NNM Multicast Manual

NNM Multicast 1.0

HP-UX, and Solaris

January 2001

Legal Notices

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty. A copy of the specific warranty terms applicable to your Hewlett- Packard product and replacement parts can be obtained from your local Sales and Service Office.

HEWLETT-PACKARD COMPANY

3404 E. Harmony Road

Fort Collins, CO 80528 U.S.A.

Use of this manual and flexible disk(s), tape cartridge(s), or CD-ROM(s) supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs in their present form or with alterations, is expressly prohibited.

Trademark Notices

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

Windows NT® is a U.S. registered trademark of Microsoft Corporation.

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

Netscape™ and Netscape Navigator™ are U.S. trademarks of Netscape Communications Corporation.

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

Oracle7™ is a trademark of Oracle Corporation, Redwood City, California.

OSF/Motif® and Open Software Foundation® are trademarks of Open Software Foundation in the U.S. and other countries.

Pentium® is a U.S. registered trademark of Intel Corporation.

UNIX® is a registered trademark of The Open Group.

Contents

Contents

Contents

Conventions

The following typographical conventions are used in this manual.

Table 1

Font	What the Font Represents	Example
Italic	Book or manual titles and reference page or manpage names	Refer to the *HP OVW Developer's Guide*.
	Emphasis	You *must* follow these steps.
	A variable that you must supply when entering a command	To open a specific map when starting NNM, type `ovw -map` *`map_name`*, where you supply the map name.
Bold	Terms being defined for the first time	The **distinguishing attribute** of this class...
`Computer`	Text and items on the computer screen	The `Root` map window ... The system prompts: `Press Enter.`
	Cascading menu items	Select `Edit:Find->Object by Comment`
	Command names	Use the `ovstatus` command ...
	File and directory names	`/usr/bin/X11`
	Process names	Check to see if `pmd` is running.
	Window or dialog box names	In the `IP Internet` map window...
`Computer Bold`	Text that you must enter	At the prompt, type: **`ovstatus`**.
Keycap	Keyboard keys	Press **Return**.
`[Button]`	Buttons on the user interface	Click `[NET]`. Click on the `[Apply]` button.

1 Overview

Multicast Management Technology Overview

Multicast protocols and standards have been under development for the past ten years. Multicast protocol greatly reduces the amount of network bandwidth required to send the same information to multiple locations; such as, training sessions, education classes, and updating price lists. However, as you implement multicast, new issues arise. How can you check to see if the newly implemented multicast environment is working properly? How can you quickly solve problems? NNM Multicast provides answers to the following questions and more.

Discover your multicast environment:

- "Which routers within my management domain are configured to handle multicast?"
- "Which subnets have subscribers to this group's traffic?"
- "What path does the routing tree for this group follow?"
- "Which multicast groups does this router serve?"
- "Which router is the PIM designated router for this subnet?"
- "What is the status of the multicast equipment?"

Collect multicast traffic statistics:

- "How can I collect multicast-specific performance data and set multicast-specific thresholds?"
- "What is the true impact of multimedia on my network?"
- "What proportion of network traffic is multicast?"

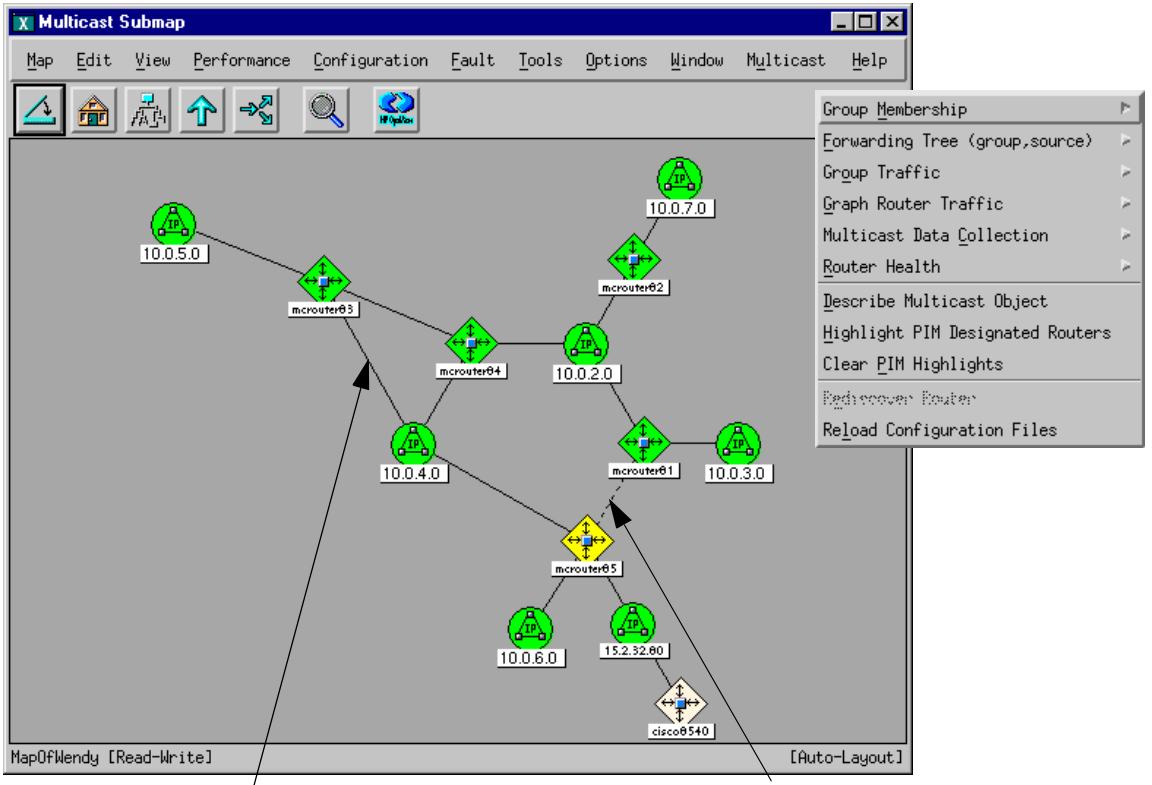
Monitor and troubleshoot current multicast activity:

- "Which group is generating all this traffic?"
- "Which hosts are the sources of this group's traffic?"
- "Which router is blocking the flow of data along the forwarding tree?"
- "A router is flooded, is that because of unicast or multicast traffic?"
- "Can I view this information over the www from a remote location?"

Multicast Routing Topology

NNM Multicast adds a new symbol to the Root level of your NNM maps.

Double-click the Multicast symbol to display the Multicast hierarchy of submaps. The parent submap, called the Multicast submap, displays all multicast-enabled routers and subnets discovered within your management domain. A new pull-down menu of multicast tools appears within the Multicast hierarchy of submaps.



A line between a router and a subnet represents an interface within the router

A line between two routers represents a direct connection.

An object is added to the NNM object database for each multicast element. This object is in addition to the one that NNM added to the object database for that same network element during the network discovery process.

For example, `Router-183` may be displayed on your Multicast submap and on the NNM Internet submap. The status of the router is calculated separately for the multicast context and the overall network context The color of each symbol indicates the current status of the device within its respective context. The symbol on the NNM Internet submap is calculated based upon total traffic error conditions, whereas the status of the symbol on the NNM Multicast submap is calculated based upon multicast error conditions.

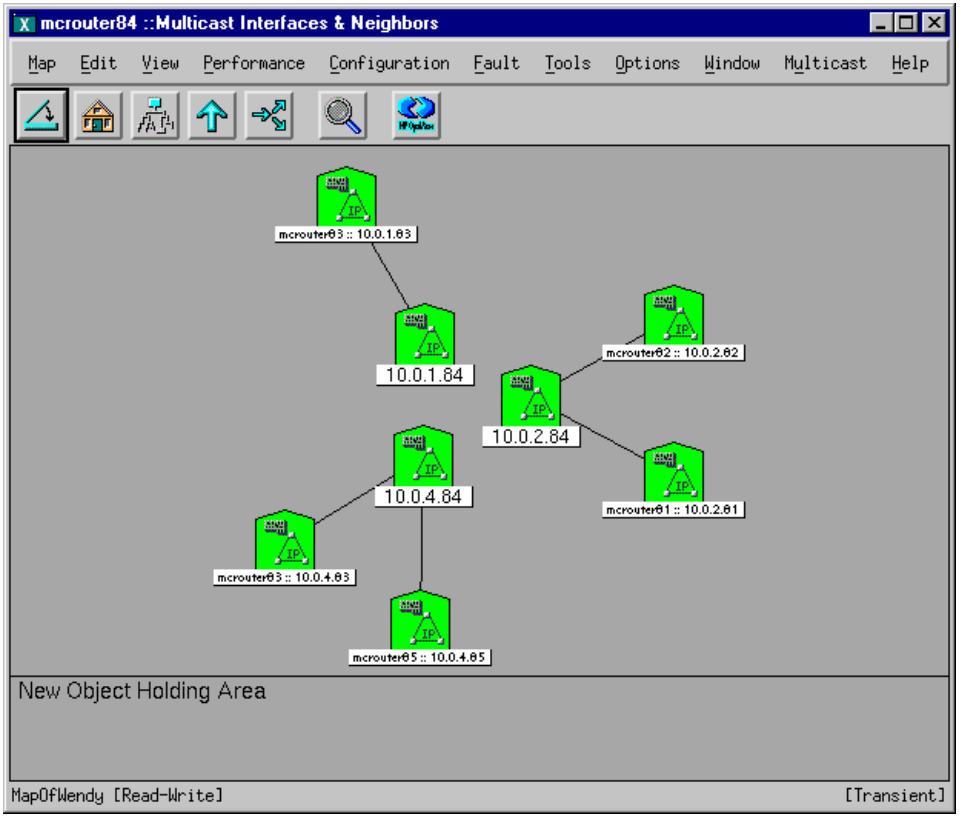
Interfaces & Neighbors submap

Double-click a router symbol on the Multicast submap to display the Interfaces & Neighbors submap. This submap includes two rings of interface symbols:

- The inner ring includes all multicast-enabled interfaces within the selected router.
- The outer ring shows the neighbor relationship to connecting interfaces on other routers.

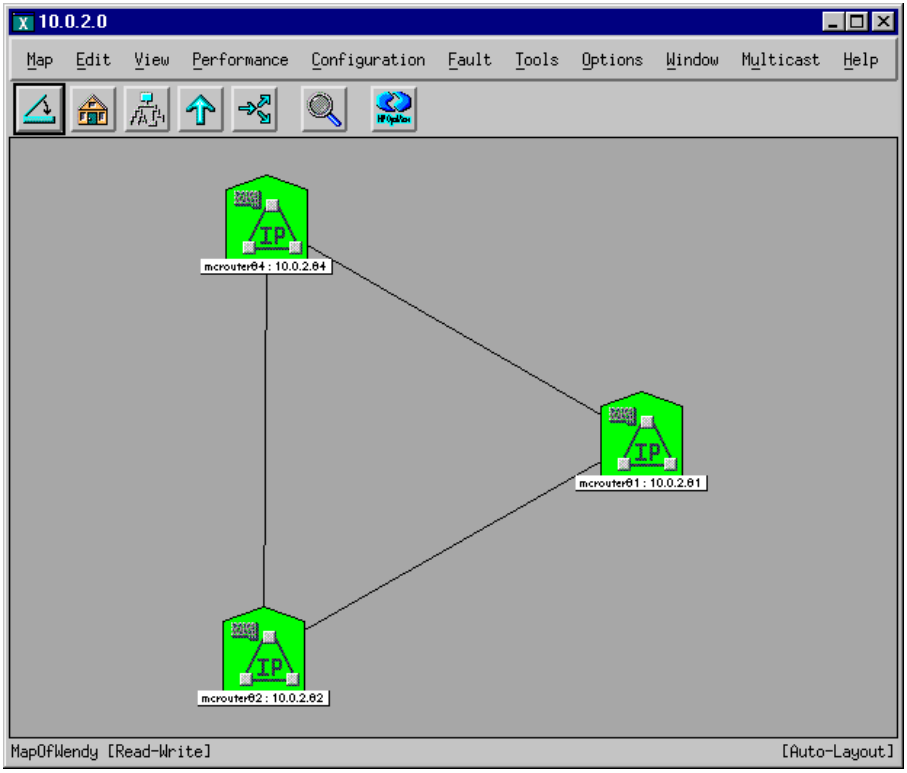
The inner ring of interface symbols are the multicast enabled interfaces within the router.

The outer ring of interface symbols are the neighbor relationships.



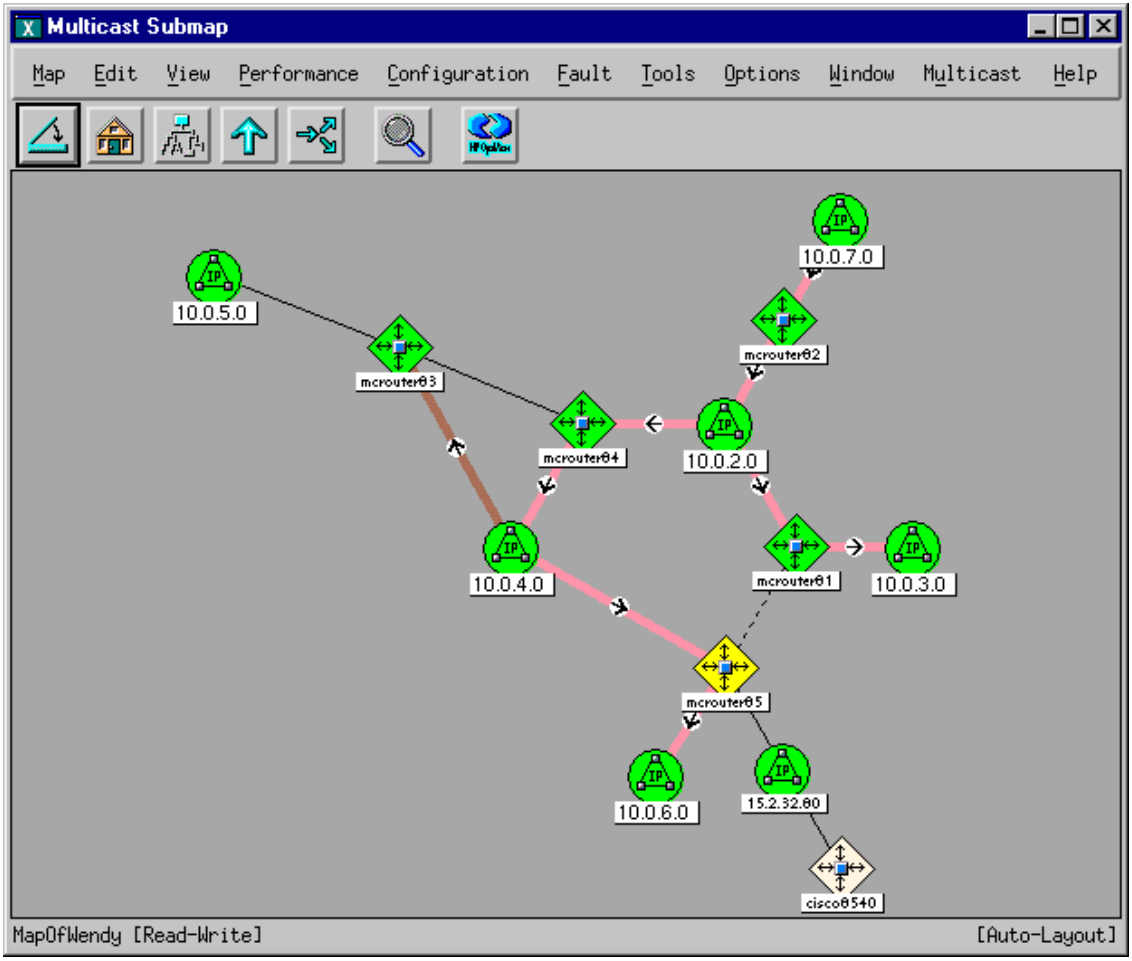
Subnet submap

Double-click a subnet symbol on the Multicast submap to display the Subnet submap. This submap shows all multicast-enabled router interfaces connected through this subnet. Connecting lines represent neighbor relationships. Typically, each interface symbol connects to all other interface symbols on this submap.

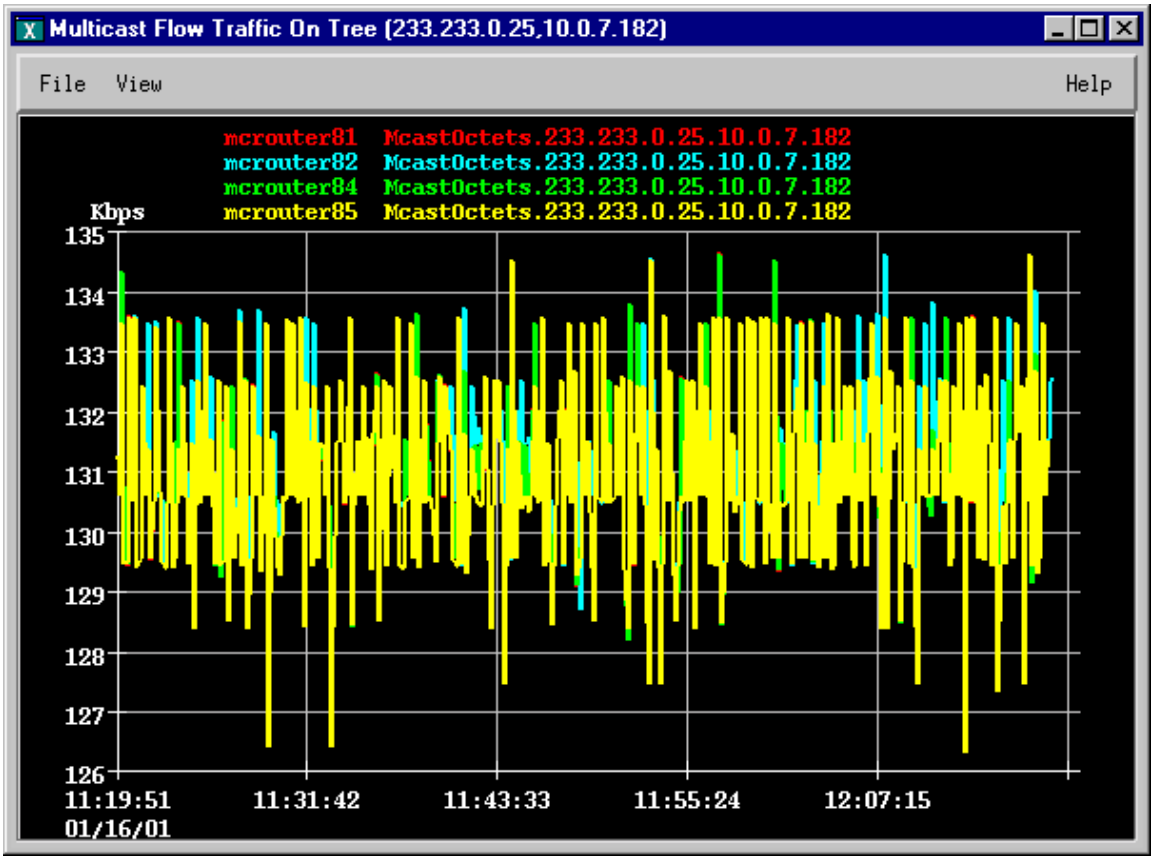


Forwarding Tree Map Overlay

After you specify a valid multicast group and source, NNM Multicast can display the forwarding tree. Arrows show the direction that data is flowing over the tree. X's indicate a pruned state. If the source machine is within your multicast management domain, the forwarding tree can be drawn from the subnet containing the multicast source. If the source machine is outside of your multicast management domain, specify a starting point by choosing one of your routers or subnets.



NNM Multicast provides a graph showing the currently displayed forwarding tree's ongoing traffic over each router.



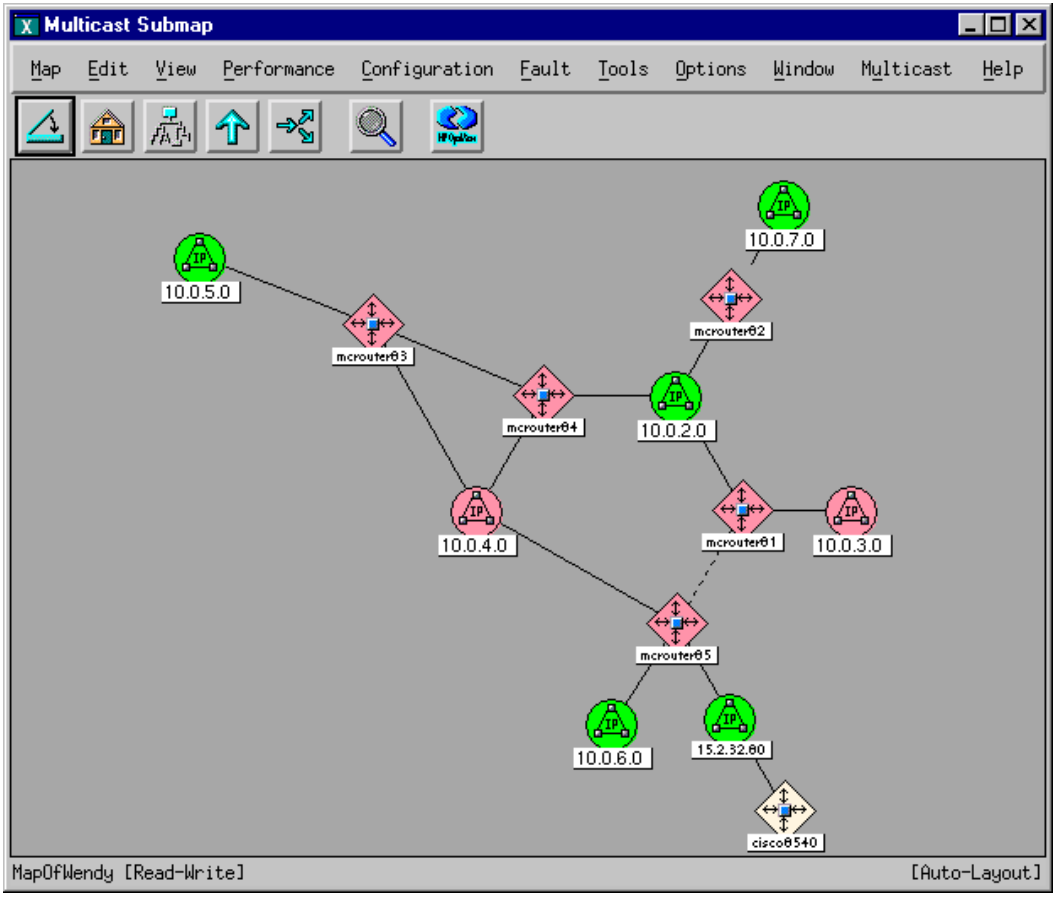
Group Membership Map Overlay

NNM Multicast can easily highlight all subnets and routers belonging to a specific multicast group:

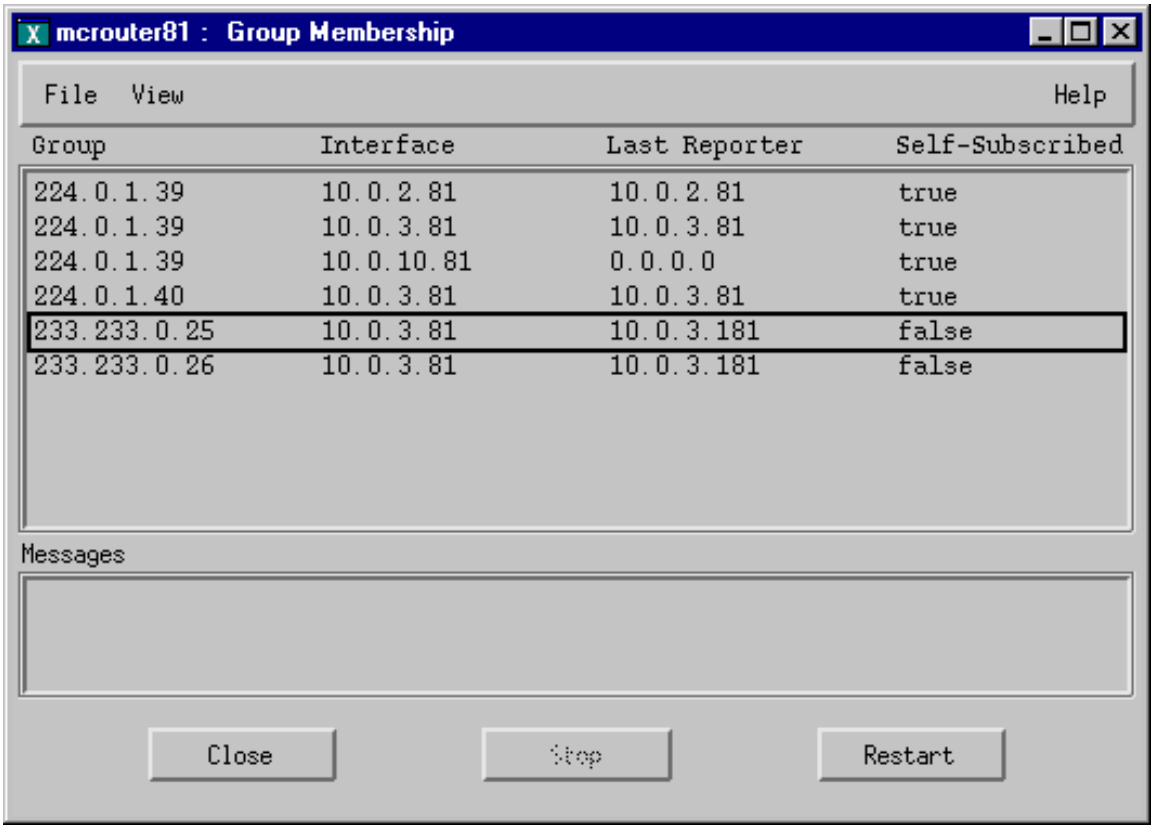
- All subnets containing at least one receiver who has issued an IGMP JOIN request for this group.
- All routers that have joined the group (self-subscribed).

  NOTE: Some routers can *passively* join groups, but their SNMP MIBs do not report a *passive* join as self-subscription. Therefore, these routers are not highlighted.

The symbols of the member routers and subnets turn pink.



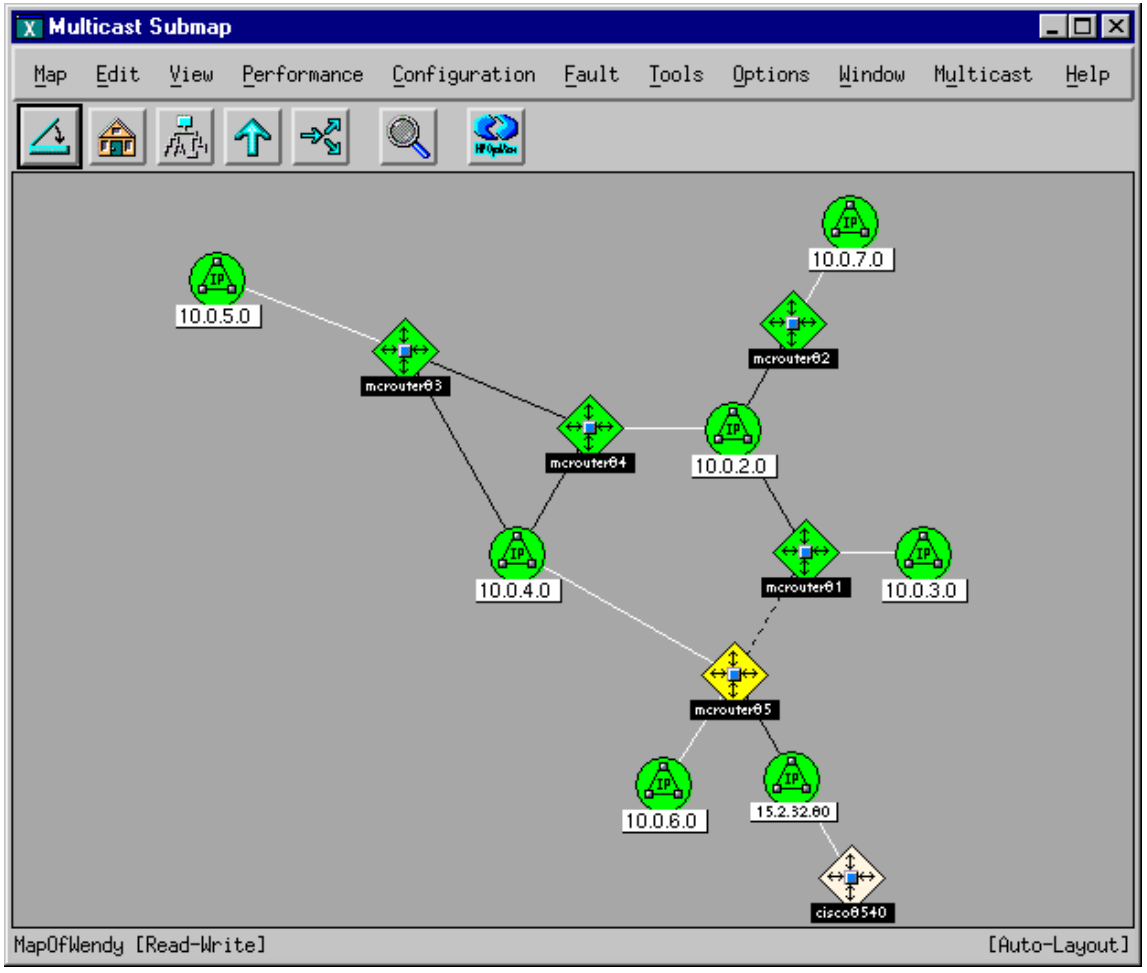
You can select any router on the Multicast submap and display a table of all Multicast Groups that have receivers (hosts that have issued an IGMP JOIN request) in the subnets that are served by this router.



PIM Designated Router Identification

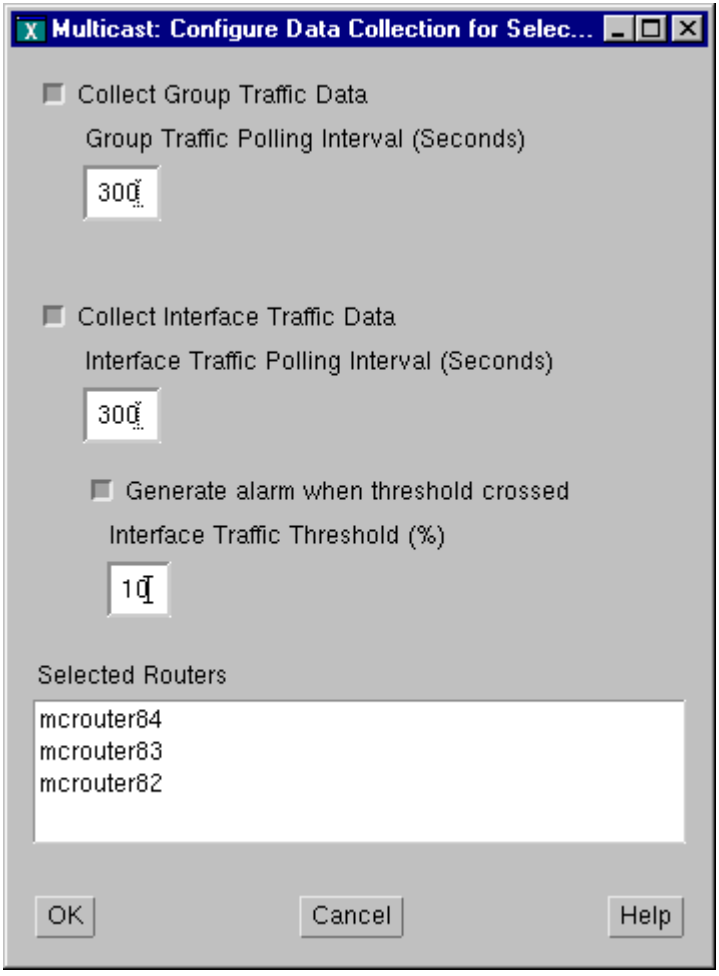
NNM Multicast can instantly identify the Protocol-Independent Multicast (PIM) designated routers within your multicast management domain. The label of the router symbol is highlighted and the interface connection being serviced by each PIM router (connecting line) is changed to white for each subnet.

PIM routing protocol, when used in your multicast environment, designates a single router on each subnet to handle IGMP JOIN requests, etc.

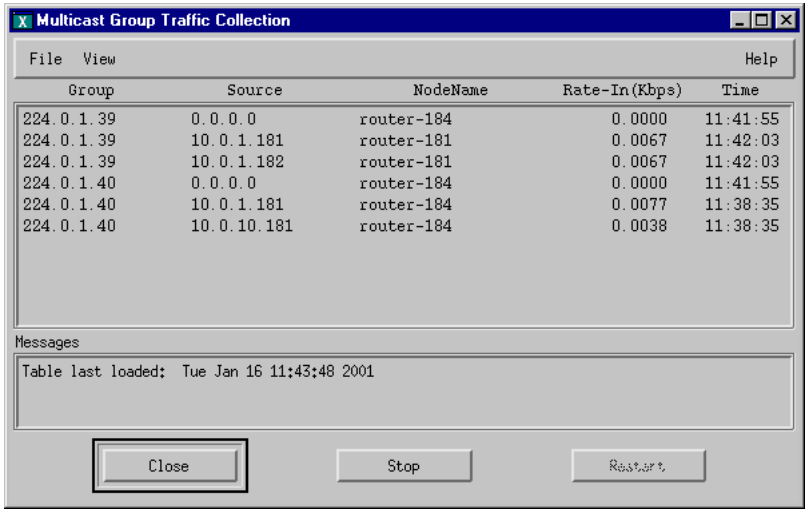


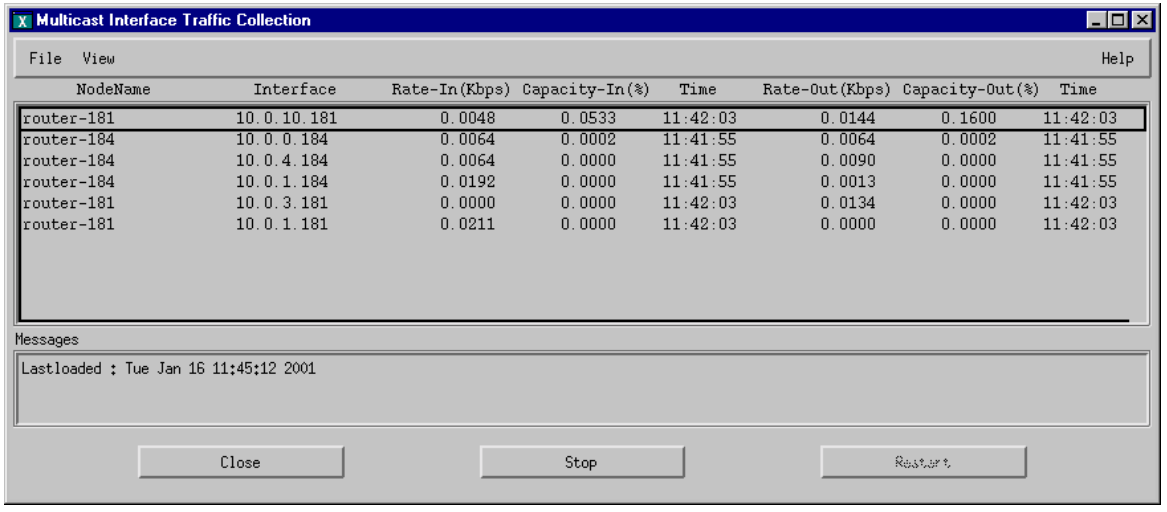
Multicast Data Collection: Group Traffic, Router Interface Traffic, Thresholds

For each router, you can configure data collection based upon multicast groups and/or based upon the total incoming and outgoing multicast traffic on each interface in the router. You can easily set up thresholds that generate an alarm if any router interface experiences multicast traffic over the specified percent of total traffic capacity.



Once your data collection is configured, NNM Multicast provides two tables showing ongoing results of all multicast group-traffic data collection and all interface multicast-traffic data collection.These tables can be viewed on your management station or over the world-wide-web from remote locations.

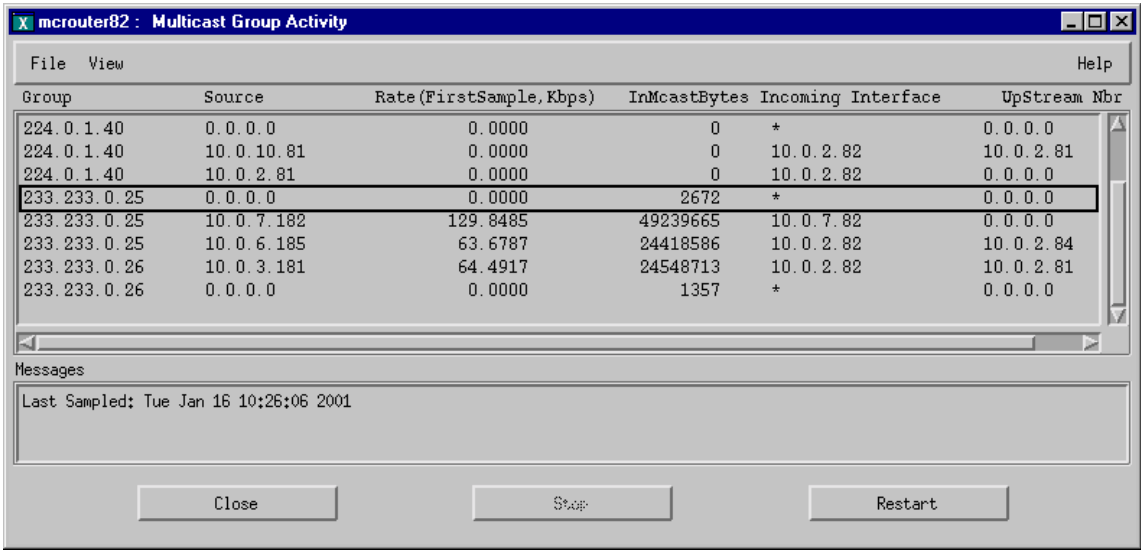




Troubleshooting Tools for the Multicast Environment

A variety of additional multicast tools are provided to help you troubleshoot real-time problems within your multicast environment.

For each router, you can display the “Show All Group Activity” table. This table shows information about each multicast (group,source) pair known by the selected router. Current multicast traffic rate is shown for a 30-second time period (beginning when you click this command).



You can also display a variety of graphs, such as:

- Graph Incoming Multicast Traffic on one or more routers.
- Graph Outgoing Multicast Traffic on one or more routers.
- Graph All Incoming Traffic on one or more routers.
- Graph All Outgoing Traffic on one or more routers.
- Graph Group Traffic for all sources of a particular group on one or more routers.

The NNM Multicast Relationship to NNM

During initial discovery, you define the multicast management domain; NNM Multicast uses a background process called *mmonitor* to discover each multicast enabled router. An object is added to the NNM object database for each multicast element. This object is in addition to the one that the NNM background process called *netmon* adds to the NNM object database during the network discovery process. By creating a duplicate object, the status of the router can be calculated separately for the multicast context and the total network context.

NNM Multicast draws an independent hierarchy of submaps of your multicast management domain. You control which multicast routers are managed or unmanaged by making entries in the `managed.mmon` and `unmanaged.mmon` files. These submaps can be viewed remotely through the NNM Launcher; however, the Multicast menu items cannot be accessed over the web.

NNM Multicast adds an alarm category called “Multicast Alert Alarms” to the NNM Alarm Browser. NNM Multicast uses the *mmonitor* background process to send multicast-related SNMP traps to the NNM alarm browser.

NNM Multicast uses the NNM SNMP Data Collector to collect and to set alarm thresholds for multicast traffic flows. You enter your choices into the Multicast Data Collection dialog box. These entries are actually stored in the NNM object database. The *mtraffic* background process uses the database entries to automatically configure NNM’s Data Collection & Thresholds feature for you.

NNM Multicast uses the NNM Grapher to graph multicast-related historical and real-time data. New menu choices provide quick access to these graphs.

NNM Multicast uses the NNM Application Encapsulator to display tables of useful multicast information, such as group membership lists and multicast traffic samplings. New menu choices provide quick access to these tables.

NOTE If you wish to limit multicast traffic to a specific percentage of a router's capacity, find out about HP OpenView PolicyXpert software. Ask your HP reseller for more information or check the `openview.hp.com` web site.

2 Installation and Configuration

Prerequisites

NNM Multicast uses SNMP multicast-related MIBs and IGMP protocol. NNM Multicast must communicate with your routers using both of these protocols (run above UDP and IP in the network protocol stack). If a router cannot respond properly to the public-domain tool *mrinfo*, it cannot be managed by NNM Multicast.

The IETF is the governing body for the process of standardizing the IP multicast protocols and MIBs. This standardization has not yet been completed for the MIBs, and the standards are evolving. All MIBs queried by NNM Multicast have either already been standardized by IETF or are in the process of being approved.

Router Requirements:

For routers to be managed by NNM Multicast, they must be capable of issuing the IGMP protocol DVMRP_ASK_NEIGHBORS2 response to the ASK_NEIGHBORS request. In other words, the router must respond to the public domain tool *mrinfo*.

Your multicast-enabled routers SNMP agent must support:

- ipMRouteMIB (version 6 or later, draft-ietf-idmr-multicast-routmib-06.txt) used to determine multicast routing, forwarding tree, etc. This is currently under the experimental branch of the MIB tree: .1.3.6.1.3.60.
- pimMIB (version 00 or later, draft-ietf-idmr-pim-mib-00.txt) used to determine PIM specific information such as rendezvous points, routing, etc. This MIB is required only if PIM is in use. This is currently under the experimental branch of the MIB tree: .1.3.6.1.3.61.
- igmpMIB (version 00 or later, draft-ietf-idmr-igmp-mib-00.txt) used to determine group membership and related information. This is currently under the experimental branch of the MIB tree: .1.3.6.1.3.59.
- MIB-II (RFC1213.txt, also IETF STD0017) used to gather router and interface information. This MIB is under the management branch of the MIB tree: .1.3.6.1.2.1.

Routers Tested to Date

Currently the following Cisco routers meet all requirements and can be monitored by NNM Multicast:

- IOS 12.0(5)S or newer 12.x versions.

Table 2-1 Known Problems with Cisco Routers

Cisco Router Operating System	Known Problem
12.0 or earlier	*Bug ID Cisco case number #CSCdm15268* ATM Subinterface missing from IPMROUTE table. This defect seems to affect ALL MIBs for ATM subinterfaces (not just multicast MIBs). Thus all the ATM subinterfaces share a common “ifIndex” in MIB-II, and you can't get any interface-specific info from the MIBs. Fixed in 12.0S, 12.0(5)S, 12.1 (any). Not fixed in 12.0 or earlier. MAY get fixed in 12.0(14), ask your Cisco representative.
Cisco 6509 IOS 12.x in “hybrid” mode, IOS 12.1(1)E, Catalyst OS 5.3(4)CSX	*Bug ID Cisco case number A824019* Multicast traffic can only be monitored in one direction. The reason for this problem is currently not known. IGMP transit failure, “mrinfo” failure. When IGMP snooping is enabled at level-2 (“set igmp enable”), the router (at level-3) does not respond to external mrinfo requests, and thus fails to respond to *mmon* discovery/monitoring. In addition, IGMP mrinfo packets are NOT forwarded through the affected 6509 to IP destinations beyond the router. Thus, NNM Multicast cannot manage any 6509 affected by this bug, and cannot manage any router that is otherwise reachable through a 6509 affected by this bug.
cat6000 12.1E Integrated:12.1(01.03)E 02 12.1(01.05)E 12.1(01.03)EC 12.1(01.05)EC	*Bug ID Cisco case number CSCdr38716* R 2 Router port gets deleted by snooping. Fixed by 12.1(2)E

Table 2-1 Known Problems with Cisco Routers

Cisco Router Operating System	Known Problem
All operating systems on the Catalyst 4000 platform	The Catalyst 4000 platform does not support any of the multicast MIBs (ipMRouteMIB, igmpMIB, pimMIB), nor does it respond to IGMP ASK-NEIGHBORS (*mrinfo*). Therefore, the Cat 4000 cannot be managed by NNM Multicast.
All as of 1/1/2001	*Bug ID Cisco case number CSCdr31072 A187437, 4/00*. ATM sub-interfaces. mrinfo contains conflicting entries (double-entry report.). NO KNOWN FIX.

NNM Management Station Requirements:

You must install NNM Multicast on an NNM Management Station that meets the following requirements:

1. HP-UX 10.20 or 11.0; or Solaris 2.6, 2.7, or 2.8
2. An installed, licensed HP OpenView Network Node Manager: NNM 6.1 running in U.S. English mode (that is, $LANG must be set to C or unset).

   For installing HP OpenView Network Node Manager, the following minimum space is recommended:

   . /etc/opt/OV - 25MByte
   . /system - 150MByte
   . /opt/OV - 225MByte
   . /var/opt/OV - ~1GByte or more for traffic data
3. Access the `http://ovweb.external.hp.com/cpe/patches/` web site and install the following, or later, consolidated patch for NNM 6.1:

   Solaris: PSOV_02835

   HP-UX 10.20: PHSS_22423

   HP-UX 11.0: PHSS_22424
4. NNM must know the *GET-Community name* for each router that will be managed by NNM Multicast.

   For best results, before installing NNM Multicast, configure NNM

with the default “SNMP Get Community” string from your environment, and if your routers have unique community strings, configure NNM to be aware of these:

a. From any NNM submap, select `Options:SNMP Configuration`, or at the command prompt, type **`$OV_BIN/xnmsnmpconf`**.

b. Select the “Global Default” line. The parameter set populates the lower section of the window.

c. Replace the “Get Community” value with “public” or the required value for your network.

d. Click [Replace] to save the values and [Close] to exit.

e. Populate the “Node” and “Wildcard” sections with any community names that are unique to your multicast-enabled routers.

Installing NNM Multicast 1.0 on HP-UX

If you are upgrading from any version of *mmon*, before proceeding, you must read Appendix E, "Migration from mmon 1.6," on page 93 for more information.

Installing NNM Multicast on a Local System

You need to gather the IP address of at least one multicast-enabled router before you proceed with installation. This router is the starting point for the NNM Multicast discovery process.

It is strongly recommended that, before you install NNM Multicast, you read "Configuring HP OpenView NNM Multicast" on page 36.

The following procedure helps you install the NNM Multicast product on your local NNM management system.

1. Log in as `root` or `superuser` to the system where you are installing NNM Multicast.
2. Create a `/tmp/multicast` directory.
3. Use FTP to place one of the following files from `http://ovweb.external.hp.com/ftp/pub/nnm_multicast` to the temporary directory that you just created:

   `NNMMulticast_HPUX10_20.tar.gz`

   `NNMMulticast_HPUX11_00.tar.gz`
4. Refer to the CHECKSUM file provided on the FTP site to ensure that the NNM Multicast installation file was successfully downloaded.
5. Use gunzip (available free from `http://www.gzip.org`) to unzip the file:

   `gunzip NNMMulticast_HPUX<xx>.tar.gz`
6. Use tar to extract the files:

   `tar xf NNMMulticast_HPUX<xx>.tar`
7. Start the installation program by navigating to the `/tmp/multicast` directory and typing:

   `./install`

8. An installation program appears on screen. It displays messages about the various NNM Multicast requirements. The program may prompt you to answer specific questions if your NNM management station has more than one IP address.

   Should an error occur, a message appears on screen that describes the error and ways to fix it. Should a fatal error occur, the installation program stops, terminates itself, and displays a message on screen that describes the problem. At this point, you must fix the error, then re-run the installation program in order to install NNM Multicast.

   Check the Multicast Installation log file for important information about the results of the install process:

   `/var/adm/sw/swagent.log`

   The NNM_Multicast_Manual.pdf file is installed into the following directory:

   `/opt/OV/www/htdocs/C/manuals/NNM_Multicast_Manual.pdf`

   You can view this file using Adobe Acrobat Reader.

9. Open the `managed.mmon` file and enter at least one multicast-enabled router's IP address before starting the NNM Multicast program for the first time. The file is located in:

   `/etc/opt/OV/share/conf/managed.mmon`

   See "managed.mon Configuration File" on page 36 for more information.

10. After editing the configuration files, follow the directions in "To start NNM Multicast" on page 47.

NOTE When you are comfortable that everything is running correctly, remove the files from the `/tmp/multicast` directory and remove the `/tmp/multicast` directory.

Installing NNM Multicast 1.0 on Solaris

If you are upgrading from any version of *mmon*, before proceeding, you must read Appendix E, "Migration from mmon 1.6," on page 93 for more information.

Installing NNM Multicast on a Local System

You need to gather the IP address of at least one multicast-enabled router before you proceed with installation. This router is the starting point for the NNM Multicast discovery process.

It is strongly recommended that, before you install NNM Multicast, you read "Configuring HP OpenView NNM Multicast" on page 36.

The following procedure helps you install the NNM Multicast product on your local NNM management system.

1. Log in as `root` or `superuser` to the system where you are installing NNM Multicast.
2. Create a `/tmp/multicast` directory.
3. Use FTP to place one of the following files from `http://ovweb.external.hp.com/ftp/pub/nnm_multicast` to the temporary directory that you just created: `NNMMulticast_SOLARIS.tar.gz`
4. Refer to the CHECKSUM file provided on the FTP site to ensure that the NNM Multicast installation file was successfully downloaded.
5. Use gunzip (available free from `http://www.gzip.org`) to unzip the file: **`gunzip NNMMulticast_SOLARIS.tar.gz`**
6. Use tar to extract the files:
   `tar xf NNMMulticast_SOLARIS.tar`
7. Start the installation program by navigating to the `/tmp/multicast` directory and typing:

   `./install`
8. An installation program appears on screen. It displays messages about the various NNM Multicast requirements. The program may prompt you to answer specific questions if your NNM management

station has more than one IP address.

Should an error occur, a message appears on screen that describes the error and ways to fix it. Should a fatal error occur, the installation program stops, terminates itself, and displays a message on screen that describes the problem. At this point, you must fix the error, then re-run the installation program in order to install NNM Multicast.

Check the Multicast Installation log file for important information about the results of the install process, and also information about steps that you need to take after installation:

`/var/adm/sw/swagent.log`

The NNM_Multicast_Manual.pdf file is installed into the following directory:

`/opt/OV/www/htdocs/C/manuals/NNM_Multicast_Manual.pdf`

You can view this file using Adobe Acrobat Reader.

9. Open the `managed.mmon` file and enter at least one multicast-enabled router's IP address before starting the NNM Multicast program for the first time. The file is located in:

   `/etc/opt/OV/share/conf/managed.mmon`

   See "managed.mon Configuration File" on page 36 for more information.

10. After editing the configuration files, follow the directions in "To start NNM Multicast" on page 47.

NOTE When you are comfortable that everything is running correctly, remove the files from the `/tmp/multicast` directory and remove the `/tmp/multicast` directory.

Configuring HP OpenView NNM Multicast

Before starting the NNM Multicast background processes, you must configure NNM Multicast's discovery process by editing the following:

- "managed.mon Configuration File" on page 36

Optionally, you can create the following file to set specified multicast-enabled routers to an "unmanaged" state:

"unmanaged.mmon Configuration File" on page 37

Optionally, you can edit the following file to control many aspects of how NNM Multicast works:

"mmon.conf Configuration File" on page 38

TIP

Once NNM Multicast is running, if you change the settings in any of the above files, you must force an update by either stopping and restarting the *mmonitor* process or by selecting the following menu item from any submap in the Multicast hierarchy:

`Multicast:Reload Configuration Files`

There are two additional files that may require attention, depending upon your multicast environment. Please read the following sections before starting the NNM Multicast background processes:

- "mmon_ma.conf Configuration File" on page 42
- "snmpCollect.lrf Configuration File" on page 43

managed.mon Configuration File

At least one entry is required in this file. This file works like a seed file that controls the discovery of multicast-enabled routers. Any routers specified in this file are set to managed during initial discovery. The file is located in:

`/etc/opt/OV/share/conf/managed.mmon`

Ensure that at least one router in each multicast-enabled network is entered into this file. Discovery starts with the routers listed in this file

and proceeds outward. Each router listed in this file is set to the "managed" status within NNM Multicast. Any neighboring mulitcast-enabled routers are also "managed' unless you specifically reference them in the `unmanaged.mmon` file.

TIP NNM Multicast uses the first interface whose IP address was discovered on each router for monitoring and data collection unless you make a specific entry in the `managed.mmon` file instructing NNM Multicast to use a specific interface.

One entry per line:

- An IP address for each router or a range of IP addresses for routers that you wish to manage.

  Consider using the loopback address so that communication with the router automatically rolls to another IP address if the loopback interface goes down.

- Fully-qualified router names (must resolve to an IP address through DNS or `/etc/hosts`).

  Wildcards are allowed for host names; for example, *.myDiv.myCompany.com

- To specify a range of IP addresses, use the format IP_address IP_mask; for example, 10.20.0.0 255.255.0.0

Usually a router name can be added into `/etc/hosts` to make it resolvable by the local host. For more details, see the comments within the `mmon.conf` file.

unmanaged.mmon Configuration File

If you wish to specify certain routers as *unmanaged*, create this optional file. You must populate this file rather than using `Edit:Unmanage Object` from the map.

TIP Remember that NNM maintains two objects in the object database for each multicast enabled router. Therefore, you can set a router to be "unmanaged" by the multicast *mmonitor* process, and set the same

router to be “managed” by the NNM *netmon* process.

Place this file in:

`/etc/opt/OV/share/conf/unmanaged.mmon`

The unmanaged routers may appear on multicast submaps as neighbors to managed routers, but are not monitored by NNM Multicast after initial discovery. Copy the format of the `managed.mmon` file.

One entry per line:

- An IP address for each router or a range of IP addresses for routers that you wish to unmanage.
- Fully-qualified router names (must resolve to an IP address through DNS or `/etc/hosts`).

  Wildcards are allowed for host names; for example, *.myDiv.myCompany.com
- To specify a range of IP addresses, use the format IP_address IP_mask; for example, 10.20.0.0 255.255.0.0

NOTE If you accidently include identical information in the `managed.mmon` file *and* the `unmanaged.mmon` file, the device is set to “unmanaged”.

After creating this file, open the `mmon.conf` file and delete the # character at the beginning of the following line:

```
FILTER    Unmanaged 1 /etc/opt/OV/share/conf/unmanaged.mmon
```

mmon.conf Configuration File

This file controls the configuration settings of the *mmonitor* background process. See the comments within this file for more information. The file is located in:

`/etc/opt/OV/share/conf/mmon.conf` (`$OV_CONF/mmon.conf`)

- HOST_IP

  (Required) IP address within your NNM management station, that NNM Multicast uses to communicate with multicast-enabled routers.

If there are multiple IP addresses for your computer, indicate the one that you wish to use for multicast management tasks. During installation, if your NNM management station had more than one IP address, your were instructed to provide the one you wanted to be entered into this file.

- CYCLE_MINUTES (default 10 minutes)

  (Required) This setting controls the frequency of the polling process for multicast-enabled routers (this polling process works independently of the other NNM discovery processes). NNM Multicast polling includes status checks and discovery cycles. If the CYCLE_MINUTES time expires while polling is in progress, NNM Multicast resets the time, doubling the polling interval for that cycle. The discovery cycles are further controlled by the SNMP_POLL setting later in the `mmon.conf` file.

  The default sets CYCLE_MINUTES to 10 (minutes). The slowest discovery cycle is the first discovery cycle (especially if many routers are not responding to SNMP). Thereafter, you can shorten the cycle if you want more timely events and updates to your multicast submaps.

  For example, initial discovery of a portion of the HP network (100 routers, 614 multicast interfaces, 931 multicast links) takes about 10 minutes. That same HP network can be routinely polled in two minutes, with the default IGMP_PARMS settings.

  To examine the current multicast polling cycle length on your network, see the logging feature for “mmonitor” on page 80.

- IGMP_PARMS 1 2 4 10 3

  (Required) This series of five parameters controls the following IGMP settings. These settings are used when NNM Multicast queries your routers for IGMP ASK_NEIGHBORS:

  1. time-out in seconds

     Number of seconds to wait for the IGMP response.

  2. minimum number of retries

     NNM Multicast requires that this parameter be set to at least 2.

     The protocol for Neighbors query (IGMP ASK_NEIGHBORS) can have a response containing multiple packets without a termination indicator. Therefore, NNM Multicast queries a router for Neighbor List at least twice to make sure that an accurate

response was received.

This parameter indicates the minimum number of times NNM Multicast performs the query. If this parameter is set to "*n*", NNM Multicast performs a Neighbor Query "*n*" times, then compares the last response (*n*th time) with the previous response. If they match, and if no other previous response had more output packets, NNM Multicast uses that response. If they don't match, NNM Multicast tries one more time and so on up to MAX times.

3. maximum number of retries

   Maximum number of times that NNM Multicast attempts to get correct response for Neighbor Query.

4. maximum burst of IGMP requests

   The discovery process is parallel. This means that *mmonitor* can ask multiple Routers in parallel for neighbor information. This number controls the maximum Neighbor Queries outstanding at one time.

5. number of discovery cycles before declaring a link "inconsistent" when the link is reported differently by the neighboring endpoints.

   A link represents a neighbor relationship between two interfaces in two different routers. NNM Multicast might receive inconsistent neighbor information if it queries in the middle of the routers' protocol data exchanges. To eliminate false alarms, it is recommended that this parameter be set to 2 or more.

   If the CYCLE_MINUTES parameter is set to 1, the minimum for this parameter is 3; if the CYCLE_MINUTES parameter is greater than 3, this parameter can be set to 2.

- FILTER Managed 1 /etc/opt/OV/share/conf/managed.mmon

  (Required) `Managed 1 <filename>`

  Specify the location of the `managed.mmon` filter file. The default location indicated above is the recommended location. This file must contain at least one entry. This file controls the starting points for the NNM Multicast discovery process. See the comments within the `mmon.conf` file for more information.

- FILTER Unmanaged 1 /etc/opt/OV/share/conf/unmanaged.mmon

  (Optional) `Unmanaged 1 <filename>`

Specify the location of the unmanaged.mmon filter file. The default location indicated above is the recommended location. This file instructs NNM Multicast to set certain discovered multicast-enabled routers to an unmanaged state. The unmanaged routers may appear on multicast submaps as neighbors to managed routers, but are not monitored by NNM Multicast after initial discovery. Create this file if you wish to implement this feature.

The settings in the unmanaged.mmon file take precedence over the settings in the managed.mmon file. Therefore, if the router is listed in both files, it is set to an "unmanaged" state.

- NODE_STATUS 4 7 3 0 3 0 6

  (Required) This series of parameters sets the status assigned by you for certain error conditions that may be discovered during SNMP data collection, such as: status when router doesn't respond to IGMP (multicast monitoring), status when router does not respond to SNMP, the impact of a down interface on the parent router's status, the impact of a disabled interface on the parent router's status, the impact of a disabled link or tunnel on the parent router's status, the impact of an inconsistent link or tunnel on the parent router's status.

  See the comments within the mmon.conf file for more information.

- SNMP_POLL

  (Optional) This is the multiplier for spacing NNM Multicast discovery polling cycles among multicast status polling cycles. If CYCLE_MINUTES is 10 and SNMP_POLL is 10, routers and their interfaces are queried for SNMP information every 100 (10x10) minutes.

  When initially discovered, routers are randomly initialized with an SNMP polling count between 1 and this setting, thereby distributing the SNMP requery activity throughout the status polling cycles.

  If this parameter is commented out, (or set to zero) routers are not queried for SNMP information after initial discovery.

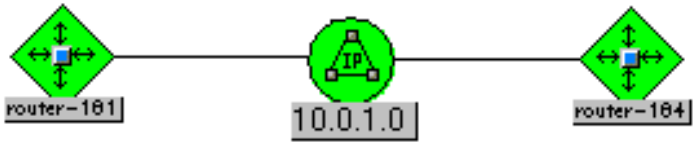
  You can manually requery a router by right-clicking the router symbol and selecting Rediscover Router.

- DOMAIN_SUFFIX

  (Optional) Used to shorten the displayed router names on the multicast submaps. See the comments within the mmon.conf file for more information.

mmon_ma.conf Configuration File

Typically, you do not need to modify this file. It contains a list of all interface types within your management domain that NNM Multicast should assume contain multi-access ports. Connection lines on the Multicast submap from interfaces on any devices listed in this file are drawn with a Subnet symbol on the connecting line. The presence of the Subnet symbol allows for the possibility of branching lines:



If you know that certain types of networks in your environment always use direct connections, you can comment out the interface type ID, and reduce the number of symbols displayed on the Multicast submap:

CAUTION

If you modify this file, you must delete the NNM object database to make a clean start, unless NNM Multicast background processes have not yet been started. See “Stopping NNM Multicast” on page 45.

For example, if *all* of your ATM interfaces are point-to-point connections, rather than multi-access connections, to prevent subnet symbols from appearing between the router symbols, comment-out or remove all entries that reference the ATM interfaces deployed in your network (for example, “37 # atm”, “49 # aal5”).

This file is located in:

`/etc/opt/OV/share/conf/mmon_ma.conf` (`$OV_CONF/mmon_ma.conf`)

The numbers in this file, one per line, represent the MIB-II values for interface type ids (mgmt.mib-2.interfaces.ifTable.ifEntry.ifType, .1.3.6.1.2.1.2.2.1.3) that should be considered “multi-access” interfaces in your management domain. See the comments within this file for more information.

These are the default entries, one interface type per line:

```
6    # ethernetCsmacd
7    # iso88023Csmacd
8    # iso 88024TokenBus
9    # iso88025TokenRing
15   # fdddi
37   # atm
49   # aa15
59   # aflane8023
60   # aflane8025
62   # fastEther
69   # fastEtherFX
71   # ieee80211
114  # ipOverAtm
117  # gigabitEthernet
```

snmpCollect.lrf Configuration File

NNM Multicast depends upon NNM's Data Collection & Thresholds feature (*snmpCollect* background process and the *xnmcollect* foreground process) to collect multicast data. To configure *snmpCollect* for optimal performance in the multicast environment, learn about the `-c` and `-n` parameters.

- -c # (lower case c)

  Frequency (in minutes) with which *snmpCollect* performs configuration checks. With NNM 6.1, when no value is specified, the default value is 24 hours.

  If the Multicast Groups in your environment are dynamic (a number of short term Multicast sessions and Groups), *snmpCollect* needs to know about the newly added group instances more frequently than the default frequency value.

  Based upon the dynamic nature of the Groups in your environment, set this variable appropriately. If set to too high, NNM Multicast Group Traffic Collection may not include all the Groups on which you

wish to collect traffic rates. If set to too small, unnecessary polling load is generated on your network.

- -n # (lower case n)

  Maximum number of concurrent SNMP requests. With NNM 6.1, when no value is specified, the default value is 5.

  The higher the number, the greater the polling load potential on the network, and the greater the throughput.

NOTE In the NNM Multicast Data Collection Configuration dialog box, if any polling interval is set to less than 1 minute (60 seconds), *snmpCollect* may require a high concurrency setting in order to work efficiently.

To set the `-c` and `-n` parameters, you must edit the *snmpCollect* local registration file:

`$OV_LRF/snmpCollect.lrf`

The `-c` and `-n` parameters belong in the third field, which is initially empty ("::") when NNM is installed. Find the line that is similar to the following two examples:

```
OVs_YES_START:pmd,ovwdb,ovtopmd::OVs_WELL_BEHAVED:20:PAUSE
OVs_YES_START:pmd,ovwdb,ovtopmd:-c 15, -D 1, -n 50:OVs_WELL_BEHAVED:20:PAUSE
```

If you change any parameter, you must notify NNM of the change. After closing and saving the `snmpCollect.lrf` file, at the command prompt type:

```
ovstop snmpCollect
$OV_BIN/ovdelobj $OV_LRF/snmpCollect.lrf
$OV_BIN/ovaddobj $OV_LRF/snmpCollect.lrf
ovstart snmpCollect
```

See the *snmpCollect*(1M) and *xnmcollect*(1) manpages for more information.

Stopping NNM Multicast

1. Log in as superuser.
2. If you wish to stop all multicast data collection, you have two choices:
   - To delete all multicast data collection configurations from the Data Collection & Thresholds program, ensure that no symbols are selected on the Multicast submap, then select `Multicast:Multicast Data Collection-->Stop`.
   - To stop multicast data collection without deleting your settings, go to the next step.
3. To stop the NNM Multicast background processes, at the command prompt, type:
   `ovstop mmonitor mtraffic`

   The Multicast submaps are still visible, but none of the menu commands will operate until the multicast background processes are restarted.
4. If you have not already done so, to stop multicast data collections:
   a. From any NNM submap, select `Options:Data Collection & Thresholds`.
   b. In the *MIB Objects Configured for Collection* list, select the following (one at a time):
      - ipMRouteOctets
      - ipMRouteInterfaceInMcastOctets
      - ipMRouteInterfaceOutMcastOctets
      - mcastIf%inutil
   c. Select `Actions:Suspend Collection`. Repeat for each of the above. (The multicast data collection settings are stored in the NNM object database. The next time that *mtraffic* is started, the database settings are used to reestablish the Data Collections & Thresholds configuration settings.)

NOTE If you want to completely start over with multicast discovery, monitoring,

and data collections by clearing out multicast information from NNM's object database, see the "Stop Everything and Start Discovery Over Again" section at the end of Chapter 5, Initial Network Discovery, in *Managing Your Network with NNM*. This book was included with NNM. It is also available:

- From the HP Documentation web site in Adobe Acrobat format (pdf): `http://ovweb.external.hp.com/lpe/doc_serv/`
- From any NNM submap in DynaText format, select `Help:Online Manuals`. Click on the NNM Runtime Collection in the left-hand list, then select Managing Your Network in the right-hand list.
- For purchase from FatBrain.com

To start NNM Multicast

1. At the command line, type **`ovstart`**. This automatically starts all background processes registered with NNM.
2. Open NNM. Select a map to which you have [read-write] access.
3. Navigate to the NNM Multicast submap by double-clicking on the Multicast symbol on the Root submap.

Uninstalling NNM Multicast

If you need to remove NNM Multicast from your computer, follow these steps.

1. Log in as root or superuser.
2. Stop all HP OpenView processes.

   At the command prompt, type **ovstop**.
3. Run the remove script located in $OV_BIN.

   At the command prompt, type **remove.mcast**

NOTE The Multicast Alert Alarms category is not removed from the NNM Alarm Browser. However, it is no longer used.

The following files are copied to /tmp/Multicast/<filename> during uninstall. If you wish to save any modifications to these files for future reference, you will find them in the /tmp/Multicast/ directory:

/etc/opt/OV/share/conf/managed.mmon

/etc/opt/OV/share/conf/mmon.conf

/etc/opt/OV/share/conf/mmon_ma.conf

/etc/opt/OV/share/conf/mtraffic.conf

/etc/opt/OV/share/lrf/mmonitor.lrf

/etc/opt/OV/share/lrf/mtraffic.lrf

/var/opt/OV/share/snmp_mibs/Experimental/Multicast/:
IGMP-MIB.my
IPMROUTE-MIB.my
PIM-MIB.my

Check the file named /var/adm/sw/swagent.log for messages regarding the uninstall process.

The multicast entries remain in the NNM databases. If you wish to remove them, see the “Stop Everything and Start Discovery Over Again” section at the end of Chapter 5, Initial Network Discovery, in *Managing Your Network with NNM*. This book was included with NNM. It is also

available:

- From the HP Documentation web site in Adobe Acrobat format (pdf): `http://ovweb.external.hp.com/lpe/doc_serv/`
- From any NNM submap in DynaText format, select `Help:Online Manuals`. Click on the NNM Runtime Collection in the left-hand list, then select Managing your Network in the right-hand list.
- For purchase from FatBrain.com

3 Getting Started with NNM Multicast

NNM Multicast Makes Your Job Easier

"How can I check to see if the newly implemented multicast environment is working properly?"

NNM Multicast provides a wealth of new tools specifically designed to help you map out (page 53), monitor (page 57), and troubleshoot (page 60) your multicast environment.

Under the Multicast pull-down menu, the following choices are available. You must have [read-write] access to the map before these work. See the NNM Multicast online help for detailed information about each one:

Group Membership->
- Highlight Subnets & Routers in a Group
- Clear Highlights
- Show Groups with Local Subscribers

Forwarding Tree (group,source)->
- Highlight Tree
- Clear Highlights
- Graph Traffic

Group Traffic->Show All Groups Activity
- Graph Group Traffic

Graph Router Traffic->
- Incoming Multicast
- Outgoing Multicast
- Incoming Multicast & Unicast
- Outgoing Multicast & Unicast

Multicast Data Collection->
- Monitor Group Traffic Collection
- Monitor Interface Traffic Collection
- Configure for Selected Routers
- Configure Default
- Stop
- Review

Router Health->Graph CPU & Memory Utilization
- Explain Status

Describe Multicast Object
Highlight PIM Designated Routers
Clear PIM Highlights
Rediscover Router
Reload Configuration Files

Mapping Your Multicast Environment

- "Which routers within my management domain are configured to handle multicast?"
- "Which subnets have subscribers to this group's traffic?"
- "What path does the routing tree for this group follow?
- "Which multicast groups does this router serve?"
- "Which router is the PIM designated router for this subnet?"
- "What is the status of the multicast equipment?"

"Which routers within my management domain are configured to handle multicast?"

Once you install NNM Multicast and supply the IP address of at least one multicast-enabled router, NNM Multicast automatically discovers all multicast-enabled routers in your management domain and draws a new hierarchy of submaps under the Multicast symbol on the Root submap. The submaps are automatically updated as changes occur within your network.

To view the Multicast topology, open NNM and double-click on the Multicast icon.

Confirm that your topology is properly discovered and drawn on the Multicast submaps. If you have questions or concerns, see Appendix A, "Troubleshooting NNM Multicast," on page 63 and "Configuring HP OpenView NNM Multicast" on page 36.

NNM Multicast periodically polls *managed* multicast-enabled routers to check on the routers' multicast status, the status of the routers' multicast interfaces, and the status of the multicast neighbor relationships or connectivity (the interval is specified as `CYCLE_MINUTES` in the `mmon.conf` file). Connectivity changes or status changes produce events that are posted as alarms in the NNM Alarm Browser under the Multicast Alert Alarms category.

NOTE The NNM Multicast submap does not support *container* objects to split

the map into smaller segments. NNM Multicast does not support *hidden* symbols within the Multicast submap hierarchy.

"Which subnets have subscribers to this group's traffic?"

On the Multicast submap, select `Multicast:Group Membership-->Highlight Subnets & Routers in a Group`.

Specify one multicast group. The status color of the following symbols on the Multicast submap changes to pink:

- All subnets that contain at least one receiver who has issued an IGMP JOIN request for this group.
- All routers that have joined the group (self-subscribed).

  NOTE: Some routers can *passively* join groups, but their SNMP MIBs do not report a *passive* join as self-subscription. Therefore, these routers are not highlighted.

"What path does the routing tree for this group follow?"

On the Multicast submap, select `Multicast:Forwarding Tree (group,source)-->Highlight Tree`.

Specify one (group,source) pair.

Discovery proceeds downstream (towards the receiver) from the designated starting point. The forwarding tree uses arrows to indicate direction of data flow, x's to indicate pruning, and color to indicate the following:

- Forwarding based upon source-specific trees is shown using *administrative "testing"* status (by default pink).
- Forwarding based upon shared trees is shown using *administrative "restricted"* status (by default brown).

A message is displayed that identifies the protocol that is being used and:

- If the PIM routing protocol is in use, the mode (dense, sparse).

- If PIM sparse-mode is in use, the rendezvous point for this group.
- Whether the shortest-path tree is used by the starting-point router.

Click on [Help] within the Highlight Forwarding Tree dialog box if you need more information.

"Which multicast groups does this router serve?"

On the Multicast submap, select the router's symbol:

- Select `Multicast:Show Groups with Local Subscribers`.

  or

- Right-click the router symbol and select `Show Groups with Local Subscribers`.

A table is displayed, listing all multicast groups for which the selected router has received at least one IGMP JOIN request on any of its interfaces. Additional useful information about each group is also displayed; such as, the IP address of the router interface assigned to each group and the last known reporter.

"Which router is the PIM designated router for this subnet?"

Select `Multicast:Highlight PIM Designated Routers` to quickly identify all PIM (Protocol-Independent Multicast) designated routers within your management domain, generally one per subnet. The name labels of the router's map symbol are highlighted and the status color of the line that represents the interface connecting the router to a subnet is changed to white.

Normally, the router whose interface has the highest IP address within a subnet automatically becomes the PIM designated router. When a host multicasts an IGMP JOIN request, only the PIM designated router acts upon the request and begins the routing process.

"What is the status of the multicast equipment?"

Highlight any router symbol on the Multicast submap, select `Multicast:Router Health-->Explain Status` to view an explanation of the current status color.

Green means that everything is working.

Blue means *unknown* status (did not respond to IGMP queries).

White means *unmanaged* (listed in the `unmanaged.mmon` file).

Any other color represents an error condition.

The status of symbols on the Multicast submap is calculated based upon multicast issues, such as status when router doesn't respond to IGMP (multicast monitoring), the impact of a disabled link or tunnel on the parent router's status, the impact of an inconsistent link or tunnel on the parent router's status. The multicast status behavior is controlled through the NODE_STATUS settings in the `mmon.conf` file.

Remember, the status of each symbol on the NNM Multicast submap is calculated separately from the status of each symbol on the NNM submaps, even though the symbols may represent the same device or subnet.

Some of the Multicast submap status change behavior is different from the behavior observed in the NNM submaps. For example:

- Links between multicast enabled routers (lines on the map) don't go "DOWN" (turn red), they are deleted from the submap when the routers no longer report a neighboring relationship.
- Interface symbols:
  - — If administratively down or disabled, remain on the submap with a brown status color.
  - — If operationally down, remain on the submap with a red status color.
  - — If removed from the router, are removed from the submap.
  - — If reconfigured with multicast disabled, are removed from the submap.
- Status changes such as interface Up/Down, additions, and deletions are posted in the NNM Alarm Browser under the Multicast category.

Monitoring Your Multicast Environment

- "How can I collect multicast-specific performance data and set multicast-specific thresholds?"
- "What is the true impact of multimedia on my network?"
- "What proportion of network traffic is multicast traffic?"
- "How can I set absolute limits on the amount of bandwidth available to multicast groups?"

"How can I collect multicast-specific performance data and set multicast-specific thresholds?"

On the Multicast submap, start multicast data collection on multiple routers by holding down the control key as you left-click multiple router symbols, and then select `Multicast:Multicast Data Collection-->Configure for Selected Routers`.

Establish data collection for one or more currently selected multicast-enabled routers by making selections within the dialog box:

- Set frequency for gathering group traffic data (which groups, transmitting from where, how much data flow).
- Set frequency for gathering the router interface's traffic data (how much multicast data is flowing in and out of each interface).
- Set a threshold for multicast traffic (percent of capacity per interface). If the multicast traffic exceeds the threshold on any interface, an alarm is posted in the NNM Alarm Browser. Duplicate alarms are prevented until a rearm event is generated upon multicast traffic dropping below 50% of the value you specify as the threshold.

Possible strategies for gathering multicast-related data are:

- Collect traffic statistics from your "backbone" routers.
- Collect traffic statistics from your "edge" or campus LAN routers.
- Collect traffic statistics from all routers.

If you have many different multicast groups in your network, and/or if your network has multicast flows using the same group from day to day,

you may find it appropriate to collect group traffic on an infrequent basis (every hour or so). This minimizes the impact of retrieving SNMP-based group traffic data from your routers.

Once the data collection is configured, you have many choices for monitoring the collected data.

"What is the true impact of a specific multimedia data stream on my network?"

To view real-time data, from the Multicast submap:

- Select `Multicast:Group Membership-->Highlight Subnets & Routers in a Group` and supply the group ID being used by the multimedia data stream.
- Select one of the router symbols, and select `Multicast:Group Traffic->Show All Groups Activity` to display a table. Locate the line within the table showing information about the (group,source) pair of the multimedia data stream. Check the traffic rate for the past 30-second time period (beginning when you selected this command).

"What proportion of network traffic is multicast traffic?"

Select one or more router symbols on the Multicast submap, and select `Multicast:Graph Router Traffic->Incoming Multicast`. This graph displays traffic rates for all incoming multicast traffic on each multicast-enabled interface within the selected router or routers.

Now select the same router symbols on the Multicast submap, and select `Multicast:Graph Router Traffic->Incoming Multicast & Unicast`. This graph displays traffic rates for all incoming traffic (multicast, unicast, and broadcast) on each multicast-enabled interface within the selected router or routers.

Display both graphs side-by-side and compare the traffic quantities.

"How can I set absolute limits on the amount of bandwidth available to multicast groups?"

If you wish to completely block multicast traffic from consuming any bandwidth beyond a specific threshold, contact your HP representative and ask for information about HP OpenView PolicyXpert software.

Troubleshooting the Multicast Environment

- "Which group is generating all this traffic?"
- "Which hosts are the sources of this group's traffic?"
- "Which router is blocking the flow of data to my multicast customer?"
- "A router is flooded, is that because of unicast or multicast traffic?"

"Which group is generating all this traffic?"

To get an answer for one router, select the router's symbol on the Multicast submap. Then select `Multicast:Group Traffic->Show All Groups Activity`. A table is displayed that lists all group/source pairs known by this router that are currently active and shows the rate of traffic for each pair.

If you wish to determine current traffic levels for all group/source pairs on all routers, make sure that you have configured multicast data collections for all routers (see previous page), then select `Multicast Data Collection:Monitor Group Traffic Collection` to view a table with the information that you need.

Monitor real-time multicast data flow by displaying two tables:

- `Multicast:Multicast Data Collection->Monitor Group Traffic Collection`
- `Multicast:Multicast Data Collection->Monitor Interface Traffic Collection`

These tables can also be accessed over the web, as long as they are currently displayed on your NNM management station. See page 74.

When you need to diagnose a fault for a particular flow, open the "Monitor Group Traffic Collection" table (from any location, web-based or on the NNM management station) to quickly identify the sources sending to the group and identify which router is reporting the highest traffic rate. At the NNM management station, you can right-click the router symbol and graph the group traffic to see live, current information.

"Which hosts are the sources of this group's traffic?"

Select the symbol of a router that has local receivers for the group (hosts that have issued an IGMP JOIN for the group), then select `Multicast:Group Traffic->Show All Groups Activity`. A table is displayed that lists all group/source pairs that are currently active.

"Which router is blocking the flow of data to my multicast customer?"

Display the group's forwarding tree (`Multicast:Forwarding Tree (group,source)-->Highlight Tree`. Click [Help] in the dialog box if you need more information).

- If the displayed forwarding tree does not reach the receiver's subnet, there may be a routing fault, or the receiver's IGMP Join Request may not be reaching its local router. Right-click the local router symbol on the Multicast submap (there may be more than one local multicast router connected to the receiver's subnet) and select `Group Membership:Show Groups with Local Subscribers`. If the multicast group in question doesn't appear on any router's list, then the receiver's IGMP Join Request is not reaching the local router. The problem is probably in the receiver client or application, or there is a problem in an interconnecting level-2 switch or hub.
- If the displayed forwarding tree does reach the receiver's subnet, select a router near the source and right-click the router symbol and select `Graph Router Traffic:Incoming Multicast`. Generate this same graph for the last hop router on the receiver's subnet. If the traffic rates are roughly equal, then the problem is probably with the receiver's client or interconnecting level-2 network equipment. If the traffic rates are not equal, you can compare traffic rates of all involved routers on one graph by selecting multiple routers along the displayed forwarding tree and then selecting `Multicast:Forwarding Tree (group,source)->Graph Traffic`.

With traffic rate graphs for the group, you can identify which routers experience lossy traffic. Check for possible packet-loss congestion or rate-limits in effect at the router interfaces on the forwarding tree where loss occurs and also upstream from the loss.

"A router is flooded, is that because of unicast or multicast traffic?"

Right-click the router's symbol on the Multicast submap, and select `Graph Router Traffic:Incoming Multicast`. This graph displays traffic rates for all incoming multicast traffic on each multicast-enabled interface within the selected router.

Now right-click the same router's symbol on the Multicast submap, and select `Graph Router Traffic:Incoming Multicast & Unicast`. This graphs displays traffic rates for all incoming (multicast, unicast, and broadcast) traffic on each multicast-enabled interface within the selected router or routers.

Display both graphs side-by-side and compare the lines to find your answers.

TIP

You can easily create your own tools that help solve problems in your multicast environment. Use NNM's Application Builder and the multicast MIBs to create graphs or tables that show the information in exactly the way you need to see it. Access to your new tool is provided through NNM's menu structure. See "Creating your own multicast application tools" in the NNM Multicast online help for more information.

A Troubleshooting NNM Multicast

NNM Multicast submaps

Why does it take so long to open NNM?

Depending upon the size of your management domain, it could take several minutes for NNM to read its database information before displaying the maps. For example, when managing 50-100 routers it may take two or three minutes to open the map. To verify that this is the cause of the delay while the map is opening, at the command prompt, type **`ovstatus mmonitor`**. You should see a message something like "Reading ovwdb"

None of the Multicast menu items work. Why?

You must have [read-write] access to the map before the Multicast features work.

The Multicast submap only has blue icons. What's wrong?

Blue icons are *unknown*. This means that NNM Multicast never received an IGMP protocol DVMRP_ASK_NEIGHBORS2 response to the ASK_NEIGHBORS request.

Verify that the router supports the multicast protocol, see "Router Requirements:" on page 28. Some routers have filters or defective software implementations that prevent them from responding to IGMP queries.

Ensure that you can "ping" at least one router specified in your `$OV_CONF/managed.mmon` file.

Check the `$OV_CONF/mmon.conf` file and make sure the HOST_IP address is valid for the NNM management station where NNM Multicast is installed.

If you made any changes to the `mmon.conf` file, either:

- Signal NNM Multicast to re-read the configuration files by navigating to the Multicast submap and selecting `Multicast:Reload Configuration Files`.

--OR--

- At the command prompt, type:

  `ovstop mmonitor`

  `ovstart`

If this doesn't resolve things, see the *Stop Everything and Start Discovery Over Again* section of the *Initial Discovery* chapter in *Managing Your Network with NNM* to find out how to delete the NNM database, and start the discovery process over again.

The NNM Multicast submap has white icons. What's wrong?

White icons are *unmanaged*.

Unmanaged elements are not polled after initial discovery. They are not included in regular status polling cycles.

Unmanaged routers are listed in the `unnmanaged.mmon` file. See "unmanaged.mmon Configuration File" on page 37 for more information. Edit this file if you wish to make changes. After making changes to the file, force NNM Multicast to acknowledge the changes by selecting `Multicast:Reload Configuration Files`.

NOTE Although it is *possible* to use the `Edit:Manage & Unmanage` menu items to change the management status of the symbols on the Multicast submaps, the symbols revert back to their previous state the next time that the multicast polling cycle runs.

Why do my routers have IP addresses instead of names on the map?

If a router is labeled with its IP address instead of a name, this means the router didn't respond to SNMP queries AND there was no corresponding name found via `/etc/hosts` and DNS.

NNM Multicast determines a "router name" (and the icon label on the submap) as follows:

1. NNM Multicast queries for the SNMP MIB-II `sysName`. This may be

shortened based upon the DOMAIN_SUFFIX setting in $OV_CONF/mmon.conf

2. If no name is identified, NNM Multicast invokes gethostbyaddr(), which uses /etc/hosts and DNS to try to find a name.
3. If no name is identified, the IP address ("x.x.x.y") is used for the router name and label on the map.

What does the color of the router or subnet or interface symbol mean?

Green means that everything is working.

Blue means *unknown* status (did not respond to IGMP queries).

White means *unmanaged* (listed in the unmanaged.mmon file).

Any other color represents an error condition.

A router is in non-Normal status when either it or one of its interfaces or multicast links is in a non-Normal status. On the multicast submap, right-click a router symbol and select Router Health:Explain Status to see the cause of a non-Normal status.

A subnet is in non-Normal status when interfaces or links/tunnels within the subnet are in some non-Normal status.

Remember that status in the Multicast context is calculated separately from status in the network health context of the regular NNM submaps. Multicast status calculations are controlled by the NODE_STATUS settings in the $OV_CONF/mmon.conf file.

It may be useful to review any alarms associate with this router:

- To review the alarms associated with this router that were received within the multicast context, select the router's symbol on the Multicast submap and select Fault:Alarms. Only those alarms associated with the selected router in the multicast context are shown.
- To review the alarms associated with this router that were received within the network health context, select the router's symbol on an NNM submap (non-multicast submap) and select Fault:Alarms. Only those alarms associated with the selected router in the network context are shown (no multicast alarms).

The forwarding tree is broken into multiple trees. Why?

The NNM Multicast submap does not support *hidden* objects. If you have hidden any router or subnet objects, the forwarding tree feature draws strange results. Hidden objects are not supported on the Multicast submaps.

Why are two router symbols referring to the same physical router?

This unusual duplication ONLY occurs if the router was specified in the `managed.mmon` file with an IP address that was *not* multicast-enabled during initial discovery. Change the IP address in the `managed.mmon` file to one that is multicast enabled. If the interface is now multicast enabled, do not change this file.

Ensure that the settings for this router's community names are correct in the `Options:SNMP Configuration` dialog box.

Select and delete both of the router symbols (that you think are duplicates) from the NNM Multicast submap: right-click `Delete`, or `Edit:Delete`.

NNM Multicast creates only one symbol as it goes through its next discovery cycle. To force NNM Multicast to immediately run a discovery cycle, select `Multicast:Reload Configuration Files`.

NNM Multicast data collection and alarms

Alarm: "Could not find intfcid corresponding to index N:router-A. Please rediscover node." What does this mean?

When a router is originally discovered, NNM Multicast collects the current interface indexes using SNMP MIB-II `ifIndex` queries. The returned values are entered into the NNM object database. The `ifIndex` can be reassigned when a router is rebooted or a router interface is added or deleted. This would cause errors until NNM Multicast runs its next discovery cycle and updates the NNM object database.

To force NNM Multicast to immediately update the object database information, right-click the router symbol on the multicast submap and select `Rediscover Router`.

To control how often NNM Multicast runs a discovery cycle set the `SNMP_POLL` parameter in `mmon.conf` file. See"mmon.conf Configuration File" on page 38.

Grapher error message, "Counter for <router-a> McastOctets.x.x.x.x.y.y.y.y wrapped (nnnn -> mmmm). Waiting for next." What does this mean?

The *ipMRouteMIB* defines a 32-bit counter for `McastOctets`. With typical multimedia multicast flows, this counter can overflow and wrap frequently. This message informs you that the counter wrap occurred. The message can be safely ignored.

Multicast Data Collection isn't happening when it should. What's wrong?

The polling cue may be running behind. See "snmpCollect.lrf Configuration File" on page 43 for more information.

The Monitor Group Traffic Collection table is missing some groups. Why?

The polling cue may be running behind. See “snmpCollect.lrf Configuration File” on page 43 for more information.

B Frequently Asked Questions

Questions about the NNM Multicast submaps

Which routers work with NNM Multicast?

See “Router Requirements:” on page 28 for information about routers supported by NNM Multicast.

Why can’t I move symbols into submaps, and “containerize” my map?

The NNM Multicast submap does not support *container* objects.

When I hide an interface that is down, the router status is still affected. Why?

The NNM Multicast submap does not support *hidden* objects.

Questions about NNM Multicast data collection and alarms

What are the important SNMP TRAPS that NNM Multicast generates?

See “Multicast-Specific SNMP Trap Definitions” on page 85.

How do I determine the best value for “CYCLE_MINUTES” in mmon.conf?

Read about the CYCLE_MINUTES SETTING. See “CYCLE_MINUTES (default 10 minutes)” on page 39.

If you want to experiment to find the ideal settings for your multicast environment, read about the logging and tracing tool that allows you to watch real time discovery activity, see “mmonitor” on page 80.

Questions about the NNM Multicast access

Can NNM Multicast be run on a collection station and forward data and alarms to an NNM management station?

Traffic data and events collected by NNM Multicast can be forwarded to an NNM management station in the normal manner. However, NNM Multicast submaps cannot be displayed on an NNM management station. The multicast submaps can be displayed on the NNM management station through NNM's web-based Launcher.

What NNM Multicast operations are available through a web browser.

You can enable a web-page view of the Monitor Multicast Group Traffic Collection table and Monitor Multicast Interface Traffic Collection table. See `Help:NNM Multicast-->Tasks, Viewing current NNM Multicast over the world-wide web` for more information.

The standard web-based view of NNM through the NNM Launcher allows remote access to the Multicast submaps. No access to the Multicast pull-down menu options are available through this interface.

The Multicast alarm category list is fully operational through the Launcher interface. Multicast alarms can be acknowledged and deleted over the web.

C Command Line Utilities and Multicast Process Options

Several utilities and process controls are available:

mdbprint

This command displays all of the multicast-related information that NNM Multicast has gathered about the specified object. `mdbprint` produces results equivalent to right-clicking router symbols on the multicast submaps and selecting `Describe Multicast Object`.

-v Verbose mode. Total deleted object count is printed, if -a is used.

-a Prints information of all objects, not only the selected object. This is similar to `ovobjprint` with multicast awareness.

<Object Name> Prints information of the object specified by name

-n <Object Name> Prints information of the object specified by name

-i <ip-Address> Prints information about the object specified by IP-Address

-o <ovwdb objectID> Prints information about the object specified by object ID used in the NNM database.

At the command prompt, type **`$OV_BIN/mdbprint`** with no arguments to see other options.

Example invocations:

$OV_BIN/mdbprint myRouter.com

$OV_BIN/mdbprint 10.5.3.1

$OV_BIN/mdbprint -a (to print information about all objects)

mdbck

NOTE This command should only be run when *mmonitor* is not running (at the command prompt, type **`ovstop mmonitor`**).

This command inspects the object database for issues and faults. No output is generated if everything is fine. You are notified if errors are discovered.

A list labeled “MCAST DELETED” reveals any objects that have been deleted from some multicast submaps, but not yet removed from all multicast submaps (thus preventing them from being deleted from the NNM object database). If you want the object removed from the NNM database, use the `Edit:Find` feature to quickly locate all instances of the object, select them, and delete them.

-f Fixes the database for any identified inconsistencies

Example invocations:

$OV_BIN/mdbck

$OV_BIN/mdbck -f

mmonlog

The entries that are displayed when running this command are from the standard NNM *nettl* logging and tracing. You can use the *netfmt* command instead of this one, if desired.

This script shows the last *N* entries in the *nettl* tracing and logging facility. It does not actually distinguish between NNM Multicast and any other NNM process entries, thus it may show regular NNM entries. With no argument it displays the last entry; with an optional numeric argument that number of most recent entries are displayed.

TIP

`mmonlog` is more useful for troubleshooting NNM Multicast if you turn *netmon* off in your environment until the multicast problem is fixed. That would ensure that all activity logged is multicast related.

<Number of Entries> Number of entries to be shown. Default is 1

Example invocations:

$OV_BIN/mmonlog (last entry displayed)

$OV_BIN/mmonlog 5 (latest 5 entries displayed)

mmonitor

mmonitor is the background process that performs multicast topology discovery and status checks. It also interacts with routers to perform "on-demand" operations such as identifying a forwarding tree. Only one *mmonitor* background process should be run at a time on one NNM management station.

mmonitor is a well-behaved process that responds to `ovstart`, `ovstop`, `ovpause`, `ovresume`, etc. It has a standard local registration file: `$OV_LRF/mmonitor.lrf`

To adjust configuration settings for this process, see "mmon.conf Configuration File" on page 38.

If you are troubleshooting *mmonitor*, the following command line switch enables logging and tracing.

-d#	Sets debug level (0 through 6 or more). All messages are printed to the `stdout` file (Standard Out). 0 (zero) = most detailed logging level 4 = a log is displayed at the start and end of every discovery cycle 6 = no messages are logged (Default Setting)

Do not run `mmonitor` in the background when you do this because you won't be able to see the real-time logging output.

For example if you are trying to fine tune the CYCLE_MINUTES setting in the `mmon.conf` file (see "mmon.conf Configuration File" on page 38), you can use logging and tracing to help determine the ideal setting.

1. In the terminal window, at the command prompt, type: **`mmonitor -d4`**
2. Watch the logging and tracing results.
3. In a text editor window, open the `mmon.conf` file and change the `CYCLE_MINUTES` setting. Save the change.
4. In the terminal window, at the command prompt, type: **`<Ctrl>-C`** . Return to step 1. Repeat until you see the results that you want in the logging and tracing output.

mtraffic

mtraffic is the background process that configures multicast data collection. It is also used to present collected data through the Monitor Group Traffic Collection table and the Monitor Interface Traffic Collection table. Only one *mtraffic* background process should be run at a time on one NNM management station. To adjust the configuration of this process, use the `$OV_LRF/mtraffic.lrf` file.

mtraffic is a well-behaved process that responds to `ovstart`, `ovstop`, `ovpause`, `ovresume`, etc. If *snmpCollect* is not running., *mtraffic* does not work.

These are the switches that can be set in the `mtraffic.lrf` file. These switches control the mode in which *mtraffic* runs.

-s 0 (zero) — (optional) Disables synchronization of the multicast data collection configurations and the *snmpCollect* data collection configurations each time *mtraffic* starts execution.

-s 1 (one) — (default) Enables synchronization of the multicast data collection configurations and the *snmpCollect* data collection configurations each time *mtraffic* starts execution. This configures NNM's Data Collection & Thresholds (*snmpCollect*) to perform the following collections:

- ipMRouteOctets
- ipMRouteInterfaceInMcastOctets
- ipMRouteInterfaceOutMcastOctets
- mcastIf%inutil

mtraffic overwrites any *snmpCollect* entries under the above names so that they match the settings entered through the Multicast Data Collection dialog box. Therefore any changes made directly in the NNM Data Collection & Thresholds interface (*snmpCollect*) are lost.

If you change any parameter, you must notify NNM of the change. After closing and saving the `mtraffic.lrf` file, at the command prompt type:

`$OV_BIN/ovaddobj $OV_LRF/mtraffic.lrf`

If you are troubleshooting *mtraffic*, the following command line switch enables logging and tracing:

-d#	Sets debug level (0 through 6 or more). All messages are printed to the `stdout` file (Standard Out). 0 (zero) = most detailed logging level 6 = no messages are logged

Do not run `mtraffic` in the background when you do this because you won't be able to see the real-time logging output.

For example, at the command prompt, type:

`mtraffic -d0`

The real-time logging activity of `mtraffic` is displayed on the terminal window.

mmap

mmap is the foreground process that creates the Multicast submap hierarchy. It starts automatically when NNM is opened, and stops automatically when NNM is closed. Multiple instances of the *mmap* foreground process can be run at a time on one NNM management station. It is registered with NNM through the `$OV_REGISTRATION/C/mmap` file.

If you are troubleshooting *mmap*, the following switch enables logging and tracing:

-d#	Sets debug level (0 through 6 or more). All messages are printed to the `stdout` file (Standard Out).
	0 (zero) = most detailed logging level
	6 = no messages are logged

For example, in the `mmap` registration file, search for "$OV_BIN/mmap" and add -d0 before the ending quote:

```
Command -Shared -Initial "$OV_BIN/mmap -d0";
```

The real-time logging activity of `mmap` is displayed on the terminal window.

D Multicast-Specific SNMP Trap Definitions

Harnessing the power of SNMP traps

NNM Multicast adds multicast-specific traps under the OpenView branch of the `trapd.conf` file (.1.3.6.1.4.1.11.2.17.1). The trap number range .0.30000000 - .0.39999999 is reserved for multicast-specific traps.

You can easily forward these traps to other network management tools:

1. Select `Options:Event Configuration` to access the NNM Event Configuration window.
2. In the Enterprise Identification list, select:

   `OpenView .1.3.6.1.4.1.11.2.17.1`
3. To gather all multicast-specific trap definitions together (rather than sorting trap definitions by their names), select `View:Sort:Sort by Event Identifiers`.
4. All traps within the range .0.30000000 - .0.39999999 were added by NNM Multicast. Select each multicast trap (one at a time) and select `Edit:Describe Event` to learn about the traps provided.
5. By default, the trap definitions instruct NNM to post an alarm in the NNM Event Browser under the Multicast Alert Alarms category.

   If you wish to forward a trap to the management software of your choosing:

   Select the trap and select `Edit:Modify Event`.

   Click on [Help] for further instructions about using the NNM Event Configuration feature.

See *Managing Your Network with NNM* for more information about working with events. It is possible to implement complex responses to a trap being received, such as dialing a pager or automatically running a script to correct a problem. It is possible to use these traps in the NNM Event Correlation System and Reporting feature.

Public Trap Definitions

The important traps occur when NNM Multicast changes status of a router, interface, link (multicast neighbor relationship), or deletes an interface or link.

The following trap definitions are included in this section so that you can intercept them to use in other network management programs:

- EVENT_NEW_NODE a.k.a. OV_MCAST_New_Node (1,3,6,1,4,1,11,2,17,1,0,30000004)
- EVENT_STATUS_CHANGE a.k.a. OV_MCAST_Status_Chg (1,3,6,1,4,1,11,2,17,1,0,30000006)
- EVENT_DELETE_OBJ a.k.a. OV_MCAST_Delete_obj (1,3,6,1,4,1,11,2,17,1,0,30000007)
- EVENT_ADD_OBJ a.k.a. OV_MCAST_Add_Obj (1,3,6,1,4,1,11,2,17,1,0,30000009)

/* EVENT_NEW_NODE */

{1,3,6,1,4,1,11,2,17,1,0,30000004},

/*1. srcOID: srcId = 14

2. srcNameOID: srcname string(for browser)

   (selection name of node, interface or first intf of nbr)

3. dataOID: srcPID (mmon process IDs)

4. dataOID: dstPID (mmon process IDs)

   (all the rest are dataOID)

5. objectId-as-int from ovwdb e.g. sprintf("%d", objectId)

6. alarm browser message string: user label for new node

7. cause-as-integer (mmon-specific)

   0 = no specific cause

   1 = interface (affects node)

```
        2 = MRINFO from IGMP report
        3 = user configuration or user request
        4 = no IGMP response
        5 = no SNMP response
        6 = inconsistent neighboring reports
        7 = MIB information from SNMP report
        8 = link/tunnel/neighboring relationship (affects node)
        9 = two nodes merged together in database
    8. IP-monitorAddr-as-uint, e.g. sprintf(%lu", monitorAddress)
    9. sysDescr
*/
/* EVENT_STATUS_CHANGE */
{1,3,6,1,4,1,11,2,17,1,0,30000006},
/*1.  srcOID: srcId = 14
    2.  srcNameOID: srcname string(for browser)
        (selection name of node, interface or first intf of nbr)
    3.  dataOID: srcPID (mmon process IDs)
    4.  dataOID: dstPID (mmon process IDs)
    5.  statusOID: statusString, per pmd, e.g. "Warning",

        "Critical", etc.

        (all the rest are dataOID)
    6.  objType (mmon specific, 1-4)
          1 = node (router), 2 = interface, 3 = "neighbor"

          (multicast link), 4 = subnet
    7.  objectId-as-int  from ovwdb e.g. sprintf("%d", objectId)
    8.  alarm browser message string
```

```
 9.  status-as-integer from OV/ovw_types.h, e.g. 6 = Warning
 10. cause-as-integer (mmon-specific)
      0 = no specific cause
      1 = interface (affects node)
      2 = MRINFO from IGMP report
      3 = user configuration or user request
      4 = no IGMP response
      5 = no SNMP response
      6 = inconsistent neighboring reports
      7 = MIB information from SNMP report
      8 = link/tunnel/neighboring relationship (affects node)
      9 = two nodes merged together in database
 ---for interface:
 11. IP-address-as-uint   e.g. sprintf("%lu", ipAddress)
 12. ifDescr
 ---for node:
 11. IP-monitorAddr-as-uint
 12. sysDescr
 ---for neighbor:
 11. interface1 IP-addr-as-uint
 12. ifDescr for interface
 13. interface1 IP-addr-as-uint
 14. ifDescr for interface2
 ---for subnet:
 11. IP-address-as-uint
 12. IP-netMask-as-uint
*/
```

```
/* EVENT_DELETE_OBJ */
{1,3,6,1,4,1,11,2,17,1,0,30000007},
/*1.  srcOID: srcId = 14
  2.  srcNameOID: srcname string(for browser)
     (selection name of node, interface or first intf of nbr)
  3.  dataOID: srcPID (mmon process IDs)
  4.  dataOID: dstPID (mmon process IDs)

     (all the rest are dataOID)
  5.  objType (mmon specific, 1-4)
       1 = node (router), 2 = interface, 3 = "neighbor"

       (multicast link), 4 = subnet
  6.  objectId-as-int  from ovwdb e.g. sprintf("%d", objectId)
  7.  alarm browser message string
  8.  cause-as-integer (mmon-specific)
       0 = no specific cause
       1 = interface (affects node)
       2 = MRINFO from IGMP report
       3 = user configuration or user request
       4 = no IGMP response
       5 = no SNMP response
       6 = inconsistent neighboring reports
       7 = MIB information from SNMP report
       8 = link/tunnel/neighboring relationship (affects node)
       9 = two nodes merged together in database
  ---for interface:
  9.  IP-address-as-uint   e.g. sprintf("%lu", ipAddress)
```

10. ifDescr

---for node:

9. IP-monitorAddr-as-uint

10. sysDescr

If cause (item 8) is "9", additional info:

11. IP-monitorAddr-as-uint for new router node

12. sysDescr for new router node

---for neighbor:

9. interface1 IP-addr-as-uint

10. ifDescr for interface

11. interface1 IP-addr-as-uint

12. ifDescr for interface2

---for subnet:

9. IP-address-as-uint

10. IP-netMask-as-uint

*/

/*EVENT_ADD_OBJ */

{1,3,6,1,4,1,11,2,17,1,0,30000009},

/* Used for interfaces and links that appear AFTER a router node has been declared "new" (see EVENT_NEW_NODE for new routers, above)*/

/*1. srcOID: srcId = 14

2. srcNameOID: srcname string(for browser)

(selection name of node, interface or first intf of nbr)

3. dataOID: srcPID (mmon process IDs)

4. dataOID: dstPID (mmon process IDs)

(all the rest are dataOID)

5. objType (mmon specific, 1-4)

1 = node (router), 2 = interface, 3 = "neighbor"

```
      (multicast link), 4 = subnet
  6.  objectId-as-int  from ovwdb e.g. sprintf("%d", objectId)
  7.  alarm browser message string
  8.  cause-as-integer (mmon-specific)
      0 = no specific cause
      1 = interface (affects node)
      2 = MRINFO from IGMP report
      3 = user configuration or user request
      4 = no IGMP response
      5 = no SNMP response
      6 = inconsistent neighboring reports
      7 = MIB information from SNMP report
  ---for interface:
  9.  IP-address-as-uint   e.g. sprintf("%lu", ipAddress)
  10. ifDescr
  ---for node:
  9.  IP-monitorAddr-as-uint
  10. sysDescr
  ---for neighbor:
  9.  interface1 IP-addr-as-uint
  10. ifDescr for interface
  11. interface1 IP-addr-as-uint
  12. ifDescr for interface2
  ---for subnet:
  9.  IP-address-as-uint
  10. IP-netMask-as-uint
*/
```

E Migration from mmon 1.6

What's New?

If you are upgrading from *mmon* 1.6, it may be useful to know:

- The menu item names have changed.
- The dialog boxes have been converted to Java.
- Extensive context-sensitive online help information is now available from each window and the NNM Help pull-down menu.
- The installation procedure for NNM Multicast is automated

Installation Information

NOTE

If upgrading from any version of *mmon* **other than 1.6**, you must:

- Upgrade to *mmon* 1.6 before proceeding.

If upgrading from *mmon* 1.6, the NNM Multicast installation script makes all necessary changes.

When upgrading from *mmon* 1.6 to NNM Multicast 1.0, all of your customizations to the following files are preserved. None of your settings are changed during installation. The new versions of these files are installed to the `/usr/newconfig/etc/opt/OV/share/conf/*` directory.

- `mmon.conf` (TIP: the new `mmon.conf` file is placed in the same location and named `mmon.conf.template`. Review this file for any new settings that you may wish to incorporate.)
- `managed.mmon`
- `mmon_ma.conf`
- `mtraffic.conf`

When upgrading from *mmon* 1.6 to NNM Multicast 1.0, the following files are replaced with new ones during installation. If you made changes, your old files are renamed `#<filename>` during NNM Multicast installation so that they are available for future reference:

`mmonitor.lrf`

`mtraffic.lrf`

Several MIB files are loaded into the NNM SNMP MIB Browser (`/var/opt/OV/share/snmp_mibs/Experimental/Multicast/`). These are the latest versions of the multicast MIBs. If you had previous versions of these MIB installed on your NNM management station, the old MIB files are renamed `#<filename>` during NNM Multicast installation:

- IGMP-MIB.my
- IPMROUTE-MIB.my
- PIM-MIB.my

When migrating to NNM Multicast, you can choose to delete the NNM object database to start fresh, or continue using your database entries from mmon 1.6. See the "Stop Everything and Start Discovery Over Again" section at the end of Chapter 5, Initial Network Discovery, in *Managing Your Network with NNM*. This book was included with NNM. It is also available:

- From the HP Documentation web site in Adobe Acrobat format (pdf): `http://ovweb.external.hp.com/lpe/doc_serv/`
- From any NNM submap in DynaText format, select `Help:Online Manuals`. Click on the NNM Runtime Collection in the left-hand list, then select Managing your Network in the right-hand list.
- For purchase from FatBrain.com

Index