HP OpenView Dashboard

For the Windows®, HP-UX, and Solaris Operating Systems

Software Version: 2.0

Operations View Integration Guide:

HP OpenView Network Node Manager

Document Release Date: July, 2006

Software Release Date: July, 2006

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

AMD is a trademark of Advanced Micro Devices, Inc.

HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Intel and Pentium are registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java™ is a US trademark of Sun Microsystems, Inc.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of The Open Group.

Support

Please visit the HP OpenView support web site at:

http://www.hp.com/managementsoftware/support

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and log in. Many also require a support contract.

To find more information about access levels, go to:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

http://www.managementsoftware.hp.com/passport-registration.html

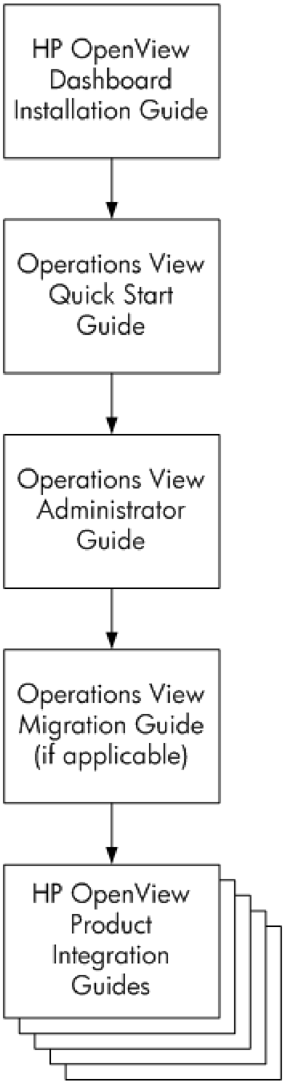
Contents

Documentation Roadmap

Figure 1 on page 12 shows the documentation roadmap for HP OpenView Dashboard Operations View. This roadmap presents a suggested order for reading the manuals available with Operations View:

1. Use the *Installation Guide* to install the product.
2. Follow the path for Operations View.
   a. Use the *Operations View Quick Start Guide* to carry out the tutorial.
   b. Read the "Essential Concepts" chapter of the *Operations View Administrator Guide* to understand the concepts of working with portlets and portal servers.
   c. Use the *Operations View Administrator Guide* to configure and maintain the product. This guide provides high-level instructions for the common tasks when working with the supplied Operations View portlets
   d. If you are migrating from HP OpenView Service Information Portal to Operations View, use the *Operations View Migration Guide* to complete this task. The *Operations View Administrator Guide* refers you to the *Operations View Migration Guide* at the appropriate point in the portal view implementation process.
   e. Reference the integration guides as needed for specific details on each supported HP OpenView management product. The *Operations View Administrator Guide* refers you to the integration guides at the appropriate points in the portal view implementation process.

Figure 1 Operations View Documentation Roadmap


HP OpenView Dashboard Installation Guide
Operations View Quick Start Guide
Operations View Administrator Guide
Operations View Migration Guide (if applicable)
HP OpenView Product Integration Guides

HP OpenView Dashboard Manuals

Table 1 describes the HP OpenView Dashboard manual set. These documents are provided in Adobe Acrobat (.pdf) format and can be found in the following directories:

- After HP OpenView Dashboard installation, in the following directory on the HP OpenView Dashboard management station:
  - *Windows*: `<install_dir>\paperdocs\dashboard\`
  - *UNIX*: `/opt/OV/paperdocs/dashboard/`
- On the product DVD-ROM in the following directory:
  - *Windows*: `\Docs\`
  - *UNIX*: `/Docs/`

For information on how to obtain the most recent documents, see Documentation Updates on page 17.

Table 1 HP OpenView Dashboard Documentation

Document Title and Filename	Main Topics
Installation Guide `Installation.pdf`	Installing and uninstalling HP OpenView Dashboard
Operations View Quick Start Guide `opview/Quick_Start.pdf`	• Running the Operations View demonstration portal view • Operations View tutorial
Operations View Administrator Guide `opview/Administration.pdf`	• Essential concepts • Planning roadmap for using Operations View • Connecting Operations View to management products • Configuring Operations View portlets • Configuring Operations View data filters • Deploying a portlet application • Troubleshooting

Table 1 HP OpenView Dashboard Documentation (cont'd)

Document Title and Filename	Main Topics
Operations View Migration Guide `opview/Migration.pdf`	• Overview of migrating from HP OpenView Service Information Portal (SIP) version 3.2 to Operations View • SIP and Operations View comparison • Migration use models • Using the Operations View Migration Wizard • Manual steps for migration • Troubleshooting
Operations View Integration Guide: NNM `opview/NNM_Integration.pdf`	• Connecting Operations View to HP OpenView Network Node Manager (NNM) • Configuring the NNM portlets • Customizing the NNM portlets • Filtering NNM data • Troubleshooting
Operations View Integration Guide: OVO and OVSN `opview/OVO_OVSN_Integration.pdf`	• Connecting Operations View to HP OpenView Operations (OVO) and HP OpenView Service Navigator (OVSN) • Configuring the OVO and OVSN portlets • Customizing the OVO and OVSN portlets • Filtering OVO and OVSN data • Troubleshooting
Operations View Integration Guide: OVIS `opview/OVIS_Integration.pdf`	• Connecting Operations View to HP OpenView Internet Services (OVIS) • Configuring the OVIS portlets • Customizing the OVIS portlets • Troubleshooting

Table 1 HP OpenView Dashboard Documentation (cont'd)

Document Title and Filename	Main Topics
Operations View Integration Guide: OVPM `opview/OVPM_Integration.pdf`	• Connecting Operations View to HP OpenView Performance Manager (OVPM) • Configuring the OVPM portlets • Customizing the OVPM portlets • Filtering OVPM data • Troubleshooting
Operations View Integration Guide: OVSD, OVPI, and OVR `opview/OVSD_OVPI_OVR_Integration.pdf`	• Connecting Operations View to HP OpenView Service Desk (OVSD), HP OpenView Performance Insight (OVPI), and HP OpenView Reporter (OVR) • Configuring the OVSD, OVPI, and OVR portlets • Customizing the OVSD, OVPI, and OVR portlets • Troubleshooting

Operations View Online Help

Operations View supplies the following graphical interfaces for portal and portlet configuration:

- Operations View Administrator Tool
- Operations View Migration Wizard (available from the Administrator Tool)

Each of the Operations View graphical interfaces includes online help files that explain that interface.

- To access the top level of the help content for each interface, use the commands on the **Help** menu.
- To access context-specific help information in the Operations View interfaces, click **Help** within the window for which you want more information.

Documentation Updates

This manual's title page contains the following identifying information:

- Software version number, which indicates the software version
- Document release date, which changes each time the document is updated
- Software release date, which indicates the release date of this version of the software

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://ovweb.external.hp.com/lpe/doc_serv/

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Documentation Conventions

The Operations View documentation uses the following conventions:

Table 2 HP OpenView Dashboard Documentation Conventions

Symbol	Meaning
`<install_dir>`	(Windows only.) The HP OpenView application directory. This directory contains all of the HP OpenView Dashboard files. The default location is: `C:\Program Files\HP OpenView\`
`<data_dir>`	(Windows only.) The HP OpenView data directory. This directory contains product configuration and data files. The default location is: `C:\Program Files\HP OpenView\data`

`<portlet_app_dir>`	The top-level directory for a deployed portlet application. This directory has the same name as the portlet application. The location of this directory depends on the installation platform and the portal server.
	• Jetspeed on Windows:
	`<install_dir>\nonOV\dashboard\jetspeed\1.6\jakarta-tomcat-5.5.9\webapps`
	• Jetspeed on UNIX:
	`/opt/OV/nonOV/dashboard/jetspeed/1.6/jakarta-tomcat-5.5.9/webapps`
	• BEA WebLogic on Windows (default):
	`<bea_install_dir>\user_projects\applications`
	• BEA WebLogic on UNIX (default):
	`<bea_install_dir>/user_projects/applications`
	`<bea_install_dir>` is the BEA WebLogic directory.

➤	A note that describes special information pertaining to the current topic.
⚑	A tip that provides an alternate way to address the current topic.
⚠	A caution that indicates a potential problem to avoid.

1 Introduction to the NNM Integration

HP OpenView Network Node Manager (NNM) provides up-to-date network status information that you can display to your end users through HP OpenView Dashboard Operations View.

For more information about NNM, see *Managing Your Network with NNM* (provided with NNM). All HP OpenView manuals are available online at the web site: **http://ovweb.external.hp.com/lpe/doc_serv**

You can integrate any combination of the following portlets into portal views. The information displayed within the portlets is gathered from one or many NNM management stations and/or NNM collection stations:

- Alarms portlet

  See The Alarms Portlet for Operations View on page 20.

- Network Health portlet

  See The Network Health Portlet for Operations View on page 20.

- Topology (submaps) portlet

  See The Topology Portlet for Operations View on page 20.

- MPLS portlet

  See The MPLS Portlet for Operations View on page 20.

The Alarms Portlet for Operations View

A collection of alarm messages gathered from one or more alarm categories within NNM. You filter the alarms in a variety of ways so that only those alarms that are relevant to a particular user are visible within each portal view.

The Network Health Portlet for Operations View

Custom gauges that track the health of network devices so that your users can monitor network performance at-a-glance. Several predefined gauges are included, such as router health and server health. You can also write your own gauge definitions to monitor whatever is important to your users. The data collection configuration required to run the gauges is automated and controlled through Operations View configuration settings.

The Topology Portlet for Operations View

A collection of submaps from one or more NNM maps. Each map must be open on the NNM management station before the desired submap can be displayed in Operations View. Drill-down through the NNM submap hierarchy can be provided, depending upon the configuration settings.

The MPLS Portlet for Operations View

A list of VPNs managed by NNM with their health information and information about components that make up the VPN. The NNM MPLS Smart Plug-in is required for this portlet.

HP OpenView Customer Views and Operations View

HP OpenView Customer Views runs on top of NNM. If you are using Customer Views, Operations View can leverage the customer model that you have already configured (such as assignment of specific devices to a specific organization) into Operations View resource mapping. For more information about leveraging the Customer Views configurations, see Chapter 7, Filtering NNM Data.

Interaction Between NNM and Operations View

Operations View running on any supported operating system can integrate with multiple NNM management stations and/or collection stations, regardless of the NNM operating system. The *Installation Guide* includes information about supported NNM versions and required patches.

In Operations View documentation, NNM management stations and NNM collection stations are both referred to as NNM management stations. Operations View portlets provide the ability to aggregate data from multiple NNM sources to display through portal views.

You can install Operations View and NNM in any order; however, you must perform at least minimum NNM configuration before you can configure the Network Node Manager portlets. For information on configuring NNM, see the documentation that came with that product.

Before using the Network Node Manager portlets, configure Operations View and NNM to communicate with each other. See Chapter 2, Configuring the Operations View Connection to NNM.

Figure 2 on page 23 illustrates how the Alarms portlet communicates with NNM.

Figure 3 on page 24 illustrates how the Network Health portlet communicates with NNM.

Figure 4 on page 25 illustrates how the Topology portlet communicates with NNM.

Figure 5 on page 26 illustrates how the MPLS portlet communicates with NNM.

Figure 2 Communication Process for the Alarms Portlet

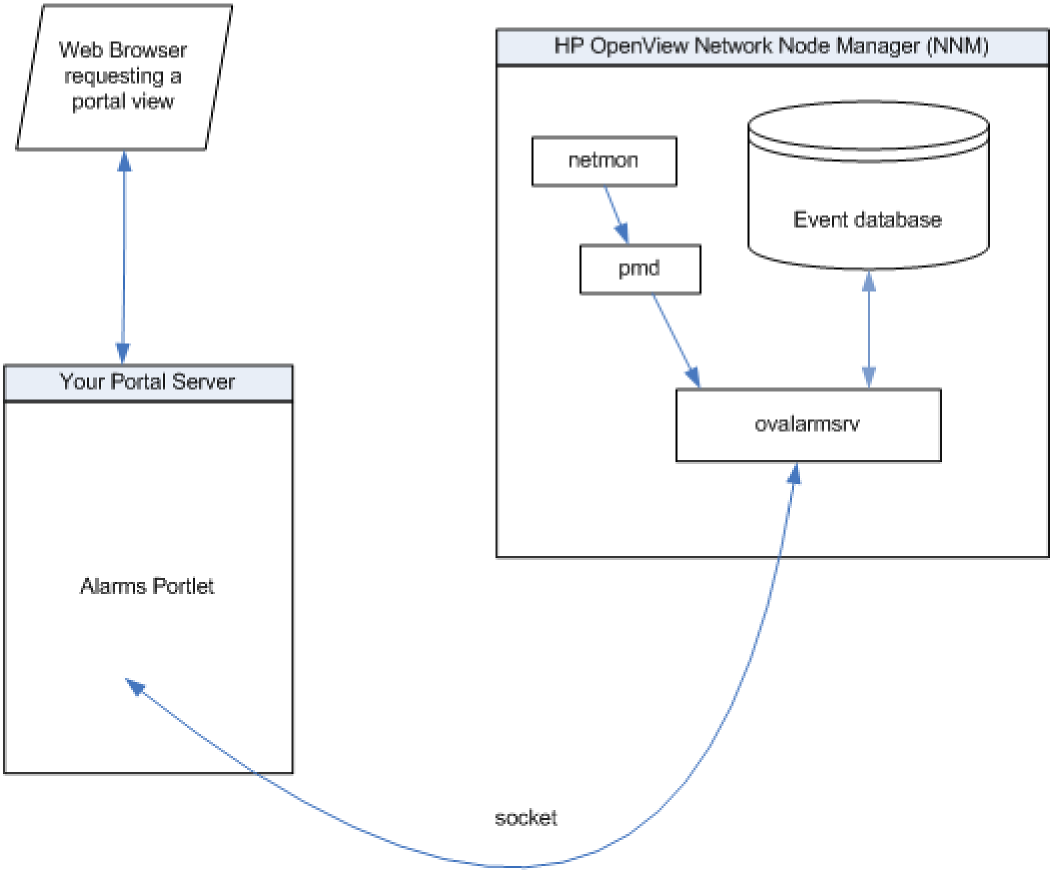

Web Browser requesting a portal view
Your Portal Server
Alarms Portlet
HP OpenView Network Node Manager (NNM)
netmon
pmd
Event database
ovalarmsrv
socket

Figure 3 Communication Process for the Network Health Portlet

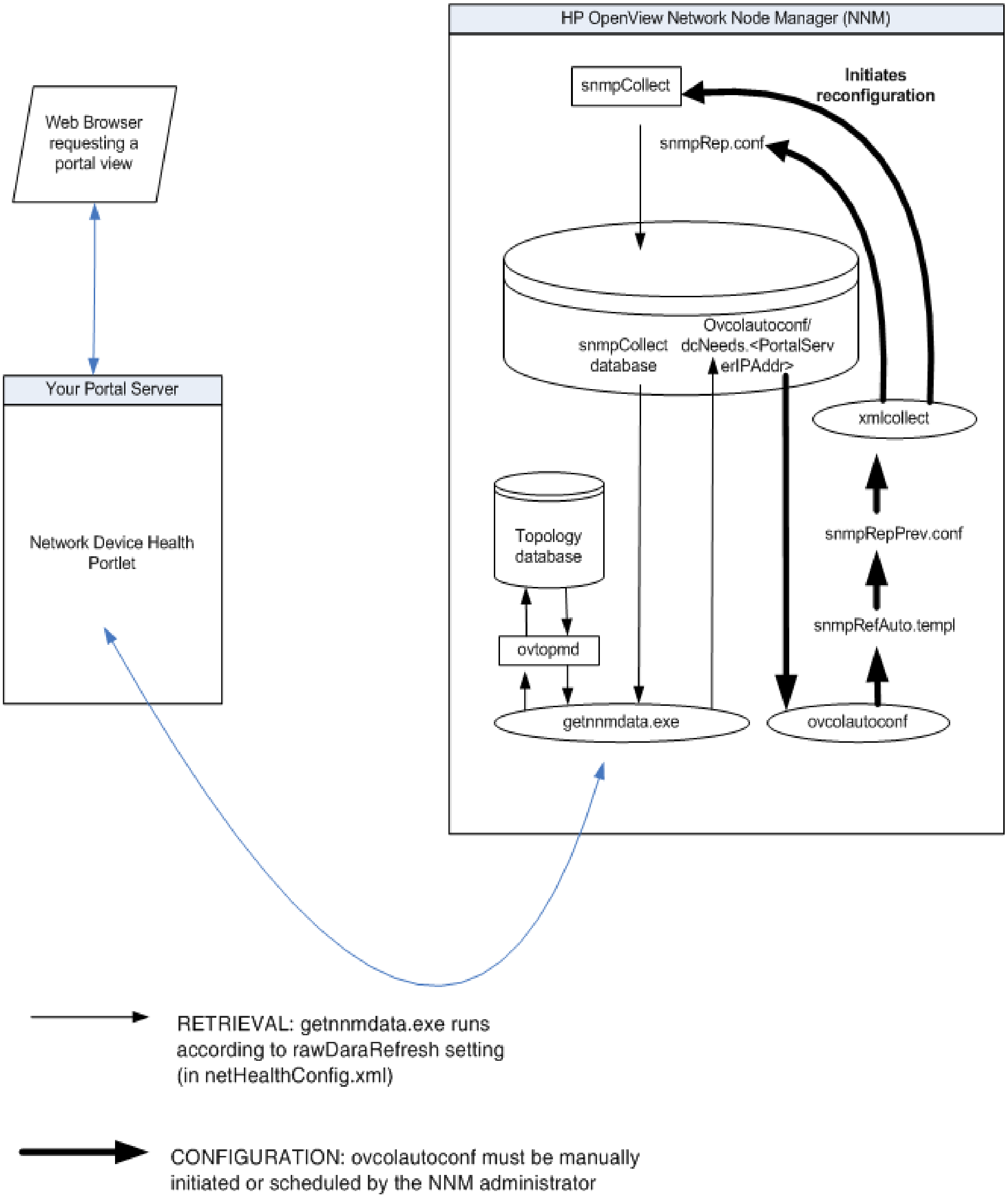

HP OpenView Network Node Manager (NNM)
snmpCollect
Initiates reconfiguration
snmpRep.conf
snmpCollect database
Ovcolautoconf/ dcNeeds.<PortalServerIPAddr>
xmlcollect
snmpRepPrev.conf
snmpRefAuto.templ
Topology database
ovtopmd
getnnmdata.exe
ovcolautoconf
Web Browser requesting a portal view
Your Portal Server
Network Device Health Portlet
RETRIEVAL: getnnmdata.exe runs according to rawDaraRefresh setting (in netHealthConfig.xml)
CONFIGURATION: ovcolautoconf must be manually initiated or scheduled by the NNM administrator

Figure 4 Communication Process for the Topology Portlet

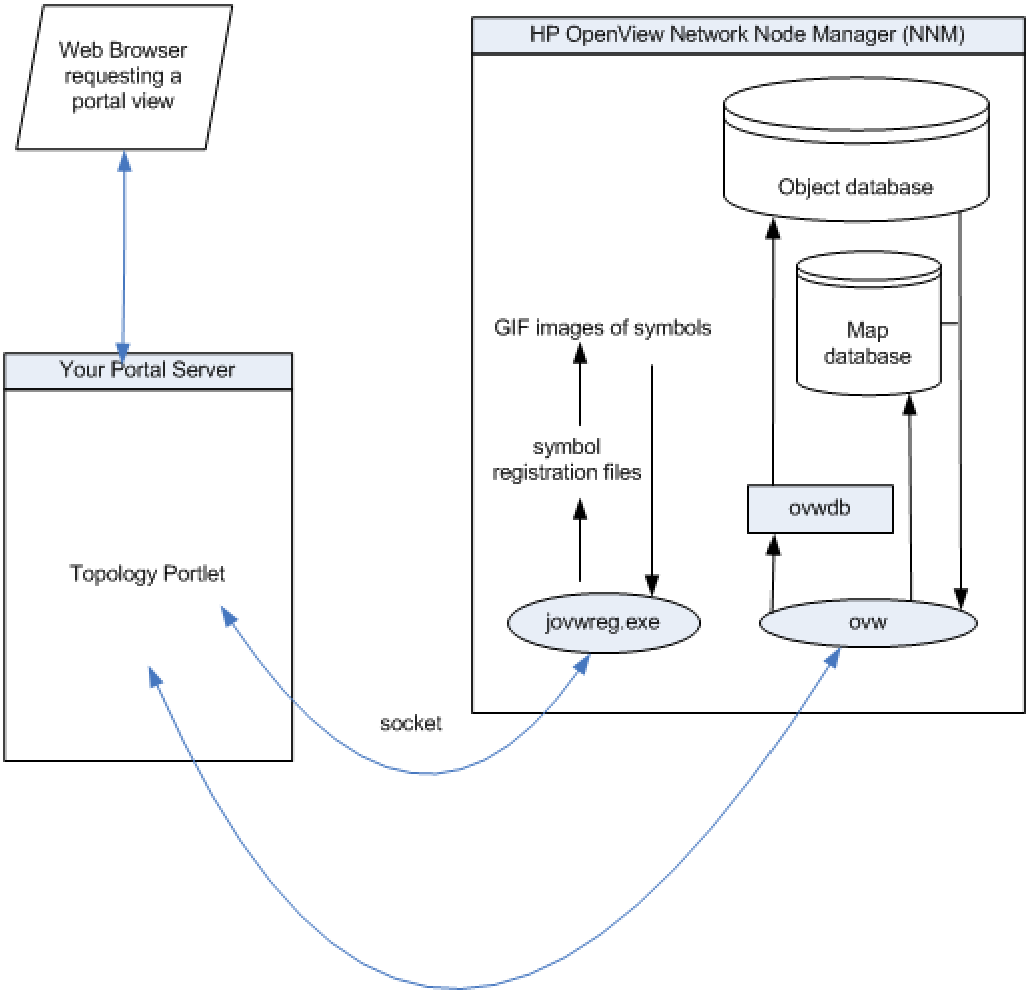
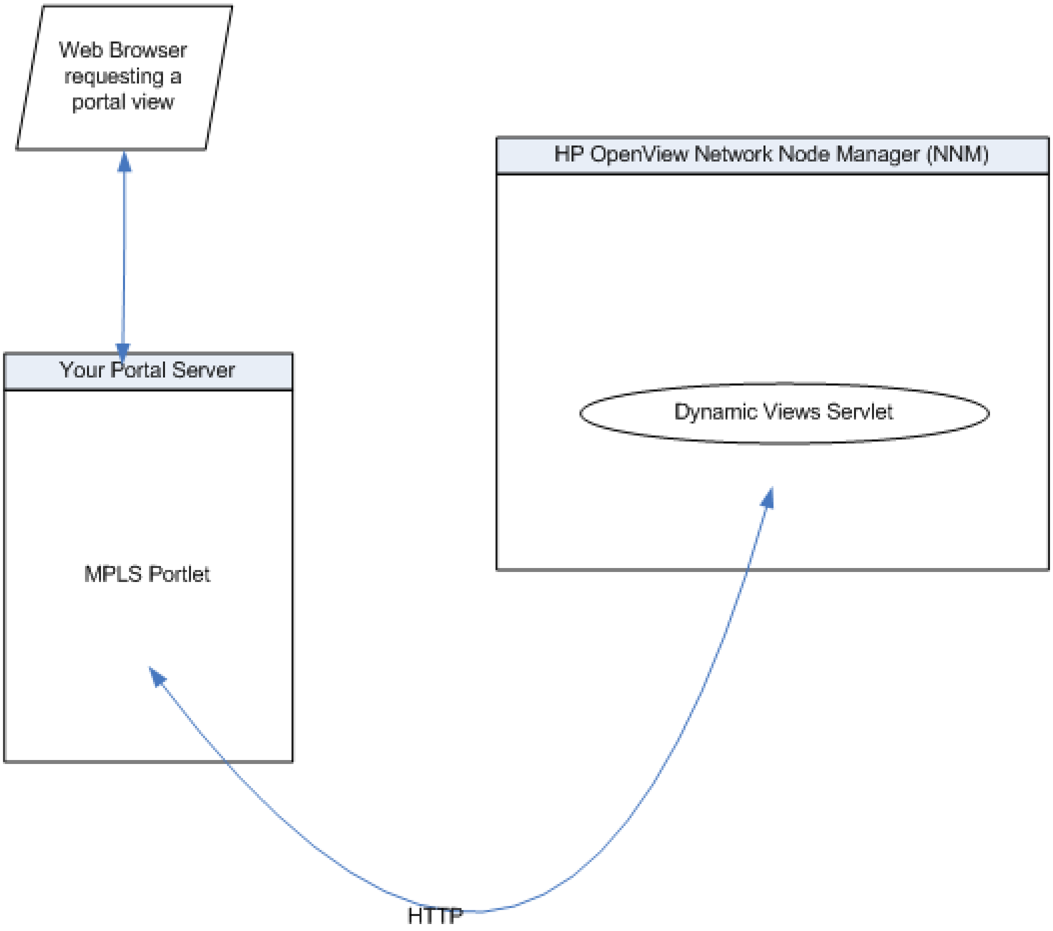


Figure 5 Communication Process for the MPLS Portlet


Web Browser requesting a portal view
HP OpenView Network Node Manager (NNM)
Your Portal Server
Dynamic Views Servlet
MPLS Portlet
HTTP

2 Configuring the Operations View Connection to NNM

To establish communication between your HP OpenView Network Node Manager (NNM) management stations and HP OpenView Dashboard Operations View, perform the following configurations on each NNM management station and on the Operations View server.

On the NNM Management Station

Perform the following steps on each NNM management station in your network:

1. Verify that you are using a version of NNM that is supported by Operations View. Refer to the *Installation Guide* for the list of supported product versions.
2. Add the Operations View server host name(s) to the following two files. In an ASCII editor, open the following two authorization configuration files (bypass this step if Operations View is running on the same computer as NNM):
   - The `ovw.auth` file controls which hosts and users are authorized to connect to NNM sessions running on the management station:
     - *Windows*: `<`*`NNM_install_dir`*`>\conf\ovw.auth`
     - *UNIX*: `/etc/opt/OV/share/conf/ovw.auth`
   - The `ovwdb.auth` file controls which hosts and users are authorized to connect to the NNM database processes:
     - *Windows*: `<`*`NNM_install_dir`*`>\conf\ovwdb.auth`
     - *UNIX*: `/etc/opt/OV/share/conf/ovwdb.auth`

Add a ***OperationsViewServerHostName* +** line to the list for each Operations View server that needs to obtain information from this NNM management station.

If you see a line that consists of two + symbols (+ +), you can bypass this step because NNM is configured to allow any computer to request information (security not implemented).

Enabling Topology Portlet Access to NNM Data

Each desired NNM map must be open on the NNM management station before submaps can be displayed in the portal view. Only submaps currently displayed on the NNM management station or *persistent* submaps (those stored in memory on the NNM management station) can be selected for display in the Topology portlet. However, submaps accessed through drill-down do not need to be *persistent*.

To enable Topology portlet access to NNM data, follow these steps:

1. NNM (ovw) must be running on the NNM management station containing the map to display in a portal view:
   - *Windows*:
     - To start the NNM services, click **Start**→ **Programs**→ **HP OpenView**→ **Network Node Manager Admin**→ **NNM Services-Start**.
     - To start the NNM interface, click **Start**→ **Programs**→ **HP OpenView**→ **Network Node Manager**.
   - *UNIX*:
     - To start the NNM background processes, log in as `root` and type:

       ```
       /opt/OV/bin/ovstart -c
       ```

     - To start the NNM interface, type:

       ```
       /opt/OV/bin/ovw
       ```

2. Open an NNM session for each map (such as the Default map) that will be accessed through the Topology portlet in the portal.

3 Ensure that each submap that to select for display in the Topology portlet (such as the Internet submap) is set to *persistent* (stored in RAM) not *transient* (generated upon request).

➤ Submaps accessed through drill-down do not need to be *persistent*.

To check or change persistence, do one of the following:

- Configure the IP Map application to enable the on-demand level:
  - *Windows*: Click **Map→ Properties**. On the Applications tab, double-click **IP Map**, and then select an On-Demand level.
  - *UNIX*: Click **Map→ Properties**. Select IP Map, click **Configure For This Map**, and then select an On-Demand level.
- Make the individual submap persistent:
  - *Windows*: Click **Map→ Submap→ Properties**. On the View tab, select the Persistent check box.
  - *UNIX*: Click **Map→ Submap→ Make the Submap Persistent.**

4 Create and customize any desired maps and submaps. (For information about map customization, see the NNM manual *Managing Your Network with NNM*.)

Consider creating a few general purpose submaps, and using Operations View data filters to display only the information that is important for a specific user (see Chapter 7, Filtering NNM Data).

5 A submap's background graphic, if any, can be automatically displayed in the Topology portlet. The graphic must be in either JPEG or GIF format, and the graphic must be placed in the following location on the NNM management station:

- *Windows*: `<NNM_install_dir>\backgrounds\*`
- *UNIX*: `/usr/OV/backgrounds/*`

To add a background graphic to a submap:

a On the NNM management station, open the NNM submap to receive a background graphic.

b Click **Map→ Submap→ Properties**.

c *Only Windows*: click the View tab.

d In the Background Graphics list, select the graphic to apply to the current submap, and then click **OK**.

For more detailed information, see the NNM's online help or the *Managing Your Network with NNM* manual.

6 If the NNM management station is restarted, you must restart each NNM session to display the submaps in the portal views.

Enabling the Network Health Portlet to Configure NNM Data Collection

The Network Health gauges that ship with Operations View require NNM to collect data using several SNMP MIB expressions. MIB expressions are a feature of Network Node Manager that allow for the creation of mathematical formulas comprised of MIB objects. MIB expressions allow you to derive more meaningful information than you could gather from individual MIB objects.

As long as you do not already have MIB expressions with the same names as the MIB expressions provided with Operations View, Operations View data collections will not conflict with any current settings in the NNM Data Collector.

To enable the Network Health portlet to configure NNM data collection, prepare the Operations View server, and then perform the following configuration on each NNM management station.

On the Operations View Server

Open a portal and display at least one Network Health portlet. Leave this portal open while completing the following steps on the NNM management station.

On the NNM Management Station

1 To verify that you do not already have MIB expressions by these names, do one of the following to open the NNM Data Collections and Thresholds window:

- At the command prompt, type:

  `xnmcollect`

- In the graphical interface, display the list of loaded MIB expressions:

  — *Windows*: Click **Edit**→ **MIB Object**→ **New**, and then select the Expressions option.

  — *UNIX*: Click **Edit**→ **Add**→ **MIB Object**, and then select the Expressions option.

Scroll through the list of MIB expression names, looking for the following names:

- p_if%util
- p_if%inerrors
- p_if%outerrors
- p_cisco5minavgbusy

2 To load Operations View's MIB expressions, at the command prompt type (no hard returns included):

- *Windows*:

```
<NNM_install_dir>\bin\xnmcollect.exe -loadExpr
<NNM_install_dir>\conf\ovcolautoconf\mibExprAuto.conf
```

- *UNIX*:

```
/opt/OV/bin/xnmcollect -loadExpr /etc/opt/OV/share/
conf/ovcolautoconf/mibExprAuto.conf
```

3 To verify that these MIB expressions were successfully loaded, open the NNM Data Collections and Thresholds window as for Step 1.

Look for these new MIB expression names in the list:

- p_if%util
- p_if%inerrors
- p_if%outerrors
- p_cisco5minavgbusy

To learn about the mathematical formulas behind the Operations View MIB expressions, highlight a name, and then click **Describe**.

For interface metrics, different formulas are used depending upon the attributes of the interface (such as speed of the interface, half-duplex versus full-duplex, etc.). In the case of CPU utilization, the expression is a single Cisco MIB object: `local.system.augBusy5`. It is described as the “5 minute exponentially-decayed moving average of the CPU busy percentage.”

For more information about MIB Expressions, click **Help→ Online Manuals→ Managing Your Network with NNM**.

➤ If you want to enable *automatic* configuration of NNM’s Data Collector to meet Operations View data requirements, continue with the remaining steps in this procedure. For information about how this process works, see The Data Collection Process for the Network Health Portlet on page 38. Otherwise, stop here and see Manually Configuring NNM’s Data Collector to Provide the Required Operations View Data on page 34.

4 To enable *automatic* configuration of the Operations View data collection requirements, create the following directory:

- *Windows*:

  `<NNM_install_dir>\databases\snmpCollect\`**`ovcolautoconf`**

- *UNIX*:

  `/var/opt/OV/share/databases/snmpCollect/`**`ovcolautoconf`**

After a few minutes (10 by default), Operations View populates the `ovcolautoconf` directory with one or more `dcNeeds.<PortalserverIPAddress>` files containing the current list of data collection requests from open portal views on each Operations View server. These files are created by getnnmdata.exe (see Figure 3 on page 24).

5 *UNIX only*: Make the ovcolautoconf directory writable by the web server process used by NNM (such as Apache's httpd) and the user or scheduler program responsible for running the ovcolautoconf command (see the next step). Verify that the directory you just created has the permissions set correctly. For example:

```
drw-rw----   2 bin        adm            24 Aug  9 16:01 ovcolautoconf
```

This UNIX permissions example allows the web server running as user bin (the default for NNM on HP-UX and Solaris) to write to the ovcolautoconf directory, and allows a user with bin permissions or a cron job running as bin to write to the ovcolautoconf directory.

6 To update NNM's Data Collector configuration files, run ovcolautoconf on each NNM management station. The ovcolautoconf command must be executed on the NNM management station either manually or as a scheduled task that you define. At the command prompt, type one of the following:

ovcolautoconf or

ovcolautoconf -verbose

ovcolautoconf creates the snmpRepPrev.conf file in the ovcolautoconf directory. In this file all Operations View requests are formatted so that they can be uploaded into NNM's Data Collector configuration files. This file is a record of the most recent configurations uploaded from Operations View into the NNM snmpRep.conf file.

To change the number of days the Operations View waits before deleting any inactive data collection configurations (default 30), type the following command. There is no way to permanently change this setting. Include this command in your scheduled script or each time you manually run ovcolautoconf:
ovcolautoconf -maxConfAge *#ofdays*

7 You can modify the Operations View collection configurations; for example, change collection intervals (15 minutes by default) or add thresholds. To modify the Operations View collection configurations, edit the snmpRepAuto.templ file. This file is a template used by the ovcolautoconf program when formatting Operations View data

collection requests for NNM's Data Collector program. It contains one entry for each MIB object or MIB expression upon which NNM's Data Collector needs to collect data.

To view the list of configured collections and make any necessary changes, at the command prompt type the following (no hard returns included):

- *Windows*: **xnmcollect -snmpColConfFile** ***<NNM_install_dir>*****\conf\ovcolautoconf\snmpRepAuto.templ**
- *UNIX*: log in as root and then type, **xnmcollect -snmpColConfFile /etc/opt/OV/share/conf/ ovcolautoconf/snmpRepAuto.templ**

Review the list. In the Source field, you will see the variable _NODE_, which is automatically replaced with any specific devices requested by Operations View. Do not change the Source field variable. You can change the other fields.

Manually Configuring NNM's Data Collector to Provide the Required Operations View Data

If you chose not to automate data collections for Operations View (see previous section), it is possible to manually configure NNM data collection configurations.

First you need to decide which Network Health gauges will be displayed within your portal. Make a list of the MIB expressions used by each of those gauges. Then, make a list of the network devices that should be monitored by each gauge.

To configure data collections for each network device under the relevant Operations View MIB expression, follow these steps:

1. In the NNM interface, click **Options→ Data Collection & Thresholds**.
2. Configure the data collections for each network device.

   If you need more information about how to do this, click **Help→ On Window**. Or, from any NNM submap, click **Help→ Online Manuals→ Managing Your Network with NNM**.

On the Operations View Server

To enable communication between Operations View and NNM, follow these steps:

1. In the Operations View Administrator Tool, navigate to the Management Stations folder.
2. To add a new NNM management station, right-click Management Stations, click **New Management Station**, and then type the fully-qualified host name of the NNM management station.

   To add NNM settings to an existing management station, select that management station in the scoping pane.
3. In the editor pane, select NNM is Installed on this System.

   The NNM tab becomes available.
4. On the NNM tab, set the configuration options as appropriate for the version of NNM running on the management station that you identified in Step 2:
   - Operating system type: Select the option that corresponds to the operating system of this management station.
   - NNM 6.2 or 6.3: Select this check box if the NNM on this management station is version 6.2 or 6.3.
   - General settings: Select the check boxes that correspond to the data on this NNM management station that you want served to the Operations View portlets:
     - Use as SNMP Data Source: NNM data from this management station contributes to the Network Health portlet. When multiple NNM management stations provide raw data to the Network Health portlet, duplication of SNMP data collection is avoided by sending collection requests for a given node to only one of the NNM management stations. The NNM management station chosen is that which first returned raw data for that node. See The Data Collection Process for the Network Health Portlet on page 38 for more information.
     - Use as Alarms Data Source: NNM data from this management station contributes to the Alarms portlet.

  - Use as OVw Symbol Source: NNM data from this management station contributes to the Topology portlet. Operations View must gather NNM symbol image files at least once. This field indicates that GIF images will be gathered from the NNM management station according to the frequency specified by the `symbolFetchRateInMin` attribute in the `topologyConfig.xml` file (default value is 1 day). Selecting this field instructs Operations View to check for and gather the updated GIF images. Because symbol images do not often change, you might want to minimize traffic by selecting this check box for only one of your NNM management stations. (An NNM management station can be used as the source for topology map information even if OVw Symbol Source is not selected.)

    To determine which symbols are currently available on a particular NNM management station, type the following URL into your web browser:

NNM Management Station Running on Windows:

http://<NNM_management_station_hostName>/OvCgi/jovwreg.exe?symbols

NNM Management Station Running on UNIX:

http://<NNM_management_station_hostName>:8880/OvCgi/jovwreg.exe?symbols

  - Use as MPLS Data Source: NNM data from this management station contributes to the MPLS portlet.

- Each check box enables one or more settings. Specify the ports and paths that the NNM management station uses.
  - The default web server port is 80 for Windows and 3443 for UNIX.
  - The default HP OpenView alarm server port is 2953.
  - The default HP OpenView Windows database port is 2447.
  - The default dynamic views web port is 7510.
  - The default dynamic views path is `/topology/home`.
- Character encoding: Enter a value in this field to notify Operations View that the NNM management station is running in a language that uses non-ASCII characters. If this field is left empty, the default locale (English) is used. This field is used only by the Topology portlet to notify Operations View of the appropriate JDK converter 1.1 values.

To determine the correct non-English encoding value, on the NNM management station, open the following file, which contains a table of JDK Converter 1.1 values for all languages:

— *Windows*: `NNM_install_directory\www\conf\locales.jconv`

— *UNIX*: `/etc/opt/OV/share/www/conf/locales.jconv`

Locate the appropriate value for this NNM management station, for example, `SJIS` for Japanese NNM running on Windows or HP-UX.

5 Click **Save**.

6 Repeat Step 2 though Step 5 for each NNM management station with which Operations View should communicate.

The Data Collection Process for the Network Health Portlet

NNM collects all SNMP data requested by Operations View and provides current information about device status.

Network Health gauges calculate the health of specific network devices using information gathered by NNM management stations. Changes are visible in the Network Health gauges each time the portal view is displayed or refreshed.

Operations View depends upon two programs that reside on each NNM management station (`getnnmdata.exe` and `ovcolautoconf.exe`) to collect requested data:

1. Each time a Network Health gauge is displayed, Operations View logs the underlying data requests.

   Operations View compiles a list of requested MIB objects and MIB expressions from any Network Health portlet gauge. The list documents which MIB objects and MIB expressions are being requested for which network devices from which NNM management stations.

   > The underlying MIB objects and MIB expressions appear in Network Health gauge definitions in the network health categories configuration. See the network health configuration in the Administrator Tool. (Within the HP OpenView Network Node Manager folder in the Portlet Shared Configurations folder.) The network health metrics and network health categories work together to define the gauges' configuration information.

2. Operations View contacts the `getnnmdata.exe` on each NNM management station that is configured in the `mgmtStations.xml` file. The frequency of this action is determined by the Raw Data Refresh Frequency setting in the Network Health Metrics configuration in the Administrator Tool (by default, every 10 minutes).

3 Operations View receives the most recent data collection results from the NNM database. Operations View also places the current request log file in the `ovcolautoconf` directory. Requests from each Operations View server are gathered and stored in a file whose name is of the form (`dcNeeds.<PortalserverIPAddress>`).

> You must create the `ovcolautoconf` directory before this step works. See Enabling the Network Health Portlet to Configure NNM Data Collection on page 30 for more information.

4 To complete the automatic configuration process, run the `ovcolautoconf.exe` command. The `ovcolautoconf` command must be executed on the NNM management station, either manually or as a scheduled task that you define. `ovcolautoconf` does the following:

- All Operations View servers' data collection needs are processed. The list of data collection requests is configured using the information in the `snmpRepAuto.templ` file and placed in the `snmpRepPrev.conf` file.
- If necessary, NNM's Data Collector configurations are updated by making Operations View additions or changes to the `snmpRep.conf` file (one of two configuration files used by the NNM Data Collector program). The `snmpRep.conf` file is used by the SNMP Data Collector as a guide for gathering data. The Operations View entries do not interfere with data collection configurations that were entered directly through NNM.
- Data collections are configured on an *as-needed* basis, rather than a *potentially* needed basis. In other words, until a gauge is displayed in a portal view, no data collection is initiated.
- If a gauge is not displayed for 30 days (default setting), the data collections are discontinued (provided they are not needed by other HP OpenView products).

> If you are worried that Operations View might modify critical data collections already defined on your NNM management stations, see Manually Configuring NNM's Data Collector to Provide the Required Operations View Data on page 34.

Selectively Disabling Operations View Data Collection Configurations

You can selectively turn off the automatic data collections configuration for any Operations View MIB expression. In the Administrator Tool on the Operations View server, select the Network Health Metrics shared portlet configuration, and clear the Auto Configure NNM's Data Collector Program check box.

Operations View requests the information for that metric from the databases on your NNM management station, but does not modify the data collection settings for that metric within NNM.

Monitoring the Size of NNM's snmpCollect Database

The NNM `snmpCollect` database on the NNM management station grows without bounds unless you take precautions.

Operations View-requested data collection data is automatically trimmed if NNM's reporting feature is in use on your NNM management station. (Check to see if one or more NNM Performance Reports are configured on the NNM system.) In the NNM interface, click **Help→ Online Manuals→ Reporting and Data Analysis** for more information.

By default, data older than one week is deleted if the NNM Reporting feature is active.

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

If Performance Reports are *not* active, the following command trims the data in the `snmpCollect` database. It can be run manually, or scheduled to run periodically, on the NNM system:

```
ovcoltosql -q -N -D <trim depth in hours> -exportset NNM_Reporting
```

For example, the following deletes all reporting/Operations View data collector data in the `snmpCollect` database older than one week in age (there are 168 hours in 7 days):

```
ovcoltosql -q -N -D 168 -exportset NNM_Reporting
```

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

Removing Operations View Data Collection Configurations from NNM

To remove Operations View data collection configuration entries from NNM's Data Collector program, at the command prompt on the NNM management station, navigate to the `ovcolautoconf` directory and type the following:

```
xnmcollect -report -delete snmpRepPrev.conf xnmcollect -event
```

NNM Ports for Operations View

The Operations View server to NNM management station communication can go through a firewall. The ports that need to be opened through the firewall to gather data for the NNM portlets are specified on the NNM tab of the management station configuration settings in the Administrator Tool. (See On the Operations View Server on page 35.)

Table 3 Alarms Portlet Port Requirements

Protocol	Default Port	Configuration Location
ovalarmsrv	2953 for NNM 6.2, or later	On the Operations View server, use the Administrator Tool to configure ports (OVAlarmSrv Port on NNM tab for management stations).

Table 4 Network Health Portlet Port Requirements

Protocol	Default Port	Configuration Location
http	8880/UNIX for NNM 6.3 and earlier 3443/UNIX for NNM 6.31 and later 80/Windows	On the Operations View server, use the Administrator Tool to configure ports (Web Server Port on NNM tab for management stations).

Table 5 Topology Portlet Port Requirements

Protocol	Default Port	Configuration Location
ovw	3700 to 3700+n	n = highest OVW session number
ovwdb	2447 for NNM 6.2, or later	On the Operations View server, use the Administrator Tool to configure ports (OVwDB Port on NNM tab for management stations)
http	8880/UNIX for NNM 6.3 and earlier 3443/UNIX for NNM 6.31 and later 80/Windows	On the Operations View server, use the Administrator Tool to configure protocol and port (Web Server Port on the NNM tab for management stations).

Table 6 MPLS Portlet Port Requirements

Protocol	Default Port	Configuration Location
http	7510	On the Operations View server, use the Administrator Tool to configure ports (Dynamic Views Web Port on NNM tab for management stations).

The following ports might be in use for your Operations View customer model data collection, depending upon how you configure the Management Data filters (see Chapter 7, Filtering NNM Data for more information).

Table 7 Customer Views Import Program Port Requirements

Protocol	Default Port	Configuration Location
http	8880/UNIX for NNM 6.3 and earlier 3443/UNIX for NNM 6.31 and later 80/Windows	On the Operations View server, the server and port are configurable through a URL specified as a customer model source in the Administrator Tool: `http://server:8880/OvCgi/getcvdata.exe`

Table 8 NNM Object Database Import Program Port Requirements

Protocol	Default Port	Configuration Location
ovwdb	2447 for NNM 6.2, or later	On the Operations View server, NNM servers and ovwdb ports are configurable through the NNM management station editor in the Administrator Tool.

Table 9 NNM Data Warehouse Export Program Port Requirements

Protocol	Default Port	Configuration Location
http	8880/UNIX for NNM 6.3 and earlier 3443/UNIX for NNM 6.31 and later 80/Windows	On the Operations View server, server and ports are configurable through the NNM management station editor in the Administrator Tool.

Running in Languages Other Than English

Any language that can be displayed within the UTF-8 codeset can be displayed through Operations View. Operations View requires that non-ASCII characters be in the UTF-8 codeset. NNM, itself, uses the traditional OS codeset (for example, Shift-JIS, EUC, or ISO 88591) and does not support UTF-8 or Unicode codesets.

Completion of the following configuration tasks allows the Alarms and Topology portlets to access non-ASCII data from NNM. (No additional steps are required for the Network Health or MPLS portlets.) These instructions assume that you have completed the steps in the previous sections of this chapter.

Configuring the Alarms Portlet to Access Non-English NNM Data

In each Operations View alarm category definition, the value of the NNM Base Category field must *exactly* match NNM's alarm category strings in the `trapd.conf` file. Therefore, if an NNM management station (from which the Alarms portlet gathers information) is running in a language that uses non-ASCII characters, you must provide a set of alarm category definitions for the localized alarm categories.

You can copy the NNM alarm category strings from NNM's `trapd.conf` file and paste them into the desired alarm category configuration settings. The Administrator Tool ensures that the alarm category definitions are saved in UTF-8 codeset.

➤ To display alarms from NNM management stations running in multiple languages in the Alarms portlet, provide multiple shared alarms configuration definitions. If all NNM management stations that provide information to Operations View run under the same language, you only need one set of shared alarms configuration definitions.

To configure the Alarms portlet to access non-English data from NNM, follow these steps:

1 Open the following two files in an editor that is running under the codeset that is in use on the NNM management station and is capable of converting or saving a file in UTF-8 codeset:

- On the NNM management station:

  — *Windows*: `<NNM_install_dir>\conf\$LANG\trapd.conf`

  Notepad runs under various language settings by changing Windows' Regional Options, Locale setting. Notepad provides a Save as option to the UTF-8 codeset.

  — *UNIX*: `/etc/opt/OV/share/conf/$LANG/trapd.conf`

  `vi` is capable of opening a file in any codeset. After editing a file using `vi` (in a codeset other than UTF-8), the UNIX `iconv` command converts most codesets into UTF-8.

- In the Administrator Tool on the Operations View server, expand the Portlet Shared Configurations folder, expand the HP OpenView Network Node Manager folder, expand the Alarm Categories folder, and then select the shared alarms configuration to modify.

2 On the NNM management station, in the `trapd.conf` file, locate the CATEGORY settings, for example:

```
CATEGORY 2 "Error Alarms" "LOCALIZED-STRING-FOR-Error Alarms"
CATEGORY 3 "Threshold Alarms" "LOCALIZED-STRING-FOR-Threshold Alarms"
CATEGORY 4 "Status Alarms" "LOCALIZED-STRING-FOR-Status Alarms"
CATEGORY 5 "Configuration Alarms" "LOCALIZED-STRING-FOR-Configuration Alarms"
CATEGORY 6 "Application Alert Alarms" "LOCALIZED-STRING-FOR-Appl Alert
Alarms"
```

3 Copy the string from the second set of quotes, and on the Operations View server, paste this string into the NNM Base Category field.

4 To localize the Operations View alarm category title, modify the Display Title field in the same manner.

5 In the Administrator Tool, click **Save**.

6 In the Administrator Tool, open any Alarms portlet, and then edit the Alarms portlet instances to point to the new localized alarm category names. See Customizing the Alarms Portlet on page 57.

Configuring the Topology Portlet to Access Non-English NNM Data

If an NNM management station (from which Operations View gathers information for the Topology portlet) is running in a language that uses non-ASCII characters, the `encoding` attribute in the Administrator Tool must specify which codeset the JDK Converter should use. If no codeset is configured, no conversion is done.

After the `encoding` attribute is set, the portal automatically translates NNM map data into UTF-8 characters.

The Java JDK Converter 1.1 can be configured on a per-NNM-management-station basis to determine how to interpret the incoming codeset.

To configure the Topology portlet to access non-English data from NNM, follow these steps:

1. On the NNM management station, open the following file:

   - *Windows*: `<`*`NNM_install_dir`*`>\www\conf\locales.jconv`
   - *UNIX*: `/etc/opt/OV/share/www/conf/locales.jconv`

   This file contains a table of JDK Converter 1.1 values for all languages.

   Locate the appropriate value for your NNM management station. Find the OS locale in which NNM is running (for example on Windows, "Japanese_Japan.932") and the corresponding JDK 1.1 Converter (for example, "SJIS"). In this case, in the next step, you would enter:

   `SJIS`

2. In the Administrator Tool on the Operations View server, expand the Management Stations folder, and then select the NNM management station. On the NNM tab, enter the appropriate `encoding` attribute for your NNM management station into the Character Encoding field.

3. To make the localized submap information visible in your portal views, ensure that the submap name uses the appropriate UTF-8 characters:

   - In the default portlet preferences, update the submap name with the localized string as it appears on the NNM management station (such as `ovw://default/`インターネット for Japanese).

- In any existing Topology portlets in a portal view: On the Topology portlet edit page, the localized submap names appear in the selection list box. To convert the submaps to the localized names, simply reinsert the submap. See Customizing the Topology Portlet on page 107.

HTTPS Support

The Operations View server to NNM management station communication cannot be configured to use the secure hypertext transfer protocol (HTTPS) at this time.

3 Working with the Network Node Manager Alarms Portlet

HP OpenView Dashboard Operations View provides the Network Node Manager Alarms portlet for integrating with HP OpenView Network Node Manager (NNM).

This chapter describes how to create, configure, use, and customize the Network Node Manager Alarms portlet. For an overview of the portlet's functionality, see Chapter 1, Introduction to the NNM Integration.

The portal view development process includes a variety of tools:

1. Use the Operations View Administrator Tool to create the Operations View portlets within a portlet application. See Creating the Alarms Portlet on page 52.
2. Use the Administrator Tool to perform initial configuration of the Operations View portlets. See Configuring the Alarms Portlet on page 53.
3. Deploy the portlet application to the portal server. For information, refer to the *Operations View Administrator Guide*.
4. Use the portal server software tools to create a portal view that includes the Operations View portlets. For information, refer to the portal server software documentation.
5. In a web browser, view the portal view and customize the contained portlets. See Using the Alarms Portlet on page 56.

   This is the only point at which end users can interact with the Operations View portlets. If you allow portlet customization, refer to the *Operations View Administrator Guide* for information about the scope and effects of portlet customization.
6. Use the Administrator Tool to maintain the Operations View portlet configurations. See Customizing the Alarms Portlet on page 57.

Creating the Alarms Portlet

Use the Administrator Tool to create the Network Node Manager Alarms portlet within an existing portlet application.

To create the Alarms portlet, follow these steps:

1. In the Administrator Tool, click **File**→ **New**→ **Portlet**.
2. In the Add New Portlet window, enter the following information:
    - Portlet Name: The name of the portlet as it appears in the portlet application in the scoping pane and in the portal server software tools.
    - The portlet name must be unique, start with a letter or underscore character, and consist of only alphanumeric and underscore characters.
    - Portlet Title: The name of the portlet as it appears in the portal server software tools and the portal view. Defaults to the portlet name.
    - Description (optional): The portlet description as it appears in the portal server software tools.
    - Portlet Type: Select OVNNMAlarms from the list.
    - Destination Portlet Application: Select the portlet application to contain the new portlet.

    The new portlet appears in the selected portlet application in the scoping pane, and the configuration information for this portlet appears in the editor pane.

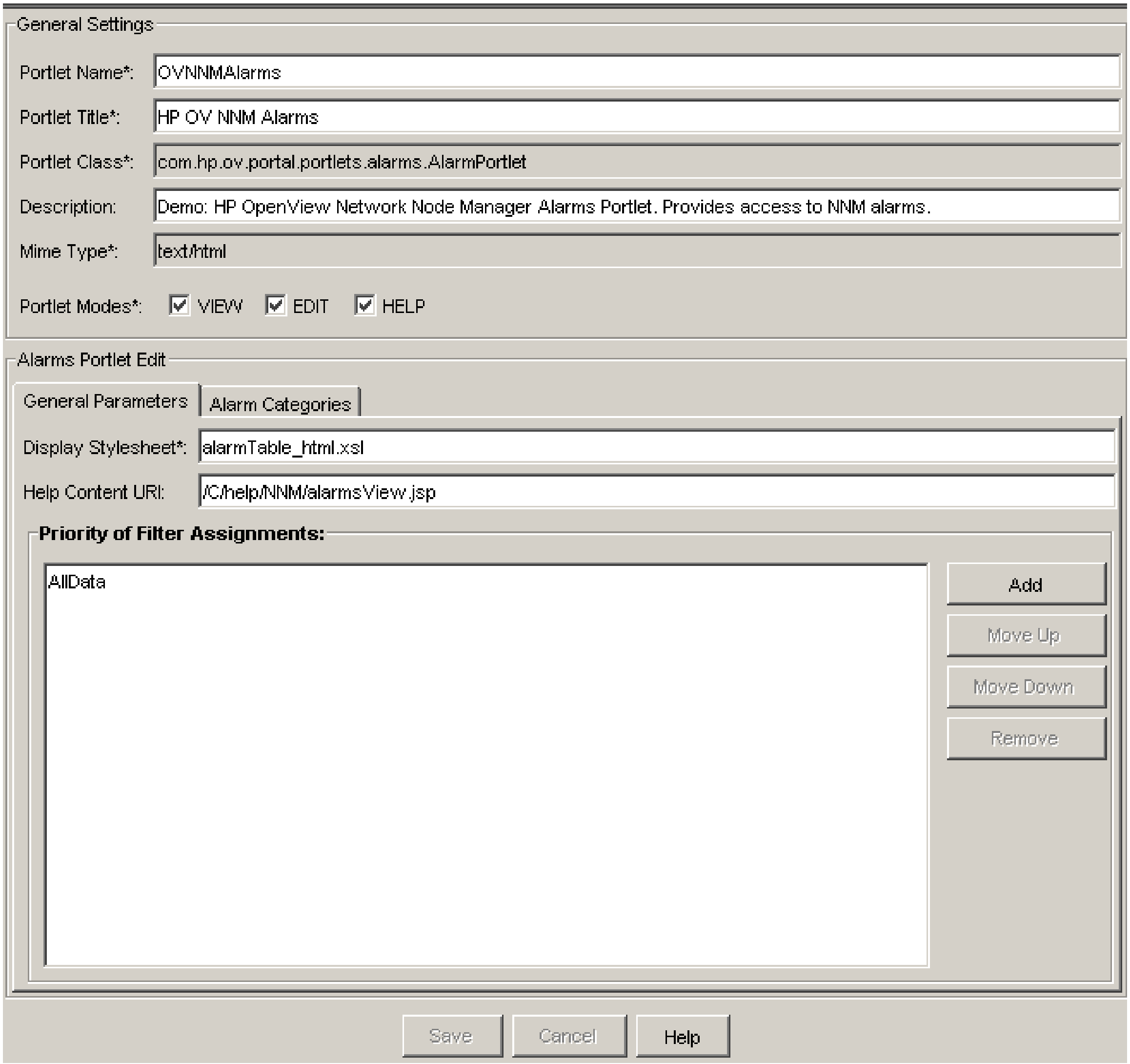
Configuring the Alarms Portlet

For information on the Network Node Manager Alarms portlet configuration options, click **Help** at the bottom of the editor pane to view the online help page.

To configure the default settings for the Alarms portlet, follow these steps:

1. In the scoping pane of the Administrator Tool, expand the Portlet Applications folder, expand the desired portlet application, and then click the name of the Alarms portlet (named OVNNMAlarms by default).

   The editor pane displays the configuration for this portlet as shown here.



General Settings

Portlet Name*: OVNNMAlarms

Portlet Title*: HP OV NNM Alarms

Portlet Class*: com.hp.ov.portal.portlets.alarms.AlarmPortlet

Description: Demo: HP OpenView Network Node Manager Alarms Portlet. Provides access to NNM alarms.

Mime Type*: text/html

Portlet Modes*: ☑ VIEW ☑ EDIT ☑ HELP

Alarms Portlet Edit

Display Stylesheet*: alarmTable_html.xsl

Help Content URI: /C/help/NNM/alarmsView.jsp

Priority of Filter Assignments:

AllData

2 In the General Settings area, make any desired changes.

3 On the General Parameters tab of the Alarms Portlet Edit area, set the configuration options. At a minimum, specify the correct values for the Priority of Filter Assignments option. See Chapter 7, Filtering NNM Data for product-specific information.

4 On the Alarm Categories tab of the Alarms Portlet Edit area, select the alarm categories to display in the portlet.

5 Click **Save**.

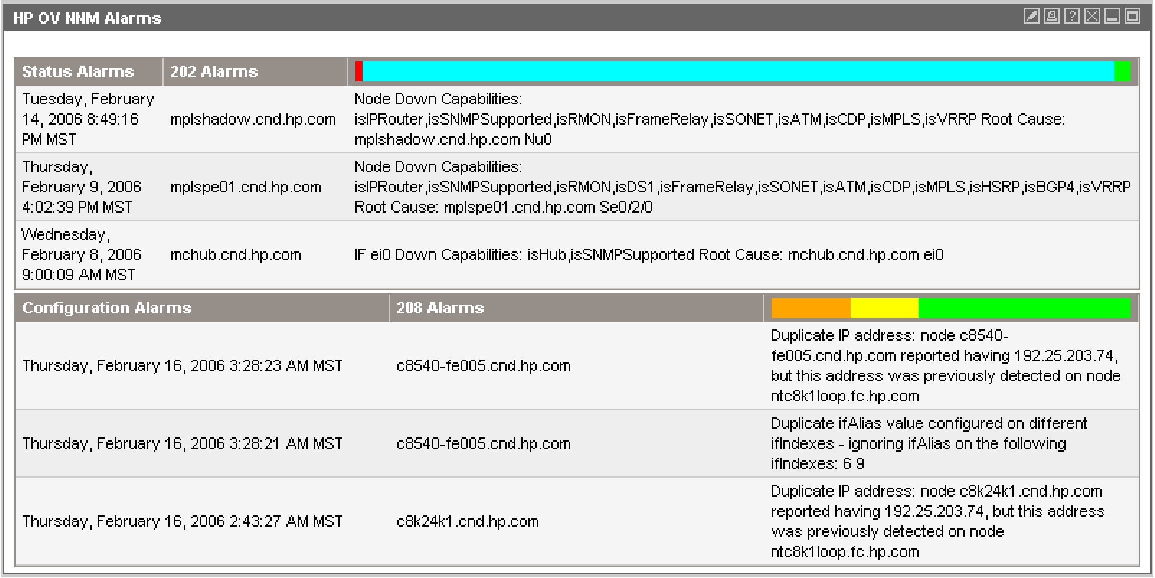
Using the Alarms Portlet

The Network Node Manager Alarms portlet presents network alarms from NNM running on one or more NNM management stations within your management domain.

Changes are visible in the Alarms portlet each time the portal view is displayed or refreshed. The alarm lists are continually updated in Operations View memory.

Figure 6 shows an example of the Alarms portlet.

Figure 6 Deployed Alarms Portlet



HP OV NNM Alarms

Status Alarms	202 Alarms	
Tuesday, February 14, 2006 8:49:16 PM MST	mplshadow.cnd.hp.com	Node Down Capabilities: isIPRouter,isSNMPSupported,isRMON,isFrameRelay,isSONET,isATM,isCDP,isMPLS,isVRRP Root Cause: mplshadow.cnd.hp.com Nu0
Thursday, February 9, 2006 4:02:39 PM MST	mplspe01.cnd.hp.com	Node Down Capabilities: isIPRouter,isSNMPSupported,isRMON,isDS1,isFrameRelay,isSONET,isATM,isCDP,isMPLS,isHSRP,isBGP4,isVRRP Root Cause: mplspe01.cnd.hp.com Se0/2/0
Wednesday, February 8, 2006 9:00:09 AM MST	mchub.cnd.hp.com	IF ei0 Down Capabilities: isHub,isSNMPSupported Root Cause: mchub.cnd.hp.com ei0

Configuration Alarms	208 Alarms	
Thursday, February 16, 2006 3:28:23 AM MST	c8540-fe005.cnd.hp.com	Duplicate IP address: node c8540-fe005.cnd.hp.com reported having 192.25.203.74, but this address was previously detected on node ntc8k1loop.fc.hp.com
Thursday, February 16, 2006 3:28:21 AM MST	c8540-fe005.cnd.hp.com	Duplicate ifAlias value configured on different ifIndexes - ignoring ifAlias on the following ifIndexes: 6 9
Thursday, February 16, 2006 2:43:27 AM MST	c8k24k1.cnd.hp.com	Duplicate IP address: node c8k24k1.cnd.hp.com reported having 192.25.203.74, but this address was previously detected on node ntc8k1loop.fc.hp.com

Customizing the Alarms Portlet

You can modify the Network Node Manager Alarms portlet in your portal view:

1. Access the portal view by logging on to the portal as a user with access to edit portlet preferences.

   The portlet must also have the EDIT mode enabled.

2. In the title bar of the Alarms portlet, click the edit button.
3. Select the Select from List option, and then configure the Displayed Alarm Categories list as desired. Click the help button if you need more information.
4. Click **OK** to save your changes and return to the main portal page.

Establishing Global Settings for Alarms Portlets

The Administrator Tool settings in the Alarm Categories editor pane affect all Alarms portlets. To locate this editor pane, in the scoping pane, expand the Portlet Shared Configuration, expand the HP OpenView Network Node Manager Configuration folder, and then select Alarm Categories. The editor pane displays the global alarm category settings.

The global configuration settings for all alarm categories are as follows:

- Maximum Number of Connections: The maximum number of (socket) connections that a portal server is allowed to establish with all NNM management stations it needs to communicate with, for gathering alarm information.

  A connection and a thread is established between the Operations View server and each NNM station for each active alarm category. Multiple portal users viewing alarms that originate from the same NNM management station share a connection as long as they all are assigned to the same role definition. When the specified maximum is reached, the least used connection is closed and a new one is opened, as needed.

  For example, an Alarms portlet that has 6 alarm categories and gathers alarms from 6 NNM management stations would require 36 socket connections per role. Multiple portlets can share the same role socket connections. When the specified number is reached, for each new subsequent connection required: (1) the least used connection is closed and (2) a new one is opened.

- Connection Time Out (seconds): The number of seconds to pause after each socket connection is opened. The smaller the number, the faster the Alarms portlet opens when a portlet is first accessed. However, the time-out value might be so short that no alarms are displayed until the portal is refreshed. Too short a time-out value can cause the “Data currently unavailable” error message to display, rather than the alarm text.

- Additional Time for Synchronous Call (seconds): The number of seconds to add to the time out when making a synchronous call to get data from the ovalarmsrv process on each NNM management station. Synchronous calls are required when you set the Older Than X Minutes attribute for an alarm category to a non-zero value in any alarm configuration. Once an Older Than X Minutes attribute is specified, alarm data cannot be cached because the time value in the filter request changes with every refresh.

- Socket Time Out (seconds): The number of seconds to wait for a socket connection to be made.
- Ovalarmsrv Reply Time Out (seconds): The number of seconds to wait each time for any response (protocol or data) from ovalarmsrv.
- Maximum Ovalarmsrv Wait Time (seconds): The maximum number of seconds to wait for a data response from ovalarmsrv. The value for this attribute should be greater than the value for the Connection Time Out attribute to allow for delays due to network traffic.
- Show Summary Line: When selected, a message displays at the bottom of each alarm category explaining current configuration settings ("configured for x alarms, received y.") When cleared, no such message is displayed.
- Show Short Date Format: When selected, the current locale setting's short date format is used. For example, US English: mm/dd/yy hh:mm:ss am/pm When cleared, the current locale's long date format is used. For example, US English: Tuesday March 20 2006 hh:mm:ss am/pm tz

Editing Alarm Categories

Operations View alarm categories are based upon existing NNM alarm categories, such as “Status Alarms” or “Threshold Alarms.” Operations View alarm categories must be defined in the Alarms Categories folder of the Administrator Tool before they can be displayed in portal views through an Alarms portlet. Although they are based upon a specific NNM alarm category, the Operations View alarm category name can be different from the base NNM alarm category name; such as “Accounting Department’s Network Problems” or “Internet Availability Alarms.”

You can modify Operations View alarm categories in a variety of ways:

- Alarm Category Configuration on page 60
- Filtering Within an Alarm Category on page 61
- Modifying An Existing Alarm Category on page 63
- Creating an Alarm Category on page 63
- Deleting an Alarm Category on page 64

Additionally, alarm categories support some filtering capabilities. See Chapter 7, Filtering NNM Data.

Alarm Category Configuration

The choices explained in this section are specified in each alarm category definition.

Alarms that pass the filter assignment (see Chapter 7, Filtering NNM Data) and the filter defined for the alarm category (see Filtering Within an Alarm Category on page 61) are further filtered by the following criteria as an AND condition before being displayed in any Alarms portlet:

- NNM Station List: Optional. A subset of NNM management stations configured in the Administrator Tool. Alarms for this category are gathered only from the specified NNM management stations. If this field is empty, all stations specified in the Administrator Tool pass.)
- NNM Base Category: Required. The alarm category currently defined in NNM that you wish to access for this alarm category.

- Match Description Substring: Optional. The portlet only displays the alarms whose messages include the specified text. If this field is empty, all descriptions pass.
- Older Than X Minutes: Optional. Wait the specified number of minutes before displaying any alarm. If this field is empty, show alarms as soon as they happen.
- Severities: Required. The NNM-defined alarm severity levels that you wish to include. No alarms pass if you specify none.
- Acknowledgement: Required. Include alarms that are acknowledged and/or unacknowledged within NNM. No alarms pass if nothing is selected.

Filtering Within an Alarm Category

The alarm categories can further restrict the set of nodes whose alarms are displayed, or from which NNM server alarms are retrieved. The following options are available to refine what is displayed for each alarm category:

- IPHost Filter: Passes only alarms from devices specified by hostname or IP address. For example:

```
10\.2\.5\.125
eagle\.wingnuts\.com
```

➤ If you use Perl5 regular expressions in your filters, only .* is allowed. The following example allows all nodes ending in ".eagle.wingnuts.com" to pass:

```
.*\.eagle\.wingnuts\.com
```

See **www.perl.com** or **www.perldoc.com** for information about Perl5 regular expressions.

- Capability Filter: The capability filter commonly refers to the capability field within the NNM database, with values such as isRouter or isNode. However, this filter can search upon any field in the NNM object database. For example:

Field	**Value** **(default value is "true")**
IPStatus	Critical
isServer	

- Organization Filter: Passes only alarms from devices included in the specified customer model's organization. For example:

  The actual nodes whose alarms are displayed result from the intersection of nodes between the current filter assignment and the nodes from the current category. It is possible at runtime for the intersection of these lists to be the empty set. In this case, no nodes are selected and no output occurs for this alarm category.

➤ When you specify more than one filter (IPHost Filter, Capability Filter, or Organization Filter), they are AND'd together. That is, alarms must pass all filtering to be displayed, not just a single criterion.

The alarm criteria can specify several different items to create a filter within the alarm category. For example, IP Host Filter: host.corp.com and Severity: critical. In this example, only alarms with the source name matching host.corp.com *and* having a severity of critical are displayed.

If any of the above support multiple values, each value is treated as an OR condition. To continue the example, with severities critical and major, alarms matching the hostname host.corp.com *and* having either a severity of critical *or* major are displayed. If multiple nodes are supplied in the node list (such as hostA.corp.com;hostB.corp.com) alarms matching *either* hostA OR hostB are displayed.

Modifying An Existing Alarm Category

To modify an alarm category, follow these steps:

1 In the scoping pane of the Administrator Tool, expand the Portlet Shared Configurations folder, expand the HP OpenView Network Node Manager folder, expand the Alarms Categories folder, and then select the alarm category to modify.

The editor pane displays the configuration for the selected alarm category.

2 Configure the alarm category as desired (see Alarm Category Configuration on page 60 for information), and then click **Save**.

⚠ If you are gathering alarms from an NNM management station running in a language other than English, see Running in Languages Other Than English on page 45 for important information about localization of the Alarms portlet.

3 In a web browser, log in to the portal to verify that the alarms appear as desired.

For information on reviewing the current global alarm category settings, see Establishing Global Settings for Alarms Portlets on page 58. One of the global choices specifies whether or not a message is displayed, at the bottom of each alarm category, explaining the number of alarms currently allowed to be displayed.

Creating an Alarm Category

When configuring a new alarm category, first decide which alarms category to use in a given portal view and from which NNM management stations to collect alarms. Operations View ships with predefined alarm categories for the standard NNM alarm categories.

To create a new alarm category, follow these steps:

1 In the Administrator Tool, click **File→ New→ NNM Alarm Category**.

2 In the Add New NNM Alarm Category window, type the name of the new alarm category.

The editor pane displays the configuration for the new alarm category.

3 Configure the alarm category as desired (see Alarm Category Configuration on page 60 for information), and then click **Save**.

⚠ If you are gathering alarms from an NNM management station running in a language other than English, see Running in Languages Other Than English on page 45 for important information about localization of the Alarms portlet.

4 In a web browser, log in to the portal to verify that the alarms appear as desired.

For information on reviewing the current global alarm category settings, see Establishing Global Settings for Alarms Portlets on page 58. One of the global choices specifies whether or not a message is displayed, at the bottom of each alarm category, explaining the number of alarms currently allowed to be displayed.

Deleting an Alarm Category

If the alarm category currently is selected for display in an Alarms portlet configuration, the category remains selected but is not displayed in the Alarms portlets.

To remove an alarm category, follow these steps:

1 In the scoping pane of the Administrator Tool, expand the Portlet Shared Configurations folder, expand the HP OpenView Network Node Manager folder, and then expand the Alarms Categories folder.

2 Right-click the name of the alarm category to delete, and then click **Delete Alarm Category**.

3 In a web browser, log in to the portal to verify that the alarm categories appear as desired.

4 Working with the Network Node Manager Network Health Portlet

HP OpenView Dashboard Operations View provides the Network Node Manager Network Health portlet for integrating with HP OpenView Network Node Manager (NNM).

This chapter describes how to create, configure, use, and customize the Network Node Manager Network Health portlet. For an overview of the portlet's functionality, see Chapter 1, Introduction to the NNM Integration.

The portal view development process includes a variety of tools:

1 Use the Operations View Administrator Tool to create the Operations View portlets within a portlet application. See Creating the Network Health Portlet on page 66.

2 Use the Administrator Tool to perform initial configuration of the Operations View portlets. See Configuring the Network Health Portlet on page 67.

3 Deploy the portlet application to the portal server. For information, refer to the *Operations View Administrator Guide*.

4 Use the portal server software tools to create a portal view that includes the Operations View portlets. For information, refer to the portal server software documentation.

5 In a web browser, view the portal view and customize the contained portlets. See Using the Network Health Portlet on page 70.

   This is the only point at which end users can interact with the Operations View portlets. If you allow portlet customization, refer to the *Operations View Administrator Guide* for information about the scope and effects of portlet customization.

6 Use the Administrator Tool to maintain the Operations View portlet configurations. See Customizing the Network Health Portlet on page 74.

Creating the Network Health Portlet

Use the HP OpenView Dashboard Operations View Administrator Tool to create the Network Node Manager Network Health portlet within an existing portlet application.

To create the Network Health portlet, follow these steps:

1. In the Administrator Tool, click **File**→ **New**→ **Portlet**.
2. In the Add New Portlet window, enter the following information:
   - Portlet Name: The name of the portlet as it appears in the portlet application in the scoping pane and in the portal server software tools.
   - The portlet name must be unique, start with a letter or underscore character, and consist of only alphanumeric and underscore characters.
   - Portlet Title: The name of the portlet as it appears in the portal server software tools and the portal view. Defaults to the portlet name.
   - Description (optional): The portlet description as it appears in the portal server software tools.
   - Portlet Type: Select OVNNMHealth from the list.
   - Destination Portlet Application: Select the portlet application to contain the new portlet.

   The new portlet appears in the selected portlet application in the scoping pane, and the configuration information for this portlet appears in the editor pane.

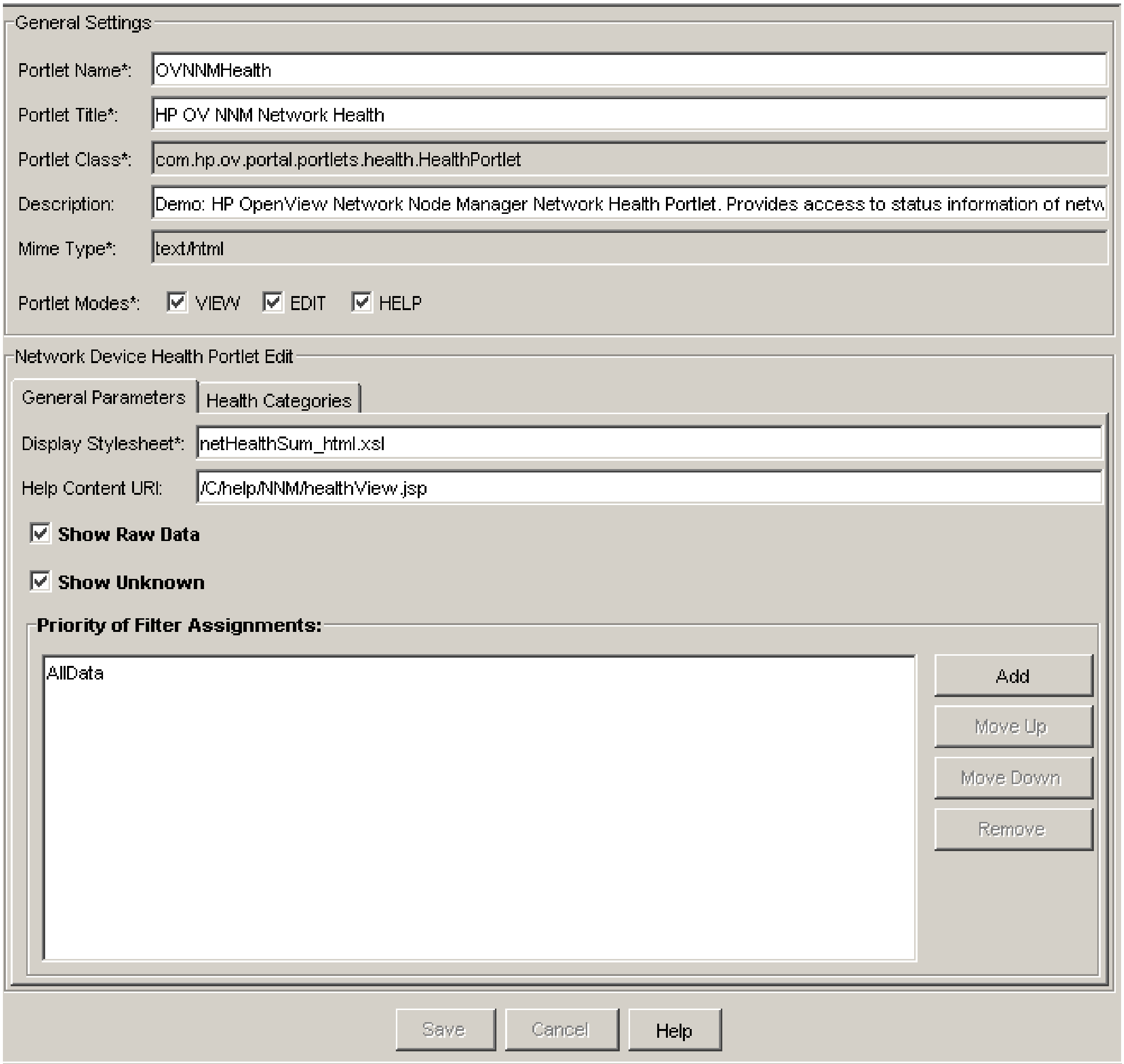
Configuring the Network Health Portlet

For information on the Network Node Manager Network Health portlet configuration options, click **Help** at the bottom of the editor pane to view the online help page.

To configure the default settings for the Network Health portlet, follow these steps:

1 In the Administrator Tool, expand the Portlet Applications folder, expand the desired portlet application, and then click the name of the Network Health portlet (named OVNNMHealth by default).

The editor pane displays the configuration for this portlet as shown here.



General Settings

Portlet Name*: OVNNMHealth

Portlet Title*: HP OV NNM Network Health

Portlet Class*: com.hp.ov.portal.portlets.health.HealthPortlet

Description: Demo: HP OpenView Network Node Manager Network Health Portlet. Provides access to status information of netw

Mime Type*: text/html

Portlet Modes*: ☑ VIEW ☑ EDIT ☑ HELP

Network Device Health Portlet Edit

Display Stylesheet*: netHealthSum_html.xsl

Help Content URI: /C/help/NNM/healthView.jsp

☑ **Show Raw Data**

☑ **Show Unknown**

Priority of Filter Assignments:

AllData

2 In the General Settings area, make any desired changes.

3 On the General Parameters tab of the Network Device Health Portlet Edit area, set the configuration options. At a minimum, specify the correct values for the Priority of Filter Assignments option. See Chapter 7, Filtering NNM Data for product-specific information.

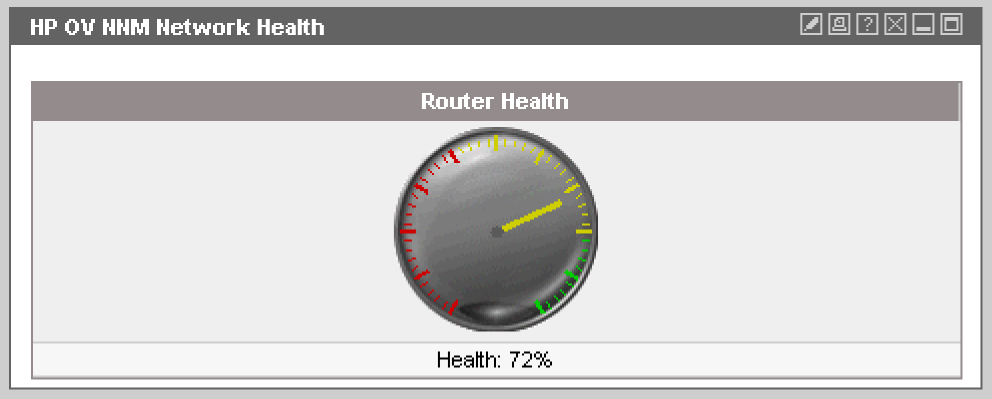
4 On the Health Categories tab of the Network Device Health Portlet Edit area, select the health categories to display in the portlet.

5 Click **Save**.

Using the Network Health Portlet

Network health is scored as a value from 0-100, with 0 being the poorest health and 100 being the best health. Figure 7 shows an example Network Health portlet.

Figure 7 Deployed Network Health Portlet



Health: 72%

Two types of information are available for Network Health:

- **Gauges** are displayed when the tab first displays in your portal, and indicate the overall health rating for all devices being monitored by the particular gauge. The gauge value is calculated based on the network health metrics defined for the portlet. Network health component groups provide a mechanism for grouping the network health metrics.
- **Detail pages** show the details that were included in the health calculation. The detail pages are displayed by clicking a gauge or the gauge's title.

Gauges

You can customize the Network Health portlet to display specific gauges. You can modify the predefined gauges or create your own to monitor any aspect of the network that is of concern to your users. Network health gauges are called network health categories in the Administrator Tool.

A network health gauge represents the mean health of all network devices being monitored by a particular gauge. For example, router health represents the mean health of all routers. If you have two routers, one with a health score of 100% and one with a score of 60%, the Router Health gauge points to 80%.

The following Network Health gauges are preconfigured and provided with Operations View:

- Router Health: Monitors the health of every device in the NNM database that has the isRouter capability setting.
- Server Health: Monitors the health of every device in the NNM database that has the isServer capability setting.
- Key Device Health: Monitors the health of every device in the NNM database that has the isKeyDevice capability setting.

  If HP OpenView Customer Views is installed and configured on your NNM management station, you probably have devices with the isKeyDevice capability. Within Customer Views, see the online help or the web-based *Concepts Guide* for information about key devices.
- CPE Health: Monitors the health of every device in the NNM database that has the isCPE capability setting (user premises equipment).

  If Customer Views is installed and configured on your NNM management station, you probably have devices with the isCPE capability. Within Customer Views, see the online help or the web-based *Concepts Guide* for information about CPE devices.
- Interface Health: Monitors the health of every interface in the NNM database that passes the interface filter assigned to the current filter.

  This gauge requires that a specific list of interfaces is established through at least one of the filtering levels allowed within the Operations View configuration. This limitation is imposed so that you don't accidently set up data collections on every interface in the entire NNM management domain. See Chapter 7, Filtering NNM Data and Filtering Possibilities for Network Health Gauges on page 77.

Details View

Health gauges might have two levels of health detail drill-down. If available:

- To view the first-level health details, click on the gauge or the health gauge title above the gauge.
- To view the second-level of health detail, click the health score values that are links in the first level health detail. Only certain values provide links.

The first column of a detail table, Resource, displays the name of the network resource (for example, the name of the Interface, Router, Server, Key Device, or Customer Premises Equipment).

The second column, Overall Health, contains the resource's health score. This score is based upon the weighted mean of a set of metrics measured on that resource.

The remaining columns display the health score for each metric used to compute network resource health. The score is a value from 0-100 derived from analysis of the metric value. You might also see the raw data value columns. You choose whether or not to present raw data in your portal views. By default, raw data is not presented.

The tables below describe the metrics used by the default gauges. The metrics identify the specific SNMP MIBs and MIB expressions for NNM to monitor on each device.

➤ For interface metrics, to obtain the most accurate reading, NNM uses a variety of formulas depending upon the attributes of the interface (such as speed of the interface: half-duplex versus full-duplex).

Table 10 Interface Health Metrics (used by all gauges)

Statistic (MIB expression used)	Default Settings Description
Up/Down Status (status)	An indication of whether the interface is up or down. An interface that is up has a status health score of 100%. An interface that is down has a status *health* score of 0%. Because this is an important measure of health, status is given double the weight (by default) of the other statistics when overall interface health is computed.
Utilization Health (p_if%util)	The percent utilization of an interface. For example, a 50% utilization rate means that NNM measured the available bandwidth on an interface, and found that 50% was being used. Higher utilization rates translate into lower utilization *health* scores.
Inbound Error Health (p_if%inerrors)	The error rate (percent) for inbound data on the interface. High error rates translate into lower inbound error *health* scores.
Outbound Error Health (p_if%outerrors)	The error rate (percent) for outbound data on the interface. High error rates translate into lower outbound error *health* scores.

Table 11 Additional Metric used by Router Health Gauge Only

Statistic (MIB Expression used)	Default Settings Description
CPU Utilization Health (p_cisco5minavgbusy)	The percent utilization of the router's CPU. For example, a 50% utilization rate means that NNM measured the available CPU bandwidth, and found that 50% was being used. High utilization rates translate into low utilization *health* scores. This is a measurement of the Cisco MIB object: `local.system.augBusy5`, the "5 minute exponentially-decayed moving average of the CPU busy percentage."

Customizing the Network Health Portlet

You can modify the Network Health portlet in your portal view:

1. Access the portal view by logging on to the portal as a user with access to edit portlet preferences.

   The portlet must also have the EDIT mode enabled.

2. In the title bar of the Network Health portlet, click the edit button.
3. Select the Select from List option, and then configure the Displayed Health Categories list as desired. Click the help button if you need more information.
4. Click **OK** to save the changes and return to the main portal page.

A newly displayed gauge is not fully functioning until the next data collection configuration update occurs so that NNM can supply the requested data. NNM's data collection is discontinued once the gauge has not been displayed in any portal view for 30 days. See Data Collection for Network Health Gauges on page 88and ovcolautoconf.exe on page 96.

When multiple NNM management stations provide raw data to the Network Health portlet, duplication of SNMP data collection is avoided by sending collection requests for a given node to only one of the NNM management stations. The NNM management station chosen is that which first returned raw data for that node. See Data Collection for Network Health Gauges on page 88 for more information.

Establishing Global Settings for All Network Health Portlets

The Portlet Shared Configuration folder of the Administrator Tool contains three folders whose configuration affects the Network Health portlet:

- Network Health Categories
- Network Health Metrics
- Network Health Component Groups

The section describes the global settings for network health categories and network health metrics that apply to all Network Health portlets.

Network Health Category Global Configuration

The Administrator Tool settings in the Network Health Categories editor pane affect all Network Health portlets. To locate this editor pane, in the scoping pane, expand the Portlet Shared Configuration, expand the HP OpenView Network Node Manager Configuration folder, and then select Network Health Categories. The editor pane displays the global network health category settings.

The global configuration settings for all health categories are as follows:

- Show Raw Data controls the display of the columns displaying the raw data returned from each metric (MIB object or MIB expression) referenced in each component metric of each gauge. The default setting is to hide these columns and only display the final *health* score.
- Show Unknown controls whether or not nodes or interfaces whose health score cannot be computed (usually, because that object's status in NNM's object database is set to `unknown`) are displayed in the gauge's details page. The default setting is to exclude information derived from devices with `"unknown"` status. If this attribute is `"on"`, rows for nodes/interfaces with `"unknown"` health status are added to the end of the detail table *if* the `maxDetail` attribute allows.

Network Health Metrics Global Configuration

The Administrator Tool settings in the Network Health Metrics editor pane affect all Network Health portlets. To locate this editor pane, in the scoping pane, expand the Portlet Shared Configuration, expand the HP OpenView Network Node Manager Configuration folder, and then select Network Health Metrics. The editor pane displays the global network health metric settings.

The global configuration settings for all network health metrics are as follows:

- Maximum Age of Data (Minutes): SNMP data collected and supplied by NNM is checked to ensure that it is no older than the specified number of minutes. Older data is ignored for health calculation purposes. This defines near real-time data. If young enough data does not exist for a particular metric, the metric is not used to compute overall health and the "Data Unavailable" message appears for that metric in Network Health detail pages.
- Maximum Number of Devices in Detail View: This sets the maximum number of rows (one per node or interface) allowed in the detail pages. If more devices pass the filtering requirements of a gauge, only the specified number of devices with the poorest health score rating are displayed.
- Raw Data Refresh Frequency (Minutes): Sets the frequency with which raw data from NNM management stations should be updated. Expressed in minutes.
- Rating Settings: This provides the mapping of the numerical scores to the general status of "critical", "normal", "minor", and "unknown".

Editing Health Categories

For each gauge, you can do the following:

- Change the displayed title.
- Control access to the detail pages.
- Change the metric components that determine how health is calculated.
- Change the filter that determines which devices are monitored for the health calculation.
- Modify a Network Health category.
- Create a Network Health category.
- Delete a Network Health category.

The following settings can be modified for an individual health gauge:

- To change the title of a particular Network Health gauge, select the health category, and then change the value of the Title field.
- To control access to the Details Tables of each Network Health gauge, set the Display Depth attribute. Designate the appropriate setting:

  1=gauge only (no links to the details pages)

  2=link provided to node-only or interface-only details

  3=links provided to node *and* to interface details (if available)

The Filtering for Category section supports two types of filtering: node selection and interface selection. See Filtering Possibilities for Network Health Gauges for more information.

Filtering Possibilities for Network Health Gauges

Whereas the filter assignment filter defines what a portlet can potentially display, filtering within a network health category provides a finer level of control over what the portlet actually displays. Either a node selection filter or an interface selection filter must be specified in each gauge's configuration. These filters control the set of nodes or interfaces whose health the gauge is calculating.

When the node selection or interface selection filter is left empty, *all* nodes and interfaces pass (if they pass the filter assignment). The node selection filter has three potential child elements that can further restrict the nodes allowed to pass:

- IPHost Filter: Passes only devices specified by hostname or IP address. You can use any Perl5 regular expressions. See your Perl5 documentation for information about valid expressions. This example allows all nodes ending in ".eagle.wingnuts.com" to pass: .*\.eagle\.wingnuts\.com

  See **www.perl.com** or **www.perldoc.com** for information about Perl5 regular expressions.

- Capability Filter: Passes only devices having the specified value within the NNM object database, ovwdb; for example, isRouter. If no value is provided, the default value used is "true".
- Organization Filter: Passes only nodes included in the organization from the simple customer model sources.

  To reuse a node list or and interface list from an organization defined within your simple customer model sources, you can select the organizations to use. Data will still be intersected with the current filter assignment in use in addition to the information allowed for these organizations.

The interface selection filter has two elements that can further restrict the interfaces allowed to pass:

- Interface Filter: Passes only interfaces specified by IP address. You can use any Perl5 regular expressions. See your Perl5 documentation for information about valid expressions. This example allows all nodes ending in ".eagle.wingnuts.com" to pass: .*\.eagle\.wingnuts\.com

  See **www.perl.com** or **www.perldoc.com** for information about Perl5 regular expressions.

- Organization Filter: Passes only interfaces included the organization from the simple customer model sources.

  To reuse a node list or and interface list from an organization defined within your simple customer model sources, you can select the organizations to use. Data will still be intersected with the current filter assignment in use in addition to the information allowed for these organizations.

When the above filters are used, they contribute to the *intersection* of the filter assignment and each gauge filter. It is possible at runtime for the *intersection* of all filters to be the empty set. In this case, no nodes or interfaces are selected and the message "Managed Objects not found" is displayed for this gauge.

Modifying An Existing Network Health Category

To modify a Network Health category, follow these steps:

1 In the scoping pane of the Administrator Tool, expand the Portlet Shared Configurations folder, expand the HP OpenView Network Node Manager folder, expand the Network Health Categories folder, and then select the health category to modify.

   The editor pane displays the configuration for the selected health category.

2 Configure the health category as desired and then click **Save**.

3 In a web browser, log in to the portal to verify that the health categories appear as desired.

For information on reviewing the current global Network Health category settings, see Establishing Global Settings for All Network Health Portlets on page 75.

Creating a Network Health Category

When configuring a new Network Health category, first decide which health category to use in a given portal view. Operations View ships with predefined health categories for the standard NNM health categories.

To create a new health category, follow these steps:

1 In the Administrator Tool, click **File**→ **New**→ **NNM Health Category**.

2 In the Add New NNM Health Category window, type the name of the new health category.

   The editor pane displays the configuration for the new health category.

3 Configure the health category as desired and then click **Save**.

4 In a web browser, log in to the portal to verify that the alarms appear as desired.

For information on reviewing the current global Network Health category settings, see Establishing Global Settings for All Network Health Portlets on page 75.

Deleting a Network Health Category

If the Network Health category currently is selected for display in a Network Health portlet configuration, the category remains selected but is not displayed in the Network Health portlets.

To remove a Network Health category, follow these steps:

1. In the scoping pane of the Administrator Tool, expand the Portlet Shared Configurations folder, expand the HP OpenView Network Node Manager folder, and then expand the Network Health Categories folder.
2. Right-click the name of the alarm category to delete, and then click **Delete Health Category**.
3. In a web browser, log in to the portal to verify that the health categories appear as desired.

Editing Network Health Metrics

The Network Health Metrics section controls how the gauge's health score is calculated on selected metrics. You can change any of the following:

- ID: A unique identifier for this metric.
- Title: A user friendly title used for this metric.
- Raw Data Source (href): Specifies the source of the raw data, using the syntax: `href="`*`<dataSource>`*`://`*`<instances>`*`/`*`<dataItem>`*
  - dataSource:

    ovtopmd = NNM's topology database for status

    snmp = NNM's SNMP data collection database
  - instances:

    %item%[0] = only one instance exists per node

    %item%[IfIndex] = all interface instances

    %item%[other] = multiple non-interface instances
  - dataItem:

    status = gather status from NNM's topology database (must use dataSource of ovtopmd)

    MIB label = The name used to identify this MIB object or MIB expression in NNM's Data Collector configuration program (xnmcollect) (must use dataSource of snmp)

    MIB Objects: MIB objects are attributes that an SNMP agent on a network device allows to be queried by an NNM management station. Currently, any MIB object that returns a numeric value is supported. (Strings are not supported.)

    MIB Expressions: MIB expressions are a feature of NNM that allow for the creation of mathematical formulas comprised of MIB objects. MIB expressions allow more meaningful information to be gathered than is possible from individual MIB objects.
- SNMP System Oid (Optional): For SNMP elements, specifies the sysObjectID to use as a means of refining NNM's data collection process.

- Auto Configure NNM's Data Collector Program: For SNMP elements, whether or not NNM's Data Collector program should be automatically configured to gather this information based upon Operations View data requirements.
- Metrics Scales: The Network Health portlet uses the metric scales to translate a MIB value into a metric. Configure the lower and user boundaries and percentage (translation) for each range.
- Rating Scales: The Network Health portlet uses the rating scale to translate a health score into a health rating. Configure the lower and upper boundaries and label (translation) for each range.

Modifying An Existing Network Health Metric

To modify a Network Health metric, follow these steps:

1 In the scoping pane of the Administrator Tool, expand the Portlet Shared Configurations folder, expand the HP OpenView Network Node Manager folder, expand the Network Health Categories folder, and then select the health metric to modify.

   The editor pane displays the configuration for the selected health metric.

2 Configure the health metric as desired and then click **Save**.

3 In a web browser, log in to the portal to verify that the health categories appear as desired.

For information on reviewing the current global Network Health metric settings, see Establishing Global Settings for All Network Health Portlets on page 75.

Creating a Network Health Metric

When configuring a new Network Health metric, first decide which health metric to use in a given portal view. Operations View ships with predefined health metrics for the standard NNM health categories.

To create a new health metric, follow these steps:

1 In the Administrator Tool, click **File→ New→ NNM Health Metric**.

2 In the Add New NNM Health Metric window, type the name of the new health metric.

The editor pane displays the configuration for the new health metric.

3. Configure the health metric as desired and then click **Save**.
4. In a web browser, log in to the portal to verify that the alarms appear as desired.

For information on reviewing the current global Network Health metric settings, see Establishing Global Settings for All Network Health Portlets on page 75.

Deleting a Network Health Metric

If the Network Health metric currently is selected for display in a Network Health portlet configuration, the metric remains selected but is not displayed in the Network Health portlets.

To remove a Network Health metric, follow these steps:

1. In the scoping pane of the Administrator Tool, expand the Portlet Shared Configurations folder, expand the HP OpenView Network Node Manager folder, and then expand the Network Health Categories folder.
2. Right-click the name of the alarm metric to delete, and then click **Delete Health Metric**.
3. In a web browser, log in to the portal to verify that the health categories appear as desired.

Editing Network Health Component Groups

The Network Health Metrics section controls how the gauge's health score is calculated on selected metrics. You can change any of the following:

- ID: A unique identifier for this metric.
- Title: A user friendly title used for this metric.
- Group Health Components: Each component group represents multiple metrics and provides the following options for grouping:
  - Vital: If yes, when this metric measures zero, the resource's health score is set to zero regardless of other health score measures. If no, normal computation is performed.
  - Weight: Controls how much emphasis is placed upon each Component (MIB object, MIB expression, or device status) being measured by a gauge. For example, if an interface's status is *down*, the status has more of an impact on the device health calculation than a high utilization measurement.
  - HRef: This is the reference to the metric ID field.

Modifying An Existing Network Health Component Group

To modify a Network Health component group, follow these steps:

1. In the scoping pane of the Administrator Tool, expand the Portlet Shared Configurations folder, expand the HP OpenView Network Node Manager folder, expand the Network Health Categories folder, and then select the health component group to modify.

   The editor pane displays the configuration for the selected health component group.

2. Configure the health component group as desired and then click **Save**.
3. In a web browser, log in to the portal to verify that the health categories appear as desired.

For information on reviewing the current global Network Health component group settings, see Establishing Global Settings for All Network Health Portlets on page 75.

Creating a Network Health Component Group

When configuring a new Network Health component group, first decide which health component group to use in a given portal view. Operations View ships with predefined health component groups for the standard NNM health categories.

To create a new health component group, follow these steps:

1. In the Administrator Tool, click **File**→ **New**→ **NNM Health Component Group**.
2. In the Add New NNM Health Component Group window, type the name of the new health component group.

   The editor pane displays the configuration for the new health component group.
3. Configure the health component group as desired and then click **Save**.
4. In a web browser, log in to the portal to verify that the alarms appear as desired.

For information on reviewing the current global Network Health component group settings, see Establishing Global Settings for All Network Health Portlets on page 75.

Deleting a Network Health Component Group

If the Network Health component group currently is selected for display in a Network Health portlet configuration, the component group remains selected but is not displayed in the Network Health portlets.

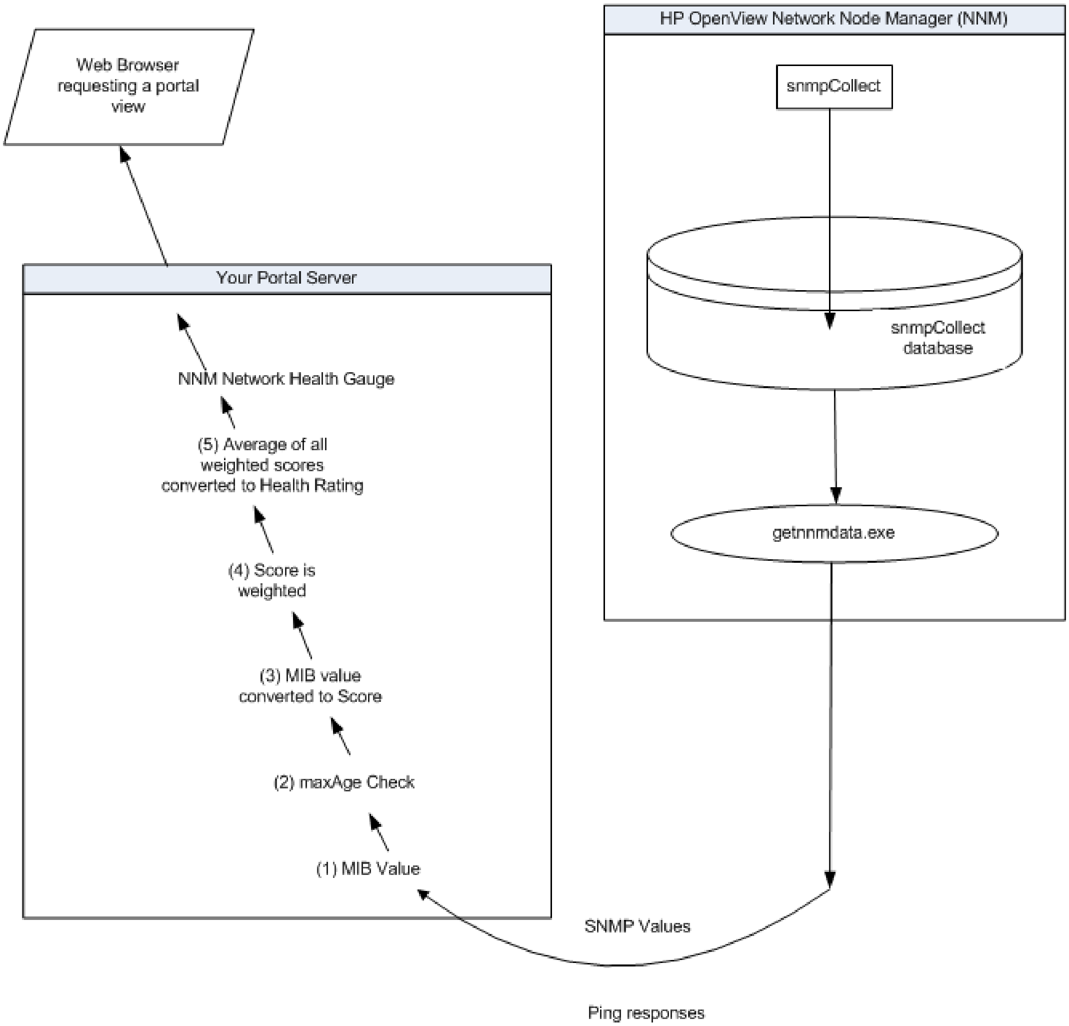
To remove a Network Health component group, follow these steps:

1. In the scoping pane of the Administrator Tool, expand the Portlet Shared Configurations folder, expand the HP OpenView Network Node Manager folder, and then expand the Network Health Categories folder.
2. Right-click the name of the alarm component group to delete, and then click **Delete Health Component Group**.
3. In a web browser, log in to the portal to verify that the health categories appear as desired.

Health Rating Calculations

This section describes the steps for calculating the health rating. You can modify any or all of the configurations used during steps.

Figure 8 Calculating Health Ratings to Display in Gauges


Web Browser requesting a portal view
HP OpenView Network Node Manager (NNM)
snmpCollect
Your Portal Server
snmpCollect database
NNM Network Health Gauge
(5) Average of all weighted scores converted to Health Rating
getnnmdata.exe
(4) Score is weighted
(3) MIB value converted to Score
(2) maxAge Check
(1) MIB Value
SNMP Values
Ping responses

1 Data is gathered through NNM, and the requested *values* are returned to the Network Health portlet.

For more information about controlling this process, see Data Collection for Network Health Gauges on page 88.

2 For SNMP data, the returned values are checked to ensure that they are valid by noting how many *minutes* have passed since they were collected by NNM. This is controlled by the Maximum Age setting for all network health metrics. This attribute affects all health gauges defined within all portal views. See Establishing Global Settings for All Network Health Portlets on page 75 for more information.

3 Each requested MIB object or MIB expression has a corresponding metric element that includes a scale for converting the returned MIB *value* to a score (translation="0-100"). You can change the translation to control how the values are interpreted.

4 The category health components for each gauge assigns a weight to each score. You can modify the weight of any scores within a gauge.

5 Based upon the weighted average (mean) of all scores, a health rating is computed for each node or interface being monitored by the gauge. The gauge's health rating is computed as the average (mean) health rating of all nodes/interfaces represented by the gauge. The rating scale is used to translate the *scores* to health *ratings*. The rating scale affects *all* gauges defined within any portal.

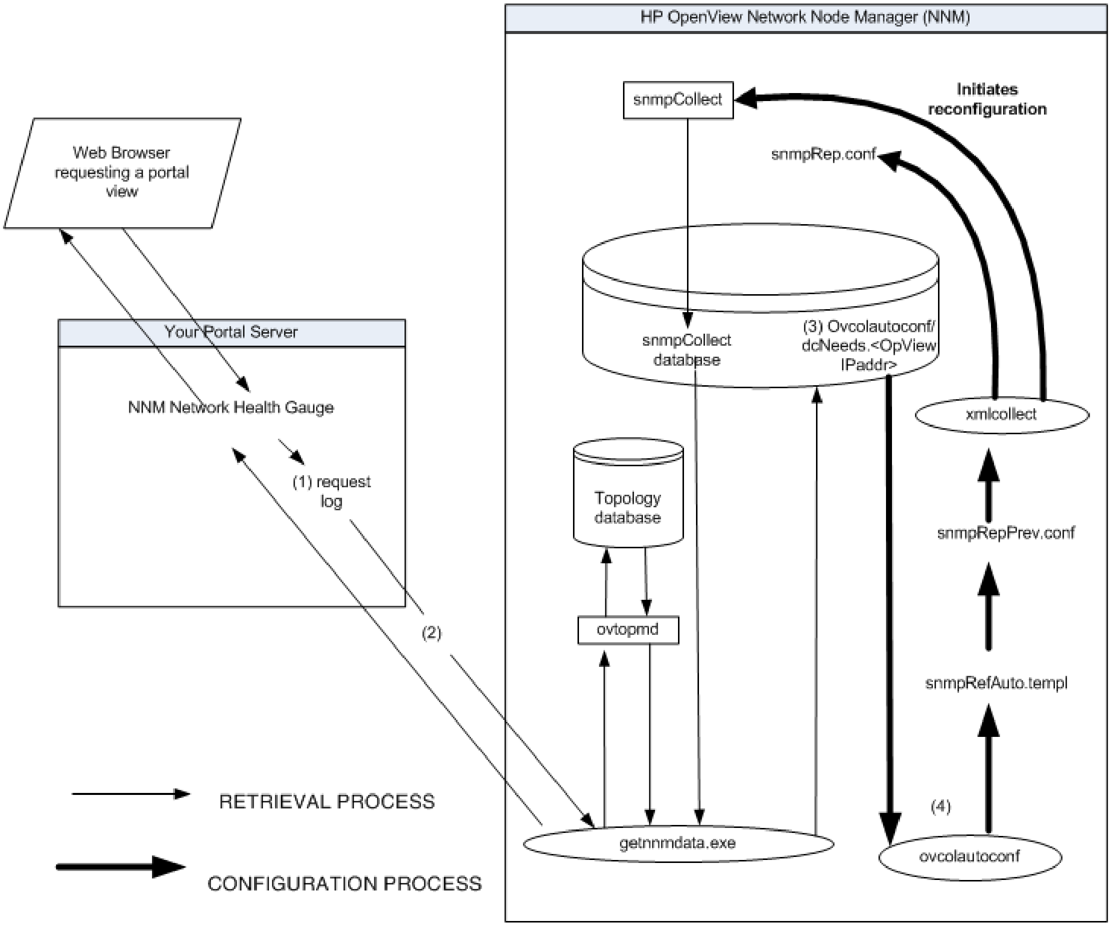
If desired, modify the rating scale. The rating controls the color of the needle on the gauge, the width of each color around the outside edge of the gauge, as well as controlling which icon displays in each row of the health detail table. See Establishing Global Settings for All Network Health Portlets on page 75 for more information about the icons.

You can change the lower and upper values, but do not change the translation values.

Data Collection for Network Health Gauges

NNM collects all SNMP data requested by Operations View and returns current information about device status.

Figure 9 Communication Process for the Network Health Portlet



When multiple NNM management stations provide raw data to the Network Health portlet, duplication of SNMP data collection is avoided by sending collection requests for a given node to only one of the NNM management stations. The NNM management station chosen is that which first returned raw data for that node. See Data Collection for Network Health Gauges on page 88for more information.

Operations View depends on two programs that reside on each NNM management station (`getnnmdata.exe` and `ovcolautoconf.exe`) to collect requested data:

1 Each time a Network Health gauge is displayed, Operations View logs the underlying data requests.

  A list of requested MIB objects and MIB expressions from any Network Health portlet gauge is compiled by the Network Health portlet. The list documents which MIB objects and MIB expressions are being requested for which network devices from which NNM management stations.

  ➤ The underlying MIB objects and MIB expressions appear in Network Health gauge shared portlet configurations. See the Raw Data Source (href) attribute for each metric that specifies exactly which MIB object or MIB expression is being requested.

2 The Network Health portlet contacts the `getnnmdata.exe` on each NNM management station that is configured through the Administrator Tool. The frequency of this action is determined by the Raw Data Refresh Frequency setting in the metrics section of the Administrator Tool (by default, every 10 minutes).

3 The Network Health portlet receives the most recent data collection results from the NNM database. The portlet also places the current request log file in the `ovcolautoconf` directory. Requests from each portal server are gathered here and stored in a file whose name is of the form (`dcneeds.`*`<PortalserverIPaddress>`*).

  You must create the `ovcolautoconf` directory before this step works. See Enabling the Network Health Portlet to Configure NNM Data Collection on page 30 for more information.

4 To complete the automatic configuration process, run the `ovcolautoconf.exe` command. The `ovcolautoconf` command must be executed on the NNM management station, either manually or as a scheduled task that you define. `ovcolautoconf` does the following:

- All portal servers' data collection needs are processed. The list of data collection requests is configured using the information in `snmpRepAuto.templ` file and placed in the `snmpRepPrev.conf` file.
- If necessary, NNM's Data Collector configurations are updated by making Network Health portlet additions or changes to the `snmpRep.conf` file (one of two configuration files used by the NNM Data Collector program). The `snmpRep.conf` file is used by the SNMP Data Collector as a guide for gathering data. TheOperations View entries do not interfere with data collection configurations that were entered directly through NNM.
- Data collections are configured on an *as-needed* basis, rather than a *potentially* needed basis. In other words, until a gauge is displayed in a portal view, no data collection is initiated.
- If a gauge is not displayed for 30 days (default setting), the data collections are discontinued (provided they are not needed by other HP OpenView products). See ovcolautoconf.exe on page 96for more information.

Network Health gauges calculate the health of specific network devices using information gathered by NNM management stations (see Health Rating Calculations on page 86). Changes are visible in the Network Health gauges each time the portal view is displayed or refreshed.

See The Data Collection Process for the Network Health Portlet on page 38 for important additional information about the Operations View data collection process for the Network Health portlet.

Relevant Files

The files in Table 12 reside on the NNM management station:

- `getnnmdata.exe`

  This is the NNM program that receives data collection requests from and communicates data collection information to Operations View. See Data Collection for Network Health Gauges on page 88.

- `dcNeeds.`*<PortalserverIPAddress>*

  These NNM files are the data request logs received from Operations View. See Data Collection for Network Health Gauges on page 88.

- `ovcolautoconf.exe` & `snmpRepAuto.templ`

  This NNM program must be run manually or scheduled to run on a regular basis in order to upload the Operations View data collection requests into NNM's data collection program. See Data Collection for Network Health Gauges on page 88 and ovcolautoconf.exe on page 96.

  The `snmpRepAuto.templ` file on the NNM management station contains the data collection settings that are assigned to each MIB or MIB expression requested by Operations View. You can modify these default settings. See Data Collection for Network Health Gauges on page 88 and snmpRepAuto.templ on page 95.

- `mibExprAuto.conf`

  This NNM configuration file defines the Operations View MIB expressions for NNM's data collection program. See Enabling the Network Health Portlet to Configure NNM Data Collection on page 30 and mibExprAuto.conf on page 93.

Table 12 Data Collection Process Files on the NNM Management Station

File Name	Windows Location *<NNM_install_dir>/*	UNIX Location
getnnmdata.exe	www/cgi-bin/	/opt/OV/www/cgi-bin/
dcNeeds.<*PortalserverIPAddress*>	databases/ snmpCollect/ ovcolautoconf/	/var/opt/OV/share/databases/ / snmpCollect/ovcolautoconf/
ovcolautoconf.exe	bin/	/opt/OV/bin
snmpRepAuto.templ	conf/ovcolautoconf/	/etc/opt/OV/share/conf/ ovcolautoconf
mibExprAuto.conf	conf/ovcolautoconf/	/etc/opt/OV/share/conf/ ovcolautoconf

mibExprAuto.conf

This file resides on the NNM management station. It contains the MIB expression definitions that are being used by Operations View for Network Health calculations. MIB expressions are an NNM feature that allows for the creation of mathematical formulas comprised of MIB objects. MIB expressions allow you to derive more meaningful information than you could gather from individual MIB objects.

Operations View preconfigured MIB expressions are defined in the `mibExprAuto.conf` file. More information is available within the file itself:

- *Windows*:

  `<`*`NNM_install_dir`*`>\conf\ovcolautoconf\mibExprAuto.conf`

- *UNIX*:

  `/etc/opt/OV/share/conf/ovcolautoconf/mibExprAuto.conf`

OPTIONAL: If you need to write your own MIB expression:

1. Before you modify the `mibExprAuto.conf` file, save a copy of the original.
2. Add your MIB expression to the `mibExprAuto.conf` file.

   Copy and modify one of the MIB expressions supplied.

   For information about writing MIB expressions, see the *Managing Your Network with NNM* book provided with NNM. See also the *mibExpr.conf* and the *mib.coerce* reference pages in NNM's online help (or the UNIX manpages).
3. Verify that the MIB files, whose objects you wish to use, are loaded into NNM. See the *Managing Your Network with NNM* book provided with NNM for more information about loading MIB files into NNM.
4. After writing your new MIB expression, you must load the new expression into NNM by typing the following at the command prompt. This command checks the syntax of your MIB expression and forces an update to NNM's `mibExpr.conf` file which allows data collections to be enabled:

   - *Windows*: **`xnmcollect -loadExpr <`*`NNM_install_dir`*`>\NNM\conf\ovcolautoconf\mibExprAuto.conf`**
   - *UNIX*: **`xnmcollect -loadExpr /etc/opt/OV/share/conf/ovcolautoconf/mibExprAuto.conf`**

5 Make a new entry into the `snmpRepAuto.templ` file so that NNM could begin collecting the requested information (see snmpRepAuto.templ on page 95).

snmpRepAuto.templ

The `snmpRepAuto.templ` file exists on each NNM management station. (See The Data Collection Process for the Network Health Portlet on page 38 for installation instructions.) If you create any new gauges, ensure that there is one entry in the `snmpRepAuto.templ` file for each MIB object and each MIB expression that needs to be collected. (See Relevant Files on page 91.)

To view the list of configured collections and make any necessary additions, at the command line type the following:

- *Windows*: **`xnmcollect -snmpColConfFile snmpRepAuto.templ`**
- *UNIX*: log in as root and then type:

  `xnmcollect -snmpColConfFile snmpRepAuto.templ`

Review the list. In the `Source` field you will see the variable `_NODE_`, which is automatically replaced with any specific devices requested by Operations View.

If you do not see each MIB object and/or MIB expression that you are using in your gauge, create a new data collector entry:

1. Highlight any MIB Object in the top half of the window, and then click **Edit→ MIB Object→ Copy.**
2. Select the new MIB object or MIB expression to collect data upon.
3. You can change the collection interval setting, otherwise leave the settings as they are. You should see the variable `_NODE_` in the `Source` field.

See also Data Collection for Network Health Gauges on page 88 and ovcolautoconf.exe on page 96.

ovcolautoconf.exe

ovcolautoconf.exe configures the NNM SNMP Data Collector (snmpCollect) to gather data requested by Operations View.

Synopsis

```
ovcolautoconf [-verbose] [-outfile <filename>] [-maxConfAge
<#ofdays>]
```

Description

ovcolautoconf is a Network Node Manager (NNM) command that configures the NNM SNMP Data Collector (snmpCollect) to gather data requested by Operations View. If invoked without the -outfile option, ovcolautoconf updates NNM's data collection configuration to reflect the Operations View SNMP data needs. Specifically, ovcolautoconf processes Operations View server configuration request files found in $OV_DB/snmpCollect/ovcolautoconf. These files have names of the form dcNeeds.<*PortalserverIPAddress*>. (For information about how these request files are placed in this directory, see The Data Collection Process for the Network Health Portlet on page 38.) The template file $OV_CONF/ovcolautoconf/snmpRepAuto.templ is used to construct data collector configuration entries corresponding to these requests. The configuration entries are then loaded into the data collector configuration file $OV_CONF/snmpRep.conf, and snmpCollect is notified that its configuration has been modified. ovcolautoconf clears the Operations View server request files after successfully processing them. The most recent data collector configuration submitted by ovcolautoconf can be found in the file $OV_DB/snmpCollect/ovcolautoconf/snmpRepPrev.conf.

If the data collection configuration needs have not changed since the last execution of ovcolautoconf, no changes to snmpRep.conf are made and no reconfiguration event is sent to snmpCollect.

ovcolautoconf automatically removes data collector configuration entries are no longer needed by Operations View. See the discussion of the -maxConfAge option below for details

To change the number of days Operations View waits before deleting any inactive data collection configurations (default 30), type the following command. There is no way to permanently change this setting. Include this command in your scheduled script or each time you manually run `ovcolautoconf`:

```
ovcolautoconf -maxConfAge <#ofdays>
```

Options

- `-maxConfAge` *<#ofdays>*
  Removes configuration entries that have gone unrequested for the specified number of days. Applies only to configuration entries submitted by `ovcolautoconf`. Default is 30 days.
- `-outfile` *<filename>*
  Don't update NNM's data collection configuration, but instead write the configuration to the specified file.
- `- verbose`
  Send verbose output, including notification of configuration entries that have been aged out, to `stdout`.

Troubleshooting

Warning and error messages are sent to `stderr`.

Files on the NNM Management Station

- *Windows*:
  - `<NNM_install_dir>\conf\ovcolautoconf\snmpRepAuto.templ`
  - `<NNM_install_dir>\conf\ovcolautoconf\mibExprAuto.conf`
  - `<NNM_install_dir>\databases\snmpCollect\ovcolautoconf\snmpRepPrev.conf`
  - `<NNM_install_dir>\databases\snmpCollect\ovcolautoconf\dcNeeds.<PortalserverIPAddress>`
- *UNIX*:

- `/etc/opt/OV/share/conf/ovcolautoconf/snmpRepAuto.templ`
- `/etc/opt/OV/share/conf/ovcolautoconf/mibExprAuto.conf`
- `/var/opt/OV/share/databases/snmpCollect/ovcolautoconf/snmpRepPrev.conf`
- `/var/opt/OV/share/databases/snmpCollect/ovcolautoconf/dcNeeds.`*`<PortalserverIPAddress>`*

See also the *ovrequestd*, *snmpCollect*, *snmpCol.conf*, *mibExpr.conf*, and the *mib.coerce* reference pages in NNM's online help (or the UNIX manpages) for information about NNM's data collection process.

5 Working with the Network Node Manager Topology Portlet

HP OpenView Dashboard Operations View provides the Network Node Manager Topology portlet for integrating with HP OpenView Network Node Manager (NNM).

This chapter describes how to create, configure, use, and customize the Network Node Manager Topology portlet. For an overview of the portlet's functionality, see Chapter 1, Introduction to the NNM Integration.

The portal view development process includes a variety of tools:

1. Use the Operations View Administrator Tool to create the Operations View portlets within a portlet application. See Creating the Topology Portlet on page 100.
2. Use the Administrator Tool to perform initial configuration of the Operations View portlets. See Configuring the Topology Portlet on page 101.
3. Deploy the portlet application to the portal server. For information, refer to the *Operations View Administrator Guide*.
4. Use the portal server software tools to create a portal view that includes the Operations View portlets. For information, refer to the portal server software documentation.
5. In a web browser, view the portal view and customize the contained portlets. See Using the Topology Portlet on page 105.

   This is the only point at which end users can interact with the Operations View portlets. If you allow portlet customization, refer to the *Operations View Administrator Guide* for information about the scope and effects of portlet customization.
6. Use the Administrator Tool to maintain the Operations View portlet configurations. See Customizing the Topology Portlet on page 107.

Creating the Topology Portlet

Use the Administrator Tool to create the Network Node Manager Topology portlet within an existing portlet application.

To create the Topology portlet, follow these steps:

1. In the Administrator Tool, click **File**→ **New**→ **Portlet**.
2. In the Add New Portlet window, enter the following information:
   - Portlet Name: The name of the portlet as it appears in the portlet application in the scoping pane and in the portal server software tools.
   - The portlet name must be unique, start with a letter or underscore character, and consist of only alphanumeric and underscore characters.
   - Portlet Title: The name of the portlet as it appears in the portal server software tools and the portal view. Defaults to the portlet name.
   - Description (optional): The portlet description as it appears in the portal server software tools.
   - Portlet Type: Select OVNNMTopology from the list.
   - Destination Portlet Application: Select the portlet application to contain the new portlet.

   The new portlet appears in the selected portlet application in the scoping pane, and the configuration information for this portlet appears in the editor pane.

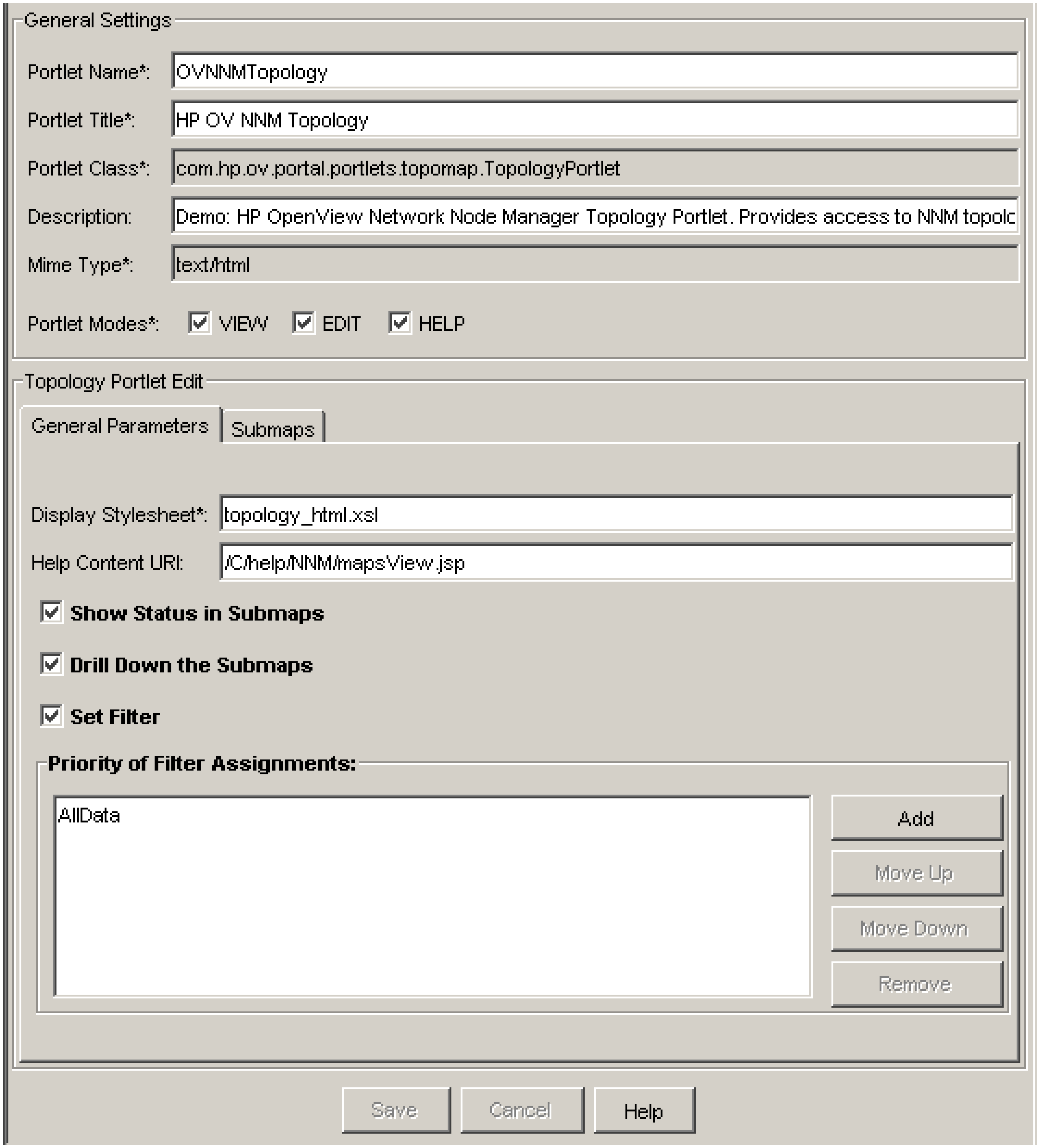
Configuring the Topology Portlet

For information on the Network Node Manager Topology portlet configuration options, click **Help** at the bottom of the editor pane to view the online help page.

To configure the default settings for the Topology portlet, follow these steps:

1. In the Administrator Tool, expand the Portlet Applications folder, expand the portlet application, and then click the name of the Topology portlet (named OVNNMTopology by default).

   The editor pane displays the configuration for this portlet as shown here.



General Settings

Portlet Name*: OVNNMTopology

Portlet Title*: HP OV NNM Topology

Portlet Class*: com.hp.ov.portal.portlets.topomap.TopologyPortlet

Description: Demo: HP OpenView Network Node Manager Topology Portlet. Provides access to NNM topolc

Mime Type*: text/html

Portlet Modes*: ☑ VIEW ☑ EDIT ☑ HELP

Topology Portlet Edit

General Parameters | Submaps

Display Stylesheet*: topology_html.xsl

Help Content URI: /C/help/NNM/mapsView.jsp

☑ **Show Status in Submaps**

☑ **Drill Down the Submaps**

☑ **Set Filter**

Priority of Filter Assignments:

AllData

2 In the General Settings area, make any desired changes.

3 On the General Parameters tab of the Topology Portlet Edit area, set the configuration options. At a minimum, specify the correct values for the Priority of Filter Assignments option. See Chapter 7, Filtering NNM Data for product-specific information.

4 On the Submaps tab of the Topology Portlet Edit area, specify the submaps to display in the portlet.

- You can name a specific NNM submap. See Specifying the Default Submaps to Display in a Topology Portlet on page 104.
- You can name a GIF image view of an NNM submap. See Specifying a GIF File Instead of a Submap on page 104

5 Click **Save**.

Specifying the Default Submaps to Display in a Topology Portlet

To add a submap to the Topology portlet using the Administrator Tool, follow these steps:

1. Configure the `ovw://`*`<NNMhostName>`*`/`*`<mapName>`*`/`*`<submap>`* path to the Submap List on the Submaps tab in the Topology Portlet Edit area. The *`<NNMhostName>`* must be the fully-qualified hostname as entered in Chapter 2, Configuring the Operations View Connection to NNM.

   ➤ If you add your submaps on the portlet edit page, the path to the submap is automatically determined.

2. The default width and height values are 550 and 400, respectively. To override these values, set the number of pixels in the Map Width and Map Height fields in the Submap List table.
3. To remove a submap from the Topology portlet, select the submap, and then click **Remove**.
4. Click **Save**.
5. Log in to the portal as the appropriate user to verify your changes.

Specifying a GIF File Instead of a Submap

To display a GIF file through the Topology portlet, use the Administrator Tool.

Use a standard URL for the Submap URL field in the Submap List table.

If only GIF files are displayed in the Topology portlet, you can ignore the following check boxes on the General Parameters tab:

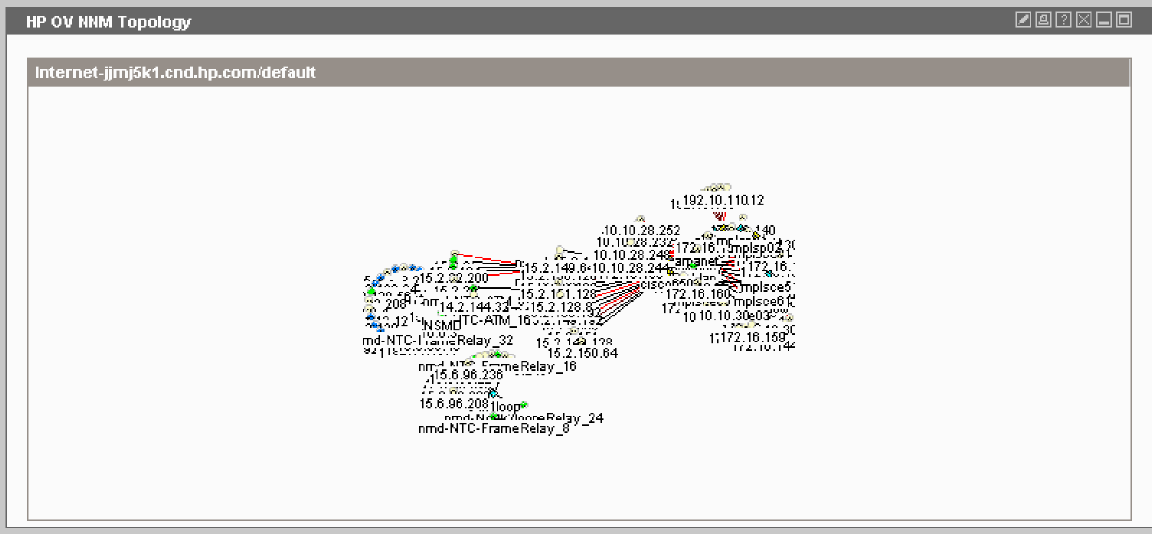
- Show Status in Submaps
- Drill Down in the Submaps
- Set Filter

Using the Topology Portlet

The Network Node Manager Topology portlet displays one or more NNM submaps. Submaps provide a graphical view of the network environment or system management information. Each submap displays a different perspective of the environment. You might be able to display another submap by clicking on a symbol; for example display a submap showing all interfaces within a router by clicking on the router symbol. Click the portlet's navigation links to return to the previous submap.

Figure 10 showns an examples Topology portlet.

Figure 10 Deployed Topology Portlet



HP OV NNM Topology

Internet-jjmj5k1.cnd.hp.com/default

Each submap that you display is associated with an NNM management station and a map. NNM management stations provide and maintain the operational SNMP/network management information.

Changes in network configuration and device status are visible in the Topology portlet submaps each time the portal view is displayed or refreshed. NNM sends the most recent information to Operations View upon demand.

Through the Operations View Topology portlet, you can display NNM-discovered nodes (objects with IP addresses or fully-qualified domain names) as well as non-NNM-discovered nodes, such as objects that were created manually (like containers or locations) or objects that were imported through use of custom applications. Non-NNM-discovered nodes are identified and filtered based on the `Selection Name` field.

Several things are important to know about the submaps displayed through the Topology portlet:

- NNM must be configured for use with the Topology portlet. For detailed information, see Enabling Topology Portlet Access to NNM Data on page 28.
- Submaps that are targeted within Topology portlets must either be currently displayed on the NNM management station or be configured as *persistent* (not *transient*) within NNM before they display in the portal. This means that the submaps must be stored in RAM on the NNM management station and not generated on-the-fly upon request.
- Submaps that are accessed through drill-down (optional behavior, default = no drill-down) might be *transient* within NNM, depending upon the global settings you choose.
- If your submaps have *auto-layout* turned off in NNM, the New Object Holding Area does not display in the portlet. You must move symbols out of the New Object Holding Area to make them visible in the portlet.
- The submaps displayed in the portlet are actually completely new redrawn versions. Outer shapes for symbols are not dynamically generated. Operations View-supported outer shapes are circle, square, diamond, hexagon and octagon. Square is the generic shape for any symbol from NNM that uses a shape that is unsupported in Operations View.

Customizing the Topology Portlet

You can modify the Topology portlet in your portal view:

1. Access the portal view by logging on to the portal as a user with access to edit portlet preferences.

   The portlet must also have the EDIT mode enabled.

2. In the title bar of the Topology portlet, click the edit button.

3. Make any desired changes. Click the help button if you need more information.

4. Set the Show Status in submap check box. All displayed submaps in this Topology portlet are affected by this symbol status setting:

   - If selected, all symbols and connection lines display their current status color from NNM.
   - If cleared, all symbols assume the NNM *administrative status* of "unmanaged" (cream colored by default). All connection lines remain black.

5. Set the Drill Down in submaps check box. All displayed submaps in this Topology portlet are affected by this setting:

   - If selected, all submaps allow drill-down access through the NNM hierarchy.

     The submaps that can be accessed through drill-down are controlled by the global settings in the `topologyConfig.xml` file. See Advanced Topic: Establishing Global Settings for All Topology Portlets on page 109 for more information.

   - If cleared, none of the displayed submaps provide drill-down access.

6. To add a submap, select the name of the NNM management station that has the submap you wish to access. The list contains all NNM management stations you configured in Chapter 2, Configuring the Operations View Connection to NNM.

7 In the Map field, type the name of the map, and then click **List Submaps**.

> ➤ Submaps must be currently displayed on the NNM management station or configured as *persistent* (not *transient*) within NNM before they are available for display in the portal. This means that the submap must be stored in RAM on the NNM management station and not generated on-the-fly upon request.

8 From the Available Submaps list, select a submap (if duplicate submap names occur in the list, verify the path displayed after the submap name).

9 Click Add. The submap name is moved to the Submaps to Display list and added to the bottom of the Displayed Submaps list.

10 To select a submap from a different NNM management station, return to Step 6, and then select the next NNM management station.

11 To adjust the order in which the submaps are displayed, in the Displayed Submaps list, select the submap name, and then click **Λ** and **V** to navigate the new submap into the correct display location.

12 To remove a submap from the Topology portlet, in the Displayed Submaps list, select the submap name, and then click **Delete**.

13 Click **OK** to save the changes and return to the main portal page.

Advanced Topic: Establishing Global Settings for All Topology Portlets

This section focuses on the following file:

- *Windows*: `<data_dir>\conf\dashboard\opview\share\portlet-config\topology\topologyConfig.xml`
- *UNIX*: `/var/opt/OV/conf/share/portlet-config/topology/topologyConfig.xml`

After you modify this file, restart the portal server. See the portal server documentation for more information.

topologyConfig.xml/dtd

There are two ways to use the Topology portlet. You can display submaps from NNM management stations (or collection stations) or you can display GIF files. The `topologyConfig.xml` file sets default settings for both of these (see the comments in the `topologyConfig.dtd` file for more information).

The following attributes control the frequency with which the Topology portlets request updated information from NNM management stations:

- `numMapRetries`
  Operations View starts checking for a specified map at port 3700. If a map is not running, Operations View increments the counter and checks on the next port. If a map was running on 3700, but not the desired map, Operations View resets the counter to 0 and checks the next port. Once the counter equals `numMapRetries`, Operations View quits searching for the requested map.
- `symbolFetchRateInMin`
  Sets the frequency (in minutes) with which Operations View contacts NNM management stations to check for changes in symbol registration files and gathers any new symbol GIF images.

The following attributes control how the submaps look and behave:

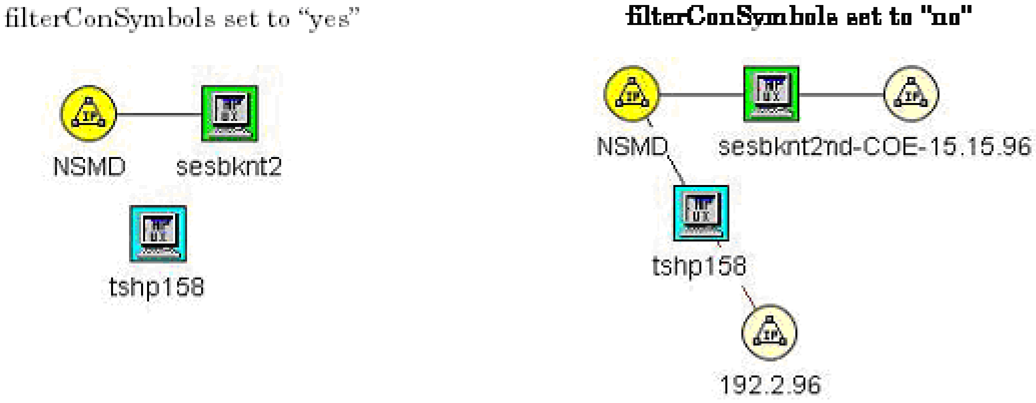
- defaultWidth & Height
  Sets the dimensions of submaps when the dimension is not specified by the submap element in the Topology portlet.
- drillDownWidth & Height
  Sets the dimensions of submaps accessed through drill-down behavior.
- loadTransientSubmaps
  Toggles drill-down access to *transient* submaps (those generated on-demand in NNM), as opposed to only allowing drill-down access to *persistent* submaps (those stored in RAM on the NNM management station) or transient submaps that are currently displayed on the NNM management station.

The following attributes control filtering for all Topology portlets. See Chapter 7, Filtering NNM Data for more information:

- defaultFilter
  - "yes": The NNM submaps are filtered according to the settings in the applicable filter assignment for the particular user.
  - "no": The filter assignment is ignored, and the submaps include all symbols that appear on the NNM management station.
- filterConSymbols
  - "yes": Only those interfaces specifically listed in any applicable InterfaceList filter element, and that passed through the current filter are displayed as connective lines in the submap.
  - "no": Connective lines representing interfaces are displayed in the portal if the node to which they are connected passes the current filter, irrespective of any limitations specified in the InterfaceList.

  Figure 11 shows example results for one submap with different filterConSymbols settings.

Figure 11 Example Results of filterConSymbols Settings



filterConSymbols set to “yes”

filterConSymbols set to "no"

6 Working with the Network Node Manager MPLS Portlet

HP OpenView Dashboard Operations View provides the Network Node Manager MPLS portlet for integrating with HP OpenView Network Node Manager (NNM).

This chapter describes how to create, configure, use, and customize the Network Node Manager MPLS portlet. For an overview of the portlet's functionality, see Chapter 1, Introduction to the NNM Integration.

The portal view development process includes a variety of tools:

1. Use the Operations View Administrator Tool to create the Operations View portlets within a portlet application. See Creating the MPLS Portlet on page 114.
2. Use the Administrator Tool to perform initial configuration of the Operations View portlets. See Configuring the MPLS Portlet on page 116.
3. Deploy the portlet application to the portal server. For information, refer to the *Operations View Administrator Guide*.
4. Use the portal server software tools to create a portal view that includes the Operations View portlets. For information, refer to the portal server software documentation.
5. In a web browser, view the portal view and customize the contained portlets. See Using the MPLS Portlet on page 119.

   This is the only point at which end users can interact with the Operations View portlets. If you allow portlet customization, refer to the *Operations View Administrator Guide* for information about the scope and effects of portlet customization.
6. Use the Administrator Tool to maintain the Operations View portlet configurations. See Customizing the MPLS Portlet on page 120.

Creating the MPLS Portlet

Use the Operations View Administrator Tool to create the Network Node Manager MPLS portlet within an portlet application that is based upon the MPLS WAR file.

To create a portlet application for the MPLS portlet and then create an MPLS portlet within that application, follow these steps:

1. In the Administrator Tool, click **Tools→ Set Portlet Application WAR File**.
2. In the Set Portlet Application WAR File window, click **Browse**, and then select the desired WAR file:

   - *Windows*:
     `<install_dir>\newconfig\dashboard\opview\opviewMPLS.war`
   - *UNIX*:
     `<install_dir>/newconfig/dashboard/opview/opviewMPLS.war`

   For more information, see Setting the Portlet Application WAR File of the *Operations View Administrator Guide*.

3. In the Administrator Tool, click **File→ New→ Portlet Application**.
4. In the Add New Portlet Application window, enter the information for the MPLS portlet application.

   For more information, see Creating a Portlet Application of the *Operations View Administrator Guide*.

5. In the Administrator Tool, click **File→ New→ Portlet**.
6. In the Add New Portlet window, enter the following information:

   - Portlet Name: The name of the portlet as it appears in the portlet application in the scoping pane and in the portal server software tools.
   - The portlet name must be unique, start with a letter or underscore character, and consist of only alphanumeric and underscore characters.
   - Portlet Title: The name of the portlet as it appears in the portal server software tools and the portal view. Defaults to the portlet name.
   - Description (optional): The portlet description as it appears in the portal server software tools.
   - Portlet Type: Select OVNNMMPLS from the list.

- Destination Portlet Application: Select the portlet application that you created in Step 4.

The new portlet appears in the selected portlet application in the scoping pane, and the configuration information for this portlet appears in the editor pane.

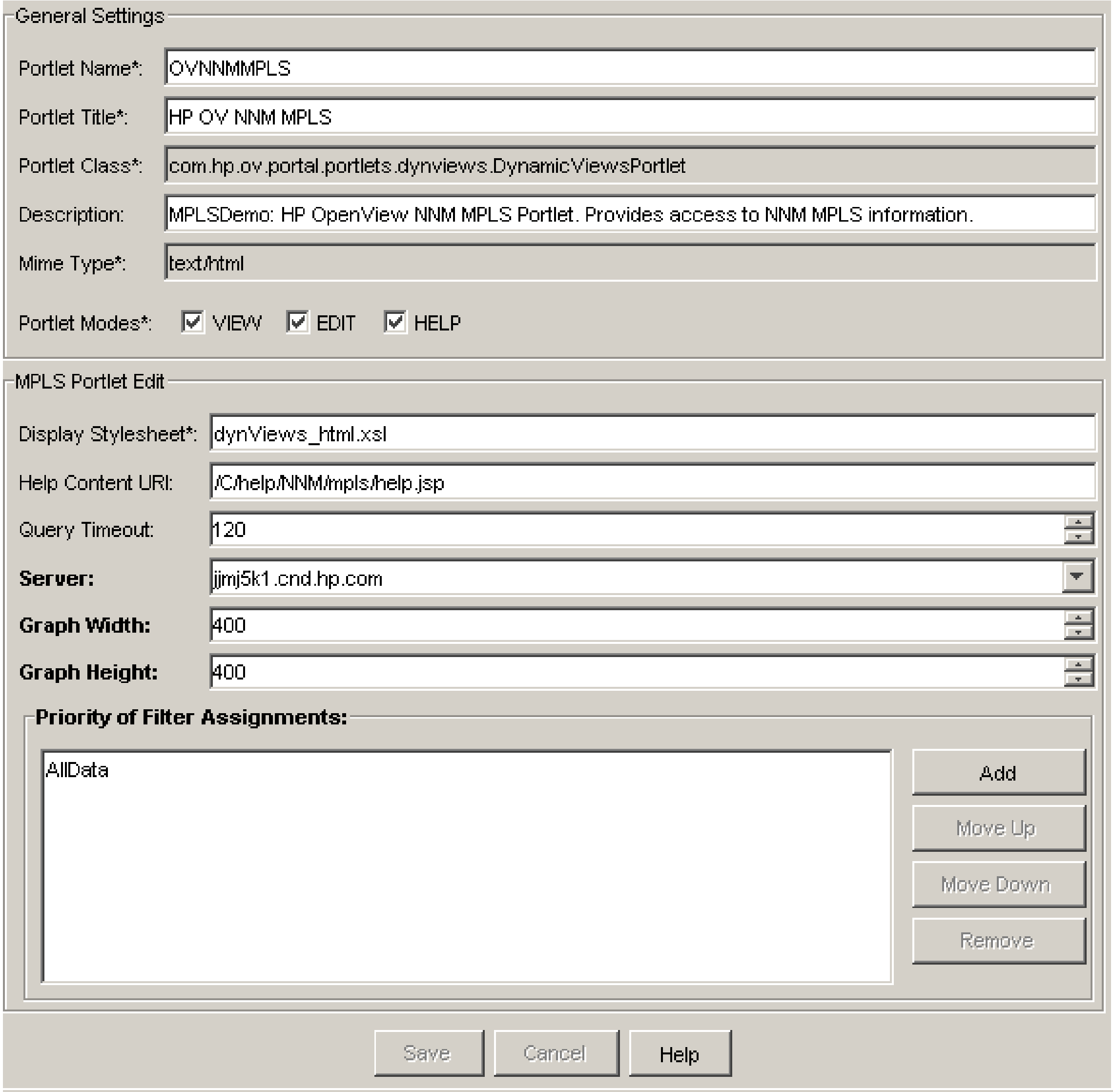
Configuring the MPLS Portlet

For information on the Network Node Manager MPLS portlet configuration options, click **Help** at the bottom of the editor pane to view the online help page.

To configure the default settings for the MPLS portlet, follow these steps:

1. In the Administrator Tool, expand the Portlet Applications folder, expand the desired portlet application, and then click the name of the MPLS portlet (named OVNNMMPLS by default).

   The editor pane displays the configuration for this portlet as shown here.



General Settings

Portlet Name*: OVNNMMPLS

Portlet Title*: HP OV NNM MPLS

Portlet Class*: com.hp.ov.portal.portlets.dynviews.DynamicViewsPortlet

Description: MPLSDemo: HP OpenView NNM MPLS Portlet. Provides access to NNM MPLS information.

Mime Type*: text/html

Portlet Modes*: ☑ VIEW ☑ EDIT ☑ HELP

MPLS Portlet Edit

Display Stylesheet*: dynViews_html.xsl

Help Content URI: /C/help/NNM/mpls/help.jsp

Query Timeout: 120

Server: jjmj5k1.cnd.hp.com

Graph Width: 400

Graph Height: 400

Priority of Filter Assignments:

AllData

2 In the General Settings area, make any desired changes.

3 In the MPLS Portlet Edit area, set the configuration options. At a minimum, specify the correct values for the following options:

- Server
- Priority of Filter Assignments: See Chapter 7, Filtering NNM Data for product-specific information.

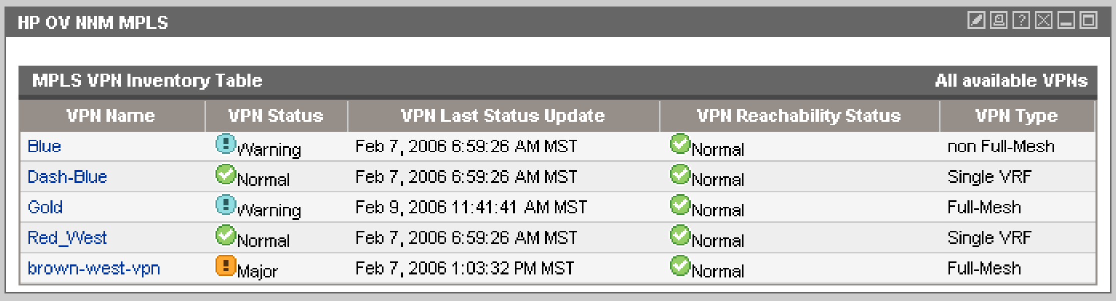
4 Click **Save**.

Using the MPLS Portlet

The Network Node Manager MPLS portlet displays one or more virtual private networks (VPNs) as managed by the NNM MPLS Smart Plug-in (SPI). Both table and graphical views of the VPN network environment is available. The information available through the MPLS portlet is a subset of the same data that is available from the MPLS information from Dynamic Views. Each VPN displays a different perspective of the environment, and can be drilled down into the most detailed information of virtual routing and forwarding (VRF) details and VRF neighbors.

Figure 12 shows an example MPLS portlet.

Figure 12 Deployed MPLS Portlet



HP OV NNM MPLS

MPLS VPN Inventory Table — All available VPNs

VPN Name	VPN Status	VPN Last Status Update	VPN Reachability Status	VPN Type
Blue	Warning	Feb 7, 2006 6:59:26 AM MST	Normal	non Full-Mesh
Dash-Blue	Normal	Feb 7, 2006 6:59:26 AM MST	Normal	Single VRF
Gold	Warning	Feb 9, 2006 11:41:41 AM MST	Normal	Full-Mesh
Red_West	Normal	Feb 7, 2006 6:59:26 AM MST	Normal	Single VRF
brown-west-vpn	Major	Feb 7, 2006 1:03:32 PM MST	Normal	Full-Mesh

The MPLS information within a portlet can be associated with a single NNM management station that has the MPLS SPI installed and configured. NNM management stations provide and maintain the operational network management information, and the MPLS portlet only provides a view into this information.

Changes in network configuration and device status are visible in the MPLS portlet each time the portal view is displayed or refreshed. NNM sends the most recent information to Operations View upon demand.

Several things are important to know about the VPNs displayed through the MPLS portlet:

- The NNM MPLS SPI must be installed and configured correctly. This can easily be determined by viewing MPLS information from Dynamic Views.
- The list of available VPNs is a filtered list. See the MPLS filtering section for additional information.

Customizing the MPLS Portlet

You can modify the MPLS portlet in your portal view:

1. Access the portal view by logging on to the portal as a user with access to edit portlet preferences.

   The portlet must also have the EDIT mode enabled.

1. Access the portal view by logging on to the portal as a user with access to edit portlet preferences.

   The portlet must also have the EDIT mode enabled.

2. In the title bar of the MPLS portlet, click the edit button.
3. Make any desired changes. Click the help button if you need more information.
4. Set the graph size. All displayed maps in this portlet are affected by this setting.
5. Select the data filter. All VPNs will be filtered in this portlet and are affected by this setting:
   - A data filter that shows all data: No data will be filtered and all information will be presented.
   - A data filter is that shows no data: No data will be presented.
   - A data filter is that shows a limited set of data: Data will be filtered and limited to the set of VPNs set within the data filter.
6. Click **OK** to save your changes and return to the main portal page.

7 Filtering NNM Data

The HP OpenView Dashboard Operations View customer model allows you to associate resources (nodes and interfaces) with users so that data is automatically filtered appropriately when the user displays any of the Network Node Manager portlets.

Before you proceed, decide for which groups you need to filter data. For example, you might need to provide portals for several divisions within your company: accounting, marketing, R&D, legal, support. You could assign lists of nodes and/or interfaces to each of these groups. Because of the assigned resource lists, each of these groups could view the same instance of an Alarm portlet, Network Health portlet, or Topology portlet, yet see only the data appropriate for them.

With the exception of the interface health gauge in the Network Health portlet, this process is *optional*. If you do not want to use the interface health gauge in the Network Health portlet and you do not want to filter data by user, specify `AllData` for the filter assignment. Refer to the *Operations View Administrator Guide* for more information about how filter assignments are assigned to particular users.

The remainder of this chapter explains how to create node lists, interface lists, and topology object lists for use in your organization definitions.

The following list specifies the type of lists that affect each Network Node Manager portlet:

- Alarms portlet
  - Node list: Only those alarms from nodes that pass through the management data filter are displayed.
  - Interface lists are ignored.
- Network Health portlet
  - Node list: Only those nodes that pass through the management data filter are included in the health calculation.

  - Interface list: For interface-oriented gauges (such as Interface Health), only those interfaces that pass through the management data filter are included in the health calculation.

- Topology portlet
  - Node list: Only those nodes that pass through the management data filter are displayed on submaps.
  - Interface list: Only those interfaces that pass through the management data filter are displayed on submaps (as connection lines).
  - Topology object list: Only those objects that are identified by selection name pass through the management data filter are displayed on submaps.

- MPLS
  - VPN List: Only the VPN names listed are displayed in the MPLS portlet.

Windows: `<data_dir>\conf\dashboard\opview\share\organizations\SimpleCustomerModel.dtd`

UNIX: `/var/opt/OV/conf/dashboard/opview/share/organizations/SimpleCustomerModel.dtd`

Your node lists, interface lists, topology object lists, and VPN lists can be defined in one or more customer model sources. The Operations View Administrator Tool simplifies the process of defining filters, including an NNM-specific customer model source that can automatically generate node lists and interface lists by gathering the required data from the NNM object database. To define a topology object list or a VPN list, you must manually create the elements. This chapter explains multiple options. These approaches are not mutually exclusive and can be used in combination:

- Creating Node Lists, Interface Lists, Topology Object Lists, and a VPN List on page 124

  Use the Administrator Tool to define lists of nodes, interfaces, and non-NNM-discovered objects (topomap objects) within your NNM management station's network environment.

- Using Customer Views Organization Data on page 129

This CGI program works only if HP OpenView Customer Views is installed and configured on your NNM management station. If you are using Customer Views, you already defined a customer model and can export that information dynamically for use in the Operations View customer model. Use the supplied CGI program to dynamically output the Customer Views customer model data as valid XML.

- Advanced Topic: Configuring Operations View to an Exported Copy of the Customer Model on page 133

  This CGI program works only if HP OpenView Customer Views is installed and configured on your NNM management station. If you are using Customer Views, you already defined a customer model. Use the supplied CGI program and save the output locally to perform a one-time migration of your Customer Views customer model to an XML file. Essentially, this gives you a one-time snapshot of the Customer Views customer model to be used as a starting point for your Operations View customer model. Use this approach if you want to leverage the NNM Customer Views customer model, but also want the flexibility to make changes.

  By using a combination of the provided CGI programs and manually created XML files, you can leverage Customer Views mappings and expand upon them to include non-IP interfaces (for example, switch ports, not supported by Customer Views).

- Dynamically Gathering NNM Node and Interface Data on page 136

  Use the supplied NNM customer model source to dynamically generate lists of nodes and interfaces from the NNM object database. Use this approach if you want to retrieve information from the NNM object database (ovwdb) and automatically return XML content for the Operations View customer model. The generated node lists and interface lists are formatted according to the SimpleCustomerModel.dtd.

- Advanced Topic: Defining a Custom Customer Model Source

  Create your own program (CGI or servlet) to generate a mapping from an arbitrary data store or provisioning system, and express it in XML that conforms to the SimpleCustomerModel.dtd. Refer to the *Operations View Administrator Guide* for information.

Creating Node Lists, Interface Lists, Topology Object Lists, and a VPN List

The Operations View customer model allows you to associate lists of resources to an organization. This section explains how to create lists of nodes, lists of interfaces, and lists of topology objects specifically for use with the Network Node Manager portlets. You can use customer model source, or you can create multiple customer model sources containing the various organizations. Your list elements can be inserted into organization definitions directly or by reference. Insertion by reference is useful when you want to use one list in multiple locations.

Customer-to-Node Mappings

To create a node list be associated with an organization in your customer model, perform the following configurations on the NNM management station and the Operations View server.

The OVO Messages portlet that communicates with HP OpenView Operations (OVO) also responds to node lists. If this sharing causes a problem, you can use two organizations. Optimize one organization's node list for the Network Node Manager portlets and the second organization's node list for the OVO Messages portlet. Refer to the *Operations View Integration Guide: OVO and OVSN* for more information.

On the NNM Management Station

If you do not already know the fully-qualified hostname or IP address of the nodes to use in your node lists, do one of the following to gather that information:

- Examine one or more NNM submaps.
- Use NNM's **Edit→ Find→ Object by Attribute** feature.
- Examine NNM's Inventory Report (accessed through the NNM Report Presenter).
- Use the NNM `ovobjprint` command. See the *ovobjprint* reference page in NNM's online help (or the UNIX manpage) for more information.

- Use the `ovtopodump` command. See the *ovtopodump* reference page in NNM's online help (or the UNIX manpage) for more information.

On the Operations View Server

1. With the organization selected, create a node list for each group of nodes. If you want to use this list in multiple organizations, give it a name that you can reference later when you are assigning node list references to another organization.
2. *Required*: For each node in this node list, enter either a fully-qualified hostname or IP address into the Name field.
3. Click **Save**.

You are now ready to associate the node lists with other organizations in your customer model, as appropriate.

Customer-to-Interface Mappings

To create an interface list that can be associated with an organization in your customer model, perform the following configurations on the NNM management station and the Operations View server.

On the NNM Management Station

For each interface, gather one of the following:

- IP-address
- `hostname/ifAlias::ifDescr`
  - hostname: The fully-qualified hostname or IP address.
  - ifAlias: The alias from the SNMP IF-MIB (rfc2863).
  - ifDescr: The first word in SNMP MIB-II (rfc1213) ifDescr string.

➤ Either `ifAlias` or `ifDescr` can be empty, but the combination must uniquely identify the interface.

To determine the required information for your interface lists, do one of the following:

- Examine one or more NNM submaps. Right-click on an interface symbol, and then click **Interface Properties**. The address, ifAlias, and ifDescr values are displayed.
- Use NNM's **Edit**→ **Find**→ **Object by Attribute** feature.
- Examine NNM's Inventory Report (accessed through the NNM Report Presentor).
- Use the NNM `ovobjprint` command. See the *ovobjprint* reference page in NNM's online help (or the UNIX manpage) for more information.
- Use the `ovtopodump` command. See the *ovtopodump* reference page in NNM's online help (or the UNIX manpage) for more information.

On the Operations View Server

1. In the scoping pane of the Administrator Tool, expand the Data Filters folder, expand the Customer Model Sources folder, expand the appropriate customer model source, and then select the organization to modify.
2. Create an interface list for each group of interfaces. If you want to use this list in multiple organizations, give it a name that you can reference when you are assigning interface lists to another organization.
3. *Required*: For each interface that needs to be included in this interface list, select the correct type. (The default type is ov-ipv4.) See On the NNM Management Station on page 125 for more information.

You are now ready to associate these interface lists with other organizations in your customer model, as appropriate.

Customer-to-Topology Object Mappings

To create topology object lists that can be associated with an organization in your customer model, perform the following configurations on the NNM management station and the Operations View server.

On the NNM Management Station

If you do not already know the selection names of the objects to use in the topology object lists, do one of the following to gather that information:

- Examine one or more NNM submaps.

- Use NNM’s **Edit→ Find→ Object by Selection Name** feature.
- Examine NNM’s Inventory Report (accessed through the NNM Report Presenter).
- Use the NNM `ovobjprint` command o print the selection names of all objects in the NNM database, specifying fields to filter on, such as `"isLocation=TRUE"`. See the *ovobjprint* reference page in NNM’s online help (or the UNIX manpage) for more information.

On the Operations View Server

1 Create a topology object list for each group of non-NNM-discovered objects. If you want to use this list in multiple organizations, give it a name that you can reference later when you are assigning topology object lists to another organization.

2 *Required*: For each object in a topology object list, verify that the `type` attribute is set to `Selection Name`, and then enter the object name assigned to the Selection Name field as the `name` attribute.

You are now ready to associate these topology object lists with other organizations in your customer model, as appropriate.

Customer-to-VPN Mappings

To create a list of VPNs that can be associated with an organization in your your customer model, perform the following configurations on the NNM management station and the Operations View server.

On the NNM Management Station

If you do not already know VPN names to use in your VPN list, follow these steps to gather that information:

1 Start NNM Dynamic Views and access the MPLS VPN View from Home Base.

2 Use the initial MPLS VPN Inventory table to view the list of VPNs. Use the names in the VPN Name column to use in the filtering steps below for Operations View.

On the Operations View Server

1. In the scoping pane of the Administrator Tool, expand the Data Filters folder, expand the Customer Model Sources folder, expand the appropriate customer model source, and then select the organization to modify.
2. For each VPN to filter for your organization, type the VPN name exactly as it appears in the Dynamic Views client. The filtering for VPNs is case-sensitive.
3. Click **Save**.

Using Customer Views Organization Data

Through use of a Customer Views-supplied CGI program, you can dynamically gather customer model data from one or more remote Customer Views servers. This program, `getcvdata.exe`, returns a complete Operations View customer model. That is, the data in the Customer Views database is exported to XML mappings that are complete and conform to the customer model data format.

Configure NNM Customer Views

The `getcvdata.exe` program is called from the Operations View server. The `getcvdata.exe` program gathers information from your Customer Views database (assuming that NNM Customer Views is configured and running on your NNM management station) and provides Operations View with a customer model source.

In the context of Customer Views, the term “organization” refers to the organizations you defined within NNM Customer Views and includes both “customers” and “providers.”

If your Customer Views program is configured for your “customers” and “providers,” go to Configure Operations View to Use getcvdata.exe on page 131.

If you have not already configured Customer Views, perform the tasks listed here. The commands for doing so are described in Table 13 on page 130. For detailed information, see the documentation that comes with Customer Views.

1. On the NNM management station, start Customer Views.
2. Create organizations.
3. Associate nodes with organizations.
4. Associate interfaces with organizations.

The `ovcustomer` command can be run interactively or in batch mode. To run the `ovcustomer` command in interactive mode, run the `ovcustomer` command and then enter specific commands at the “`ovcustomer>`” prompt. Shown below are the relevant `ovcustomer` commands:

Table 13 ovcustomer Commands

Action	Command
Create a new organization.	`ovcustomer>`**`create_org <organizationType> <organizationName>`** "customer" and "provider" are supported values for *organizationType*. An organization name with spaces should be placed in quotes (for example, `"My Customer"`).
Print the list of organizations.	ovcustomer>**print_org**
Associate a node with an organization.	ovcustomer>**add_associations_to_org <*organizationName*> <*Hostname*>**
Print the nodes associated with a specific organization.	ovcustomer>**print_associated_node <*organizationName*>**
Associate an interface with an organization.	ovcustomer>**add_associations_to_org <*organizationName*> <*IPaddress*>**
Print the interfaces associated with a specific organization.	ovcustomer>**print_associated_interface <*organizationName*>**

Configure Operations View to Use getcvdata.exe

1. In the Administrator Tool, import `getcvdata.exe` as a customer model source. Use the following URL. If you add the `?Organization=orgName` string, you can query Customer Views for the data about one particular organization:

    - If your NNM management station is running on *Windows*:

```
http://<NNMHostname>/OvCgi/getcvdata.exe
http://<NNMHostname>/OvCgi/getcvdata.exe?Organization=orgName
```

    - If your NNM management station is running on *UNIX*:

```
http://<NNMHostname>:8880/OvCgi/getcvdata.exe
http://<NNMHostname>/:8880/OvCgi/getcvdata.exe?Organization=orgName
```

Refer to the *Operations View Administrator Guide* for more information.

> When collecting data from Customer Views that is running in a language other than English, set the locale using the `AcceptLang` and `&Developer` CGI parameters (both are required):
>
> `http://host/OvCgi/getcvdata.exe?AcceptLang=ja&Developer`
>
> The value of `AcceptLang` is a Web locale. NNM converts the web locale to an operating system locale by using the locale mapping table in: `<NNM_install_directory>/www/conf/locales.mapping`.
>
> For example, the `AcceptLang` value `ja` translates into the locale `ja_JP.SJIS`.

`getcvdata.exe` supports the following parameters:

- *Organization*: Generates information for only one specified Customer Views organization.

  `Organization="orgname"`

- `OrgList`: Generates a list of all the organizations and their attributes: `name`, `type`, and `ExternalKey`. Not including child information (nodes, interfaces, and services).
- `?AcceptLang` and `&Developer`: When Customer Views is running in a language other than English.

- null: When no attributes are specified, `getcvdata` returns all information for all the customers in the Customer Views database.

2 If you configure Operations View to call `getcvdata.exe` from multiple Customer Views servers, import each one as a customer model source.

3 To verify that `getcvdata.exe` is working as expected, in the Customer Model Sources folder in the scoping pane of the Administrator Tool, select the data source that you just imported, and then view the contents.

You are now ready to associate these organizations in your customer model with filter assignments for specific users, as appropriate. Refer to the information about managing filter assignments in the *Operations View Administrator Guide*.

Advanced Topic: Configuring Operations View to an Exported Copy of the Customer Model

The `getcvdata.exe` program is automatically installed with NNM 6.2 or greater. This program generates an XML file of the data from each Customer Views database. Each XML file is a complete Operations View customer model mapping that conforms to the customer model data format.

On the NNM Management Station

The `getcvdata.exe` program gathers information from your Customer Views database (assuming that NNM Customer Views is configured and running on your NNM management station) and generates an XML file of organizations and their associated nodes and interfaces in the format required by Operations View.

In the context of Customer Views, the term “organization” refers to the organizations you defined within NNM Customer Views and includes both “customers” and “providers.”

If you have not already configured Customer Views, do so before proceeding (see Configure NNM Customer Views on page 129). For detailed information, see the documentation that comes with Customer Views.

To generate an XML file of the information in your Customer Views database, on the NNM management station:

1 At the command prompt, type:

- *Windows*: **<*NNM_install_dir*>\www\cgi-bin\getcvdata.exe > C:\temp\*uniqueFileName*.xml**
- *UNIX*: **/opt/OV/www/cgi-bin/getcvdata.exe > C:/temp/*uniqueFileName*.xml**

This command returns all information for all the customers known by the Customer Views server.

> ➤ When collecting data from Customer Views that is running in a language other than English, make sure that you save the new XML file in the UTF-8 codeset before placing the file on the Operations View server. See Running in Languages Other Than English on page 45 for more information.

2 Copy the `uniqueFileName.xml` file or files that you just created over to the Operations View server. Place these XML files in the following directory:

- *Windows*: `<data_dir>\conf\dashboard\opview\share\organizations`
- *UNIX*: `/var/opt/OV/conf/dashboard/opview/share/organizations`

> ➤ You can create subdirectories to contain your XML files within the organizations directory.

On the Operations View Server

1 Open each `uniqueFileName.xml` file that you created in On the NNM Management Station on page 133.

The first line within each generated XML file is a reference to the location of the `SimpleCustomerModel.dtd` file. Your XML file is not valid unless the path to its governing `DTD` file is correctly listed at the top of the file. Enter the appropriate information as explained in the following example of a DTD reference in XML file located in the `organizations` directory:

```
<!DOCTYPE SimpleCustomerModel SYSTEM "SimpleCustomerModel.dtd">
```

2 Validate the syntax of your XML files. Refer to the *Operations View Administrator Guide* for information on the `ovopviewxmlvalidate` tool provided with Operations View.

3 Import the XML file as a customer model Source in the Administrator Tool. Refer to the *Operations View Administrator Guide* for information.

You are now ready to associate these organizations in your customer model with filter assignments for specific users, as appropriate. Refer to the information about managing filter assignments in the *Operations View Administrator Guide*.

Dynamically Gathering NNM Node and Interface Data

Through use of a supplied NNM-specific customer model, you can dynamically gather node and interface lists from the NNM object database (`ovwdb`) of one or more NNM management stations. The data generated by the NNM simple customer model is a partial customer model. Essentially, the generated content consists of node lists and interface lists that can be mapped to the organizations defined in your customer model files.

These lists of nodes and interfaces are generated every 10 minutes and are stored in memory on the Operations View server. You place references to these lists in your organization definitions.

Configure the NNM Simple Customer Model

1. In the scoping pane of the Administrator Tool, expand the Portlet Shared Configurations folder, expand the HP OpenView Network Node Manager folder, and then select NNM Simple Customer Model.
2. Select the NNM management station to query from the Hostname list.

   Verify that the OVwDB Port field is configured correctly for communicating with this NNM management station. (See Chapter 2, Configuring the Operations View Connection to NNM for more information).
3. Click **Add** near the top of the editor pane.
4. In the Add New Simple Customer Model Filter window, type the name for the list to be generated and select whether this is a node or interface list.

   The name you type will be used in the organizations that refer to this list.
5. Enter the desired query specifications on the Node Selection or Interface selection tab, depending on the filter type you selected in Step 4.

   Each query serves as a filter that is applied to the NNM object database (ovwdb). The filter specifications define which nodes and interfaces are returned.

   Decide how your filter is defined. You can use any combination of two kinds of filtering:

   - **Perl regular expression-based filtering**. Use Perl5 regular expressions within `IPHost Filter` or `IPInterface Filter` sections.

When writing filters, use Perl5 regular expressions. For example: `.*\.eagle\.wingnuts\.com`

See **www.perl.com** or **www.perldoc.com** for information about Perl5 regular expressions.

- **Capability filtering**. The capability filter commonly refers to the NNM capability filters such as `isRouter`, `isNode`, and so forth. However, a capability filter can utilize *any* NNM object database field within the NNM object database (ovwdb).

  An empty capability filter yields the empty set, which allows nothing to pass.

  — To generate a complete list of the currently defined ovwdb *fields*, at the command prompt on the NNM management station, type:

  ```
  ovobjprint -f > filename
  ```

  — To identify the valid *values* for a particular field, at the command prompt on the NNM management station, type:

  ```
  ovobjprint -a "field_name" > filename
  ```

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

6 For node lists: Input all node selection criteria to which your customer model organization definitions refer. The returned node lists are ready to reference within the customer model. You have two choices within a node list: IPHost Filter or Capability Filter.

The IPHost Filter filters upon hostname. You can use Perl5 regular expressions such as: `.*\customer1\.com`

The Capability Filter can utilize *any* field within the NNM object database (ovwdb). If no value is specified, the value is assumed to be true. This approach can be useful for using capabilities such as `isServer`.

7 For interface lists: Input all interface selection criteria to which your customer model organization definitions refer. The returned interface lists are ready to reference within the customer model. Interface filters have one selection criterion available that can use Perl5 regular expressions such as: `*.\.112\.*.*`

> ➤ The NNM simple customer model only supports interface lists consisting of IP addresses. If you need to use the non-IP address interface format, manually create this list in your customer model. See Creating Node Lists, Interface Lists, Topology Object Lists, and a VPN List on page 124.

8 To verify that `getcvdata.exe` is working as expected, in the Customer Model Sources folder in the scoping pane of the Administrator Tool, select the NNM Simple Customer Model data source, and then view the contents.

You are now ready to associate these node lists and interface lists with organizations in your customer model, as appropriate. Refer to the *Operations View Administrator Guide* for information.

8 Troubleshooting the NNM Integration

General

Certain Portlets Take a Long Time to Display Data

Certain portlets require significant initial load times because a large amount of data is passed over the network when the portlet is first accessed. As a result, the first person displaying these portlets experiences the longest delay. To enhance your end user's experience, any time the portal server is restarted, log in to the portal and open any portal view that contains one or more of the following portlets:

- Network Health
- Service Graph
- Service Browser
- Service Health
- Service Card

If you open the portal view after the portal server startup, the required information is already cached when your users access their portals. Your users won't experience the delay. It is not necessary to perform a log in for each portal user. A single log in, viewing the above listed portlets, is sufficient.

Network Node Manager Portlets Do Not Display Data

One of the NNM management stations (that Operations View gathers data from) might be in the early phase of an NNM backup procedure.

Wait for NNM's backup to proceed beyond the ovpause state. The portlets display when the NNM management station issues an ovresume command. If the browser time-out limit is exceeded while you are waiting, you must click **Refresh** to display the portlets.

Alarms Portlet

The Portal Does Not Display Alarms Data

Possible Cause A:

Alarm categories can be configured to filter alarms in a number of ways. If you implement a capability filter within an alarm category's node selection definition, the Alarms portlet has a dependency upon NNM's ovwdb process.

The portal might not be communicating with ovwdb.

Solution A:

Restart ovwdb on the target system by using the ovstart command.

Possible Cause B:

The portal might not be communicating with `ovalarmsrv`.

Solution B:

1 Use the ovstatus command to validate the status of ovalarmsrv.

2 Restart ovalarmsrv, if necessary, by issuing the ovstart command.

3 Try to communicate directly with ovalarmsrv:

   a **`telnet`** ***`<NNMStationName> <ovAlarmsSrvPort>`***

   b In the telnet window, type: **`0:0:CATEGORIES:TestUser`**

   c If you get a response, the ovalarmsrv process is running.

   d In the telnet window, type **`6`** to end communications.

Possible Cause C:

Invalid port configured for ovalarmsrv.

Solution C:

1 If the port number configured for an NNM system is invalid, the alarm portlet will not be able to obtain alarms for display from this system. Check which port each NNM station is communicating with. The port that the bits respond on depends on the entries in the services file.

On UNIX, the `services` file resides in `/etc/services`. `Ovalarmsrv` has two entries: `ovalarmsrv` and `ovalarmsrv_cmd`. The value that is set in the file determines which port `ovalarmsrv` runs on. (The same is true of `ovwdb.`)

On Windows, the `services` file resides in `WINNT\system32\drivers\etc\services`.

1. Modify the entry or entries for management stations in the Administrator Tool, as necessary, to match what you find.
2. Refresh the portal view.
3. If you still do not see data, verify that you are communicating with `ovalarmsrv` on each NNM station listed in the Administrator Tool by completing step 3 in the solution to Possible Cause B.

Possible Cause D:

Specified NNM stations do not match those in the Administrator Tool.

Solution D:

Resolve the differences by editing the alarm category definition and the management station configurations in the Administrator Tool.

Possible Cause E:

Alarms categories defined in the portlet preferences do not match the configured alarm categories.

Solution E:

Make sure they match, using the Administrator Tool for default portlet preferences and the portlet edit page for Alarms portlets (if they have been modified from the default values).

Possible Cause F:

Base categories used in alarm category definition file not valid for the given NNM station.

Solution F:

Make sure you are using valid NNM base categories for the stations you are connecting to.

Possible Cause G:

No data passed filters.

Solution G:

Check the filter assignments defined for this user. A user can access the portlet edit page to view the current filter assignments.

Check any substring match, Older Than X Minutes sevs, acks, or node selection filters defined for this category.

Possible Cause H:

No NNM stations configured in the Administrator Tool.

Solution H:

- Make sure stations are listed.
- Make sure the correct `ovAlarmSrvPort` is listed.
- Make sure `alarmsDataSource` is set to yes.

Possible Cause I:

Time-out values are too short.

Solution I:

See The Portal Does Not Display a Specific Alarm Category on page 143

Possible Cause J:

The configured NNM stations do not have Use As Alarm Data Source enabled.

Solution J:

Make sure that the Use As Alarm Data Source field is set to yes.

The Portal Does Not Display a Specific Alarm Category

Possible Cause A:

Time-out values are too short.

Solution A:

1 Modify the following attributes in the Administrator Tool. More information about these attributes is available in Establishing Global Settings for Alarms Portlets on page 58:

- Maximum Number of Connections: The maximum number of (socket) connections that a portal server is allowed to establish with all NNM management stations it needs to communicate with, for gathering alarm information.
- Connection Time Out (seconds): The number of seconds to pause after each socket connection is opened.
- Additional Time for Synchronous Call (seconds): The number of seconds to add to the time out when making a synchronous call to get data from the ovalarmsrv process on each NNM management station.
- Socket Time Out (seconds): The number of seconds to wait for a socket connection to be made.
- Ovalarmsrv Reply Time Out (seconds): The number of seconds to wait each time for any response (protocol or data) from ovalarmsrv.
- Maximum Ovalarmsrv Wait Time (seconds): The maximum number of seconds to wait for a data response from ovalarmsrv.

2. Refresh the portal view.

SNMP Data Collection

Data Collection Configuration Did Not Get Updated to Reflect Changes in Gauge Definitions or Customer Model Configurations

Symptom:

The expected data collection did not happen for devices added to a network health gauge by expanding the filters or adding or creating a new gauge. Or, the expected data collection did not happen after changing or adding a configuration for a particular organization in the customer model.

Possible Cause:

- Automatic data collector configuration might not have been enabled on the NNM stations.
- The `ovcolautoconf` program might not have run since you made the change. NNM's SNMP data collection configuration is updated by this program.
- The Network Health portlet containing this gauge definition has never been displayed.
- The Network Health portlet has not been displayed within the last 30 days. `ovcolautoconf` removes configuration entries for data that has not been requested within the last 30 days. (30 is the default and can be overwritten with the `-maxConfAge` option on `ovcolautoconf`.)
- Operations View might not yet have sent its configuration requests to the NNM stations.
- `ovcolautoconf` might be experiencing errors.

Solution:

1. Enable `autoDCConfig` if it is not already enabled. See The Data Collection Process for the Network Health Portlet on page 38 for information.
2. Display the Network Health.
3. Wait ten minutes.
4. Run ovcolautoconf. At the command prompt on the NNM systems, type: `ovcolautoconf -verbose`.(You might wish to run this command as a scheduled task.) Note that for UNIX `/opt/OV/bin` must be in your path.

Collected data generally appears within a half hour of executing this command.

Any network device that you want to be included in the SNMP data collection process must be a *managed* device within the NNM topology database, and NNM must know the correct SNMP GET community name for that device before the device will be included in the SNMP data collection process.

For information about the steps required when Operations View requests SNMP data from NNM, see the The Data Collection Process for the Network Health Portlet on page 38 and Data Collection for Network Health Gauges on page 88. Verify that each step of the process is working correctly.

For other possible causes and solutions, see Error: “Data unavailable” in Details Table for All Scores Except Interface Status on page 150.

NNM Data Collector Files of Operations View Information Are Not Being Trimmed

Symptom:

NNM’s snmpCollect database is growing without bound.

Possible Cause:

No steps have been taken to trim the NNM snmpCollect database.

Solution:

See the NNM manual *Managing Your Network with NNM* or Monitoring the Size of NNM’s snmpCollect Database on page 40 for information on how to trim data in the snmpCollect database.

ExtraneouS Data Collections Are Being Gathered for Network Health Gauges

Symptom:

When I check the file `snmpRepPrev.conf`, there are entries for devices for which I do not want to collect data.

Possible Cause A:

Are you collecting more data than you need? Check each customer model source definition. Check your network health filter specifications within each gauge definition compared to the filter specifications in your customer model source definitions.

Solution A:

As necessary, modify the customer model sources and/or the node selections and interface selections in the configuration for each gauge.

Possible Cause B:

The unwanted entries might have been added at an earlier time, but due to Operations View configuration changes, they are no longer needed.

Solution B:

By default, `ovcolautoconf` removes configuration entries that have not been needed for 30 days. Run `ovcolautoconf`, using the `-maxConfAge` option if desired, to remove younger entries. Seeovcolautoconf.exe on page 96.

Network Health Portlet

Error: "Currently not configured" Instead of Gauge

Symptom:

No data is displayed in the gauge. The "Currently not configured" error message appears instead.

Possible Cause A:

No NNM stations are configured in the Administrator Tool, or there are no NNM stations configured with the `snmpDataSource` attribute set to "yes."

Solution A:

Make sure there is at least one NNM station entry in the Administrator Tool with the `snmpDataSource` attribute set to "yes."

Possible Cause B:

The combination of the filter assignments and the gauge's node selection or interface selection results in no filtering. In other words, all nodes/interfaces pass the filters. Computation on *all* nodes/interfaces is not supported. See the log file for specific error messages.

Solution B:

Limit the number of devices that pass the gauge's filters by doing one or more of the following. For more information about filters, see Filtering Possibilities for Network Health Gauges on page 77:

- Narrow the filter assignment for this user.
- In the configuration for the gauge, narrow the node selection or interface selection filter.

Error: "Managed objects not found" Instead of Gauge

Symptom:

No data appears in the gauge. The "Managed objects not found" error message appears instead.

Possible Cause A:

The combination of the user's filter assignment and the gauge's node selection or interface selection filter settings are so restrictive that no network devices can pass. An entry will be logged to the log file, such as "No Nodes found for health summary category <*category name*>" or "No Interfaces found for health summary category <*category name*>".

This is most likely to occur with Key Device Health, CPE Health, and Server Health.

Solution:

In NNM, select `Edit->Find->Object By Attribute` to determine if there are any devices with the specified capability set to true (`isKeyDevice`, `isCPE`, `isServer`). If such nodes exist, do they pass the user's filter assignment? If the desired capability is not set for one or more nodes, see *Managing Your Network with NNM* for information about how to set NNM object capabilities for the various network devices.

If necessary, modify the organizations specified in the filter assignment and/or modify the node selection or interface selection filter in the configuration for the gauge. For more information, see Filtering Possibilities for Network Health Gauges on page 77.

Possible Cause B:

An NNM station entry in the Administrator Tool is incorrectly specified.

Solution B:

Verify that the `ovwdbPort` attributes specified in the Administrator Tool are correct. For more information, see the online help in the Administrator Tool or On the Operations View Server on page 35.

Error: "Data currently unavailable" Instead of Gauges

Symptom:

No data appears in any gauge. The "Data unavailable" error message appears instead.

Possible Cause A:

The log file contains a detailed message about the problem. There might be a configuration error in the gauge. (For example, the href for a health Element might be invalid.)

Solution A:

Check the log file for a detailed message about the problem.

Possible Cause B:

The `hostname` or `webSrvPort` attributes in the Administrator Tool might be incorrectly specified.

Solution B:

Verify that the `hostname` and `webSrvPort` attributes are correct. See the online help in the Administrator Tool or On the Operations View Server on page 35 for more information.

Error: "Data unavailable" in Details Table for All Scores Except Interface Status

Symptom:

"Data unavailable" appears instead of data in the detail tables.

Possible Cause A:

The NNM SNMP Data Collector might not be configured to collect the data needed by Operations View.

Solution A:

See Data Collection Configuration Did Not Get Updated to Reflect Changes in Gauge Definitions or Customer Model Configurations on page 145 and The Data Collection Process for the Network Health Portlet on page 38.

Possible Cause B:

NNM might not be able to contact the nodes in question via SNMP.

Solution B:

In NNM, highlight the node, and select `Tools->SNMP MIB Browser` and walk the MIB2 interfaces group to see if the node is responding to SNMP requests. If it is not responding, there are several possibilities:

- The node might be down. Does the Interface Status column show "Down"? Does the node respond to ping?

- NNM might be using the wrong SNMP GET community string for the node. In NNM, select `Options->SNMP Configuration` to determine what community string NNM is using for the node. If you change one of these, while logged in as `root` or administrator, at the command prompt, type **`snmpCollect -C <`*`nodename`*`>`**
- The node's SNMP agent is not up or not responding.

Possible Cause C:

Network Node Manager is having problems with the SNMP data collection process.

Solution C:

Run **`ovstatus-c snmpCollect`** on NNM to verify `snmpCollect` is running. See NNM log file `../log/snmpCol.trace` on the NNM system.

Possible Cause D:

By default, the Operations View health gauges only use data up to 1 hour old. Perhaps the data is too old to be considered "near real-time" by network health.

Solution D:

To increase the acceptable age for SNMP data, increase the value of the Maximum Age attribute in the health metrics configuration section (the value represents minutes). This setting affects all gauges in all portlets.

Possible Cause E:

Did you enable automatic data collection configuration on the NNM station? If so, did you edit the `snmpRepAuto.templ` file directly? If there is a syntax error in this file, the data collection process will fail.

Solution E:

If the problem arose after you edited the `snmpRepAuto.templ` file, restore the `snmpRepAuto.templ` file to its last working state and following the directions in `snmpRepAuto.templ` when making changes.

Error: "Data unavailable" on One Row of Details Table (for a Particular Node or Interface)

Symptom:

“Data unavailable” appears in the detail tables.

Possible Cause A:

NNM might not be able to contact the node in question via SNMP.

Solution A:

For single MIB values, in NNM highlight the node, and select `Tools->SNMP MIB Browser`. Walk the MIB2 interfaces group to see if the node is responding to SNMP requests. For collections on MIB expressions, in NNM go to `Options->Data Collections & Thresholds:SNMP`, highlight the collection in question, and choose `Actions->Test SNMP`.

If it is not responding, there are several possibilities:

- The node might be down. Does the `Interface Status` column show `Down`? Does the node respond to ping?
- NNM might be using the wrong SNMP GET community string for the node. In NNM, select `Options->SNMP Configuration` to determine what community string NNM is using for the node. If you change one of the community strings and want to immediately attempt to reinitialize for a particular node (instead of waiting until the scheduled data collection check), while logged in as `root` or administrator, at the command prompt, type **`snmpCollect -C <`*`nodename`*`>`**
- The node’s SNMP agent is not up or not responding.

Possible Cause B:

An SNMP agent patch might be required on the node in question.

Solution B:

If the node is an HP-UX node, the column is `Interface % Utilization`, and the raw utilization value is greater than 100%, this is due to a known SNMP agent defect on HP-UX. The 11.0 patch for the HP-UX SNMP Agent software that fixes this problem is PHNE_21673 from the following web site:

`http://www.hp.com`, then click “technical support”, “unix and mpe/ix servers”

Note: When this agent defect is encountered, a warning is logged in the log file: “Data value XYZ does not fall into any of the specified XML ranges.”

Possible Cause C:

NNM might have incomplete network interface information.

Solution C:

Check for valid IF Index values in NNM's topology database. In NNM, highlight the node, drill down into the node's Interface submap. Right click on an interface in question, and select `Interface Properties`. Examine the `Interface #` field. If this is blank or 0 (zero), Network Health is not able to retrieve SNMP data from this node. Such interface numbers values sometimes occur when NNM's discovery has not been allowed to complete for a node. Verify that NNM's `netmon` process is running. Is NNM's auto-discovery enabled? Are the node and interface *managed* within NNM?

Possible Cause D:

The node in question might not support one of the MIB variables used in computing that column value.

Solution D:

The most common case of this is the `CPU Utilization` column in the first level of node drill down. This uses the Cisco MIB variable `cisco.local.lsystem.avgBusy5`, hence non-Cisco nodes will display the "Data unavailable" string for this column.

One approach to determining which MIB variable is unsupported is to let `snmpCollect` tell you what is wrong:

1. Toggle on `snmpCollect` tracing: `snmpCollect -T`
2. Toggle on `snmpCollect` verbose tracing: `snmpCollect -V`
3. Force a collection check on the node in question: `snmpCollect -C` *<nodename>*
4. Toggle off `snmpCollect` verbose tracing: `snmpCollect -V`
5. Toggle off `snmpCollect` tracing: `snmpCollect -T`
6. Examine `$OV_LOG/snmpCol.trace` for messages indicating why `snmpCollect` couldn't set up the collections for that node.

In general, you can do the following to determine which MIB variables are used in computing health column values:

1. Go to the health metrics configuration in the Administrator Tool, and then find the metric whose title matches the column title in question (for example, CPU Utilization).
2. Look at the last part of the href attribute of the Element to determine the NNM MIB expression/variable used. For example, `href="snmp://%item%[0]/p_cisco5minavgbusy"` indicates that the MIB expression `p_cisco5minavgbusy` is being used.

3 If a MIB expression (not a simple MIB variable) is being used, to determine which MIB variables are requested in the mathematical formula, open NNM and select `Options->Data Collection & Thresholds: SNMP`. Find the expression in the `MIB Objects Configured for Collection` list. Double-click on the entry. This will bring up a dialog box. Click on `[Describe]`:

  - **Direct NNM MIB expression**: shows the mathematical formula of MIB variables that the direct MIB expression is using.
  - **Indirect NNM MIB expression**: shows a list of possible direct MIB expressions in use. The actual direct MIB expression used will depend upon the attributes of the interface. To determine which direct MIB expression is being requested from a specific node, exit the `Description` dialog box, and in the `MIB Object Collection Summary` list click on the node in question and select `Actions->Test SNMP`. Note which direct MIB expression is being requested for each interface (for example, `IfHDplxUtilization`). Exit the `Test SNMP` dialog box.

Unfortunately, there aren't many options when a node does not support an SNMP variable used to compute health. You can do one of the following:

- Remove the category health component from the gauge's configuration. In this way, the associated SNMP variable/expression will not be used in computing health.
- Configure the node selection or interface selection such that only nodes supporting that MIB variable pass from the organizations in the desired filter assignment.

Error: "Data unavailable" in One Column of Details Table (for All Nodes or Interfaces)

Symptom:

"Data unavailable" in detail tables for all nodes.

Possible Cause A:

The node in question might not support one of the MIB variables used in computing that column value.

Solution A:

See Solution D: on page 153.

Possible Cause B:

There might be an error in the specification of the requested MIB variable or MIB expression, preventing NNM's `snmpCollect` process from performing any collections on this metric.

Solution B:

Check for MIB variable/expression validity. See "Data unavailable" error message on one row of details table (for a particular node or interface) on the previous page.

For information about the steps required when the Network Health portlet requests SNMP data from NNM, see Data Collection for Network Health Gauges on page 88. Verify that each step of the process is working correctly.

Nodes or Interfaces Missing from Details Table

Symptom:

You expected more nodes to pass the filters than are displayed within the Detailed Network Health table.

Possible Cause A:

By default, only 20 rows are displayed within any Detailed Network Health table, although more than 20 might be included in the health calculation.

Solution A:

By default, only the 20 least healthy nodes/interfaces are shown. Increase the value of the Maximum Number of Devices in Detail View setting in the health metrics configuration. This setting affects all gauges within portlets.

If you increase the number of rows displayed and still have nodes missing, verify that the filter assignment node selection or interface selection filters are correctly defined.

Possible Cause B:

The missing nodes or interfaces might currently have status of "unknown" in the NNM object database. This happens when the device is unreachable from the NNM management station due to some connection device being down (such as a router).

Solution B:

By default, devices with an “unknown” status are excluded from the details table. If you wish to include “unknown” devices, change the Show Unknown setting in the network health categories configuration. This setting affects all gauges within all portlets. The unknown devices, if any, will be placed at the bottom of the table, following any “known” devices.

Reading on the Gauge Does Not Match the Values in the Details Table

Symptom:

The values displayed in the Detailed Network Health table do not seem to support the final value displayed on the gauge.

Possible Cause:

By default, only 20 rows are displayed within any Detailed Network Health table, although more than 20 might be included in the health calculation.

Solution:

By default, only the 20 least healthy nodes/interfaces are shown. Increase the value of the Maximum Number of Devices in Detail View setting in the health metrics configuration. This setting affects all gauges within portlets.

Score for a Node Does Not Match the Values Given for Its Interfaces in the Next Lower Level of Details Table

Symptom:

The values displayed for a node’s interfaces in the Detailed Network Health table don’t seem to support the value displayed for the overall node.

Possible Cause:

By default, only 20 rows are displayed within any Detailed Network Health table, although more than 20 might be included in the health calculation.

Solution:

By default, only the 20 least healthy nodes/interfaces are shown. Increase the value of the Maximum Number of Devices in Detail View setting in the health metrics configuration. This setting affects all gauges within portlets.

What does the 100% health score mean? How do I display more information about how health scores are calculated?

Symptom:

I want to display more information about the health score calculation in the details table.

Possible Cause:

The Show Raw Data setting in the health categories configuration might not be set.

Solution:

To display the maximum amount of information about how health scores are calculated, select the Show Raw Data check box in the health categories configuration.

Note that Show Raw Data applies to all gauges within portlets.

Data Collection Seems to Switch from One Router Interface to Another

Symptom:

The data collected for a particular interface in a router is questionable.

Possible Cause:

Each time a router reboots, the SNMP interface index mapping is reconfigured. The ifIndex numbers assigned might drift from one interface to another. The NNM Data Collector is using `ifIndex` to identify interface instances. The collected data might be coming from a different interface after each router reboot.

Solution:

The drift of `ifIndex` numbers will stabilize when the health portlet data collection configuration is updated by executing the `ovcolautoconf` command on the NNM system. The problem only appears after router reboots.

Topology Portlet

“Data currently unavailable” Message Appears Below a Submap’s Title Bar

Symptom A:

Log message: ERROR: Connection to OVW lost.

Possible Cause A:

The NNM ovwdb process on an NNM management station is not running. The Topology portlet is dependent upon this process to supply information.

Solution A:

Run the `ovstart` command on the NNM management station.

Symptom B:

Log message reads:

```
error Topology:Ovw    Thread-19    985636515095    An ovw
serving the map default was not found on the host
jorma.cnd.hp.com. Tried the following port(s):3700 3701
```

Possible Cause B1:

ovw is not running on the server with the map open.

Solution B1:

Start ovw on the server with the map open.

Possible Cause B2:

The map is running, but the map is running with a session number greater than 0 and there is a gap of *numMapRetries* in the sequence of ovw session ports.

Solution B2:

Exit the ovw session and restart it so that it uses the lowest available session number.

Symptom C:

Log message reads:

```
Permission denied. The map default was not found on the host
nganesan.cnd.hp.com
```

Possible Cause C:

OVW authorization not configured on the remote server.

Solution C:

Modify `ovw.auth` and `ovwdb.auth` on remote server.

Symptom D:

error Topology:Ovw Thread-21 985710826476 Database not available

Possible Cause D:

Wrong ovwDbPort specified in the Administrator Tool.
Data Currently Unavailable

Solution D:

Fix ovwDBPort setting in the Administrator Tool.

Symptom E:

Log file reads:

error Topology:Ovw Thread-19 988141835579 The submap name might be incorrect or if Customer Views is installed the submap name is not unique. If this is the case, specify the whole path.

Possible Cause E1:

Submap is not persistent.

Solution E1:

Make the submap persistent.

Possible Cause E2:

Submap name is misspelled, or if Customer Views is installed, the submap name might not be unique.

Solution E2:

Specify the whole path. Correct spelling.

Possible Cause E3:

Submap has been deleted and no longer exists

Solution E3:

Remove submap name from configuration file or re-create submap.

Topology Portlet Hangs When Displaying a Submap

Possible Cause A:

The NNM management station is in the pause state, for example for a backup procedure.

Solution A:

Wait until the backup complete (or run the `ovresume` command).

Possible Cause B:

There is an ovw running on the server that is hung. This might or might not be the ovw for the map having the submap to be displayed. (For example, a hung ovw can occur if you exit out of a Reflection X session without closing ovw.)

Solution B:

Check to make sure all ovw processes that are running are responding. If any of the ovw processes are hung, manually stop the process.

Possible Cause C:

It might not be hung but might just be taking a long time to find the map. This could occur if *numMapRetries* is high or there are many session number gaps between the running ovw sessions. Time outs will generally only be a problem on the Windows operations system.

Solution C:

One solution is to exit and restart all the ovw sessions. This will restart the ovw sessions with contiguous session numbers.

Possible Cause D:

Another process on port 3600 or 3601. Check log file. Calling `OvwInitSession` on port.

Solution D:

Determine port configuration on the NNM management station.

"Managed objects not found" Message Appears in the Submap Area

Possible Cause A:

It might be that there are no symbols in the submap.

Possible Cause B:

It might be that a filter has been applied that results in no objects passing the filter for that particular submap.

Solution:

Change the filter that you are applying.

None of the Icon Symbols Appears Correctly

Possible Cause A:

No topology symbol images (GIF files) have been gathered from your NNM management station and copied to the Operations View server. Therefore, Operations View can only display the background shape (circle, square, etc.) for map symbols.

Solution A:

In the Administrator Tool, verify that the Use A OVw Symbol Source check box is selected for at least one NNM management station configuration.

Possible Cause B:

The wrong web server port is specified in the Administrator Tool. Therefore, no topology data can be gathered from your NNM management station.

Solution B:

Check the log file for the following message:

```
error Topology:SymbolRefreshCache   Thread-21   985709926656 You
might want to check the webSrvPort for <NNMstationHostName>:8880
java.net.ConnectException: Connection refused: no further
information
```

In the Administrator Tool, verify that the web server port actually in use by the NNM management station is specified in the Web Server Port setting. To determine which port is configured for the NNM web server, ask your NNM administrator. On an NNM management station running in *UNIX*, see `/opt/OV/apache/conf/httpd.conf`

Some of the Icon Symbols Do Not Appear Correctly

Possible Cause A:

If you add or change NNM's topology symbols, Operations View gathers the new symbol information from your NNM management station and copies the GIF files to the Operations View server according to the following settings:

- The setting of the Use As OVw Symbol Source check box in the management station configuration in the Administrator Tool.
- `topologyConfig.xml` file's `symbolFetchRateInMin` attribute.

Solution A:

In the Administrator Tool, verify that the Use A OVw Symbol Source check box is selected for at least one NNM management station configuration.

To force Operations View to update the NNM topology symbol information, in the Administrator Tool, select the Use A OVw Symbol Source check box for this management station, and then refresh the portal view.

Submap Background Graphic Does Not Appear

Note: Only the default background graphics in the `<`*`OV directory`*`>/backgrounds` directory are certain to work across servers.

Possible Cause:

The background graphics file was not found in the expected location on the portal server.

Solution:

Install the background graphics on the portal server in the same location as the remote server.

"Currently not configured" Message Appears below Topology Portlet Title Bar and No Submap Appears

Possible Cause A:

The hostname in the Submap URL setting does not match the hostname in the Administrator Tool.

The log file contains:

```
error Topology:Ovw    Thread-21   985710426012   The host
nganesan.cnd.hp.com is not specified in mgmtStations.xml
```

Possible Cause B:

No management stations configured in the Administrator Tool

The log file contains:

error mgmtStations Thread-21 985710619802 There are no NNM stations configured in mgmtStations.xml. At least one station must be configured for NNM portlets to operate."

Topology Portlet Opens Slowly

Possible Cause:

You are getting map data from multiple NNM stations, and they all have the same applications installed (i.e., the same symbol information).

Solution:

In the Administrator Tool, select the Use A OVw Symbol Source check box for only one NNM management station and clear this check box for all other NNM management stations.

Index

hp®

invent

Java™
COMPATIBLE