCII characters; this is called the filter definition file. The format and contents of this file make up the subject of this appendix.

The filter definition file for all the filters you use with HP OpenView Network Node Manager (discovery, topology, map, and persistence) is *install_dir*\conf\C\filters on Windows operating systems and $OV_CONF/$LANG/filters on UNIX systems.

After you install NNM, the filter definition file contains a selection of useful definitions that you may be able to use as is, or with some modifications.

The filter definition file has several key components, and they appear in the file in the following order:

- Set definitions.
- Filter definitions, which each include one or more Attribute Value Assertions.
- Filter-Expression definitions, which each refer to one or more filters.

Each of these components is described in considerable detail in later sections of this appendix.

The filter definition file contains many instances of the above elements, always in order. That is, all set definitions are together at the top of the file, all filter definitions follow next, and all filter-expression definitions are at the end of the file.

As you examine the filter and filter-expression definitions in the sample filter definition file ("Default Filter File" on page 197), you will notice that some are intended for use as map filters, others are for discovery filtering. This distinction helps clarify the purpose of each filter and its components, and simplifies your troubleshooting of new or modified filters. Also, remember which types of filters are intended to *exclude* items and which are to *include*. Refer to Table 2-1 on page 38 for more information.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1359
Doc: 3740

Filters and Filter-Expressions

The whole purpose of the filter definition file is to define the filters that are used with the scalability features of NNM. You have two basic types of filters: "simple" filters (which are simple only in that they do not refer to other filters), and filter-expressions.

Filters and filter-expressions are closely related and used identically. Everywhere else, they are referred to broadly as "filters." Within the filter definition file, however, there is a distinction between them:

- A **filter** is a combination (or "expression") of one or more Attribute Value Assertions.[1]
- A **filter-expression** is a combination (or "expression") of one or more previously defined filters. In other words, a filter-expression is a "high- level filter," created by combining lower-level filters that are already defined.

In every other respect, a filter-expression is exactly like a filter. You use filters and filter-expressions in exactly the same way. That is, anywhere a filter can be used, a filter-expression can also be used. Although most of the examples in this section uses filters, filter-expressions would be equally valid in those same examples.

You use logical, also called Boolean, operators (that is, And (`&&`), Or (`||`), and Not (`!`)), and normal precedence grouping via parentheses, to combine multiple filters in a filter-expression, or to combine multiple Attribute Value Assertions (AVAs) in a filter.

Defining filters and filter-expressions has two important rules:

1. A filter definition can include *only* AVAs. A filter definition can *not* include filters or filter-expressions.
2. A filter-expression definition can include *only* filters or filter-expressions that are defined earlier in the filter file. A filter-expression definition can *not* include AVAs.

1. See "Attribute Value Assertions" on page 172 for more details.

Sets

String-valued attributes can be tested for membership in a set. A **set** is simply a list of strings. The only operation available on sets is the test for membership.

You can enumerate the members of a set in two ways:

- Within the filter file itself, according the filter file grammar.[1]
- In a separate file, where set members are listed, one per line. You cannot use wildcards or ranges. If the set member begins with a slash ("/"), it is used as the absolute pathname of such a file. Relative pathnames and environment variables are invalid. In the Windows operating system, filter files must use the forward slash and should include a drive specification.

Files and member strings can be mixed in the same set definition. Set definitions can not be nested.

1. See "Filter File Grammar" on page 187 for details

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1360
Doc: 3740

Attribute Value Assertions

An **attribute value assertion** (**AVA**) is a statement about the value of an attribute. For example, here is an AVA about the `"IP Hostname"` attribute:

```
"IP Hostname" == "server7"
```

An object can be compared against an AVA to determine whether that assertion is true or false for the object. In other words, an AVA is a condition that an object either does or does not meet. When an AVA is tested against a particular object, one of three results can occur:

- The object does not have that attribute.
- The object has the attribute, but the value of the attribute does not match the value in the filter.
- The object has the attribute, and the value of the attribute matches the value in the filter.

The above AVA will be false when the object has an IP hostname attribute, but the IP hostname of the object is *not* "server7". It will *also* be false when the IP hostname attribute is not present in an object.

The above AVA will only be true when the object has an IP hostname attribute, and the IP hostname of the object is "server7". Similarly the AVA `isRouter==TRUE` is only true for routers.

AVAs are defined in terms the of fields of an object and possible values of those fields. The fields used in creating AVAs for filters are a subset of the fields contained in the object database (`ovwdb`).[1]

NOTE Many field names in the object database have embedded white space. Any field name or field value containing white space must be enclosed in double quotes (for example `"Selection Name"`).

In the object database, attributes can have four types:

1. See "Filterable Objects and Attributes" on page 181 for the specific fields you can use in filters.

- Boolean
- Integer
- String
- Enumerated

Attribute value assertions fall into one of these four categories, depending on the attribute type.

After a short section that discusses the operators that are valid in AVAs, AVAs for each of the above types of attributes are covered in more detail.

NOTE Attribute Value Assertions can only be tested against literal constant values. The attributes of two different objects cannot be tested against each other.

Valid Operators for AVAs

These are the operators that you can use to express AVAs:

Operator	Meaning
==	Equal to
!=	Not equal to
>	Greater than
>=	Greater than or equal to
<	Less than
<=	Less than or equal to
~	Like, which used for pattern matching.[1]
!~	Not like, also used for pattern matching.
IN	Is a member of the set

1. See "String AVAs" on page 175 for more information.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1361
3740
Doc:

TIP Filters are "short-circuit" evaluated. This means NNM only reads far enough to get an answer, then doesn't read the rest of the filter definition. For best performance, put likely TRUE clauses first when OR-in, and put likely FALSE clauses first when AND-ing.

Table A-1, Operators Allowed in AVAs for Each Field Type, shows which of these operators are valid in particular AVAs, depending on the field type of the attribute.

Table A-1 Operators Allowed in AVAs for Each Field Type

Operator	ovwStringValue	ovwEnumValue	ovwIntValue	ovwBooleanValue
==	Yes	Yes	Yes	Yes
!=	Yes	Yes	Yes	Yes
>	Yes	No	Yes	No
>=	Yes	No	Yes	No
<	Yes	No	Yes	No
<=	Yes	No	Yes	No
~	Yes	No	No	No
!~	Yes	No	No	No
IN	Yes[1]	No	No	No

1. Valid only if the value of the expression is the name of a defined set. See "Sets" on page 171 for details.

Boolean AVAs

Boolean AVAs can be expressed with just an attribute name (with an optional, leading NOT operator), or can be explicitly tested against the keyword values TRUE and FALSE. For example, testing for a object being a router can be expressed in either of the two following ways:

```
(isRouter)

(isRouter == TRUE)
```

Specialized Pattern Matching in NNM Filters

There are two special types of string-valued AVAs for which NNM provides specialized pattern matching on the associated attributes:

SNMP Object IDs (SNMP OIDs)	In a filter, an SNMP OID is identified as a leading period followed by decimal octets separated by periods. For example: `.1.3.6.34.2.209`
IP addresses	An IP address is identified as a string of exactly four (4) decimal octets separated by periods, but *without* a leading period: `23.26.11.14`

Three types of specialized pattern matching are available—wildcards, ranges, and sets. Set patterns are available only for SNMP OIDs. You can replace any decimal octet in an IP address or SNMP OID with a special pattern matching string.

NOTE Do not overlook the "Caution" block in "Set Specifications in SNMP OIDs" on page 179.

Wildcard Characters in SNMP OIDs and IP Addresses For IP address and SNMP OID pattern matching, the wildcard operator is the asterisk (*). An asterisk in an IP address indicates that any value is acceptable in the given decimal octet.

For example, to pass any address in the Class A IP network "23", you would use the following in your AVA:

```
"IP Address" ~ 2 3.*.*.*
```

The wildcard character acts slightly differently for SNMP OIDs. In this case, a wildcard indicates that any value *for zero or more* decimal octets is acceptable. For example, the following pattern:

```
.1.4.5.1.*.13.2.*
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1362
Doc. 3740

matches any OID with ".1.4.5.1" followed by any number of decimal octets of any value (including no octets at all), followed by "13.2" followed by zero or more trailing decimal octets. Therefore, the above pattern would match the following OIDs:

- .1.4.5.1.13.2
- .1.4.5.1.22.33.13.2
- .1.4.5.1.13.2.14.55.232
- .1.4.5.1.22.44.33.13.2.23.32.1

but not:

- .1.4.5.1.13 (no 2 after the 13)
- .1.4.5.2.2.13.2 (no 1 after the 5)
- .1.4.5.1.33.22.2 (missing the 13)

Range Specifications in SNMP OIDs and IP Addresses A range is expressed by a decimal integer, a hyphen (-), and another decimal integer that is greater than the first. Decimal octet values between 2 and 68 would be specified as follows:

```
2-68
```

A range indicates that any value in the range (inclusive) is acceptable in the given decimal octet. Ranges are significant for the given decimal octet only, in both SNMP OIDs and IP addresses. The values specified in a range must be in their natural order, from smallest to largest; a reversed range (like, for example, 68-2) is not permitted.

The following are more examples of valid SNMP OIDs and IP address AVAs, using sets, wildcards, and ranges in combinations:

```
("IP Address" ~ 23.2.*.*)
("IP Address" ~ 23.2.3-9.*)
("IP Address" ~ 23.2.16-22.0-1)
("SNMP sysObjectID" ~ .1.3.6.*.9.5)
("SNMP sysObjectID" ~ .1.3.6.8-9.*)
("SNMP sysObjectID" ~ .1.3.6.7-8.12-13)
```

Set Specifications in SNMP OIDs In SNMP OIDs (but not IP addresses), you can specify a set of decimal octets in any position by separating the members by a comma. For example, in the following AVA:

```
("SNMP sysObjectID" ~ .1.3.6.34.8,9,11,23)
```

would match the following SNMP OIDs:

```
("SNMP sysObjectID" ~ .1.3.6.34.8)
("SNMP sysObjectID" ~ .1.3.6.34.9)
("SNMP sysObjectID" ~ .1.3.6.34.11)
("SNMP sysObjectID" ~ .1.3.6.34.23)
```

CAUTION To invoke special pattern matching on IP address and SNMP OID strings, either the "like" operator (~) or "not like (!~) *must* be used.

Furthermore, to use NNM's specialized pattern matching facility, the IP address or SNMP OID string *must not* be enclosed in quotation marks. The presence of enclosing quotation marks means that the string will be treated as a regular expression, and *not* given specialized pattern matching; the absence of such quotation marks means the comparison *will* use NNM's specialized pattern matching facility.

The difference is important. Consider this AVA, where the value is quoted:

```
"IP Address" ~ "23.18.3.*"
```

With the quotation marks around the value (`"23.18.3.*"`), it is treated as a regular expression. The result is that *many* IP addresses beginning with "`23.18.3`" would cause the AVA to evaluate to `TRUE`, including, for example, `23.18.34.7`, which was probably not intended. In fact, even some strange and improbable IP address strings (like, for example, `23518.3711.1011.23033`) would pass this AVA. The reason is that, for regular expressions, the period character (`.`) matches *any* character in that location of the comparison string (including, confusingly, the period character itself).

However, if we use the same AVA, but *without* the quotation marks around the value (`"IP Address" ~ 23.18.3.*`), NNM's special pattern matching facility guarantees that only IP addresses in the apparently intended range would cause the AVA to evaluate to `TRUE`.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1363
Doc 3740

Excluding a Node

For the purposes of building and using filters, a node can be thought of as a "super-object", which comprises the node and all its interfaces.

Thus, if a node object passes a filter, the filter will also pass all interfaces of the node regardless of whether they would, considered in isolation, pass the filter.

Similarly, if an interface passes a filter, the node object it belongs to, and all other interfaces of that node, also pass the filter.

Consequently, if you want a filter to exclude a node, the filter must block the node object itself and all of its interfaces.

NOTE Keep in mind that the `ovfiltertest` command does not follow this pattern. Instead of treating a node and its interfaces as a "super-object,", the `ovfiltertest` command treats nodes and interfaces as separate objects. See the *ovfiltertest* reference page in NNM online help (or the UNIX system manpage) for more information.

Relationships Between Nodes and Interfaces

You can create a filter that combines nodes and interfaces, as shown in the following example.

```
nodeNinterface "" {(vendor = "SUN") && (IP Address ~ 15.2.112.*)}
```

Valid Operators for Logical Combinations of AVAs or Filters

AVAs, filter names, and filter-expression names are combined to create filter and filter-expression definitions (as noted before, *only* AVAs are allowed in a filter definition, and AVAs are *never* allowed in a filter-expression definition).

You use the following operators to create logical combinations (or "expressions") of these components. Likewise, you combine filters or filter-expressions in a filter-expression definition with these operators:

Operator	Meaning
&&	Logical "and", used to combine multiple AVAs and filter names into logical expressions.
||	Logical "or", used to combine multiple AVAs and filter names into logical expressions.
!	Logical negation, used to negate stand-alone field names and other logical expressions. Fields that are already part of an expression cannot be negated; rather the entire expression should be negated.

Use parentheses—"(" and ")"—to specify explicit precedence in a group of operations. For example, a filter definition might look like this:

```
Filtr1 "" { isRouter && (numInterfaces > 1) }
```

Or a filter-expression definition might look like this:

```
FiltrExpr1 "" { (Filtr1 || Filtr2) && Filtr3 }
```

Filterable Objects and Attributes

The following four tables specify, for each type of object, the attributes (fields) for which filters can be defined. This is a subset of the objects and attributes in the ovwdb database.

Table A-2 Filterable Fields in Node Object

Field	Field Type
IP Hostname	String
IP Status	Enumerated
isATM *	Boolean
isBGP4 *	Boolean
isBridge	Boolean
isCDP *	Boolean
isCollectionStationNode	Boolean
isConnector	Boolean
isDS1 *	Boolean

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1364
Doc: 3740

Table A-2 Filterable Fields in Node Object (Continued)

Field	Field Type
isDS3 *	Boolean
isFrameRelay *	Boolean
isHSRP *	Boolean
isHub	Boolean
isIP	Boolean
isIPRouter	Boolean
isIPV6 *	Boolean
isIPX	Boolean
isIPXRouter	Boolean
isMcClusterMember	Boolean
isMPLS *	Boolean
isNetWareServer	Boolean
isNode	Boolean
isOSPF *	Boolean
isRMON *	Boolean
isRMON2 *	Boolean
isRouter	Boolean
isSONET *	Boolean
isSNMPSupported	Boolean
isSTP *	Boolean
isVRRP *	Boolean
isWireless *	Boolean
NetWare Server Name	String

Table A-2 Filterable Fields in Node Object (Continued)

Field	Field Type
Selection Name	String
SNMPAgent	Enumerated
SNMP sysContact	String
SNMP sysDescr	String
SNMP sysLocation	String
SNMP sysName	String
SNMP sysObjectID	String
TopM Interface Count	Integer
vendor	Enumerated

IMPORTANT * Fields marked with an asterisk have no effect on discovery filters.

Table A-3 Filterable Fields in Interface Object

Field	Field Type
isInterface	Boolean
isIP	Boolean
isIPX	Boolean
IPX Address	String
IP Address	String
IP Status	Enumerated
IP Subnet Mask	String
Selection Name	String

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1365
3740
Doc:

Table A-3 Filterable Fields in Interface Object

Field	Field Type
SNMP ifDescr	String
SNMP ifName	String
SNMP ifPhysAddr	String
SNMP ifType	Enumerated
TopM Network ID	Integer
TopM Node ID	Integer
TopM Segment ID	Integer

Table A-4 Filterable Fields in Segment Object

Field	Field Type
IP Segment Name	String
IP Status	Enumerated
isBusSegment	Boolean
isFDDIRingSegment	Boolean
isSegment	Boolean
isSerialSegment	Boolean
isStarSegment	Boolean
isTokenRingSegment	Boolean
Selection Name	String
TopM Interface Count	Integer
TopM Network ID	Integer

Table A-5 Filterable Fields in Network Object

Field	Field Type
IP Address	String
IP Network Name	String
IP Status	Enumerated
IP Subnet Mask	String
IPX Address	String
IPX Network Hop Count	Integer
isIP	Boolean
isIPX	Boolean
isNetwork	Boolean
Selection Name	String
TopM Default Seg ID	Integer
TopM Interface Count	Integer
TopM Segment Count	Integer

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1366
Doc: 3740

Valid values for the enumerated fields can be found in the files listed in Table A-6, Value Definitions for Enumerated Fields,

Table A-6 Value Definitions for Enumerated Fields

For the field named:	The enumerated values are defined in:
`IP Status`	On Windows operating systems: *install_dir*\fields\C\ip_fields On UNIX systems: $OV_FIELDS/$LANG/ip_fields
`SNMP ifType`	On Windows operating systems: *install_dir*\fields\C\snmp_fields On UNIX systems: $OV_FIELDS/$LANG/snmp_fields
`SNMPAgent`	On Windows operating systems: *install_dir*\fields\C\snmp_fields On UNIX systems: $OV_FIELDS/$LANG/snmp_fields
`vendor`	On Windows operating systems: *install_dir*\fields\C\ovw_fields On UNIX systems: $OV_FIELDS/$LANG/ovw_fields

Filter File Grammar

The following is the formal Backus-Naur Form (BNF) grammar for a filter file. See "Filters" on page 37 for details about where such a file is used.

```
Filter_File          ::=   Filters
                           | Filters FilterExprs
                           | Sets Filters
                           | Sets FiltersFilterExprs

Sets                 ::=   "Sets" "{" Set_Stmts"}
                           | "Sets" "{" "}"

Set_Stmts            ::=   Set_Stmt
                           | Set_Stmts Set_Stmt

Set_Stmt             ::=   SetName Description "{" Memberlist"}"

Memberlist           ::=   Member_Stmt
                           | Memberlist "," Member_Stmt

Member_Stmt          ::=   StringOrIdentifier
                           | <absolute_file_pathname>

Filters              ::=   Filters" "{" Filter_Stmts"}"
                           | "Filters" "{" "}"

Filter_Stmts         ::=   Filter_Stmt
                           | Filter_Stmts Filter_Stmt

Filter_Stmt          ::=   FilterName Description "{" Expression"}"

Expression           ::=   Expression "&&" Expression
                           | Expression"||" Expression
                           | "!" Expression
                           | "(" Expression ")""
                           | BoolExpr
                           | SetExpr

BoolExpr             ::=   FieldName
                           | FieldName ExprOperator <string>
                           | FieldName ExprOperator <integer>
                           | FieldName PatternOperator <string>
```


RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1367
Doc 3740

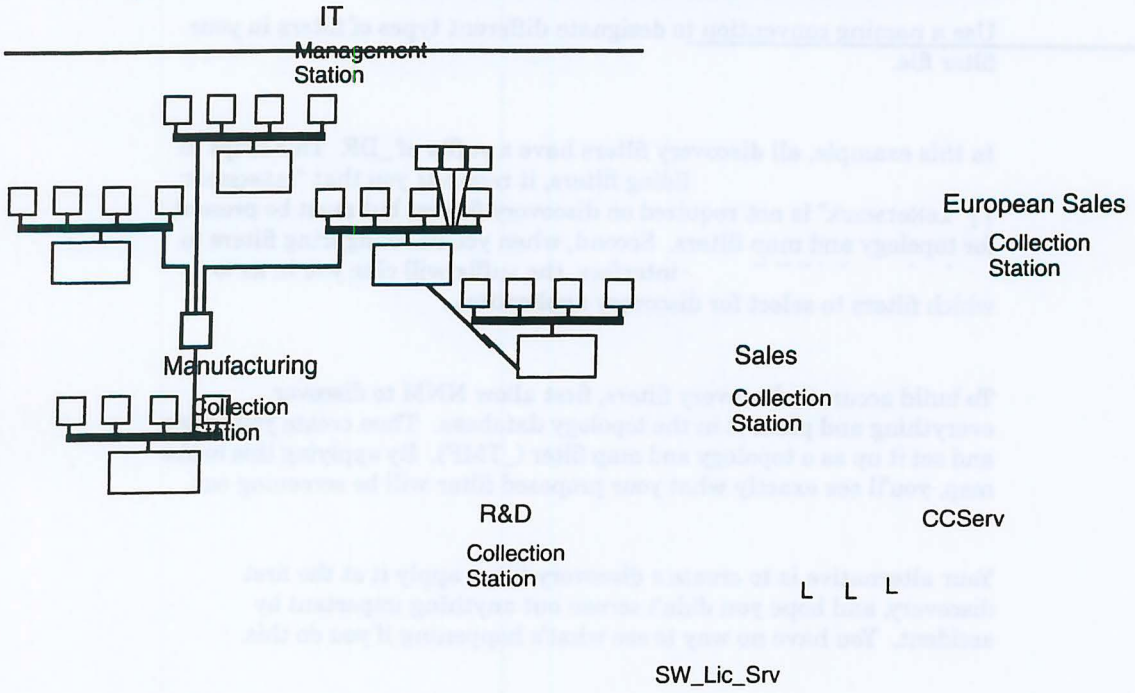
```
SetExpr              ::=    FieldName "IN" SetName

FilterExprs          ::=    "FilterExpressions" "{" FilterExpr_Stmts "}"
                            | "FilterExpressions" "{" "}"

FilterExpr_Stmts     ::=    FilterExpr_Stmt
                            | FilterExpr_Stmts FilterExpr_Stmt

FilterExpr_Stmt      ::=    FilterExprName Description "{" FiltExpr "}"

FiltExpr             ::=  FiltExpr "&&" FiltExpr
                            | FiltExpr "||" FiltExpr
                            | "!" FiltExpr
                            | "(" FiltExpr ")"
                            | FilterName

FieldName            ::=  StringOrIdentifier

ExprOperator         ::=  "==" | "!=" | "<" | "<=" | ">" | ">="

PatternOperator      ::=  "~" | "!~"

FilterExprName       ::= <unquoted_string>

FilterName           ::= <unquoted_string>

SetName              ::= <unquoted_string>

StringOrIdentifier   ::= <quoted_string> | <unquoted_string>

Description            ::=  <quoted_string>
```

Filter File Example

This example describes how these rules translate into usable filters for a sample network management solution. Hemispheres-Petroleum Company has decided to implement HP OpenView Network Node Manager's distribution capabilities to gain control over their overall network. They have a typical network organization that parallels their personnel organization -- local area networks for the Research and Development, Manufacturing, and Sales departments, with an additional network in place in Paris for European Sales. The network architecture is diagrammed in Figure A-1.

The IT department will be responsible for managing these networks, along with their own. They have decided to have a collection station for each department report to the management station in IT.

Figure A-1 Hemispheres-Petroleum Company Network Layout



RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1368
3740
Doc:

The default filter file shipped with NNM has several useful building blocks already in place. (The default filter file appears on page 197.) Simple filters appear in the second section of the files, in the format `FilterName "Description" { AVA }`. For example, look at the line that says `Hubs "Any multi-port repeater" { isHub }`. The name of the filter, as it would later be used from the `ovw` user interface or in building filter expressions, is Hubs. `netmon` compares every node's SNMP response, looking for the `isHub` property. Any object possessing this property fits the filter `Hubs`. Similarly useful simple filters are in place for Networks, Segments, Nodes, IPRouters, Bridges, SNMPNode, HPNodes, and NonHPNodes.

Setting Up Collection Domains

Collection domains are specified through discovery filters. Setting these up demonstrates several tips that will help you manage filters for your network.

TIP Use a naming convention to designate different types of filters in your filter file.

In this example, all discovery filters have a suffix of _DF. This helps in building filters, it reminds you that "`isSegment || isNetwork`" is not required on discovery filters, but must be present for topology and map filters. Second, when you're configuring filters to interface, the suffix will clue you in as to which filters to select for discovery application.

TIP To build accurate discovery filters, first allow NNM to discover everything and place it in the topology database. Then create your filter and set it up as a topology and map filter (_TMF). By applying this to the map, you'll see exactly what your proposed filter will be screening out.

Your alternative is to create a discovery filter, apply it at the first discovery, and hope you didn't screen out anything important by accident. You have no way to see what's happening if you do this.

First set up the collection domain for the IT department's own management station. Using the pattern filter named `EngrLan` in the default filter file, add a filter named `ITLan_DF`, which includes the IP address range for IT nodes (15.2.107-117):

```
ITLan_DF "IT's IP subnet" { ("IP Address" ~ 15.2.107-117.*) }
```

Reading that back, the name of the filter is `ITLan_DF` and can be referred to by filter expressions and user interface fields that ask for a filter name. It passes objects whose IP Address field in their SNMP data is between (is like) 15.2.107.* and 15.2.117.*.

Now build a filter expression (combination of filters) to turn that into a topology and map filter:

```
ITLan_TMF "IT's IP subnet" {("IP Address" ~ 15.2.107-117.*)|| NetsNSegs}
```

The addition of `NetsNSegs`, a standard NNM filter, passes all objects with SNMP data matching `isSegment` or `isNetwork`. A discovery filter includes these by default, but topology and map filters must add them explicitly. Networks and segments are required so that node objects will have containers in which to reside. Without them, your map database becomes corrupted.

Now is the time to use the tip above. First allow NNM to discover everything and place it in the topology database. Then apply the TMF filter to the map using `ovtopodump -f`, showing exactly what will be screened out.

The IT network management administrator sets up similar filters for `SalesLan`, `MfgLan`, `RDLan`, and `ESalesLan`. Here is the filter file so far (without all the comment lines):

```
Filters {
Networks "Any network" { isNetwork }
Segments "Any segment" { isSegment }
NetsNSegs "All networks & segments" { isNetwork || isSegment }
Nodes "Any node" { isNode }
IPRouters "Any IP Router" { isIPRouter }
Bridges "Any bridge" { isBridge }
Hubs "Any multi-port repeater" { isHub }
SNMPNode "Any node supporting SNMP" { isNode && isSNMPSupported }
HPNodes "Hewlett-Packard nodes" { isNode && ( vendor == "Hewlett-Packard" ) }
UBNodes "Ungermann-Bass Nodes"  { isNode && vendor == "Ungermann-Bass" }
NonHPNodes "Non-HP nodes" { isNode && ( vendor != "Hewlett-Packard" ) }
ITLan_DF "IT's IP subnet" { ("IP Address" ~ 15.2.107-117."*) }
SalesLan_DF "Sales's IP subnet" { ("IP Address" ~ 15.2.125-140.*) }
MfgLan_DF "Manufacturing's IP subnet" { ("IP Address" ~ 15.2.145-160.*) }
```


RQS nº 05/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1369
3740
Doc:

```
RDLan_DF "R&D's IP subnet" { ("IP Address" ~ 15.2.175-250.*) }
ESalesLan_DF "European Sales's IP subnet" { ("IP Address" ~ 192.5.32-50.*) }
}

FilterExpressions {
ITLan_TMF "IT's IP subnet map filter" { ITLan_DF || NetsNSegs }
SalesLan_TMF "Sales's IP subnet map filter" { SalesLan_DF || NetsNSegs }
MfgLan_TMF "Manufacturing's IP subnet map filter" { MfgLan_DF || NetsNSegs }
RDLan_TMF "R&D's IP subnet map filter" { RDLan_DF || NetsNSegs }
ESalesLan_TMF "European Sale's IP subnet map filter" { ESalesLan_DF || NetsNSegs
}
}
```

With these filters, each collection station can specify its own domain of interest with no overlap.

TIP Build your overall filter file once and propagate it from your management station to all the collection stations. Use RCS for version control on the file and `rcp` to copy it to the collection stations. This way you know exactly what each collection station operator is looking at. You retain control over the file contents. And you can see a collection station's view of the network from the management station by applying the collection station's topology filter as a map filter on the management station.

Excluding Nodes

Take another look at the Sales LAN. It includes three laptop computers for sales people who are often on the road. The network operator really doesn't need to track whether those nodes are up or down, so write a DHCP filter that can exclude them:

```
SalesLaptops "Laptop units often offline in Sales
department" {"IP Address" ~ 15.2.135-140.*}
```

Now in a filter expression you can refer to `{SalesLan && !(SalesLaptops)}`. This is rather long, but it allows you to identify those laptops separately sometimes. Certainly, you could use this in a topology filter on the Sales collection station that would disable the status of these nodes being sent to the management station continuously.

You could also have specified `&& !("IP Address" ~ 15.2.135-140.*)` on the overall `SalesLan` filter if you knew you would never want the laptops included.

CAUTION

When negating the "is like" operator (~), place the negation *outside* of the expression. This is necessary due to NNM discovering all level 2 interfaces, including objects like serial cards which have no IP address. When no IP address is present, the object is assigned 0.0.0.0. If you negate the operator, as in `"IP Address" !~ 1.2.3.4`, you will inadvertently *include* all non-IP level 2 interfaces. By negating the expression, as in `!("IP Address" ~ 1.2.3.4)`, you get the set of all objects that *have* an IP address, and it is not like the one in the expression.

Failover Filters

What would happen if the Sales collection station failed? Assuming you have the management station configured for failover, all the nodes that the Sales collection station has in its topology database are polled by the management station. A failover filter would specify only the most critical nodes for which the management station would actually pick up status polling.

Sales is currently a fairly small department, so no filter is needed yet. When the Sales department grows, IT will probably want to limit which ones qualify for management failover.

Important Node Filters

Suppose the hub between the management station and the Sales collection station (actually, all the collection stations in this example) goes down. The management station will log an event that the hub is down, with secondary information that each of the nodes behind the hub is also unreachable. Getting that hub back online is a top priority, and most of the other stations are indeed secondary -- except that credit card authorization server. Access to that server is critical to business and the network operator needs to know about that immediately. By setting up an important node filter, you can assure that this node always qualifies as a primary event in the alarm browser.

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1370
3740
Doc:

```
SalesImptNodes "Critical nodes to have primary alarms if
Sales becomes unreachable" { "IP Hostname" == "ccserv" }
```

Similarly, the network management administrator creates important node filters for the other departments and adds them to the file.

Topology Filters

Looking at performance on the management station, IT realizes that they still see every node in the network -- it's as if they had never bothered with collection stations at all. Every bit of information is getting passed right on up to the management station.

Reviewing the Manufacturing LAN, they realize that it contains over 100 actual nodes, mostly PCs automating fabrication processes. At this point, PCs are not critical to your success, but the production servers from which they run their inventory and instruction data are vital. The collection station operator can monitor the availability of the PCs. All you need to monitor at the management station are the servers.

Use the set construct in the filter file to build your topology filter that only forwards information about the servers to the management station.

```
Sets{
MfgServersSet = { "parts", "prefab", "finalfinish",
"inventory" }
}
```

The previous filter expression for Manufacturing was `MfgLan_TMF "Manufacturing's IP subnet map filter" { MfgLan_DF || NetsNSegs }`. You still only want the Manufacturing domain, and you do want all the networks and segments. Use the set of servers to limit what gets forwarded:

```
MfgLan_TMF "Manufacturing's IP subnet map filter"
      { (MfgLan_DF && MfgServersSet) || NetsNSegs }
```

The collection station in Manufacturing uses `MfgLan_DF` to discover all nodes in its domain. The topology database on the collection station contains all these nodes. When the collection station starts to forward information to the management station, it applies `MfgLan_TMF` to the data stream. Only the servers in the `MfgServersSet` and the networks and segments pass the filter and get sent to the management station. The management station's topology database contains only this information and not the rest of the nodes on the Manufacturing LAN.

The network administrator in IT creates similar topology filters to reduce clutter coming in to the management station from the other collection stations.

Map Filters

The management station serves various operators in the IT department. Connie has received extensive training in troubleshooting connector devices, and specializes in them throughout the network. Sergai only cares about the servers for the various departments. Look at each of their map filters.

The filter expression from which Connie works looks like this:

```
Connectors "All connector devices"
      { Bridges || IPRouters || Hubs }
```

But there is a problem. IT's topology filter from Manufacturing, for example, only passes servers, networks, and segments. They'll have to modify the topology filter to give you the connector information first:

```
MfgLan_TMF "Manufacturing's IP subnet map filter"
      { (MfgLan_DF && MfgServersSet)
        || Connectors || NetsNSegs }
```

Now Connie needs a map filter which includes `NetsNSegs` for her map database to work:

```
Connectors_MF "All connector devices"
      { Bridges || IPRouters || Hubs || NetsNSegs }
```

With this map, Connie will see all the connecting devices from all the LANs.

Using the Network Presenter

With so many PCs on the site, IT hires Paul to keep them all up and running. But Paul's map on the management station has a problem. It says there are no PCs for him to manage. You have specifically filtered out the PCs before they reach the management station.

You could add all the PCs back in for all the topology filters. Paul would have one view with all the PCs and could do combined trend analysis. However, the management station topology database would get bogged down and everyone would have to filter them back out with their map filters.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1371
Doc

You might think to purchase a separate management station for Paul and set up the collection station topology filters to only send PC information. However, topology filters are defined only once per collection station; a collection station cannot pass different data to different management stations.

As an alternative, Paul can use the Network Presenter through his web browser to act as a console on each of the collection stations. He would have more windows to watch, but network traffic would be minimized. Paul would be able to see the maps, but he would not be able to do any NNM administration through the Network Presenter since it is read-only.

This is an example of the trade-offs your organization will consider during your network management planning phase.

Default Filter File

The following is the default filter file, based on the above grammar:

```
//
// @(#)$OV_CONF/$LANG/filters
// @(#)HP OpenView NNM Pre-Release X.06.20 (Pre-Preview)  Jan 17 2001
// @(#)Copyright (c) 1990-2001 Hewlett-Packard Company
// $Revision: /main/PULSAR/PULSAR_REP/NEPTUNE/4 $  $Date: 2001/01/11 23:58 UTC $
//
// This is the default filter file.  These filters are examples
// which may be useful in your environment.  Feel free to modify this
// file and/or add your own.
// See OVfilterIntro(5) for more information on this file.
//

// Sets are a simple way to list string values to test
// against in a filter.  The "IN" operator tests a field value
// for membership in a set defined here.
//

Sets {

        // These are simple examples of sets.
        //
        // servers "Set of Servers" { "sv1", "sv2", "sv3" }
        // gateways "Backbone gateways " { "gw1", "gw2", "gw3" }
        //
        // sets can include a filename which contains the entries.
        // On Windows, the set file must be on the partition where NNM
        // is installed.

        // routers "Set of Routers" { /openview/conf/routers.set }
}

//
// Filters and FilterExpressions are used as Topology, Discovery,
// Map or Persistence filters.  Applications which use filters
// (like ipmap(1), ovtopmd(1m), ovtopodump(1), and ovtopofix(1m))
// can take the name of a Filter or a FilterExpression.
//

Filters {

       // The following filters are potentially useful as either Discovery
```


RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1372
3740
Doc:

```
// or Topology filters, or components for building Map filters.
//
// NOTES CONCERNING DISCOVERY FILTERS:
// Networks and Segments are not directly testing with Discovery
// filters (and so there is no need to include
// "isNetwork || isSegment" in these filters).
// However, it does not hurt to include networks or segments in
// a discovery filter, so long as you realize that they will not
// be acted on.
//
// Since nodes are only discovered in managed networks, the network
// must already exist and be managed before the filtering test
// will be applied.  New networks connected to discovered nodes will
// be discovered unmanaged.   For discovery filters,
// a node and all its interfaces can be thought of
// as a single object. If any interface or the node itself passes the
// filter, the node and all of its interfaces will pass the filter.
//
// ovtopofix -f follows the discovery filter semantics and only
// applies to locally monitored objects.  However, if a network or
// segment is empty after the processing of the nodes with the -f
// option, that segment or network will also be removed.
//
// ovtopodump(1) also follows the discovery filter semantic, and
// the filter only applies to nodes/interfaces.
//
// NOTES CONCERNING MAP AND TOPOLOGY FILTERS:
// For these filters, all objects are subject to filtering.
// One must specify the networks and segments to be passed.
// Furthermore, objects are displayed/included only if all their
// parent objects (submaps) pass the map/topology filter.  For example,
// if no networks would pass the filter ("isNetwork" is not included),
// then all segments and non-gateways nodes would be filtered out.
// Like Discovery filters, if any interface or
// node passes a Map filter, the node and all of its interfaces
// also pass the filter.
//
// See the FilterExpressions section for map and topology
// filter examples.
//

Networks "Any network" { isNetwork }
Segments "Any segment" { isSegment }
Nodes "Any node" { isNode }
```

```
// The following filters are primarily for example purposes, though
// they might be useful as discovery filters.  They do not generally
// make sense as map or topology filters because they do not specify
// the inclusion of networks and segments.  They also make sense as
// parts of a filter expression.

Routers "Any Router" { isRouter }
IPRouters "Any IP Router" { isIPRouter }
Bridges "Any bridge" { isBridge }
Hubs "Any multi-port repeater" { isHub }
SNMPNode "Any node supporting SNMP" { isNode && isSNMPSupported }

// The next filter is useful for defining map and topology filters
// (see the FilterExpresssions section).  It is not
// particularly useful as a discovery filter
// since all networks and segments automatically pass Discovery
// filters.  Nor is it useful as a standalone
// map filter, since it doesn't pass any nodes.

NetsNSegs "All networks & segments" { isNetwork || isSegment }

// This filter specifies that only objects that support IP should
// be included.  This filter should be used as a topology filter on
// any collection station discovering non-IP information (Level 2
// or IPX only nodes or networks) that is forwarding to a
// NNM 4.X management station.  This will not completely remove
// all non-IP information (e.g. IPX interfaces on a node that also
// supports IP will come through), but will limit the impact on the
// management station, and make migration to NNM 5.X easier.

IPOnlyObjects "Only objects that support IP"
        { isIP || isSegment }

// The following filters are examples that you can customize to
// match your environment.

// LocalLAN "Nodes with interfaces on the 15.2.112-119 subnet"
//      { "IP Address" ~ 15.2.112-119.* }
// NeighborLANs "Node with interfaces on the neighboring LANs on site"
//      { "IP Address" ~ 192.1.2-10.* }
// HPNodes "Hewlett-Packard nodes"
//      { isNode && ( vendor == "Hewlett-Packard" ) }
// NonHPNodes "Non-HP nodes"
//      { isNode && ( vendor != "Hewlett-Packard" ) }

// These are example filters using the sets defined above.
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1373
3740
Doc:

```
// GatewaysSet "Any designated Gateway node"
//       { "IP Hostname" in gateways }
// ServersSet "Any designated Server node"
//       { "IP Hostname" in servers }

// The next filter is useful for defining map and topology filters
// (see the FilterExpresssions section).  It is not
// particularly useful as a discovery filter
// since all networks and segments automatically pass Discovery
// filters.  Nor is it useful as a standalone
// map filter, since it doesn't pass any nodes.
//
// The network name below assumes an entry in /etc/networks.
// If no such entry exists, the actual network name will be
// something like "15.2.112".
// MyNet "The network in which I'm interested"
//       { isNetwork && "IP Network Name" == "yellow-lan" }

// This filter would be an example of a way to pass all objects
// contained in the subnet 15.2.112.0 with a subnet mask
// of 255.255.248.0 (so the subnet range is 15.2.112.0 to
// 15.2.119.255).  Note that the inclusion of "isSegment" is
// not a concern, because all segments outside of this network
// would be filtered out because the networks containing them
// were filtered out.  We must have some specification of segments
// if we want the segment contents to be included.

// EngrLan "The 15.2.112 subnet used by engineering"
//       { ("IP Address" ~ 15.2.112-119.* ) || isSegment }

// This filter accomplishes the same thing, but is more restrictive
// in the specification of segments to only include segments in that
// engineering network.  This assumes there is an entry in /etc/networks
// such that the subnet gets the name "engr-LAN", and hence the segments
// in that network all have a name of form "engr-LAN.<something>"
// Generally, the above will accomplish what you want, but this
// may be necessary in some situations if you want specific segments.
// In particular, it works well if you want to use this to EXCLUDE
// the objects in this network.  See the example in the Filter
// expressions below.

// EngrLan2 "The 15.2.112 subnet used by engineering"
//       { ( "IP Address" ~ 15.2.112-119.* ) ||
//         ( "IP Segment Name" ~ "engr-LAN.*" ) }
```

```
        // The following are some sample DHCPFilters.
        // They can be specified by using the Network Polling Configuration
        // dialog application, xnmpolling, on the Status Polling page.

        // DHCPSubnet "Addresses in subnet 15.70.177 are DHCP allocated"
        //      { "IP Address" ~ 15.70.177.* }

        // DHCPNode  "A particular address is DHCP allocated"
        //      { "IP Address" ~ 15.70.177.9 }

        // DHCPRange "IP Addresses from 15.70.177.5 through 15.70.177.10"
        //      { "IP Address" ~ 15.70.177.5-10 }

        //
        // Access to various nodes based on SNMP MIBs that have
        // been discovered as supporting a particular MIB
        //

        CDPnodes "Nodes supporting Cisco Discovery Protocol" { isCDP }
        ATMnodes "Nodes supporting ATM" { ("SNMP ifType" == "ATM")  ||
            ("SNMP ifType" == "atmLogical") ||
            ("SNMP ifType" == "atmDxi") ||
            ("SNMP ifType" == "atmFuni") || ("SNMP ifType" == "atmIma") }
        DS1nodes "Nodes supporting DS1" { "SNMP ifType" == "T-1 Carrier (ds1)" }
        DS3nodes "Nodes supporting DS3" { "SNMP ifType" == "T-3 Carrier (ds3)" }
        SONETnodes "Nodes supporting SONET" { "SNMP ifType" == "SONET" }
        FrameRelayNodes "Nodes supporting Frame-Relay" {
            ("SNMP ifType" == "Frame Relay") ||
            ("SNMP ifType" == "Frame Relay Service") ||
            ("SNMP ifType" == "frameRelayInterconnect") }
        RMON1nodes "Nodes supporting RMON-1" { isRMON }
        RMON2nodes "Nodes supporting RMON-2" { isRMON2 }
        // Short-hand for any RMON device
        RMONnodes "Nodes supporting RMON-1 or RMON-2" { isRMON || isRMON2 }
}

// FilterExpressions are simply combinations of filters defined in the
// same filter file (above).  FilterExpressions make it simple to
// combine filters without reproducing the expressions of each
// filter again

FilterExpressions {

        // One can turn the filters defined above into viable map or
        // topology filters by simply adding "|| NetsNSegs".  (Doing so
        // does not invalidate the filters as discovery
        // filters.  It just adds a superfluous test.)
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1374
3740
Doc:

```
NetInfrastructure "Any network connecting device and what they connect"
        { Routers || Bridges || Hubs || NetsNSegs }
NetBackbone "Networks and gateways/routers"
        { Routers || Networks }

// The following combines the two set filters
// defined above into one FilterExpression.
// It works unmodified as a discovery filter.
// To work as a map filter, network and segment filtering
// must be added (see below).

// VitalNodes "All Gateways and Servers"
//      { GatewaysSet || ServersSet }
// One can turn the filters defined above into viable map or
// topology filters by simply adding "|| NetsNSegs".  (Doing so
// does not invalidate the filters as discovery
// filters.  It just adds a superfluous test.)

// VitalNodesMap "All nets & segs, but only gateway and server nodes"
//      { GatewaysSet || ServersSet || NetsNSegs}
// LocalLANView "All nets & segs, but only local nodes"
//      { LocalLAN || NetsNSegs }

// Using the filters defined above that include only a specific
// network, we can also exclude the specific network like this
// Note the use of the more specific form to exclude only the segments
// in the engineering lan.  This could have been specified directly
// as a negation in the filter part, but this form works well if you
// have several networks to manipulate in this manner.
// EverythingButEngr "Everything but the engineering LAN"
//      { !EngrLan2 }

// Of course the above filter expressions, when used as
// map filters, pass all networks and segments.  You
// may wish to see only a particular network.  The following map
// filters accomplish this.  Note that though segments
// and nodes from other networks will pass the filters, IP Map
// will ignore them because their parent networks will not pass.
// NOTE:  These filters will not work as Discovery
// filters because all network and segments automatically pass
// Discovery and Topology filters.

// MyNetMap "Only the network of interest and all its constituent parts"
//      { MyNet || Segments || Nodes}
// MyVitalNodesMap "Gateways, servers and segments in net of interest"
//      { MyNet || Segments ||  GatewaysSet || ServersSet }
```

```
        // This is a map persistence filter which ensures that
        // all Ungermann-Bass are kept in memory and up to date.
        // Note that this will also keep any containing submaps in memory.

        // PersFilter "Objects to keep in map memory"
        //      { HPNodes }
}
```


RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1375
3740
Doc:

B Using NNM Under a Mixed Codeset Environment

1969

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1376
3740
Doc:

This chapter covers requirements for using NNM's alarm browser, `xnmevents`, in a mixed-codeset environment. These steps are not required if you are using the web interface to alarms, `jalarms`.

Event forwarding in NNM's distribution and scalability model expects that the management station and the collection station share a codeset. That is, if a management station is operating under the ISO8859-1 codeset, then the collection station must share its data using the ISO8859-1 codeset.

This restriction is minimal for English and European language users since ISO8859-1 contains both English (ASCII) characters and most of the European accented characters. Furthermore, NNM is not localized to any of the European languages.

However, this restriction becomes a problem for the Japanese language users that may need to use both Japanese EUC and Shift-JIS codesets. For instance, if a management station is running under Japanese EUC, but one of its collection station is running under Japanese Shift-JIS, the management station's GUI will fail to display the Shift-JIS data obtained from a Shift-JIS collection station. This is because a management station assumes that the data from the collection stations are using the same codeset as itself, and parses and displays all data (including the Shift-JIS data) as Japanese EUC data. This results in a data corruption of all Shift-JIS characters.

Therefore, in this mixed codeset environment, the collection stations must be configured to forward event data to the management station using ASCII only, and furthermore, "user events" must not contain non-ASCII characters. Since ASCII is a subset of all other codesets, data from the collection station will not be corrupted by the management stations' GUI.

SNMP traps do not support non-ASCII characters, but NNM does not prevent you from forwarding events that contain non-ASCII characters. Do not generate user-sendable events containing non-ASCII characters, if these events are forwarded from a collection station to a management station. For example, do not send events, such as the "`OV_Popup_Message`" or "`OV_Message`," with non-ASCII characters, using the `snmptrap` command from a collection station to a management station.

When configuring a collection station to operate under a mixed-codeset environment (Japanese system users should see Table B-1, Mixed Codeset Environment for Japanese Systems,), the following steps should be taken:

1. Create a new file called `$OV_CONF/ovlang.conf` (for example, `C:install_dir\conf\ovlang.conf`) that contains the following two entries, each on a separate line:

   ```
   ovtopmd
   netmon
   ```

   If you need to forward threshold events, add `snmpCollect` to `ovlang.conf`.

2. Restart the `ovw` processes by executing the following commands:

   ```
   ovstop
   ovstart
   ```

NOTE There is no need to remove or clear the `ovtrapd.log` file of a management station, but if it contains data from this collection station prior to this step, that data may be corrupted.

The first two steps will force the collection station to generate data forwarded to the management station with English/ASCII characters only. However, data that is not forwarded to a management station will continue to operate using the codeset specified by you or by the environment.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1377
3740
Doc:

Table B-1 Mixed Codeset Environment for Japanese Systems

Collection Station's System/Codeset	Management Station's System / Codeset			
	Windows / SJIS	HP-UX/SJIS	HP-UX/EUC	Solaris/EUC
Windows/SJIS	(1)	(1)	(2)	(2)
HP-UX/SJIS	(1)	(1)	(2)	(2)
HP-UX/EUC	(2)	(2)	(1)	(1)
Solaris/EUC	(2)	(2)	(1)	(1)

(1) -- this is not a mixed codeset environment; no configuration necessary.

(2) -- this a mixed codeset environment; configure the collection station to forward ASCII data to the management station.

Glossary

A

agent In the network management model, the agent is the component that "instruments" or provides management information about a particular network device, such as a file server, to a network management system. *See also: proxy agent.*

C

client A computer system, on a network, that accesses a service from another computer (server). A client may run any arbitrary operating system.

client/server A concept that functionally divides the execution of a unit of work between activities initiated by an end user or program (client) and resource responses (server) to the activity request.

collection domain The set of nodes and other objects for which trend data collection and threshold checking is occurring on a collection station. Frequently the discovery domain and the collection domain include the same set of nodes and objects. Discussions in this document assume that is the case, and use this term to refer to both. *See also: management domain, discovery domain.*

collection station A management station that acts as a collection point for information being gathered on managed elements. *See also: management station.*

correlated events Multiple events analyzed by NNM and presented under a single event in the browser.

D

discovery domain The set of nodes and other objects actively being discovered and monitored by an NNM station.

discovery filter Specifies which devices an NNM station is actively discovering and monitoring. *See also: filtering.*

F

failover Configuring a management station to pick up status polling duties for a collection station that goes into critical status.

failover filter List of specific nodes the management station should poll, leaving the status of the rest as they were when the collection station went critical.

filtering Refers to the process of limiting the object the user is interested in having discovered, monitored, displayed, etc., by determining certain attributes that are of interest to the user. Filtering generally is used to limit processing to a subset of information already available, to reduce the cognitive load on the user, align presentation with the users needs, and generally reduce system load by filtering the amount of data handled as soon as possible. *See also: discovery filter, failover filter, map filter, persistence filter, and topology filter.*

I

IP address The Internet Protocol address is a network level address assigned to each system is a TCP/IP network. It is 4 bytes long. An example IP address is 192.215.15.46.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 1378
Doc: 3740

M

management application Software that obtains and presents information from agents, or proxy agents. The information is usually presented in a graphical user interface.

management console An instance of the user interface from which you can control applications that do network and system management. The console may be on the system that contains the management software or it may be on another system in the management domain.

management domain The set of all nodes and other objects in the network that are of interest to the user.

management station The computer system used in the management of other objects in the network, system, and software environment. Management stations run network or system management services, daemons, processes, and/or management user interfaces. Management clients, management servers, management consoles, and stand-alone management systems are all examples of management stations. *See also: collection station.*

map A set of related objects, symbols, and submaps that provides a graphical and hierarchical presentation of your network and its systems. Because a map is defined by the collections of submaps it comprises, you never view a map directly, but rather one or more of its submaps. Maps are derived from the HP OpenView Windows object database, and multiple maps can be created from the same object database. *See also: submap.*

map filter Defines what objects in the HP OpenView Windows object database will be permitted on the map. Objects that are rejected by a map filter remain in the management station's topology database, and are still subject to status polling. Map filtering occurs on a per-map basis, not a per-display basis. *See also: filtering.*

N

node A termination point for two or more communication links - or more simply, a device on a network. The node can serve as the control location for forwarding data among the elements of a network, as well as perform other networking, and in some cases local processing functions.

O

object A computer system, interface card, printer, or any other device or object that appears in the network.

P

persistence filter Specifies one or more objects which are required to be in memory at all times, and therefore are not permitted to be on a transient submap. *See also: filtering, persistent submap, persistent object.*

persistent object An object which has passed a persistence filter, and is therefore in memory whenever the map on which it resides is open. Any submap that contains a persistent object is automatically a persistent submap. *See also: persistent submap, persistence filter.*

persistent submap A submap that is always in memory, either because it is above the configured persistence level, because it

contains a persistent object, or because it is the child of a persistent object. *See also: transient submap.*

primary collection station When applied to a particular object, this refers to the collection station which has been chosen as having primary responsibility for monitoring the object. In particular, it is used to determine the status and other attributes of the object. A given object may be reported and monitored by multiple collection stations, but only one station will be the primary station. *See also: secondary collection station.*

proxy agent A proxy agent performs information preparation and exchange on behalf of a device it is representing. For example, an agent is a proxy if it is located on the file server but is representing a client. *See also: agent.*

R

root submap A standard, top-level submap for every map.

router A router uses a packet's destination address to determine which network or network segment is its destination.

S

server A computer system that provides services to other computer systems on the network. A server could be a file server and provide data storage, application, routing, and print services.

secondary collection station When applied to a particular object, refers to a collection station that is known to be monitoring the object, but which has not been chosen as the primary collection station.

site A group of nodes connected completely by a Local Area Network (LAN), i.e. all at the same geographic location.

SNMP Simple Network Management Protocol. A protocol running above TCP/IP used to exchange network management information. SNMPv2C has extended functionality over the original protocol.

station *See: workstation, collection station, or management station.*

submap A particular view of the network environment, consisting of related symbols that are displayed in a single window. Multiple submaps can be displayed simultaneously. Submaps are typically (though not necessarily) organized in a hierarchy, with the root submap at the top of the hierarchy. *See also: map.*

T

TCP/IP Transmission Control Protocol/Internet Protocol. A set of protocols for Layers 3 and 4 of the seven-layered Open Systems Interconnect network model

topology filter A topology filter at a collection station defines the subset of local topology data that management stations can see. *See also: filtering.*

transient submap A submap that is not necessarily in memory at all times, but which is available "on-demand" when the operator opens it. Any submap that can be recreated at any time based wholly on topological information is potentially a

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1379
3740
Doc:

transient submap, depending on how and whether the on- demand submap feature is enabled. *See also: persistent submap.*

W

workstation A computer or terminal that is connected to the network.

Index

Symbols

%REMOTE_MANAGERS_LIST%, 57, 97, 140, 155

A

applications
  backward compatibility, 68
  integrating, 26, 68, 125
attribute value assertion
  See AVAs
automated managed-state, 18, 74
AVAs, 172
  boolean, 174
  enumerated, 175
  enumerated field values, 186
  evaluating, 172, 174
  filterable fields, 181
  integer, 175
  operators, 173
  regular expressions, 176
  special pattern matching, 177
  string, 175
  whitespace in field name, 172

B

backup, 18, 88
backward compatibility
  applications, 68
benefits of scalability, 15

C

capacity, 21
  centralized-hierarchical model, 97
  collection stations, 86
  devices, 34, 84
  management console, 34
  remote monitoring, 85
centralized model, 92
  discovery filters, 93
  management consoles, 93
  map filters, 93
  on-demand submaps, 93
  web GUI, 93
centralized-hierarchical model, 95
  capacity, 97
  discovery filters, 96
  failover, 96
  management consoles, 96
  map filters, 96
  on-demand submaps, 96
  web GUI, 96
codeset,mixed, 206
collection domain, 46
  overlapping, 52
collection station, 33
  changing primary station for an object, 151
  checking status, 145, 146
  configuration overview, 57
  configuring, 133
  configuring remote communication, 141
  connections, 36
  determining if a node is, 137
  determining primary, 150
  failover, 51
  how many to have, 86
  identifying with Station view, 23
  in DIDM, 21
  introduction, 22
  listing monitored objects, 138
  managing, 138
  new primary, 55
  preferred, 54
  primary vs. secondary, 53
  removing from management station, 141
  security configuration, 133
  serving multiple management stations, 36
  synchronization, 144
  topology filter, 41
  troubleshooting, 147
  unmanaging, 140
configuration
  remote, 56
configuration files
  filter, 169
  nfsconf, 113
  ov.conf, 50, 139
  ovwdb.auth, 119
  pcnfsd.conf, 113
  snmpd.conf, 133
  trapd.conf, 27, 60
configurationfiles
  ovtopmd.lrf, 135
configuring
  collection station, 133
  collection station security, 133
  demand level, 121
  discovery filter, 128

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1380
3740
Doc:

Index

event forwarding, 154
failover, 150, 153
failover filter, 153
filters, 127
management console, 109
management stations, 137
on-demand submaps, 121
overlapping domains, 150
persistence filter, 124
topology filter, 134
UNIX console client, 117
UNIX console server, 112
Windows NT console for UNIX server, 115
Windows NT console server, 111
connections between components, 36
connector down, 60
forwarding, 62
important node filter, 193
console
See management console
cooperative independent model, 103
discovery filters, 104
management consoles, 104
map filters, 104
on-demand submaps, 104
threshold events, 104
topology filters, 104
web GUI, 104
correlated events, 60
forwarding, 60
custom views, 72

D

data collection
threshold, 28
trend data, 28, 159
databases, 159
SQL, 28
data-stream filters, 37
demand level
changing, 122
configuring, 121
devices
limit per station, 34
DHCP, 39, 192, 197
discovery filtering, 40
applying to previously discovered objects, 129
centralized-hierarchical model, 96
configuration, 128
cooperative independent model, 104
example, 190
fully centralized model, 93
hierarchical model, 100
distributed internet discovery and monitoring
architecture, 48
configuring, 133, 137, 150
internals, 46
introduction, 20
distribution, 19, 20, 33
architecture, 49
benefits, 15
DIDM configuration overview, 56
distributed internet discovery and monitoring, 16, 20
models, 89
network connections, 36
overview, 15
processes, 48
risks of, 86
the GUI, 109
threshold monitoring, 18

E

ECS, 60
EMANATE, 134
events, 27, 57, 59
configuring forwarding, 154
correlated, 60
forwarding, 18, 42, 62, 63
map filtering, 43

F

failover, 18, 51, 86
centralized-hierarchical model, 96
configuring, 153
disabling, 153
filter,configuration, 52, 153
hierarchical model, 101
failover filter
configuration, 153
failover filter configuration, 52
fault tolerance, 18
fields,filterable, 181
filter expression, 170
filtering, 48, 72
and scalability, 17
configuration, 127, 128

discovery, 40, 128
example, 189
filter definition file, 43, 44, 197
important nodes, 193
introduction to, 19
map, 42, 48, 127
overview, 37
performance, 17, 19
persistence, 26, 68
topology, 41, 50, 134
utilities, 45
filters, 169
attribute value assertion See AVAs
boolean expressions, 174
default file, 197
enumerated expressions, 175
enumerated field values, 186
example, 189
excluding a node, 180, 192
failover,configuring, 153
filterable fields, 181
formal grammar, 187
integer expressions, 175
language definition, 169
pattern matching, 177
regular expressions, 176
relationship between nodes and interfaces, 180
sets, 171
string expressions, 175
testing, 45
types of, 37, 38
find, 67
forwarding, 18
events, 59, 154
threshold events, 62

H

hierarchical model, 98
discovery filters, 100
failover, 101
management consoles, 100
map filters, 100
multiple levels, 99
on-demand submaps, 100
performance, 102
threshold events, 101
topology filters, 100
web GUI, 100
high availability, 18

I

inform request, 59
integrating applications
on-demand submaps, 125
interface
automatic managed-state, 18, 74
Internet level, 122
IP discovery and monitoring, 16
ipmap, 48, 61, 64, 68

L

LAN, 36
languages,international, 206
large maps, viewing, 17, 29, 87
list
of remote managers, 57
localization, 206

M

managed interfaces
automated, 18, 74
management console, 17, 20, 24, 33, 70, 73
capacity, 110
centralized-hierarchical model, 96
choosing mount point, 118
configuration overview, 110
cooperative independent model, 104
fully centralized model, 93
hierarchical model, 100
introduction, 24
modifying ovwdb.auth file, 119
platform, 110
prerequisites for, 109
read-only vs. read-write maps, 72
security, 119
supported configurations, 109
undoing, 120
UNIX client, 117
UNIX server, 112
Windows NT console for UNIX, 115
Windows NT server, 111
management domain, 46
management station, 22, 33
changing overlap mode, 152
changing primary collection station, 151
configuring, 137
remote communication, 141

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1381
3740
Doc:



Index

configuring collection stations to manage, 138
connections, 36
identifying with Station view, 23
overlapping domains, 55
removing collection station, 141
synchronization, 144
troubleshooting, 147
unmanaging a collection station, 140
managing
locally monitored objects, 132
map filtering, 42
centralized-hierarchical model, 96
configuration, 127
cooperative independent model, 104
events, 43
example, 191, 195
fully centralized model, 93
hierarchical model, 100
recalculating for a map, 43, 68
maps, 72
Microsoft Terminal Server, 75
mixed codeset, 206
model, 33
centralized-heirarchical, 95
cooperative independent, 103
fully centralized, 92
hierarchical, 98
multi-level hierarchical, 99
monitoring domain, 46

N

Neighbor view, 163, 164
netmon, 40, 48, 49, 50, 51, 56, 58, 61, 99
limits, 84
network level, 122
Network Presenter, 25
See also web GUI, 17
NFS, 70, 109
diskless, and management consoles, 70
nmdemandpoll, 144
NNM 250
limitations, 34
multiple licenses to increase node limit, 87
nodes, excluding via filtering, 180

O

on-demand submaps, 26, 64
and find, 67
and submap list dialog, 67
centralized-hierarchical model, 96
changing demand level, 122
changing persistence filter, 125
configuring, 121
cooperative independent model, 104
disabling, 67, 122
fully centralized model, 93
hierarchical model, 100
inital configuration, 64
integrating applications, 125
ipmap and ovw, 64
performance, 17
persistence filters in, 26, 68
recalculating persistence of submaps, 69
sharing, 72
terms, 64
operators, 42
ovaddobj, 135
ovcoltosql, 28, 160
overlap mode, 152
overlapping collection domains, 52, 53, 55, 86
configuring, 152
ovfilter utilities, 45
ovrepld, 48, 50, 58, 62
ovstart, 49
ovtopmd, 48, 49, 50, 61, 135
ovtopmd.lrf, 135
ovtopodump, 138, 150
ovtopofix, 40, 129
ovtrapd, 59, 61
ovwdb, 70
ovwdb.auth file, 119
ovwrs, 51
ovwsetupclient command, 120

P

packet loss rate, 141
panner, 17, 29
partitioned internet submap, 87
Path view, 163, 165
performance, 16, 21, 97
hierarchical model, 102
memory, 26
persistence filtering, 26, 68, 69
changing, 125
configuring, 124
persistent submaps, 64
pmd, 59, 61
primary collection station, 53, 150
changing, 151

preferred, 54, 152
with failover, 55
processes, distribution for IP discovery and monitoring, 48

Q

quick navigator, 17, 30

R

remote communication
configuring, 141
remote configuration, 56
remote managers list, 57, 97, 155
replication of topology, 50
resident submaps, 64
retry count, 141

S

scalability, 15
benefits, 15
general considerations, 84
strategies for deployment, 87, 89
secondary collection station, 53
security
collection station configuration, 133
management console, 119
segment level, 122
Service Guard, 18, 50, 86, 93, 96, 100, 104, 119, 139
set-defining filters, 37
sets, 171
snmpd.conf, 133
SNMPv2C
inform request, 59
SQL databases, 28
Station view, 145, 146
collection station
checking status, 146
submap list dialog, effect of on-demand, 67
submaps
partitioned, 87
synchronization, 144

T

Terminal Server, 75
threshold events
cooperative independent model, 104
forwarding, 62, 154
hierarchical model, 101
monitoring, 27
remote, and remote actions, 63
threshold monitoring, 18, 28
timeout value, 141
topology filtering, 41, 50
changing, 135
configuration, 134
cooperative independent model, 104
events, 42, 63
example, 191, 194
hierarchical model, 100
removing, 136
topology replicator, 50
transient submaps, 64
trapd.conf, 59
traps, 59
troubleshooting
communication between management station and collection station, 147

U

UDP, 59
undoing
management console, 120
on-demand submaps, 122
UNIX, 117
unmanage
automated, 18, 74
unmanaging
collection station, 140
objects, 132
use models, 89
centralized-hierarchical, 95
cooperative independent, 103
fully centralized, 92
hierarchical, 98

V

view
Neighbor, 163, 164
Path, 163, 165
Station, 145, 146
views
custom, 42, 72

W

WAN, 15, 36
and remote monitoring, 85, 94, 97
configuring, 141
web GUI, 17, 25

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1382
3740
Doc:

Index

centralized-hierarchical model, 96
cooperative independent model, 104
fully centralized model, 93
hierarchical model, 100
web server, 25
wide area network
See WAN

X

xnmsnmpconf, 58
xnmtopoconf, 49, 52, 53, 54, 56, 57, 58, 132, 137, 140, 141, 147, 152
xnmtrap, 60
X-terminals, 33, 34
and management consoles, 73

CORREIOS

Manuais Técnicos

Pregão nº 118/2003 – CPL/AC

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1383
3740
Doc:

Manual - II

HP OpenView Network Node Manager

Managing Your Network with HP OpenView Network Node Manager

Version: 6.4



Manufacturing Part Number : J5323-90000

January, 2003

© Copyright 2003 Hewlett-Packard Company.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1384
3740
Doc:

Legal Notices

Warranty.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices.

No part of this document may be copied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

©Copyright 1983-2003 Hewlett-Packard Company, all rights reserved.

Contains software from AirMedia, Inc.

© Copyright 1996 AirMedia, Inc.

Trademark Notices.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

Windows NT® is a U.S. registered trademark of Microsoft Corporation.

Windows® 2000 is a U.S. registered trademark of Microsoft Corporation.

1957

Windows® and MS Windows® are U.S. registered trademarks of Microsoft Corporation.

Netscape™ and Netscape Navigator™ are U.S. trademarks of Netscape Communications Corporation.

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

Oracle7™ is a trademark of Oracle Corporation, Redwood City, California.

OSF/Motif® and Open Software Foundation® are trademarks of Open Software Foundation in the U.S. and other countries.

Pentium® is a U.S. registered trademark of Intel Corporation.

UNIX® is a registered trademark of The Open Group.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1385
3740
Doc:

1950

1. Network Management with NNM

The Network Management Challenge 39
How Network Node Manager Can Help 39
Moving to Proactive Network Management 40
Poll for Network Information 40
Watch for Events 41
Network Management Functions 42
Fault/Problem Management 43
Performance Management 45
Configuration and Change Management 46
Additional HP OpenView Product Information 47

2. How Does NNM Work?

Collecting Critical Information 51
SNMP's Network Management Model 51
Desktop Management Interface (DMI) 54
Automatic Discovery and Layout 56
How IP Discovery and Layout Work 56
How IPX Discovery and Layout Work 57
Interactions Between IPX Discovery and IP Discovery 58
Level 2 Discovery 59
Event Reduction Capabilities 61
NNM's Databases 62
Operational Databases 62
Data Warehouse 63

3. Resources Available While Learning NNM

Resources Included with NNM 67
NNM Online Help System 67
Tip of the Day 69
Manuals: Printed and Online 69
Release Notes 71
Reference Pages (Manpages) 71
The contrib Directory 74
The support Directory 74
White Papers 75

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1386
3079
3740
Doc:

Resources and Services Available Through HP 76
HP Web Sites 76
HP Consulting Service 76
HP Education 77
HP Product Support 77
OpenView Forum 77
Summary of HP OpenView Web Sites 78

4. Planning Your NNM Configuration

Budgeting Time for Planning and Configuration 81
Time for Planning 81
Time for Configuration 81
Taking Over NNM from Someone Else 82
Understanding the Network Information Needs of Your Organization 83
Who Needs What Information? 83
Work Sheet for Planning 85
Knowing Your Network 87
Deciding to Manage or Not to Manage Devices 87
Starting with a Well-Configured Network 90
Consistent IP Addressing Scheme 90
Consistent Name Resolution Scheme 91
SNMP Agents and Their MIBs Configured 93
DMI Service Providers and Their MIFs Configured 94

5. Initial Network Discovery: Options and Troubleshooting

Install Network Node Manager (if you have not already done so) 100
Installing IPX Transport Software (Windows only) 100
Establishing Universal Pathnames (UNIX only) 100
Discover the Network... Let NNM Do It 103
Overview 103
Start the NNM Services (background processes) 105
Make Sure NNM's Services Are Successfully Running 106
Open NNM 106
Configure an Inventory Report 107
Let NNM Run Over Night to Populate the Maps 107
Verify the Accuracy of the Initial Discovery 109

Printing the Inventory Report 110
Viewing the Properties of Your Network Configuration 111
Finding Specific Devices on the Map 113
Interactively Expand/Limit Your Management Domain 117
Adding Networks to Your Management Domain 117
Managing an Unmanaged Network Device 118
Unmanaging a Managed Network Device 118
Automatically Expand Your Management Domain 119
Create a Seed File Specifying Multiple IP Networks to Manage 120
Use loadhosts 122
Expand the IPX Hop Count (Windows only) 123
Automatically Limit Your Management Domain 124
Create a netmon.noDiscover File to Exclude Devices 125
Use loadhosts 127
Create a Discovery Filter Identifying Which Devices to Include 128
Modify the oid_to_type File to Unmanage Devices by Type 129
Limit the IPX Hop Count (Windows only) 130
Troubleshooting Discovery 131
IP Discovery and Layout 131
General IP Suggestions 144
IPX Discovery and Layout (Windows only) 153
Stop Everything and Start Discovery Over Again 161

6. Preserve Your Sanity: Backup and Polling Configuration

Backup/Restore to Protect Your Investment of Time 165
How Does the Backup Work? 166
Backing Up and Archiving All Critical Files 167
Restoring All of NNM (procedures/options) 171
Restoring Part of NNM (procedures/options) 173
Troubleshooting Information 174
Custom Scripts 176
Controlling the Amount of Traffic Generated by NNM 178
Status Polling 181
Configuration-Check Polling 183
Connector Topology Polling 184
New Node Discovery Polling (IP, Level-2, and IPX) 184

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1387
3740
Doc:

Controlling Level-2 Device Discovery and Layout 185
Secondary Failure Polling. 192
Fine-Tuning the Polling Services. 193
Watching NNM's Polling Queue. 194
Running NNM Without Network Polling 195

7. Map Making Fundamentals

Maps versus Submaps 199
Maps 199
Submaps 200
Understanding Objects versus Symbols 203
Objects 204
Symbols 207

8. Map Customization

Putting It All Together. 212
Which Maps for Which Users. 212
Copying the Default Map. 215
Your Map Strategy 215
Controlling the Display of Devices Attached to Switches or Bridges 217
Turning On Star Configuration for Attached Devices 218
Turning Off Star Configuration for Attached Devices 219
Giving Your Network Symbols Meaningful Names 221
Turning Connection Labels on or off. 223
Configuring Trunking and Meshing 225
Establishing Submap Persistence Settings 229
By Logical-level of Your Network's Structure 230
By Presence of Specific Devices 230
Controlling Which Devices Appear on the Map 232
Creating a Map Filter. 232
Using the Hide Feature 233
Changing/Adding Object Attribute Fields 235
Changing the Value in an Attribute Field. 236
Changing Symbol Type to Switch Attribute Sets 237
Adding Attribute Fields in the Object Database. 238
Making the Maps Look Like Your World 240

1946

Controlling the Placement of the Symbols on Your Map 241
Adding Your Own Submaps 244
Customizing the Internet Level of Your Network Map 247
Customizing Network-, Segment-, or Node-Level Submaps 256
Background Graphics 260
Creating Your Own Map Symbols 263
What Is a Symbol 263
Specifying the Placement and Size of the Submap Windows 266
Window Geometry 266
Submap Overlay 266
Miscellaneous Configuration Changes 268
Windows Operating System 268
UNIX Operating Systems 269
Controlling Symbol Status 270
Object Status Colors 270
Compound Status 274
Creating New NNM Features to Meet Your Team's Needs 278
Adding to NNM's Menu Structure 278
Creating Executable Symbols with Custom Behaviors 279

9. Controlling Map Access

Establishing and Communicating a Process for Requesting Changes to the Map . . 286
Not Allowing Team Members to Make Changes 286
Allowing Team Members to Make Changes 286
Setting User Preferences Within NNM 287
Using Command Line Startup Options 289
Options 289
Examples 290
Using Operating-System Level File Permissions for the Map 292
Windows: Setting Permissions 293
UNIX: Setting Permissions 294
Using the Context Feature to Control Menu Choices 296
Using NNM's Predefined Contexts 296
Creating Your Own Contexts 297
Using ARF Files to Control Menu Choices 299
ARF File Modifications Example 305

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1388
3740
Doc:

Allowing Others to View NNM from Many Computers 317
Remote Consoles 317
NNM's Web Interface 318
Microsoft Terminal Services 318
Closing All Current Sessions 319

10. Keeping Up with Events on Your Network: Beyond the Maps

How NNM's Event System Works 323
SNMPv1 Traps / SNMPv2c Traps and Informs 325
DMI Events (Indications) 327
Alarm Browser Overview 329
Displaying Alarms 330
Alarm Categories/Alarm Browser Windows 331
Acknowledging Alarms 334
Filtering Alarms 335
Deleting Alarms 337
NNM's Map and the Alarm Browser 338
Specifying Additional Actions on Alarms 339
Launching Specific Views or URLs from Alarms 340
Configuring the Alarm Browser 342
Controlling the Size of the Event Database 343
Controlling the Size of the Alarm Browser's State File 344
Controlling How Many Alarms to Delete Automatically 345
Copy or Restore the Alarm Browser's State File 347
Controlling How the Alarm Browser Looks 347
Assigning Alarm Categories 348

11. Event Reduction Capabilities: Getting to the Root Cause

NNM's Event Reduction Capabilities 352
Correlation Concepts 354
De-Duplication of Alarms 358
ECS Correlations 360
NNM's Built-In Correlations 360
Command Line Control 380
Correlation File Structure 381
Troubleshooting 381

Obtaining Additional Event Correlations 382
Correlation Composer Correlators 386
NNM's Built-In Correlators 386
Correlator Fact Store File 397
Troubleshooting 397
Creating Additional Correlators 398
What is an SNMP Variable-Binding and How Do I Identify One? 404
Look within the MIB File 404
Check the Alarm Message Text in the Alarm Browser 405
Special SNMP Variable-Bindings within NNM Interface and Node Status Alarms 405

12. Customizing Events: Doing It Your Way

SNMP MIB Browser 412
Loading MIBs in the MIB Database 413
Prerequisites 414
Procedure Tips 415
DMI Browser 417
Creating DMI Queries 417
Loading DMI-to-SNMP Event Mappings 419
If a MIB Translation of the MIF File Is Available 420
If No MIB Translation of the MIF File Is Available 420
Event Configuration Overview 422
Prerequisites 422
Event Configuration Window 423
Controlling Alarm Message Posting and Text 431
Defining Automatic Actions for Events 433
Variables and Special Characters Allowed 436
Defining Additional Actions 441
Using the MIB Application Builder 443
Prerequisites 444
Procedure Tips 445
Data Collection & Thresholds 447
Prerequisites 447
Procedure Tips 449
Defining Thresholds for Monitored MIB Objects 453
Collecting and Storing Textual Data 460

1844
ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1389
3740
Doc:

Creating and Using MIB Expressions 460
Unique Properties of the SNMP MIB Object sysObjectID 465

13. Using Event Data

Graphing SNMP Data 471
. 471
Graphing Historical and Real-Time Data in the Same Graph 473
Grapher Operations 474
Printing a Graph 475
Data Warehouse 476
Data in the Data Warehouse 478
Reporting 478

14. NNM on the Web

Overview 484
Setting Up the HP OpenView Web 485
Role Configuration Files for the HP OpenView Web 486
The HP OpenView Launcher 492
Launcher User Interface 492
Configuring the Launcher 494
HP OpenView Network Presenter 501
Starting the Network Presenter 501
The Network Presenter Window 502
Network Presenter versus NNM on a Management Station 503
Configuring the Network Presenter 505
Using Symbol Registration Files and Bitmaps 506
Listing Multiple Maps in the Launcher 508
SNMP Data Presenter 509
Configuring the SNMP Data Presenter 511
Alarm Browser 512
Using and Configuring the Alarm Browser 513
Event Reduction 515
Reporting Interface 516
Additional Views 518
Neighbor View 518
Path View 519

Node View 520
CDP View 521
Station View 522
Internet View 522
Port-Address Mapping 522

15. Maintaining NNM

Daily Tasks 527
Check Running Services 527
Check Disk Space 527
Trim Files 528
Weekly Tasks 531
Back Up NNM 531
Check Polling Performance 531
Check Web Launcher Log Files 532
Monthly Maintenance Tasks 533
Check Patch Releases 533
Check License Requirements 533
Yearly Maintenance Tasks 534
Evaluate Latest Release 534
Other Maintenance Tasks 535
Enabling/Disabling Automatic Startup 535
Customizing the Startup Configuration 535

A. NNM Services and Files

Services and Files 541
Background Services 541
Foreground Services 543
Web CGI Programs 545
Behavior of the Services and Files 547

B. Network Troubleshooting Tools

Tools in NNM on a Management Station 555
Map Snapshots 555
Performance Tools 556
Configuration 562

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1390
Doc: 3740

Fault Resolution Tools 566
Miscellaneous Tools 569
Tools in NNM's Web Applications 575
HP OpenView Launcher 575

C. Troubleshooting NNM Itself

General Troubleshooting Considerations 579
When You Need More Information 579
Preventive Practices 579
Characterizing the Problem 582
Distinguish Local versus Remote Problems 582
Remote Nodes' Level of Manageability 582
Context: What Changed? 583
Duration: How Long or How Often? 583
Context: What Action Was Performed? 583
Troubleshooting Background Services 584
The httpd Background Service 586
The netmon Background Service 587
The ovactiond Background Service 590
The ovalarmsrv Background Service 590
The ovcapsd Background Service 591
The ovspmd Background Service 592
The ovrepld Background Service 594
The ovtopmd Background Service 594
The ovtrapd Background Service 599
The ovuispmd Background Service 600
The ovwdb Background Service 602
The pmd Background Service 604
The ovrequestd Background Service 607
Troubleshooting Data Collector Problems 608
Set-community Name and Trap-dest Loss Upon Re-Installation 612
Troubleshooting Web Components 613
Language Selection Problems 614
HP OpenView Launcher 615
Network Presenter 618
Alarm Browser 619

1940

SNMP Data Presenter 620
Troubleshooting NNM Operations 623
Runtime Components 623
Network Management Operations 626
Browsing an Internet MIB 628
Building and Executing MIB Applications 628
Configuring Events 631
Event Reduction Capabilities 632
Loading Internet MIBs 633
X Windows Components (UNIX operating systems only) 635
Online Help 636
Troubleshooting Windows Applications 637
Problems Launching Applications 637
Windows Operating System Tools 637
Recommended Logging and Tracing Practices 639
Logging and Tracing 639
Web Launcher Error Log 653
Improving Traffic Management and Performance 654
Traffic Management 654
Performance 656

D. Changing All the Symbols for a Particular Device

Procedure 662
Example 663
Create a Symbol Registration File 664
Copy and Modify the Symbol Graphics 664
Map a sysObjectID to the New Symbol 666
Define the Capabilities for Computer_workstation_700 667
Inform NNM about the New Fields 668
Provide Additional Information in the oid_to_type File 669
Update the Database 670
Verify Symbol Changes 671
Back Up Your Efforts 673

E. Changing an Object's Vendor and SNMP Agent

How NNM Discovers Vendor and SNMP Agent Values 676

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1391
3740
Doc:

When the Vendor and SNMP Agent Would Not Be Set 677
Procedure 678
Example 679

Index 685

1938

Support

Please visit the HP OpenView web site at:

`http://openview.hp.com/`

There you will find contact information and details about the products, services, and support that HP OpenView offers.

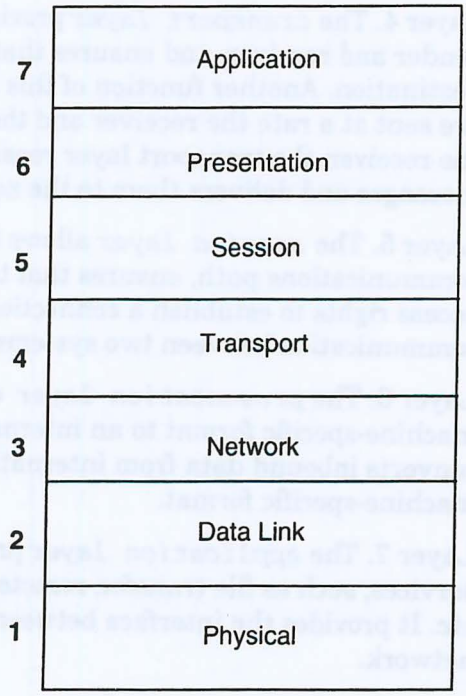
The support area of the HP OpenView web site includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1392
3740
Doc:

Figure 1 shows the layers of the OSI model.

Figure 1 Layers in the OSI Model



In a layered scheme, messages originate from the top layer (Layer 7) of a transmitting computer, move down to the lowest layer (Layer 1) and travel across the network media to the receiving computer. The message arrives at the lowest layer (Layer 1) of the receiving computer and moves up through its various layers to Layer 7.

Each of the layers is described below.

- Layer 1. The *physical layer* establishes the actual physical connection between the computer equipment and the network, and provides the transmission of bits from one system to another.
- Layer 2. The *data link layer* provides the transmission of packets, and performs error detection and correction functions to ensure that a packet contains the same information received as sent.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1393
3740
Doc:

- Layer 3. The *network layer* determines the path that will be taken through the network. The network layer also controls the rate at which the network accepts packets, to avoid and recover from congestion.
- Layer 4. The *transport layer* provides for the flow of data between sender and receiver, and ensures that the data arrives at the correct destination. Another function of this layer is to ensure that packets are sent at a rate the receiver and the application can cope with. At the receiver, the transport layer reassembles the packets into messages and delivers them to the next highest layer.
- Layer 5. The *session layer* allows the setup and termination of a communications path, ensures that the sender is authentic and has access rights to establish a connection, and synchronizes the communication between two systems.
- Layer 6. The *presentation layer* converts outbound data from a machine-specific format to an international standard format. It converts inbound data from international format to a machine-specific format.
- Layer 7. The *application layer* provides the software for network services, such as file transfer, remote login, remote execution, e-mail, etc. It provides the interface between user programs and the network.

Network Management Protocols

You should be familiar with the terminology and concepts of network management protocols, specifically the following.

SNMPv1 (Simple Network Management Protocol version 1)

SNMP is the most common management protocol in use in data networks. It provides a means of obtaining information from, and sending information to, network devices. SNMP is based on the manager-agent model, and uses Management Information Bases (MIBs) to exchange information between them (see "Exchanging Management Information" on page 27). Using the SNMP protocol, a manager can query and modify the status and configuration information on each managed device by making requests to the agent running on the managed device. All commands use the UDP/IP protocol, which means that communication between the manager and the agent is connectionless. SNMP operates at Layer 7, the application layer.

1932

SNMPv2C (version 2) SNMPv2C includes the basic functions of SNMPv1, and adds new message types, standardized multiprotocol support, enhanced security, new MIB objects, and a way to co-exist with SNMPv1. SNMPv2C is useful for the retrieval of large amounts of management information using fewer network resources.

UDP (User Datagram Protocol) UDP is a protocol that allows an application program on one machine to exchange datagrams with an application program on another machine, without acknowledgments or guaranteed delivery. UDP operates at Layer 4, the transport layer.

TCP/IP (Transmission Control Protocol/Internet Protocol) TCP and IP are the two most widely-used Internet protocols, with TCP providing transmission of data on IP networks, and IP containing addressing and control information for packets to be routed. TCP operates at Layer 4 of the OSI model, while IP operates at Layer 3.

TCP/IP plays a significant role as a common denominator in interconnecting devices and networks, and is widely used to connect computers with dissimilar technologies. Most management solutions require TCP/IP as an information source and information carrier.

ICMP (Internet Control Message Protocol) ICMP is the part of IP that handles error and control messages. It operates at Layer 3, the network layer. ICMP supports an `echo` function, which sends a packet on a round-trip between two hosts. `ping`, which sends a signal to see if an interface is up and running, is based on this feature. ICMP can also send an address mask request that returns the address of the subnet mask on the remote system. This feature is important for non-SNMP devices.

IPX (Internet Packet Exchange) IPX is a network protocol that allows personal computers to communicate on local area networks and wide area networks. Operating at Layer 3 of the OSI model, IPX establishes a connection between the sender and the receiver. When a message is sent and the receiver does not issue a response, the message is simply retransmitted. IPX uses a broadcast technique to track all the computers and services on the network.

ARP/RARP (Address Resolution Protocol) ARP is used at Layer 2, the link layer, to map an IP address to a MAC (or link level, or hardware) address. RARP (Reverse Address Resolution Protocol) is used to map a MAC address to an IP address.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls: Nº 1394
3740
Doc:

DHCP (Dynamic Host Configuration Protocol)DHCP allows IP addresses to be allocated on a temporary basis (a lease). When the lease for an IP address expires, the address can be reused by a different node. This is useful in environments supporting mobile users who connect to the network with a laptop from many different places. This helps alleviate the problem of limited IP addresses and simplifies TCP/IP client configurations.

Protocols and the OSI Model

Figure 2 illustrates which protocols operate at the various layers of the OSI model. This illustration shows the major protocols used in network management; there are other protocols that are not shown in this illustration.

Figure 2 **Protocols Operating at the OSI Layers**

	Layers in the OSI Model	Protocols Operating at the OSI Layers
7	Application	SNMP Berkeley Services ARPA Services
6	Presentation	
5	Session	
4	Transport	TCP UDP
3	Network	IP/IPX ICMP
2	Data Link	ARP/RARP IEEE 802.x DHCP MAC address
1	Physical	10BASE2 10BASE5

Network Hardware Devices

The basic kinds of network communication devices include repeaters, hubs, bridges, routers, and switches. Figure 3 shows the layers at which these devices operate. These hardware devices operate at different layers of the OSI model, use different protocols, and perform different functions, thus requiring different levels of monitoring for network management. NNM will assist you with this task.

Figure 3 Hardware Devices Operating at the OSI Layers

Layers in the OSI Model		Protocols Operating at the OSI Layers	Hardware Devices at the OSI Layers
7	Application	SNMP Berkeley Services ARPA Services	Gateways
6	Presentation		
5	Session		
4	Transport	TCP UDP	
3	Network	IP/IPX ICMP	Routers Switches
2	Data Link	ARP/RARP IEEE 802.x DHCP MAC addresses	Switches Bridges
1	Physical	10BASE2 10BASE5	Simple Repeaters Hubs

- Simple Repeaters

  Simple repeaters operate at Layer 1, the physical layer, and are generally used to connect two network segments into one large segment, or to expand an existing segment. There is no filtering of messages transmitted between the two segments. A simple repeater

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1395
3740
Doc:

enhances data signals and thus can be used to extend maximum cabling distances. There is no network intelligence built into a simple repeater; it is used strictly for signal propagation.

- Hubs

  Hubs operate at Layer 1, the physical layer. A hub is simply a multiport repeater, and can be used to increase overall network size and number of nodes on a single segment. A hub allows you to isolate faults within the subnet and add stations to a segment without disrupting the entire network.

- Bridges

  Bridges operate at Layer 2, the data link layer. A bridge is used to allow networks with different physical signaling, but with compatible data link addressing schemes, to communicate. Bridges help reduce traffic on a backbone LAN by filtering any information coming from one segment to another that does not need to be forwarded through the backbone. A common use for a bridge is to allow users on an Ethernet LAN and a Token Ring LAN to communicate with each other.

- Switches

  Switches operate at Layer 2, the data link layer. The function of a switch is to dispatch data to its destination, which it determines from the packet's lower-layer media access control (MAC) address. A switch, like a bridge, limits traffic, and does not understand network protocols. A fairly new device is the multi-layer switch, or routing switch, which operates at Layer 3, and combines the intelligence of a router with the efficiency of a switch, thus routing data at higher speeds.

- Routers

  Routers operate at Layer 3, the network layer. A router is used to connect two networks with different technologies, and provides an intelligent means of transferring packets from one network to the other. A router also forwards traffic among multiple hubs and bridges.

- Gateways

1928

Gateways operate at Layer 7, the application layer, and can encompass all seven of the OSI model layers. A gateway is a computing system that can be programmed to do any number of intricate protocol conversions and negotiations, such as between IP and IPX.

Exchanging Management Information

There are two standard logical information exchange bases used to communicate about the configuration and status values of managed objects — MIBs for SNMP-based objects and MIFs for DMI-based objects.

MIBsThe data exchanged between managers and agents on an SNMP-based system uses the **Management Information Base** (MIB). A MIB is a standard set of definitions for exchanging information about hardware and software components. Each MIB contains a group of objects, which specify a structure and format for defining manageable elements.

Types of MIBs There are several MIBs with which you should be familiar.

- MIB-I

  MIB-I is the original standard for explaining and defining the exact information base needed for monitoring and controlling devices on TCP/IP networks. The objects included in MIB-I are essential for configuration control and fault monitoring. All other MIBs are built upon and include the definitions of MIB-I.

- MIB-II

  MIB-II extends the information defined in MIB-I by expanding the set of objects defined in the MIB. The types of objects added to MIB-II include those for dealing with various transmission media types, and those for using SNMP to control and monitor the network management itself.

- RMON MIB

  The Remote Monitoring (RMON) MIB defines information that can be collected by remote monitoring devices. The main functions of the RMON MIB are to provide offline operation of remote devices, pre-emptive monitoring, problem detection and reporting, data analysis, and support for multiple managers.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1396
3740
Doc:

- Bridge MIB

  There are two modes of bridging — transparent mode and source route. The Bridge MIB defines objects needed to manage a bridge operating in transparent mode, as well as some objects applicable to all types of bridges. NNM includes a Source Route Bridge MIB that, although not used by NNM for discovery, can be used for your own needs.

- Repeater MIB

  The Repeater MIB defines objects used to manage repeater devices, including multiple repeaters and non-standard repeaters.

- MAU MIB

  The MAU MIB defines objects used to manage Medium Attachment Units (MAUs). These MAUs may be connected to IEEE 802.3 repeaters or to 802.3 (Ethernet-like) interfaces.

- Private MIBs

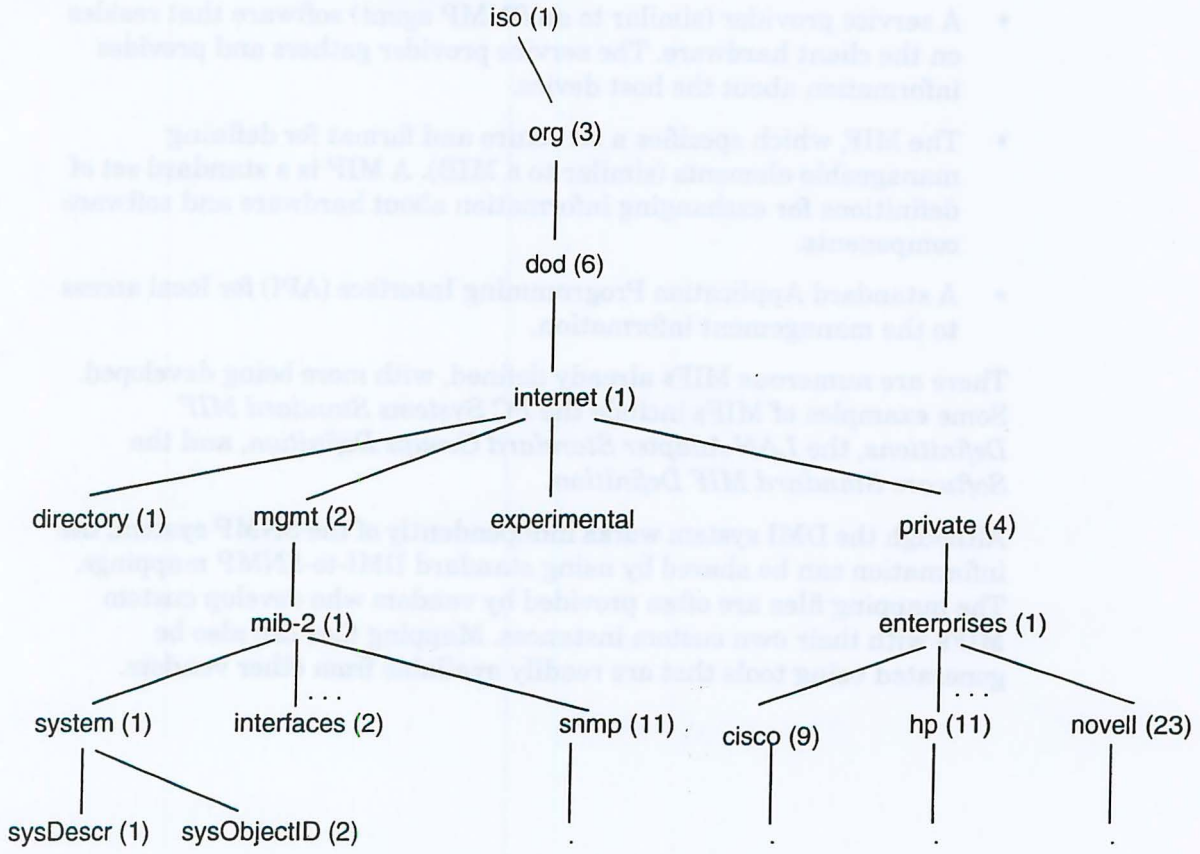
  Private MIBs are extensions to a MIB, usually developed by a vendor or a workgroup, to manage specific devices. The most common objects in these MIBs relate to information about the physical configuration and software configuration of a device.

How MIBs Are OrganizedMIB objects are conceptually organized in a hierarchical tree structure. Each branch in the tree has a unique name and numeric identifier. Intermediate branches of the tree serve as a way to group related MIB objects together. The "leaves" of the tree represent the actual MIB objects. Figure 4 illustrates the tree structure, with special attention to the Internet MIB tree.

A MIB object is uniquely identified (named) by its place in the tree. A full object identifier consists of the identifier of each branch along the path through the tree hierarchy, from the top of the tree. For example:

.iso.org.dod.internet.mgmt.mib-2.system.sysObjectID
(.1.3.6.1.2.1.1.2)

Figure 4 **MIB Organization**



MIB Objects and InstancesA specific type or class of management information is called a **MIB object** (for example, a system description or an interface status). The existence of a particular returned value for a MIB object in the agent database is called an **instance**. Some MIB objects have only a single instance for a given agent system (for example, system description). Other MIB objects have multiple instances for a given agent system (for example, interface status for each interface on the system).

MIFs A **MIF** is a **Management Information Framework** for objects conforming to the Desktop Management Interface specification.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1397
3740
Doc:

The **Desktop Management Interface** (**DMI**) facilitates the management of PCs in a networked environment by providing a common interface and information access method. DMI provides a management framework that consists of three elements:

- A service provider (similar to an SNMP agent) software that resides on the client hardware. The service provider gathers and provides information about the host device.
- The MIF, which specifies a structure and format for defining manageable elements (similar to a MIB). A MIF is a standard set of definitions for exchanging information about hardware and software components.
- A standard Application Programming Interface (API) for local access to the management information.

There are numerous MIFs already defined, with more being developed. Some examples of MIFs include the *PC Systems Standard MIF Definitions*, the *LAN Adapter Standard Groups Definition*, and the *Software Standard MIF Definition*.

Although the DMI system works independently of the SNMP system, the information can be shared by using standard DMI-to-SNMP mappings. The mapping files are often provided by vendors who develop custom MIFs with their own custom instances. Mapping files can also be generated using tools that are readily available from other vendors.

General Operating System Knowledge

In addition to understanding networking concepts, it is critical that you have a good working knowledge of the operating system, or systems, that are present on your network. This book does not attempt to explain any concepts of the UNIX®[1] or the Windows®[2] operating systems. It frequently refers to commands and functions of these operating systems, without further explanation. Refer to the documentation that came with your operating system for more information.

Cross-Platform Issues

Since it is likely that your network environment contains a combination of systems, you need to be aware of the differences between their operating systems. Some of the differences are listed below.

- Reference pages in NNM's online help on a Windows operating system are called manpages on a UNIX operating system.
- Directories and paths are different on each system. Consult the *ov.envvars* reference page in NNM's online help (or the UNIX manpage) for a mapping of paths across systems.
- Watch your use of the forward slash (/) and the backslash (\) when entering pathnames. When switching from a UNIX operating system to a Windows operating system, it is easy to misuse one for the other.
- Do not use spaces in directory names or file names.
- Watch the use of upper and lower case of file names. Even though the Windows operating system preserves file name case, not all applications on the Windows operating system distinguish between upper and lower case. In addition, case is significant on UNIX operating systems.
- On Solaris systems, `pc nfs` must be installed, and the `pcnfsd` process running, before a Solaris management station will interoperate with a Windows operating system.

---

1. The term *UNIX* in this manual refers to HP-UX and Solaris operating systems only.
2. See the *Release Notes* for supported versions of *Windows* operating systems.

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1398
3740
Doc:

- If you are using remote consoles running a Windows operating system with a management server running a UNIX operating system, be sure your NFS client product on the Windows operating system supports file locking. Not all do.

For More Information

If you need more information about networking or operating system concepts, the following documentation may be helpful.

Internet Request for Comments (RFC) Documents

Copies of RFCs are shipped on Network Node Manager's installation CD. RFC file names other than those mentioned in Table 1 may be included in the *Windows* and *UNIX* directories mentioned below.

Windows: installed on your hard drive through a custom installation in the *install_dir*\doc\RFC directory.

UNIX: in the $OV_DOC/RFCs directory.

Table 1 Where to Find RFC Documents about MIBs

To find out about...	See...	Filename
How MIB objects are defined	*RFC1155: Structure and Identification of Management Information for TCP/IP-based Internets*	rfc1155.txt
The protocol used to manage the MIB objects	*RFC1157: A Simple Network Management Protocol (SNMP)*	rfc1157.txt
The format for creating MIB object files	*RFC1212: Concise MIB Definitions*	rfc1212.txt
The objects contained in the Internet-standard MIB	*RFC1213: Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*	rfc1213.txt
Defining objects for managing MAC bridges	*RFC1493: Definition of Managed Objects for Bridges*	rfc1493.txt
Defining objects for managing IEEE 802.3 Medium Attachment Units (MAUs)	*RFC1515: Definition of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)*	rfc1515.txt
Definitions of Community-based SNMPv2C	*RFC 1901:Introduction to Community- based SNMPv2*	rfc1901.txt

RQS nº 03/2005 - CN
CPMI - CORREIOS
Fls. Nº 1399
3740
Doc.

Table 1 Where to Find RFC Documents about MIBs (Continued)

To find out about...	See...	Filename
MIB definition language for managed objects	*RFC1902:Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)*	`rfc1902.txt`
MIB definition language for conformance and capability definitions	*RFC 1904: Conformance Statements for version 2 of the Simple Network Management Protocol (SNMPv2)*	`rfc1904.txt`
Definitions of SNMPv2C protocol	*RFC 1905: Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*	`rfc1905.txt`
Definitions of SNMPv2 transport mappings for IP, IPX, and DDP	*RFC 1906: Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)*	`rfc1906.txt`
Definitions of SNMPv2 MIBs for IP, IPX, and DDP	*RFC 1907: Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)*	`rfc1907.txt`
MIB definition language for refined data types	*RFC 1903: Textual Conventions for version 2 of the Simple Network Management Protocol (SNMPv2)*	`rfc1903.txt`
Co-existence guidelines for SNMPv1 and SNMPv2	*RFC 1908: Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework*	`rfc1908.txt`
Defining objects for managing IEEE 802.3 baseband repeaters	*RFC2108:Definition of Managed Objects for IEEE802.3 Repeater Devices*	`rfc2108.txt`

Table 2 Where to Find RFC Documents about DMI and MIFs

To find out about...	See...	Filename
Desktop Management Interface 2.0 Standard	*DMTF: Desktop Management Interface Specification, version 2.0*	`dmi-v20.doc`

1920

Table 2 Where to Find RFC Documents about DMI and MIFs (Continued)

To find out about...	See...	Filename
Access to DMI instrumentation and events using SNMP	*DMTF: DMI to SMP Mapping Standard, Version 1.0*	`dmi-snmp.doc`
General information about the DMTF and DMI	Desktop Management Task Force web site	`www.dmtf.org`
Defining objects for managing MAC bridges	*RFC1493: Definition of Managed Objects for Bridges*	`rfc1493.txt`

Web Sites

There are numerous sites on the World Wide Web that contain lists of reference materials and links to other useful networking sites. Hewlett-Packard does not endorse these sites, but has found them to contain informative references. Note that the URLs for these sites are subject to change without notice, but were valid as of the date of printing of this document.

Table 3 Web Sites Related to Network Management

Web Site URL	Description
`www.ovforum.org`	The web site of HP OpenView Forum, an association of users and developers of HP OpenView network and system management solutions
`www.iol.unh.edu/training/index.html`	Tutorial documents on network technologies and network management
`www.ietf.org`	The web site of the Internet Engineering Task Force
`netman.cit.buffalo.edu`	Archives for `comp.dcom.net-management`
`www2.tmforum.org`	The web site of the TeleManagement Forum

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1400
3740
Doc:

Table 3 Web Sites Related to Network Management (Continued)

Web Site URL	Description
www.dmtf.org	The web site for the Distributed Management Task Force, Inc.
www.opengroup.org	The web site for The OpenGroup (X/Open and OSF®)
www.ieee.org	The web site for the Institute of Electrical and Electronic Engineers
www.simple-times.org	The *Simple Times* newsletter

The Network Management Challenge

As a network administrator, you are under increasing pressure to perform the necessary tasks to meet the business demands of your organization. Some of the challenges you often face include:

- Dealing with user dissatisfaction in the face of increasing user expectations. Users want to be able to have the tools they want, when they want them to maintain their productivity.
- Deploying network services so that end users maintain productivity from their desktop systems.
- Keeping the systems operating 24 hours a day, 7 days a week.
- Producing faster, more predictable response times.
- Integrating and managing diverse and complex technologies — networks, servers, databases, applications, legacy systems, web-based systems—all from different vendors.
- Managing multiple sites and global distribution.
- Moving to proactive management techniques to keep it all running smoothly.

Clearly, the demands on a network administrator are great. Network management is now a high-pressure situation where more services are requested on tight schedules with fewer resources.

How Network Node Manager Can Help

Network Node Manager is the foundation from which most of the HP OpenView products operate. When installed, the other HP OpenView products appear as added functionality within NNM. NNM not only functions as a solution on its own, but can collect data for, and forward data to, other HP OpenView products. It is the starting point for implementing a network management solution.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1401
3740
Doc:

Moving to Proactive Network Management

By using proactive, rather than reactive, network management, you can reap the true benefits of NNM. Several things must be present in order for proactive network management to be a reality.

- First, you must find out the current state of your network—what devices are present, how they are configured, how they are behaving, their performance levels, what is currently going wrong. NNM does this for you by polling for network information and screening problems through event correlation.
- Second, you must identify trends and determine how to optimize the network by changing configurations, replacing network devices, etc. NNM assists you by collecting historical information. You can easily access the historical data that NNM gathers and use it in your favorite statistical analysis programs.
- Third, you must learn how to predict what might go wrong, determine how to prevent it from happening, and learn to avoid future problems. NNM allows you to monitor thresholds of your choosing for critical network devices.

Poll for Network Information

The first step to proactive network management is to gather all the information that you can about the current state of your network.

NNM continually polls for:

- Status of objects (for example, up, down, or marginal).
- Network topology changes, including the discovery of new nodes.
- Configuration changes.

You can configure thresholds for NNM to monitor on critical network devices and configure NNM to notify you or your team members when anything goes wrong. For example, you can set thresholds on CPU loads, disk space used, interface and link errors, and collected MIB data. You can configure NNM to dial a pager when any of these situations become critical.

Watch for Events

NNM actively notifies you when an important event occurs. The event is reflected by a change in the color of the device's symbol on the map, and is reported through NNM's Alarm Browser.

Each category of alarms has a corresponding button that changes color to show the highest severity alarm in the category. Thus, you are immediately notified of potential or current problems.

You can browse through alarms to help you diagnose problems. You can view alarms by specific node or other sort criteria to help you solve problems quickly. The event reduction features in NNM monitor incoming alarms, identify patterns of common network problems, and for an identified problem, post one meaningful alarm with all related alarms nested beneath.

You can define the format of alarm messages so that they are most useful to your team. Your team can use the Alarm Browser to notify everyone else about which issues are being covered.

You can use event customization to automate some of the common fault management tasks for your team by using NNM to configure automatic actions upon the receipt of specific alarms. You can also filter out less important events, or simply send them to a log file.

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1402
Doc. 3740

Network Management Functions

Network management can be defined in general terms as the ability to have a single point of control to accomplish the activities required to manage a network. Network Node Manager provides an integrated tool for the network manager to control and manage multiple networked systems and applications from a single graphical representation of the network.

When properly implemented, a network management station can result in:

- Reduced downtime of network systems and devices.
- Quick detection and correction of network problems without disrupting the network.
- The ability to monitor data to anticipate problems (predictive).
- The ability to log information for historical analysis.
- The ability to perform an action when some pre-defined event or situation has occurred.

To understand how Network Node Manager and other HP OpenView products address these problems, it is helpful to break network management down into functional categories, listed below. Following this list is an explanation of how NNM and other HP OpenView products help you manage these areas.

- Fault and Problem Management

  This function detects, isolates, and controls problems, or faults, on the network. This is carried out by network status monitoring, alarms, alerts, reporting, and predictive tools.

- Performance Management

  This function measures the performance of network hardware, software, and media, such as throughput rate, percentage utilization, error rates, and response time, through the collection and analysis of data about the network.

- Configuration and Change Management

This function is responsible for finding and setting up the network devices that control the behavior of the network. This function also includes central control of configurations.

- Accounting Management

  This function obtains statistical information on network use. You can collect and process data related to resource consumption on the network, track each individual and group's utilization of resources, and control access to the network for individuals and groups.

- Security Management

  This function protects the network and its interconnections, systems, and network management information from unauthorized access, unauthorized use, and other harm.

Fault/Problem Management

NNM's Capabilities

Often times the most difficult management task is identifying the source of a problem when it occurs. NNM helps you identify problems and errors, recognize trends, and proactively avoid problems. NMM lets you:

- Automatically discover the IP and IPX nodes in your network.
- Automatically monitor your network's status through the map interface and the event browser interface.
- Manage any vendor device that supports the Simple Network Management Protocol (SNMP). NNM manages both standard and enterprise-specific Management Information Base (MIB) objects.
- Manage non-SNMP nodes that use IP or IPX protocols.
- Manage any vendor device that supports the Desktop Management Interface (DMI). NNM monitors both standard and enterprise-specific Management Information Format (MIF) objects.
- Include new enterprise-specific Internet MIBs in NNM's MIB. Once you have loaded the new MIB module on the management station, you can access any of the MIB objects defined in that MIB module.
- Build new MIB applications (without programming) for Internet-standard and enterprise-specific MIBs. Once you have built a MIB application, you can monitor objects through the menu bar.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls! Nº 1403
Doc 3740

- Define event thresholds for MIB objects; for example, an event can be generated when the disk usage on a particular device exceeds a limit.
- Define actions to be taken upon receipt of an SNMP trap.
- Manage event storms and improve the information content of events by suppressing unwanted, redundant events and adding new, more informative events, using NNM's event reduction strategies: de-duplication, ECS correlations and Correlation Composer correlators.
- Integrate your own fault detection applications into the menu bar to yield an integrated management solution.
- Diagnose network faults and performance problems from one location, and diagnose problems by looking at trends over time. This includes customizing and automating the monitoring of your network and the response of management stations to events.
- Launch Systems Management Server (SMS) Administrator, or view the SMS properties of a node. From SMS Administrator, you can select a node and open the submap containing that node.
- Launch Windowsoperating system applets such as the Event Viewer, Performance Monitor, and Registry Editor from within NNM on remote systems with the Windowsoperating system.

Other HP OpenView Products' Capabilities

HP OpenView NNM Extended Topology Extended Topology augments NNM by discovering and displaying additional device connectivity information that you can use to diagnose network problems. It includes:

- Management of heterogeneous switched layer 2 environments and routed layer 3 environments.
- An enhanced web user interface with dynamic views.
- Views from protocols and technology running on top of your network, such as OSPF and VLAN.
- Launching targeted views from events for rapid problem resolution.

HP OpenView Operations IHP OpenView Operations is an event and problem management solution that allows you to identify, locate, correlate, and resolve system and network faults. It includes:

- A central management console for monitoring events.
- Intelligent agents that can be preconfigured to solve problems immediately without interacting with the management console.
- Management of workstations running UNIX operating systems, the Windows operating systems, Novell Netware, and legacy systems.
- Integration with other OpenView products.

Performance Management

NNM's Capabilities

Figuring out how to fine-tune your network's performance can be a real challenge. To assist in this task, NNM gathers and reports information on network performance, availability, inventory, and exceptions. NNM can forward information to other HP OpenView products that provide statistical analysis on the data.

The following is a brief summary of NNM information gathering features:

- Automatically monitor your network's status.
- Collect historical MIB information about MIB objects and MIF events, store the data for trend analysis, and graph collected data. This helps you determine performance trends.
- Automatically set thresholds based upon standard deviations of historically collected data.
- Automatically collect data and generate General Availability and General Inventory reports.
- Manage and modify reports using the NNM Report Configuration Interface.
- Manage information being collected and stored in the data warehouse.
- Integrate your own performance monitoring applications with the menu bar to yield an integrated management solution.
- Diagnose network faults and performance problems from one location, and diagnose problems by looking at trends over time. This includes customizing and automating the monitoring of your network and the response of management stations to events.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1404
3740
Doc:

Configuration and Change Management

NNM's Capabilities

Keeping track of the devices on your network, their configurations, and their interrelationships can be time consuming. NNM helps you keep a record of this information, by allowing you to:

- Store critical configuration information from devices such as routers and switches.
- Track inventory of the devices on the network.
- Generate snapshots of your network before any departmental moves to speed reconstruction after the move.

Additional HP OpenView Product Information

You can find additional information about other HP OpenView products and solutions at `http://openview.hp.com`.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1405
3740
Doc:

1406

2 How Does NNM Work?

ROS nº 03/2005 - CN -
CPMI - CORREIOS
Fls.: Nº 1406
Doc: 3740

When you set up NNM to run on a management station, your team can access NNM from the management station, from remote consoles, or from the worldwide web. All three forms of access tie into the same databases running on the management station. Therefore, all members of your team continuously see the most current information. NNM works for you in the following ways, as explained in this chapter:

- Maps out your network for you. The map symbols change color to indicate if something is wrong (page 56).
- Collects critical information about your network and maintains a current log of alarms that you need to know about (page 51).
- Correlates collected information to help you quickly determine the probable cause of problems (page 61).
- Maintains a relational database from which data can be exported for historical analysis using your choice of statistical programs (page 62).
- Provides easy access to report generation, see the NNM online help for more information. See also the *Reporting and Data Analysis* online manual. You can create reports using a set of predefined templates that are populated from the data warehouse.

The remainder of this book then leads you through the process of understanding, configuring, customizing, and troubleshooting NNM.

Collecting Critical Information

NNM uses several protocols to maintain communication channels with each managed device on your network. These include:

- SNMPv1; SNMPv2
- TCP/IP
- IPX/DMI
- UDP
- ICMP
- ARP/RARP

Since SNMP is the primary protocol used for NNM's communications, an understanding of the SNMP management model will help you better understand how NNM works.

NNM also uses other, lower-level families of protocols (sometimes referred to as services), such as the ARPA family, the Berkeley family, and the NFS family. These protocols are used for functions such as file transfer, e-mail, or remote login.

SNMP's Network Management Model

The network management model consists of a network management station, managed nodes with agents, and a network management protocol. NNM uses SNMP as its standard protocol, and uses this protocol to communicate over other protocols, such as TCP/IP, IPX, and UDP.

The Role of Manager and Agents

A manageable network consists of one or more network management stations (manager), a collection of SNMP agents, and network objects.

- A **manager** is an application that executes network management operations to monitor and control agent systems. The implementation of these network management operations is called the manager.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1407
Doc 3740

- An **SNMP agent**, which resides on a managed node, is an application that acts on behalf of an **object** to perform network management operations requested by the manager.
- An **object** is anything that will be managed, such as a host, gateway, terminal server, hub, bridge, application, or database.

A manager and an agent may exist on the same system. The manager and agent communicate using the Simple Network Management Protocol (**SNMP**). Network Node Manager supports both SNMP version 1 (SNMPv1) and Community-based SNMP version 2 (SNMPv2C). SNMP permits the following activities:

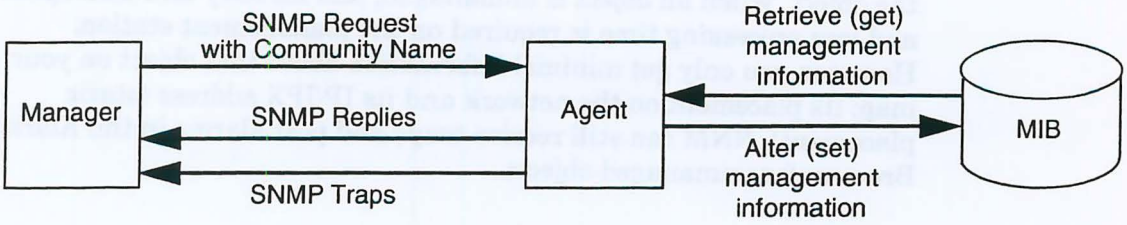
- A manager can retrieve management information from an agent. (The actual mechanism to retrieve management information depends upon the SNMP versions supported by the agent, and can include `get`, `getNext`, and `getBulk`.)
- A manager can alter, or `set`, management information on the agent's system.
- An agent can send information to the manager without an explicit request from the manager. This operation is called a **trap** in SNMPv1, or a **notification** in SNMPv2C.

Traps and notifications alert the manager to changes that occur on the agent system, such as a reboot. The agent must usually be preconfigured to know where to send traps or notifications (see page 325).

SNMP requests for information from an agent are accompanied by a **community name**. A community name is much like a password; it must be correctly received from the manager before information can be accessed from the agent. You must inform NNM about the community names that are in use on your network (see page 145). The manager accesses the agent's MIB object instances using SNMP's `get`, `getNext`, `getBulk`, and `set` operations.

Figure 2-1 shows a simplified diagram of the manager-agent interactions just described.

Figure 2-1 Manager-Agent Communication through SNMP



Basic SNMP Services

There are six basic operations associated with SNMP. They are:

- `get` request. Reads a value from a specific variable.
- `getNext` request. Traverse information from a table of specific variables.
- `getBulk` request.
- `get` response. Replies to a `get` or a `set` request.
- `set` request. Writes a value into a specific variable.
- `trap` or `notification`. A message initiated by the agent without requiring the management station to send a request.

Managed versus Unmanaged Objects

A **managed object** is one that is actively being polled by NNM to determine its status and configuration. An **unmanaged object** is one that exists in the databases and within maps, but is not being polled by NNM.

NNM gives you the choice of managing or not managing objects, depending on your information needs and network resources.

When an object is managed, NNM can obtain any information that you specify about that object (as long as that object's protocol is supported). The more objects you manage, the more memory and disk space is required on the management station. In addition to the information that you specify, the management station will need processing power for the

ROS nº 03/2005 - C
CPMI - CORREIO
Fls. Nº 1408
3740
Doc:

routine status and configuration polling and the event monitoring of each managed object. If an object is critical to the network function, then you should manage it.

If the object is not critical to the functioning of your network, you might choose to *unmanage* it; which means that NNM will not actively monitor the object. When an object is unmanaged, less memory and disk space and less processing time is required on the management station. However, you only get minimal information about that object on your map: its placement on the network and its IP/IPX address (static placement). NNM can still receive traps and post alarms in the Alarm Browser for unmanaged objects.

Desktop Management Interface (DMI)

The Desktop Management Interface (DMI) is a parallel management strategy to SNMP. DMI standards were developed by the Desktop Management Task Force (DMTF). Although DMI is entirely independent from the SNMP protocol, there are many similarities:

- The DMI **client** is similar to the SNMP management station.
- The DMI **service provider** is similar to the SNMP agent and must be running on each remote DMI device.
- The DMI **MIF** (Management Information Format) file is similar to the SNMP MIB file and defines the management information that can be provided by the service provider (event) or requested by the client (get/set).
- The **DMI event** is similar to the SNMP trap.

If your management station is running NNM on the Windows operating system, during discovery polling, NNM **subscribes** to receive DMI events from all managed systems running DMI version 2.0. All DMI events are received by NNM's ovcapsd service (background process) and converted to SNMP traps as specified in the Desktop Management Task Force's DMI to SNMP Mapping Standard. The SNMP-equivalent message is posted to NNM's Alarm Browser.

NOTE If your management station is running NNM for a UNIX operating system, you must communicate with the DMI service provider indirectly through an SNMP agent installed on the remote DMI-enabled device itself along with a DMI-to-SNMP mapping agent. The SNMP agent then

handles all communications. Therefore, NNM doesn't need to subscribe to the DMI service provider in order to receive DMI events from this node.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1409
3740

Automatic Discovery and Layout

When you start the NNM background processes, all IP and Level 2 devices (devices that support bridge, repeater, and MAU MIBs) on your network are automatically discovered and mapped out. If you are running NNM on a management station running the Windows operating system, IPX devices are also discovered and mapped out. This map is a visual representation of the communications channels established between NNM and the devices in your network. Be aware that this map is not a physical representation; rather, it is a logical representation. The accuracy of these communications channels between NNM and your network devices determine whether or not NNM can provide the information you need in order to manage your network.

The initial polling process may take several hours, or even over night, to discover all the devices on your network. However, it is worth the wait! You start benefiting from NNM immediately. You will use NNM's default map, and Alarm Browser to pin-point any gaps in your well-configured network scheme.

How IP Discovery and Layout Work

The `netmon` service (background process) uses a combination of SNMP requests and ICMP `pings` transmitted over UDP and IPX to find out about the nodes on your network.

To discover the nodes on the network, `netmon` needs access to the following information:

- The subnet mask from the agent on the management station.
- The address of the default router in the management station's routing table.
- SNMP information from, at a minimum, the default router, and from other routers and nodes on the network.

For `netmon` to work, it requires the following:

- The management station must be correctly configured for networking.
- The management station must be running an SNMP agent.

- Nodes must be up and responding to ping requests to be discovered.
- All gateways/routers and the management station must have correctly configured subnet masks for all interfaces.

During IP discovery, netmon works best in these situations:

- The more routers in the network the better; and those routers should be running configured SNMP agents.
- The more nodes running configured SNMP agents the better.
- The more SNMP information netmon gets the better; for example, valid ARP caches and, from serial connections to routers, routing tables.

Information about the discovered nodes is stored in NNM's databases and is used to automatically generate the network map.

Over time, NNM will discover new nodes on the network. However, if a new node never talks with a gateway or other nodes on the network that support SNMP, NNM may not find it. In this instance you can use menu items within NNM to send a low-level ICMP ping that forces NNM to discover the node; or you can add the node manually.

How IPX Discovery and Layout Work

If you are running NNM on a management station running the Windows operating system, in addition to discovering IP nodes on your network, netmon performs IPX discovery of your network. However, the methods used are very different from those used for IP discovery. The IP discovery process relies primarily on SNMP queries to gain hints of new IP nodes. For IPX discovery, netmon relies on using broadcast versions of various IPX protocols to discover the nodes, then uses SNMP once the node is discovered to fill in additional information about the node. In particular, netmon will be able to determine that an IPX node supports IP only if that node supports SNMP over IPX.

While the discovery model is different, the layout results in the submap are very similar. IPX network symbols are created in the Internet submap, connected by IPX gateways. IPX network symbols can be exploded to display segment and node submaps. However, IPX nodes always are connected to a single segment in the IPX network.

To discover IPX nodes on the network, netmon requires the following:

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1410
3740
Doc:

- The management station must be correctly configured for IPX networking.
- At least one IPX server or router must be connected to the same network as the management station.
- Nodes must be up and responding to IPX diagnostic requests to be discovered.

During IPX discovery, `netmon` works best in the following conditions:

- The management station is not also an IPX/NetWare gateway.
- Servers, routers, and nodes in the environment respond to IPX diagnostic, Routing Information Protocol (RIP), and Service Advertising Protocol (SAP) requests.
- IPX nodes in the environment support SNMP over IPX.

As with IP discovery, the information about the discovered nodes is stored in the NNM's databases and is used to automatically generate the network map.

Because `netmon` uses broadcasts, most IPX nodes should be recognized after the first few IPX polling cycles. After the default IPX discovery interval of six hours, most IPX nodes will be discovered, with the majority coming soon after the initial discovery cycle at system installation or startup. However, this discovery rate will vary depending on the number and type of nodes in the network. So before you start to troubleshoot `netmon`, allow the process sufficient time to discover your network. This may require allowing IPX discovery to run over night.

Interactions Between IPX Discovery and IP Discovery

If an IPX node supports SNMP over IPX, `netmon` will attempt to use the MIB-II `ipAddrTable` to also include IP addresses and interfaces on the IPX node, as well as using the other MIB-II variables to provide additional information. When a node is discovered to support both IP and IPX, the following rules apply:

- Preference is generally given to the IP values as the name and labels for the node.
- After a node is determined to support IP, IP will be the preferred SNMP transport protocol.

- If a node is first discovered as an IP node, and a later IPX node is discovered to have the same set of IP addresses via SNMP, the IP node may be deleted in favor of the IPX node. For this reason, we recommend that you delay extensive map customization until IPX discovery is complete.

Level 2 Discovery

NNM takes advantage of information provided in three standard MIBs to discover bridges (switches) and hubs. These MIBs are the bridge MIB (RFC 1493), the repeater MIB (RFC 2108), and the 802.3 MAU MIB (RFC 1515). If a network device supports any of these MIBs, `netmon` will use the information reported to develop a model of the topology which better represents how and to what the device is interconnected.

In the case of switches and bridges, additional information is gathered from the bridge MIB. In the case of hubs, addition information is gathered either from the repeater MIB or the 802.3MAU MIB.

The status of non-IP or non-IPX interfaces on switches, bridges, and hubs is determined via SNMP based on the administrative and operating status of the port.

If the MAC address of a node, which does not support IP or IPX, is reported by any of these MIBs, the node is added to the topology relative to the device which hears it. A label for this device is determined by the MAC address reported by the network interface card. Because no MAC layer control message protocol is available, the status of the devices is determined indirectly via information provided by the surrounding network elements.

Trunking and Meshing

Configuring two or more ports between two network devices into a single group is referred to as port trunking. This is done to increase the available bandwidth between the two devices. For example, you can increase the available bandwidth between two devices, such as two ethernet switches, by configuring a group of two or more connections between the two devices.

Meshing involves connecting devices on the network via multiple paths. Meshing is used when devices are used in a critical function and redundant network connectivity is required.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1411
3740
Doc:

You can configure NNM to label port trunking and meshing connections with information you add to the `netmon.equivPorts` file. See "Configuring Trunking and Meshing" on page 225 for more information.

information helps NNM detect changes and communicate them to various NNM services. The topology database is stored in a proprietary HP OpenView format.

Event Database

The event database is the repository for SNMP traps and OVW events that are received by NNM. It also stores events that are output from the Event Correlation Service (ECS). In addition, the event database stores information for the event browser tools about the state of the events displayed in the web browser applications. The information in the event database is displayed in the Alarm Browser.

Trend Database

The trend database (sometimes called the `snmpCollect` database) stores MIB data and threshold information that is gathered through the `snmpCollect` service (process). Information from the trend database is used in the Reporting and the Data Collection features, and can be viewed with the Grapher feature of NNM on a management station.

Data Warehouse

The NNM data warehouse stores data exported from the NNM databases into a relational database. You export this data to the data warehouse using the `Tools:Data Warehouse` menu choices (`Export Topology`, `Export Events`, and `Export Trend Data`).

You can use the information in the data warehouse to define your own reports. You can also use the NNM web Reporting interface to configure and view reports. When you create a report using the web Reporting interface, NNM automatically starts exporting the appropriate data to the data warehouse.

An embedded relational database is provided with NNM, and Oracle® and SQLServer are also supported.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1412
3740
Doc:

1190

3 Resources Available While Learning NNM

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1413
3740
Doc:

There are many resources included with NNM that will help you use the product more effectively. In addition, there are also multiple additional services available through HP.

Resources included with NNM:

- Online help system (page 67)
- Tip of the Day (page 69)
- NNM's manuals, both printed and online (page 69)
- Release notes (page 71)
- Online reference pages/manpages (page 71)
- `contrib` programs (page 74)
- `support` directory (page 74)
- White papers (page 75)

Resources and services available through HP:

- HP web sites (page 76)
- HP Consulting Service (page 76)
- HP Education (page 77).
- HP Product Support (page 77)
- OpenView Forum (page 77)

1888

Resources Included with NNM

NNM Online Help System

NNM includes an online help system that contains all the specific procedural information you will need while you are working with NNM. The help system has extensive search capabilities and a comprehensive index so you can easily find information. You can print or copy pages or sections of help information that are appropriate for the most common tasks for your organization.

TIP The help system includes hyperlinks that make it more convenient and informative. By clicking on designated link words, you gain instant access to more topics and information related to your currently selected topic.

The online help system enables you to display information on the features of NNM, explains how to perform tasks with NNM, and includes conceptual information about how NNM works. Help entries are available from three general locations:

- `Help` menu
- `[Help]` button on dialog boxes
- Help from some symbol pop-up menus

Using the Help Menu

The contents of the `Help` menu varies from one submap to another, depending on additional installed applications. The `Help` menu also differs between NNM on a workstation running the UNIX operating system, NNM on a workstation running the Windows operating system, and the NNM web interface.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1414
Doc: 3740

Printing Information from Online Help

NNM for the Windows operating system uses a standard Microsoft® Windows help system. Each help window has a `Print` button or menu item that you can use to print the current topic. You can also select multiple topics in the help table of contents, then print those topics.

On UNIX operating systems, you can select a topic in the `Contents` window of help, then select the `Print` menu item. In the `Print` dialog box, select `Print Topic` to print only that topic. If you want to print all the subtopics under that topic, select `Print Topic and All Subtopics`.

You can then combine these help printouts into a binder for future reference. This is especially useful for frequently-accessed information, so that you do not have to access the help system every time you need to look up a common task or function. You can also use these printouts to create your own operating manuals.

Searching for Information

The most efficient way to find a particular help topic is index search. You access index search via the `Index` tab in the help system on a Windows operating system or by the `Index` button on a UNIX operating system. Every topic in the help system is indexed by the keywords that are used in the topic. When using index search, enter the word that best describes what you are looking for and that is most likely to narrow down your search. For example, if you want to find help on automatic map generation, enter the word "automatic" or "auto-generate" rather than the word "map." Those words are more likely to find the entry that you want.

In a Windows operating system only: another way to find information is by using the `Find` function in the online help. The `Find` function searches every word in every topic for the word or phrase of your choice, and returns a list of the titles of topics where those words or phrases appear.

Customizing Information for Your Organization

You can create custom information for your team or for a specific site within your organization. Simply copy and paste the contents of a help window to a word processor. Then add your own site-specific information or specific procedural information for your tasks to the help text. This can save you time when writing your own training or procedural manuals.

Using Online Help Independently from the Software (Windows only)

The NNM help system on the Windows operating system is designed so that you can copy the help volume onto a diskette, take it with you, and run it independently of the software—whether on your home computer or traveling with you on your laptop.

Copy the following files to a floppy disk. These files are found in the *install_dir*\help\%LANG% directory:

- *help_file_name*.hlp
- *help_file_name*.cnt

Double-click on the *help_file_name*.hlp file to start the help system.

Using Dialog Box Help

The [Help] button in a dialog box explains the purpose of the dialog box.

Using Symbol Pop-up Menu Help

The right mouse button pop-up menu on a selected symbol may contain a help item for that symbol. You can customize this menu through the application registration file (ARF) to add a help topic if it does not already contain one.

Tip of the Day

When you start NNM on the Windows operating system, the Tip of the Day appears. Add new tips by editing the *install_dir*\help\%LANG%\tipOfTheDay.txt file. Turn off Tip of the Day by removing the check from the Show tips at startup check box located in the Help:Tip of the Day menu.

Manuals: Printed and Online

NNM includes a library of detailed reference materials for your use. Some are provided in printed form, some are provided online as PDF files. Get additional information from the online help or the release notes. The following manuals are provided with NNM.

- *Installation Guide for HP OpenView Network Node Manager*

RQS nº 03/2005 - CN - CPMI CORREIOS
Fls. Nº 1415
3740
Doc:

This manual contains instructions about installing and configuring NNM.

- *Welcome to Network Node Manager*

  An overview of NNM, its features, and its capabilities.

- *Managing Your Network with HP OpenView Network Node Manager*

  This manual (that you are currently reading) contains detailed information to help network administrators configure, maintain, and troubleshoot NNM for their team.

- *Correlation Composer's Guide*

  This manual provides information about the HP OpenView Correlation Composer. You can use the Correlation Composer to create new event correlation logic. Be sure to read the information in Chapter 11, "Event Reduction Capabilities: Getting to the Root Cause," on page 351 before you start.

- *Guide to Scalability and Distribution for HP OpenView Network Node Manager*

  This advanced manual outlines the steps you need to take to deploy NNM across multiple management stations within your organization. It contains specific configuration procedures for using the scaling and distribution features of NNM. These features are important when the size of your organization's network exceeds the resources of one NNM management station. They allow you to divide the work load among multiple management stations, yet share the network management information as needed.

- *Reporting and Data Analysis with HP OpenView Network Node Manager*

  This manual is available only online and contains information about configuring and using NNM's reporting and data warehouse features. This book also contains information about how to export the historical data collected by NNM for your use with other statistical analysis programs of your choice.

- *Creating and Using Registration Files*

  This advanced manual is available only online and contains information about how to create and modify NNM's registration files, customizing the appearance and behavior of NNM.

- *Integrating HP OpenView Reporter*

  NNM and HP OpenView Reporter can be integrated, so that Reporter can query the NNM data warehouse to generate reports that help you to solve real network problems. This manual shows you how to configure the integration, as well as how to run and view reports. It also describes the preconfigured reports that are provided.

To access the online manuals shipped with NNM, use the `Help` menu. When you choose `Online Manuals`, a list of manuals appears. Choose the manual you want to view, and follow the instructions in the viewer.

Numerous additional HP OpenView online manuals are available at the following web site: `http://www.docs.hp.com`

Release Notes

For information about NNM that becomes available after this book is published, refer to the `ReleaseNotes` directory or the `README.html` file on the CD-ROM.

Release notes are available on your hard drive after installing NNM. You can access the release notes from NNM's menu `Help:NNM:Release Notes` (or on the Windows operating system under `Start:Programs:HP OpenView:HP OpenView Online Documentation:NNM Release Notes`).

You can also launch the release notes in your web browser:

Windows:

install_dir\www\htdocs\%LANG%\ReleaseNotes\README.html

UNIX: `/opt/OV/www/htdocs/$LANG/ReleaseNotes/README.html`

NOTE In this manual, `C` and `$LANG` in directory listings are variables for the language currently in use. `C` contains the English version.

Reference Pages (Manpages)

Reference pages (Windows operating system) or manpages (UNIX operating system) document NNM configuration possibilities in much greater detail than you will find any place else. These pages include information about every possible parameter and available command line

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1416
3740
Doc:

option, as well as useful background information that may be helpful when troubleshooting issues. These pages are named according to the function or feature that they are documenting.

Throughout this book, you will be referred to specific reference pages (manpages) for more information about the topic being discussed. You may want to browse through this resource collection yourself. You will find many more reference pages than are mentioned in this book.

Accessing Reference Pages

On Windows operating systems, reference pages are provided through the help system. You can access them from these locations:

- `Start:Programs->HP OpenView->HP OpenView Online Documentation->NNM Reference Pages`.
- Any submap within NNM, through the `Help` menu.

TIP

If you are not sure which reference page to access for a specific issue, use the `Find` feature of the help system. `Find` searches every word in every reference page and provides a list of all places where the word appears. For example, if you want to learn about the `netmon` service's parameter choices and relationship to other services, type `netmon` in the `Find` dialog box.

Accessing Manpages

On HP-UX systems, the following procedure is just one suggestion for displaying or printing manpages. This procedure requires that you have manpages installed locally on your system. (If your network provides manpages remotely instead (for example, from a central server), then check with your system administrator about how to access them.)

1. Determine where on your system the manpage files are kept. Type

   `echo $MANPATH`

   You should see a list with one or more directories. Multiple directories will be separated by colons (for example, `/usr/local/man:/usr/man`). It is recommended that you check the contents of each directory to make sure it actually has manpage files in it.

If you do not see a list of directories or you get no response to the `echo $MANPATH` command, refer to the section "Establishing Universal Pathnames" in Chapter 5.

2. Determine what syntax and options the `man` command is using. At a command-line prompt, type:

   `strings /usr/bin/man | grep col`

   You should receive a message similar to the following:

   ```
   tbl -TX %s |neqn|nroff -h -man|col -x > %s
   tbl -TX %s |neqn|nroff -man|col -x|%s
   ```

3. Use the command syntax shown in Step 2 in one of two ways:

   - Specify the qualified path of the directory containing manpage files as the `%s` value in the command.

     Example: you know that the *bggen*(1) manpage is stored in the `/usr/man/man1` directory on your system, but you are not currently in that directory. To display this manpage online, type the following command:

     `tbl -TX /usr/man/man1/bggen.1 |neqn|nroff -man|col|more`

     Example: to send the *bggen*(1) command's manpage to a file for printing instead, type the following:

     `tbl -TX /usr/man/man1/bggen.1 |neqn|nroff -man|col > /filename`

   - `cd` to the directory on your system that contains manpage files. Then specify just the command name and number as the `%s` value.

     Example: you are in the `/usr/man/man1` directory. Display the *bggen*(1) command's manpage online by typing:

     `tbl -TX bggen.1 |neqn|nroff -man|col| more`

     Example: to send this manpage to a file for printing instead, type the following:

     `tbl -TX bggen.1 |neqn|nroff -man|col > /filename`

On Solaris systems, consult your system documentation for information on accessing manpages online or printing them.

ROS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1417
3740
Doc:

The contrib Directory

The NNM `contrib` directory is a collection of programs and extensions to existing NNM programs that HP programmers have developed and want to share with NNM users.

The `contrib` directory contains a README file explaining the files in the directory. Many of the individual programs have README files as well, which contain information specific to the program.

When you install NNM on a UNIX operating system, the `contrib` directory is installed by default.

To install the `contrib` directory on a Windows operating system, you must use the "Custom Installation" feature.

The files are installed in:

Windows: *`install_dir`*`\contrib\NNM`

UNIX: `$OV_CONTRIB/NNM`

These programs are not supported by Hewlett-Packard and, as such, you use them at your own risk.

The support Directory

The NNM `support` directory is a collection of programs and Perl scripts that HP support engineers have developed and want to share with NNM users.

The `support` directory contains a README file explaining the files in the directory.

When you install NNM on a UNIX operating system, the `support` directory is installed by default.

To install the `support` directory on the Windows operating system, you must copy and paste the `support` directory from the NNM Installation CD to the management station's hard drive. Place the `support` directory in the following location:

The files are installed in:

Windows: *`install_dir`*`\support\*.*`

UNIX: `opt/OV/support/*`

These programs are not supported by Hewlett-Packard and, as such, you use them at your own risk.

White Papers

White papers are documents that explain various technical aspects of NNM and network management in general. Often these topics are not documented elsewhere.

When you install NNM on a UNIX operating system, the current white papers are installed by default.

To install the white papers on a Windows operating system, you must use the "Custom Installation" feature.

The white papers are installed in:

Windows: `install_dir\Doc\WhitePapers`

UNIX: `$OV_DOC/WhitePapers`

ECT nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1418
3740
Doc:

Resources and Services Available Through HP

You can find more information from the following sources:

- HP web sites
- HP Consulting Services
- HP Education
- HP Product Support
- OpenView Forum

HP Web Sites

General Information

Using a web browser, you can learn more about HP OpenView by visiting the main HP OpenView web page at: `http://openview.hp.com`.

This web site contains information on current products, as well as literature that you can print or download for viewing. There are links to HP technical support and sales offices.

Product Manuals

There is also a web site for accessing current HP OpenView product technical manuals that you can download and print. These manuals are available in PDF format. Its URL is:

`http://openview.hp.com`

Click on the `Support` icon, then select `Manuals`.

Another web site presents HP OpenView product manuals in searchable web-based format: `http://www.docs.hp.com`.

HP Consulting Service

The HP Consulting Service provides a wide range of consulting services, including initial installation and configuration, and network planning and organization. They can also help you plan and implement advanced strategies to help you take the best advantage of NNM's capabilities to

meet the specific needs of your organization. For more information about their services, visit the main HP Conculting web site, `http://www.hp.com/go/consulting`.

HP Education

HP Education presents numerous classes on Network Node Manager and HP OpenView, geared toward different levels of training. For more information about course descriptions and class schedules, visit the main HP OpenView web site, `http://openview.hp.com`.

HP Product Support

HP has more than 40 Response Centers worldwide offering telephone support in native languages and time zones. To register for telephone support, contact your local HP sales representative, or browse the HP OpenView web site at `http://openview.hp.com`.

In addition, HP offers software and materials support contracts so that you can automatically receive the newest versions of applications as they are available.

OpenView Forum

OpenView Forum is an association of users and developers of HP OpenView network and system management solutions. An independent corporation, the OpenView Forum represents a vast body of practical knowledge and experience provided through conferences, a web server, an email reflector, and personal contacts.

The OpenView Forum online discussion center provides members with a place where they can gain information and knowledge, and provide feedback to software developers about HP OpenView products.

OpenView Forum sponsors a conference each year, which is attended by vendors and more than 1000 Forum members. You can find out more about OpenView Forum at their web site: `http://www.ovforum.org`.

RQS nº 03/2005 - CN - CPMI - CORREIOS
Fls. Nº 1419
Doc: 3740

Summary of HP OpenView Web Sites

Table 3-1 presents a summary of the HP OpenView Web sites.

Table 3-1 Summary of HP OpenView Web Sites

HP Web Site	Contents
openview.hp.com	The primary web site for HP OpenView. Contains links to: HP OpenView training information Product literature Product manuals
www.hp.com/go/consulting	HP Consulting Services
www.docs.hp.com	Product manuals in searchable web-based format.
openview.hp.com-click on support panel	Access to HP support.
www.ovforum.org	OpenView Forum's web site where you can exchange information with other OpenView users.

1876
21

4 Planning Your NNM Configuration

RQC Nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1420
3740
Doc:



In order to get NNM the most benefit from NNM, you will probably want to configure NNM for your particular environment. NNM is a powerful program that can be configured in many ways. You need to budget time for planning how you wish to configure NNM and time for actually doing the configuration.

In order to make the whole process run as smoothly as possible, this chapter explains the issues to consider as you begin:

- "Budgeting Time for Planning and Configuration" on page 81
- "Taking Over NNM from Someone Else" on page 82
- "Understanding the Network Information Needs of Your Organization" on page 83
- "Knowing Your Network" on page 87
- "Starting with a Well-Configured Network" on page 90

Budgeting Time for Planning and Configuration

NNM is an extremely flexible program that can be configured to meet a large number of business needs. Read through this entire chapter before you begin configuring NNM. Clearly identify the specific ways in which you will use NNM to assist you in managing your management domain, to minimize the time you spend configuring NNM.

Time for Planning

If your management domain is small, this planning process could be quick. If your management domain is large and complex, it may take multiple meetings to gather the information that you need.

Time for Configuration

A quick sketch of the configuration process outlined in this book is:

- Install NNM--initial discovery, customization, and troubleshooting.
- Establish backup procedures for NNM's critical files.
- Configure NNM's active polling configuration.
- Configure the maps.
- Configure the event monitoring system.
- Decide what historical information is most useful, and establish data collection toward that objective.
- Establish the maintenance procedures and schedule.

Network management is complex and specific to each organization's needs. NNM can best assist you to meet your network management goals if it is optimally configured. Allow sufficient of time for the configuration process.

You need to have a clear idea about what devices you want to monitor, what kind of information you need from these devices, and how often you need the information.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1421
3740

Taking Over NNM from Someone Else

If you are responsible for taking over after someone else installed and configured NNM, browse through the chapters in this book in the order in which they are presented. As you read along, rather than configuring NNM, simply access all the configuration points as they are described to determine how NNM is currently configured. Once you understand the current configuration, you can go back through the process and implement your own ideas.

Understanding the Network Information Needs of Your Organization

To use NNM to its full potential, start with a clear idea of the business needs that NNM must address. You need to understand the groups within your organization and their information needs. You also need to start with a good understanding of your network itself.

Who Needs What Information?

First identify the groups within your organization who need access to information about the network. For example, upper management, facilities, technical support, and the printers group.

Then, identify what information each group needs, why they need it, and how they will use the information. For example, do they need real-time monitoring of specific devices around the clock or only during specific shifts for network troubleshooting? Do they need to know monthly trends of the volume of network traffic generated by each department for planning purposes?

Use the work sheet provided (page 85) as a starting point and detail the information needs of each group. Then decide which groups could share a map. Have a clear idea about what information everyone needs and how they want to receive that information before you start.

Ideal Uses for Maps

- At-a-glance notification that something has gone wrong.

  NNM's color-coded status notification alerts your team members immediately when a network or device is in trouble.

- Connectivity at-a-glance.

  A visual untangling of your network, the definitive authority of how everything is connected. The map is kept up-to-date automatically.

- Simultaneous monitoring of multiple sites.

RQS nº 03/2005 - CN -
CPMI - CORREIOS
Fls. Nº 1422

NNM can span multiple sites. In addition to NNM's map and alarm list, NNM's pull-down menus provide troubleshooting tools that allow your team to gather information and troubleshoot problems at the remote site.

- Quick response time.

  NNM's maps can be configured with floor plans of your site to speed your team's efforts in investigating hardware failures. If your team has a high turn-over rate, well designed maps can reduce training time.

- Establishing sphere of influence or management regions.

  You can have different maps for different areas of responsibility on your network. A map can manage a specific physical portion of your network or partition information about your network. Maps can have specific constraints and characteristics, run different applications, cover different geographic areas, and/or set compound status differently. You can customize maps so that they become a projection of your team member's responsibilities, showing what your team member wants to see about your network without requiring him/her to sifting through unneeded data.

Ideal Uses for the Alarm Browser

- Instant awareness of failures.

  NNM's Alarm Browser guarantees the speediest possible response, since your team members know instantly when trouble arises.

- Watching trends.

  Configure NNM to post threshold alarms from your mission-critical devices. Your team members detect developing trouble and start resolving it before users encounter network failures.

- Identify the device that is most likely causing the problem.

  NNM's event correlation system identifies the source device of certain issues and consolidates all alarms that were generated as a result of the root cause issue under the main alarm message.

- Automate responses.