

# **HP OpenView Reporting and Network Solutions**

**Multicast Smart Plug-in**  
to  
**Network Node Manager**

**Administrator's Guide**

**Software Version: 2.1**

**for HP-UX, Solaris operating systems**



**i n v e n t**

**Manufacturing Part Number: None**

**April 2004**

© Copyright 2004 Hewlett-Packard Development Company, L.P.

---

## Legal Notices

### **Warranty.**

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

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

### **Restricted Rights Legend.**

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company  
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

### **Copyright Notices.**

©Copyright 2004 Hewlett-Packard Development Company, L.P.

No part of this document may be copied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

### **Trademark Notices.**

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

UNIX® is a registered trademark of The Open Group.

**1. Overview**

Multicast Management Technology Overview . . . . .	10
Multicast Routing Topology . . . . .	11
Interfaces & Neighbors Submap . . . . .	13
Subnet Submap . . . . .	14
Forwarding Tree Map Overlay . . . . .	15
Group Membership Map Overlay . . . . .	17
IP Address Identification . . . . .	19
PIM Designated Router Identification . . . . .	20
Multicast Data Collection: Group Traffic, Router Interface Traffic, Thresholds . . . . .	21
Troubleshooting Tools for the Multicast Environment . . . . .	23
The Multicast SPI Relationship to NNM Advanced Edition . . . . .	24

**2. Installation and Configuration**

Prerequisites . . . . .	28
Router Requirements . . . . .	28
NNM Management Station Requirements . . . . .	29
Installing the Multicast SPI 2.1 on HP-UX . . . . .	31
Installing the Multicast SPI on a Local System . . . . .	31
Installing the Multicast SPI from a Remote System with a CD-ROM Drive . . . . .	32
Installing the Multicast SPI 2.1 on Solaris . . . . .	35
Installing the Multicast SPI on a Local System . . . . .	35
Installing the Multicast SPI from a Remote System with a CD-ROM Drive . . . . .	36
Installing the Multicast SPI on NNM Advanced Edition Remote Console (Management Console) . . . . .	40
Multicast SPI on the NNM Advanced Edition Server . . . . .	40
Multicast SPI on NNM Advanced Edition Remote Consoles . . . . .	40
Configuring the Multicast SPI . . . . .	42
managed.mmon Configuration File . . . . .	43
unmanaged.mmon Configuration File . . . . .	45
mmon.conf Configuration File . . . . .	47
mmon_ma.conf Configuration File . . . . .	54
snmpCollect.lrf Configuration File . . . . .	55
Starting the Multicast SPI . . . . .	57
Stopping the Multicast SPI . . . . .	58
Uninstalling the Multicast SPI . . . . .	60
Entering License Information . . . . .	62
Troubleshooting for Licensing . . . . .	64

---

# Contents

## 3. Getting Started with the Multicast Smart Plug-in

The Multicast SPI Makes Your Job Easier	68
Mapping Your Multicast Environment	69
“Which routers within my management domain are configured to handle multicast?”	69
“Which multicast groups does this router serve?”	70
“Which subnets have subscribers to this group’s traffic?”	71
“What path does the routing tree for this group follow?”	71
“Which router or subnet contains the given IP address?”	72
“Which router is the PIM designated router for this subnet?”	72
“What is the status of the multicast equipment?”	73
Monitoring Your Multicast Environment	75
“How can I collect multicast-specific performance data and set multicast-specific thresholds?”	75
“What is the true impact of a specific multimedia data stream on my network?”	76
“What proportion of network traffic is multicast traffic?”	76
“How can I set absolute limits on the amount of bandwidth available to multicast groups?”	77
Troubleshooting the Multicast Environment	78
“Which group is generating all this traffic?”	78
“Which hosts are the sources of this group’s traffic?”	79
“Which router is blocking the flow of data to my multicast customer?”	79
“A router is flooded, is that because of unicast or multicast traffic?”	80

## A. Troubleshooting the Multicast Smart Plug-in

The Multicast SPI Submaps	82
Why does it take so long to open NNM ?	82
Multicast menu commands don’t work. Why?	82
The Multicast submap has blue icons. What's wrong?	82
The Multicast SPI submap has white icons. What's wrong?	85
How are symbol names (symbol labels) determined by the Multicast SPI?	86
A router symbol on the Multicast submap doesn’t make sense.	88
What does the color of the router or subnet or interface symbol mean?	88
The router symbol color keeps switching between green and red. What happened?	89
The router symbol color keeps switching between green and orange. What happened?	90
The connection symbol keeps switching from black to red. What happened?	91

The forwarding tree is broken into multiple trees. Why? . . . . .	92
Why are two router symbols referring to the same physical router? . . . . .	92
Are there any limits to the number of devices that the Multicast SPI can manage? . . . . .	92
Why is a single physical interface appearing in two different routers? . . . . .	93
The PIM Designated Router is not highlighted for some of the submaps. Why? . . . . .	93
The Multicast SPI Data Collection and Alarms . . . . .	94
The network is flooded after installing the Multicast SPI . . . . .	94
Alarm: “Router X failed to respond to some SNMP queries.” . . . . .	94
Alarm: “Could not find intfcd corresponding to index N:router-A. Please rediscover node.” . . . . .	95
Multicast Data Collection isn’t happening when it should. . . . .	95
When I type “ovstatus mmonitor”, I get the error message “Terminated due to invalid configuration.” . . . . .	96
The Multicast SPI Graphs and Tables . . . . .	97
Grapher error message, “Counter for <router-a> McastOctets.x.x.x.y.y.y wrapped (nnnn -> mmmm). Waiting for next.” What does this mean? . . . . .	97
I used to see historical data with the Graph Group Traffic. Now I only see live traffic. . . . .	97
The Monitor Group Traffic Collection table is missing some groups. Why? . . . . .	97
The traffic collection tables are empty. Why? . . . . .	97
Performance . . . . .	98
The Multicast SPI performance is very slow and/or is using a high percentage of the management station’s CPU. . . . .	98
Web Interface . . . . .	99

## B. Frequently Asked Questions

Questions about the Multicast Smart Plug-in Submaps . . . . .	102
Which routers work with the Multicast SPI? . . . . .	102
Why can't I move symbols into submaps, and “containerize” my map? . . . . .	102
When I hide an interface that is down, the router status is still affected. Why? . . . . .	102
How are multicast tunnels depicted on the Multicast SPI submaps? . . . . .	102
The Multicast submap is empty. Why? . . . . .	105
How does the Multicast SPI discovery process work? . . . . .	105
Questions about the Multicast SPI Data Collection and Alarms . . . . .	107
Multicast data collections are not happening. Why? . . . . .	107
What are the important SNMP TRAPS that the Multicast SPI generates? . . . . .	107
Why do the Monitor Group Traffic Collection and Monitor Interface Traffic Collection tables open slowly? . . . . .	107
How do I determine the best value for “CYCLE_MINUTES” in mmon.conf? . . . . .	108

---

# Contents

How do I determine the best value for “IGMP_PARMS” in mmon.conf? . . . . .	108
How can I get information from the NNM Object Database (ovwdb)? . . . . .	108
Questions about Accessing the Multicast SPI . . . . .	109
Can the Multicast SPI be run on a collection station and forward data and alarms to an NNM management station? . . . . .	109
What Multicast SPI operations are available through a web browser? . . . . .	109
How do I access the web-based Multicast SPI operations apart from the NNM menu commands? . . . . .	109

## C. Command Line Utilities and Multicast Process Options

mdbprint . . . . .	113
mdbck . . . . .	114
mmonlog . . . . .	115
mmonitor . . . . .	116
mtraffic . . . . .	118
mmap . . . . .	120
Logging and Tracing for the Multicast SPI . . . . .	121
Switch Options . . . . .	122
Environment Variables . . . . .	125

## D. Multicast-Specific SNMP Trap Definitions

Harnessing the power of SNMP traps . . . . .	128
Public Trap Definitions . . . . .	130

## E. Migration to the Multicast Smart Plug-in 2.1

What’s New? . . . . .	140
Multicast 2.0 to Multicast 2.0 with the Consolidated Patch Number PHSS_28159/PSOV03228. . . . .	140
Multicast 2.0 with the Consolidated Patch Number PHSS_28159/PSOV03228 to the Multicast Smart Plug-in 2.1. . . . .	143
Migration from Multicast 2.0 to the Multicast SPI 2.1 . . . . .	146

---

## Support

Please visit the HP OpenView web site at:

<http://openview.hp.com/>

There you will find contact information and details about the products, services, and support that HP OpenView offers.

You can go directly to the HP OpenView support web site at:

<http://support.openview.hp.com/>

The support site includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information





---

# **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? The Multicast Smart Plug-in (SPI) 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 a particular 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

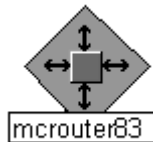


The Multicast SPI adds a new symbol to the Root level of your HP OpenView Network Node Manager (NNM) Advanced Edition maps.

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. The Multicast menu lists tools for managing the multicast-enabled routers and subnets. This menu appears on the submaps in the Multicast hierarchy.

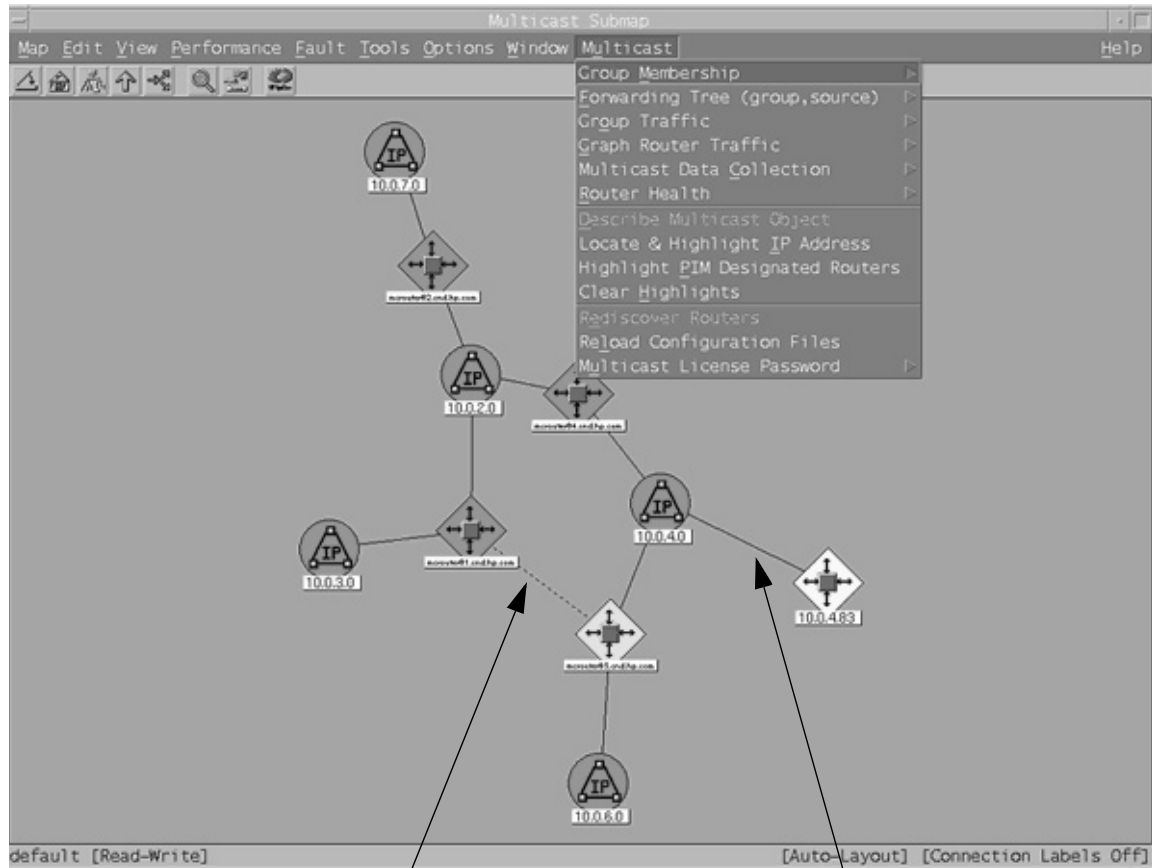
Figure 1-1 shows the Multicast Submap.

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. The name of the multicast object ends with a “space” character to distinguish it from the database object of the same name that was added by NNM during the discovery process.



For example, `mcrouter83` may be displayed on your Multicast submap and on the NNM Internet submap. The name of the multicast object actually ends with a space character (`mcrouter83` ) on the Multicast 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 Multicast submap is calculated based upon multicast error conditions.

**Figure 1-1 Multicast Submap Showing the Multicast Menu Commands**



A dashed line between two routers represents a multicast tunnel. A solid line between two routers represents a direct-connect neighbor relationship.

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

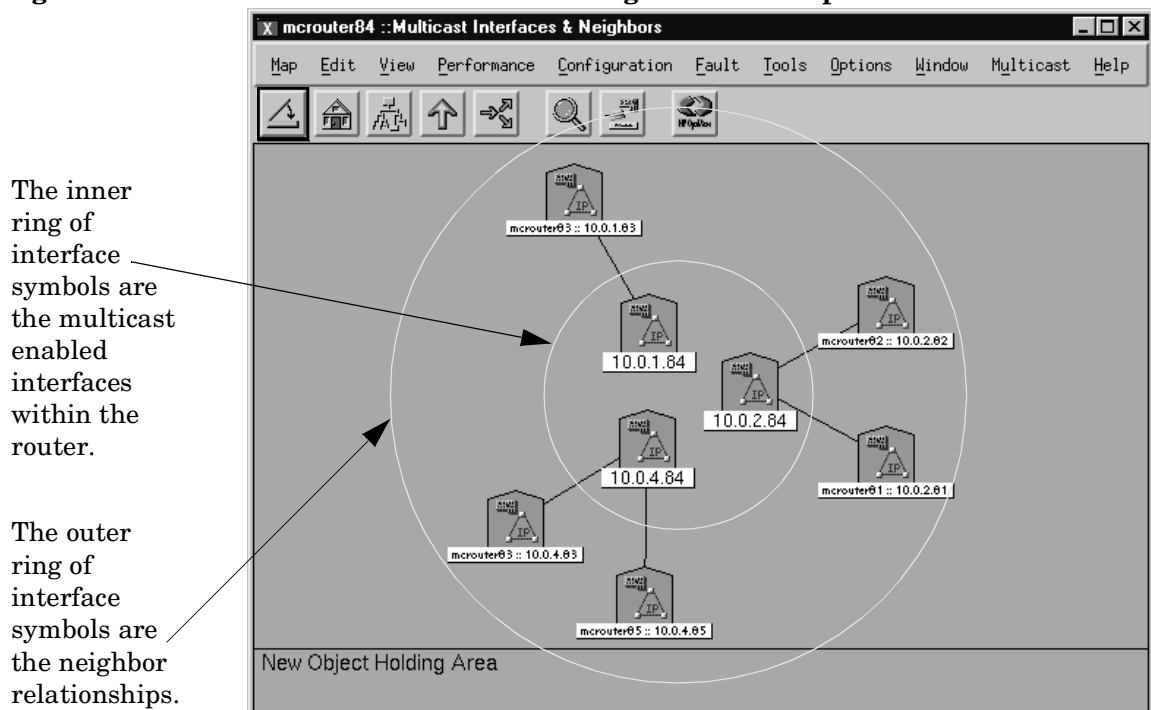
## Interfaces & Neighbors Submap

This submap is only available if you have READ/WRITE access to the map. Double-click a router symbol on the Multicast submap to display the Interfaces & Neighbors submap. This submap displays the interface symbols arranged in two rings:

- The inner ring includes all multicast-enabled interfaces within the selected router. (If you are using anycast for fail-over protection, the labels of the interface icons have the router name appended to the address, since the address is a duplicate IP address.)
- The outer ring shows the neighbor relationship to connecting multicast-enabled interfaces on other routers.
- Multicast neighbor relationships that utilize tunnel interfaces (also called “multicast tunnels”) are depicted with dashed connection lines. See “How are multicast tunnels depicted on the Multicast SPI submaps?” on page 102 for examples and more information about multicast tunnels.

Figure 1-2

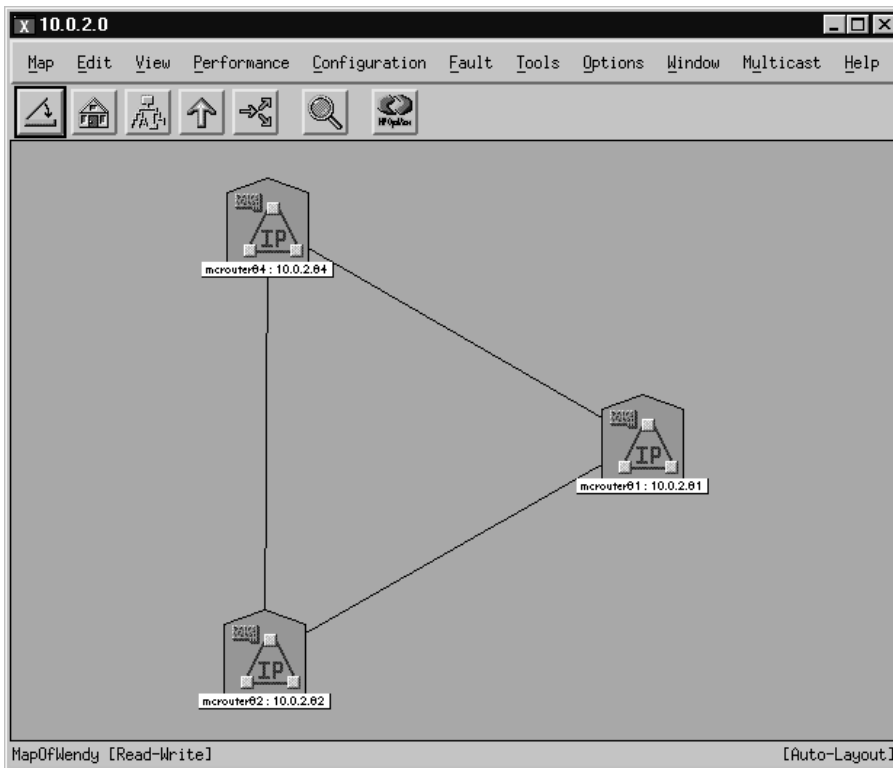
### Multicast Interfaces & Neighbors Submap



## 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.

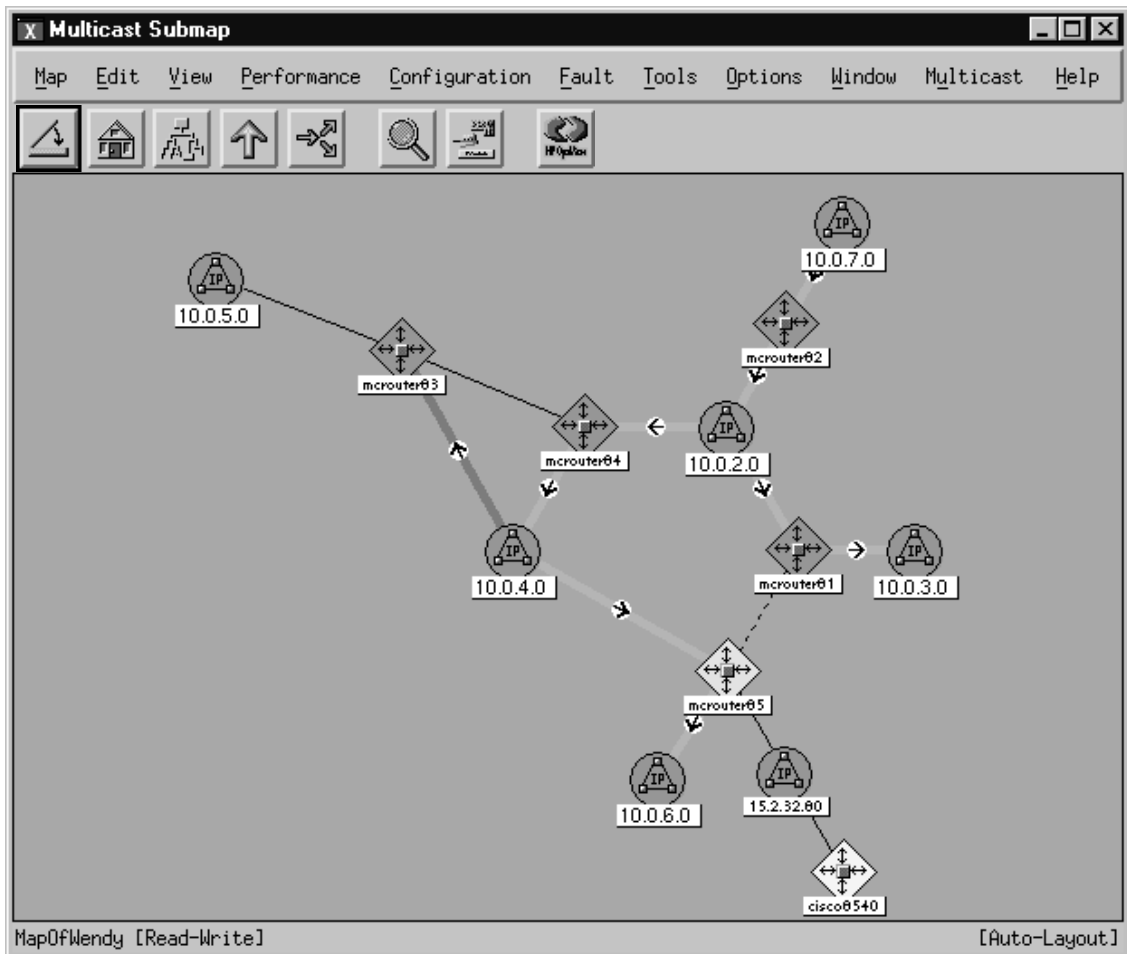
**Figure 1-3** Multicast Subnet Submap



## Forwarding Tree Map Overlay

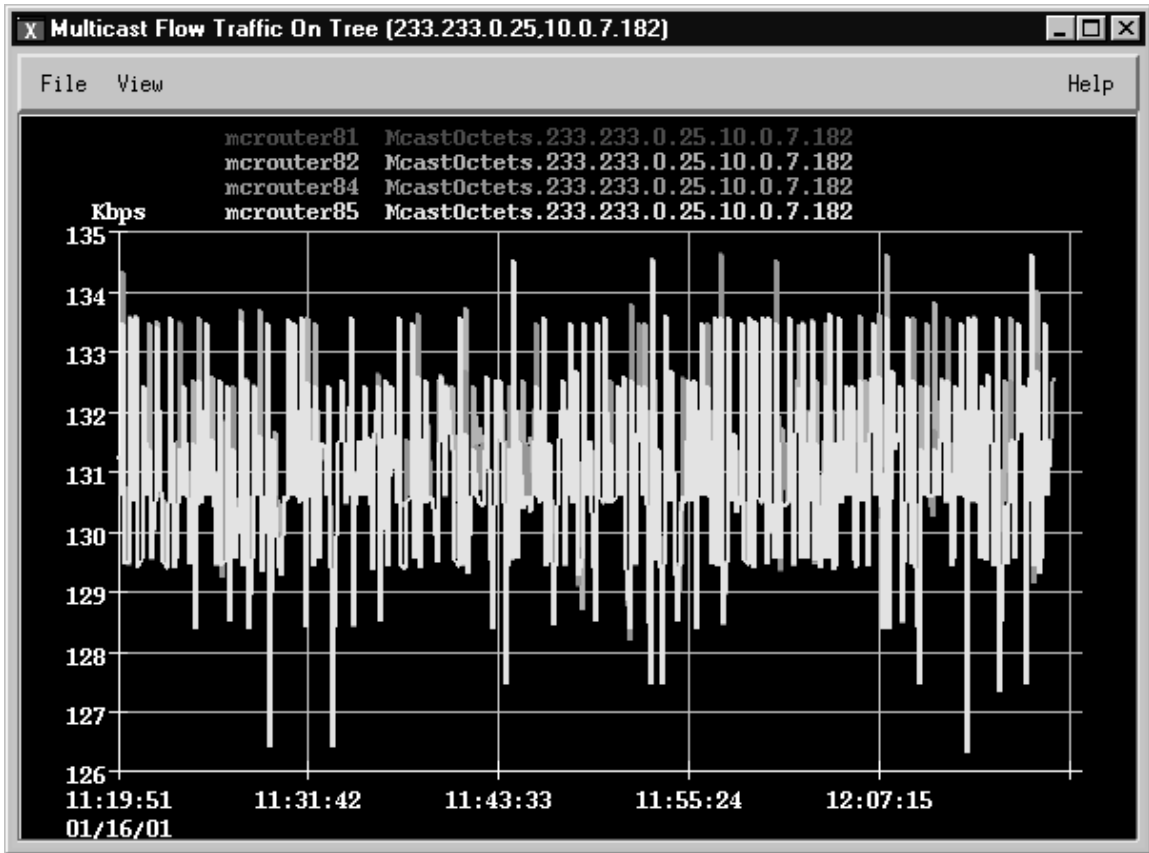
After you specify a valid multicast group and source, the Multicast SPI can display the forwarding tree. Arrows show the direction that data is flowing over the tree. Xs indicate a pruned state. If the source machine is within your multicast management domain, the forwarding tree can be drawn from the 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.

Figure 1-4 Multicast Forwarding Tree



The Multicast SPI can collect data about the traffic on each multicast-enabled router and provides a graph showing the currently displayed forwarding tree's ongoing traffic over each router.

**Figure 1-5** Graph of Multicast Traffic on the Forwarding Tree





## Group Membership Map Overlay

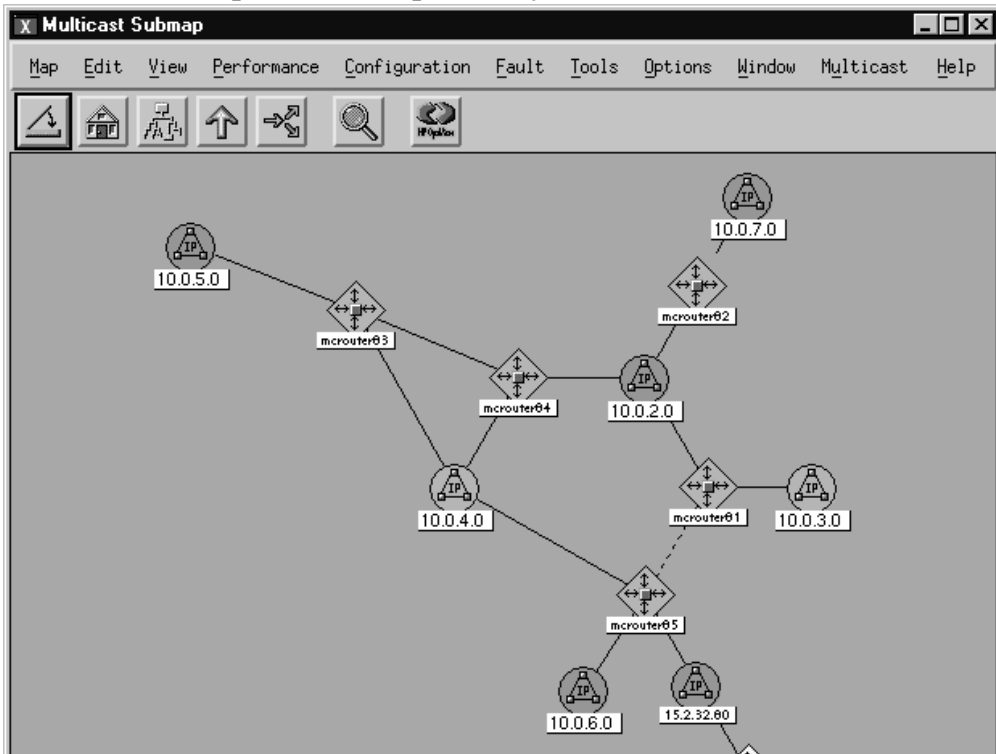
The Multicast SPI can easily highlight all subnets and routers belonging to a specific multicast group:

- 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: A Cisco Router can be configured to bypass the standard IGMP protocol and join multicast groups through the “static group” IOS command. Routers that have joined the multicast group in this manner cannot be detected reliably. If a Cisco Router is configured with the “static group” command on a software loopback interface, the Multicast SPI infers that the router has joined the group (self-subscribed).

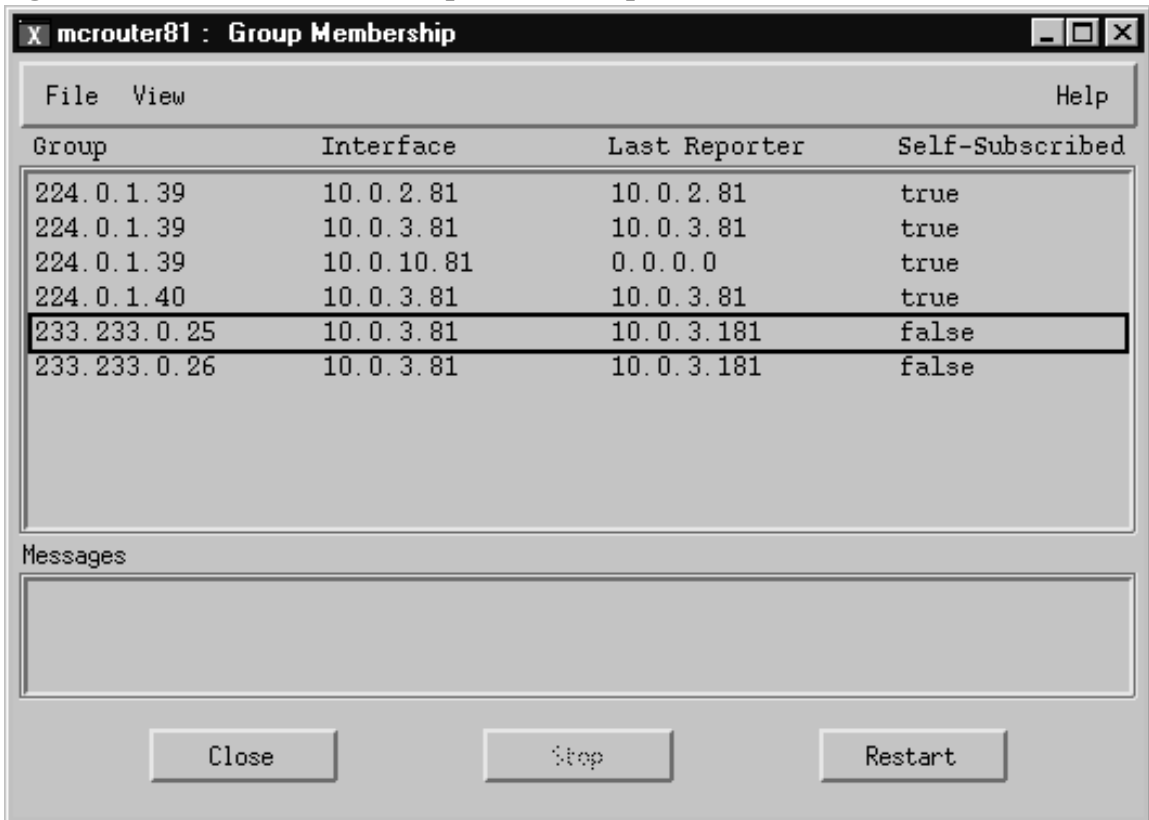
The symbols of the member routers and subnets turn salmon color.

Figure 1-6 Group Membership Overlay



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.

**Figure 1-7** Table of Group Membership



The screenshot shows a window titled "mcrouter81 : Group Membership" with a menu bar containing "File", "View", and "Help". Below the menu bar is a table with the following data:

Group	Interface	Last Reporter	Self-Subscribed
224.0.1.39	10.0.2.81	10.0.2.81	true
224.0.1.39	10.0.3.81	10.0.3.81	true
224.0.1.39	10.0.10.81	0.0.0.0	true
224.0.1.40	10.0.3.81	10.0.3.81	true
233.233.0.25	10.0.3.81	10.0.3.181	false
233.233.0.26	10.0.3.81	10.0.3.181	false

Below the table is a "Messages" section with an empty text area. At the bottom of the window are three buttons: "Close", "Stop", and "Restart".

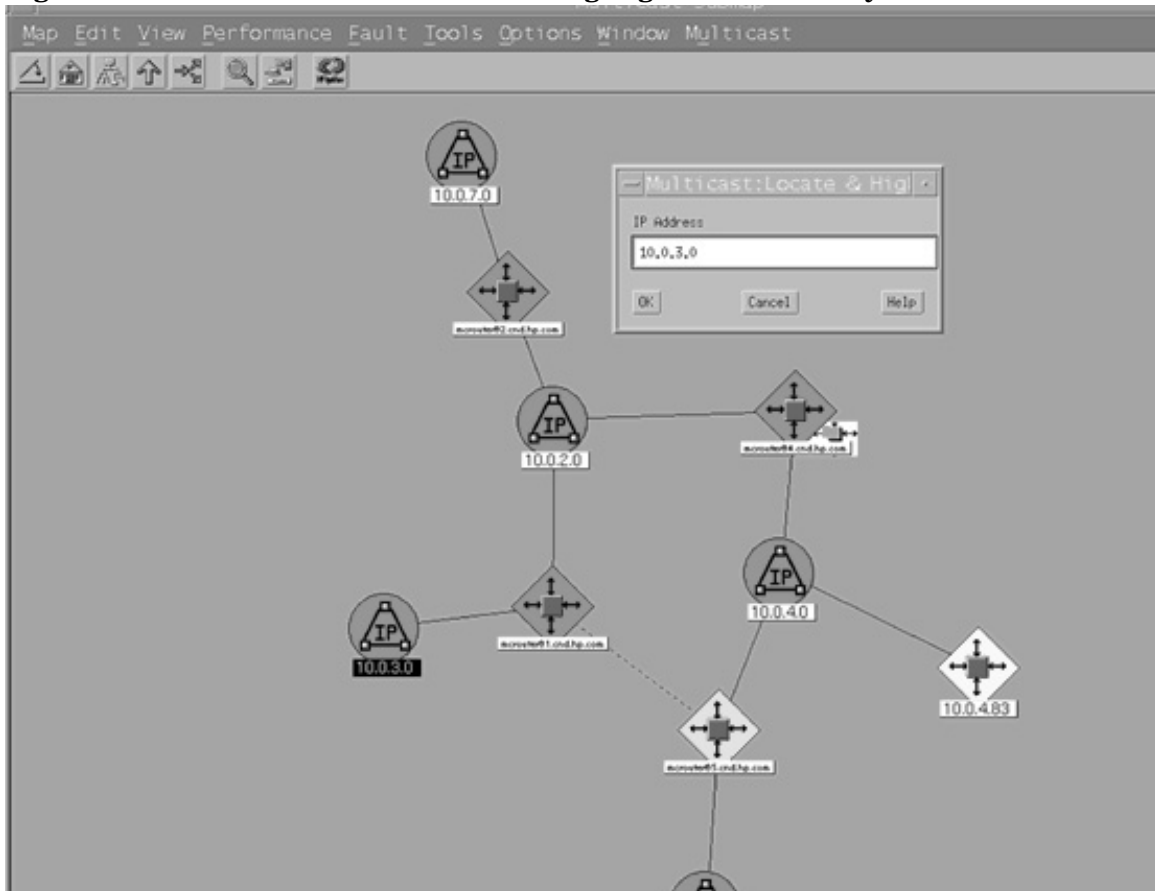
## IP Address Identification

The Multicast SPI can locate a specific IP address within the multicast topology. This information is useful when troubleshooting a problem with the multicast traffic to or from a specific IP address.

If the specified IP address belongs to one of the routers that the Multicast SPI manages, that router symbol and the connection that represents the interface are highlighted. If the specified IP address does not belong to one of these routers, the symbol for the containing subnet is highlighted.

Figure 1-8 shows the Multicast Submap with the router for the 10.0.3 subnet highlighted.

**Figure 1-8** IP Address Locate & Highlight Functionality

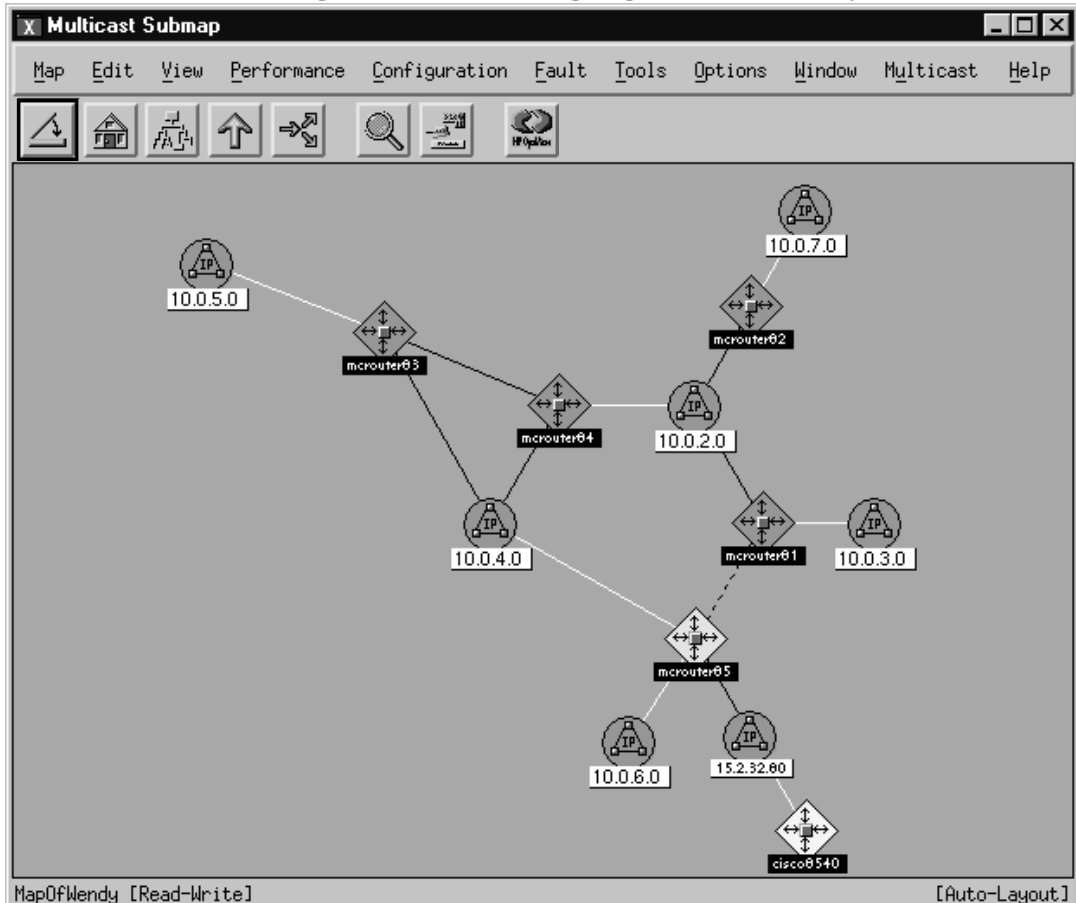


## PIM Designated Router Identification

The Protocol-Independent Multicast (PIM) routing protocol, when used in your multicast environment, designates a single router on each subnet to handle IGMP JOIN requests. When a Multicast problem arises on a host in a subnet, the nearest PIM designated router is the best place to start looking for answers to the problem.

The Multicast SPI can instantly identify the PIM designated routers within your multicast management domain. The labels of all PIM designated router symbols are highlighted and the interface connection being serviced by each PIM router (connecting line) is changed to white for each subnet.

**Figure 1-9 PIM Designated Routers Highlight Functionality**



---

## 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. You can configure automatic responses to multicast threshold alarms, such as dialing a pager or launching a script to fix the problem (see page 128 for more information).

**Figure 1-10**

### Multicast Data Collection Configuration Dialog Box

**X Multicast: Configure Data Collection for Selected R...**

Collect Group Traffic Data  
Group Traffic Polling Interval (Seconds)  
300

Collect Interface Traffic Data  
Interface Traffic Polling Interval (Seconds)  
300

Generate alarm when threshold crossed  
Interface Traffic Threshold (%)  
10

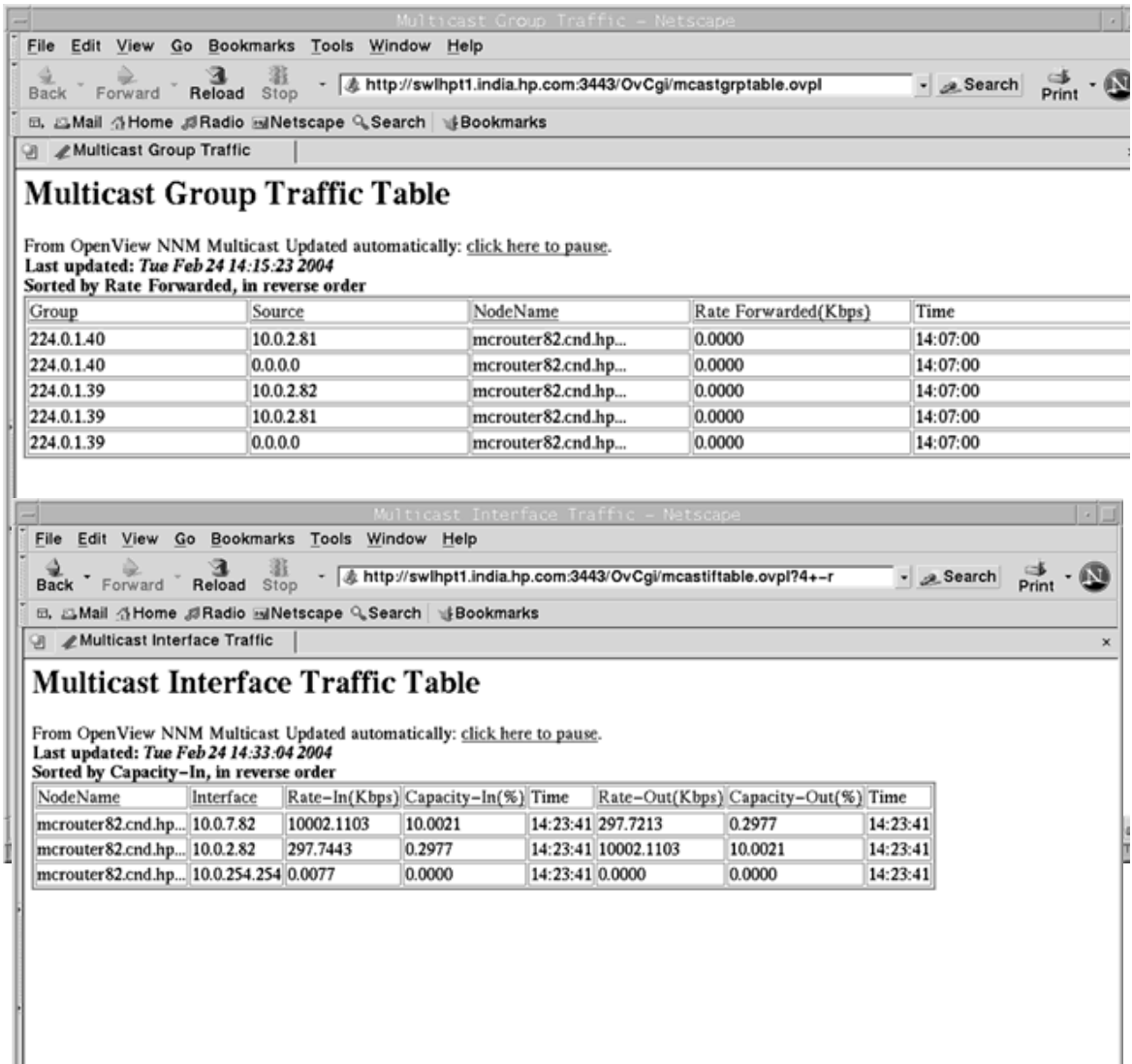
Selected Routers  
mcrouter83  
mcrouter81  
mcrouter82

OK Cancel Help

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

After your data collection is configured, the Multicast SPI provides two tables showing ongoing results of all multicast group-traffic data collection and all interface multicast-traffic data collection. These results are displayed in web browser windows. These tables can be viewed on your management station or over the network from remote locations.

**Figure 1-11 Multicast Traffic Data Collections**



## 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).

**Figure 1-12 Table of Multicast Group Activity**

Group	Source	Rate (FirstSample, Kbps)	InMcastBytes	Incoming Interface	UpStream Nbr
224.0.1.40	0.0.0.0	0.0000	0	*	0.0.0.0
224.0.1.40	10.0.10.81	0.0000	0	10.0.2.82	10.0.2.81
224.0.1.40	10.0.2.81	0.0000	0	10.0.2.82	0.0.0.0
233.233.0.25	0.0.0.0	0.0000	2672	*	0.0.0.0
233.233.0.25	10.0.7.182	129.8485	49239665	10.0.7.82	0.0.0.0
233.233.0.25	10.0.6.185	63.6787	24418586	10.0.2.82	10.0.2.84
233.233.0.26	10.0.3.181	64.4917	24548713	10.0.2.82	10.0.2.81
233.233.0.26	0.0.0.0	0.0000	1357	*	0.0.0.0

Messages  
 Last Sampled: Tue Jan 16 10:26:06 2001

Buttons: Close, Stop, Restart

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 Multicast SPI Relationship to NNM Advanced Edition

During initial discovery, you define the multicast management domain; the Multicast SPI uses the mmonitor background process 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 object that the NNM's netmon background process added to the NNM object database during the network discovery process. By creating a duplicate database object for each multicast-enabled router, the status of the router can be calculated separately for the multicast context and the internet context.

---

**TIP**

The NNM netmon process can be disabled without affecting the Multicast SPI. Disabling netmon reduces polling traffic but does not change the Multicast SPI's ability to managed the multicast-enabled routers.

---

The Multicast SPI draws submaps of your multicast management domain that are independent NNM's discovery and status polling (done by the netmon and Extended Topology processes). The multicast submaps are not affected by NNM filters (such as NNM's map filter or discovery filter). You control which multicast routers are managed or unmanaged by making entries in the managed.mmon and unmanaged.mmon files. The multicast submaps can be viewed remotely through the NNM Launcher; however, the Multicast menu commands cannot be accessed over the World Wide Web.

The Multicast SPI adds an alarm category called Multicast Alert Alarms to the NNM alarm browser. The Multicast SPI uses the mmonitor background process to send multicast-related SNMP traps to the NNM alarm browser.

The Multicast SPI 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 stored in the NNM object database. The mtraffic background process uses the database entries to automatically configure NNM's Data Collection & Thresholds feature.



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

The Multicast SPI 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.

Overview

**The Multicast SPI Relationship to NNM Advanced Edition**

---

## **2 Installation and Configuration**

## Prerequisites

The Multicast Smart Plug-in (SPI) uses SNMP multicast-related MIBs and, optionally, a subset of the IGMP protocol. The Multicast SPI uses SNMP (run above UDP and IP in the network protocol stack) to communicate with multicast-enabled routers. By default, the Multicast SPI also uses IGMP for discovery. However, if a router cannot respond properly to the public-domain tool *mrintfo*, the Multicast SPI cannot use IGMP and must use SNMP only. In this case, set the `DISCOVERY_VIA_SNMP` parameter in the `mmon.conf` file for SNMP-only discovery and management. For more information, see “`mmon.conf` Configuration File” on page 47.

## Router Requirements

For a router to be managed by the Multicast SPI, its SNMP agent must support the following MIBs:

- 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`.

The MIB-II object `sysName` must be set, and must be unique for each multicast-enabled router that you wish to manage.

- `ipMRouteStdMIB` or `ipMRouteMIB` used to determine multicast routing, and forwarding tree information. It is located either:
  - under the experimental branch of the MIB tree (version 6 or later, `draft-ietf-idmr-multicast-routmib-06.txt`) `.1.3.6.1.3.60`.
  - IETF standard RFC 2932 `1.3.6.1.2.1.83`
- `igmpStdMIB` or `igmpMIB` used to determine group membership and related information. It is located either:
  - under the experimental branch of the MIB tree (version 00 or later, `draft-ietf-idmr-igmp-mib-00.txt`) `.1.3.6.1.3.59`.
  - IETF standard RFC 2933 `1.3.6.1.2.1.85`

- pimMIB (version 00 or later, draft-ietf-idmr-pim-mib-00.txt) used to determine PIM specific information such as rendezvous points. This MIB is required only if PIM is in use. This is currently under the experimental branch of the MIB tree: .1.3.6.1.3.6.1.

For a router to be discovered with IGMP, it 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*.

## NNM Management Station Requirements

You must install the Multicast SPI on an NNM management station that meets the following requirements:

1. HP-UX 11.0 or 11.11 (Not HP-UX 11.20, no IA 64); or Solaris 2.8 or 2.9.
2. The current list of required operating system patches is met. For this list, see the file appropriate to your operating system in the `/opt/OV/www/htdocs/C/ReleaseNotes/Required_OS_Patch_Lists` directory.
3. An installed, HP OpenView Network Node Manager, NNM Advanced Edition 7.01, with an enterprise-level license. Also, install the latest consolidated patch: from any NNM Advanced Edition submap, select Help:NNM->Patches and Updates. Follow the links to check for the most recent patch available.

Network Node Manager Advanced Edition can be running in any language; however, the Multicast SPI always appears in English at this time.

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

- 512 MB RAM
- 1 GB free disk space
- 768 MB free swap space

#### 4. Configuring NNM.

NNM must know the *GET-Community name* for each router to be managed by the Multicast SPI.

For best results, before installing the Multicast SPI, 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 dialog box.
- 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.
- f. If deploying the Multicast SPI in a *private network* setting (for example in a test environment using 10.\*.\* IP addresses), to prevent performance problems caused by time-outs due to name resolution failures:
  - Either configure your name resolution service for the test machines.
  - Or create a wildcard entry in NNM’s `Options:SNMP Configuration` dialog box for the IP address space that is not configured through your name resolution service. For example 10.0.\*.\*

---

**NOTE**

---

The SNMP data collection time-out settings are also set in this `SNMP Configuration` dialog box.

## Installing the Multicast SPI 2.1 on HP-UX

---

### NOTE

If you are upgrading from any previous version of Multicast, you must read Appendix E, “Migration to the Multicast Smart Plug-in 2.1,” on page 139 before proceeding. This appendix provides information about migrating from Multicast 2.0.

---

The Multicast SPI comes with a 60-day trial license. After you have installed the Multicast SPI, request a permanent license password. See “Entering License Information” on page 62 for more information.

This section describes the ways you can install your the Multicast SPI product:

- On a local HP-UX system (the most common type of installation).
- From a different HP-UX machine that has a CD-ROM drive (if your system does not).

For Solaris systems, see “Installing the Multicast SPI 2.1 on Solaris” on page 35.

For NNM Advanced Edition remote consoles, see “Installing the Multicast SPI on NNM Advanced Edition Remote Console (Management Console)” on page 40.

### Installing the Multicast SPI on a Local System

To install all required components of the Multicast SPI product on your local system, follow these steps.

---

### CAUTION

If you try running `swinstall` instead, several critical steps are excluded.

---

1. Log in as `root` to the NNM 7.01 management station where you wish to install the Multicast SPI.
2. Set the `DISPLAY` variable by typing:  

```
export DISPLAY=hostName:0.0
```

## Installing the Multicast SPI 2.1 on HP-UX

3. Insert the Multicast SPI CD into the CD-ROM drive.

4. Mount the CD-ROM disk by typing:

```
/etc/mount /dev/dsk/device_name /cdrom
```

where **device\_name** is the specific name of your CD drive.

5. Use the `cd` command to change to the `/cdrom` directory.

6. Start the installation program by typing: **./install**

7. An installation program appears on screen.

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 the Multicast SPI.

When the installation is finished, check the `/var/adm/sw/swagent.log` file if you want more detailed information about the completed installation steps.

8. See the Multicast SPI release notes located in the root directory of the installation CD.

9. Use the `cd /` command to back out of the `/cdrom` directory.

10. Unmount the CD-ROM disk by typing

```
/etc/unmount /dev/dsk/device_name /cdrom
```

where **device\_name** is the specific name of your CD drive.

11. Remove the Multicast SPI CD from the CD ROM drive.

12. Go to “Configuring the Multicast SPI” on page 42.

13. Go to “Starting the Multicast SPI” on page 57.

14. Go to “Entering License Information” on page 62.

## Installing the Multicast SPI from a Remote System with a CD-ROM Drive

If your system (the target system) does not have a CD-ROM drive attached, you can use another system (the source system) with a CD-ROM drive to install the Multicast SPI on your system.



On the source system where the CD-ROM drive is located, do the following:

1. Log in as `root`.
2. Insert the Multicast SPI CD into the CD-ROM drive.
3. Mount the CD-ROM drive by typing

```
/etc/mount /dev/dsk/device_name /cdrom
```

where **`device_name`** is the specific name of your CD drive.

4. Export the CD-ROM file system (by completing steps a and b below) so that the target workstation can NFS mount it:

In the examples below, `marion` is the name of the source HP-UX workstation where the CD-ROM drive is physically mounted, and `marvin` is the name of the target workstation.

- a. Add the following line to the file, `/etc/exports`:

```
/cdrom -ro,root=marvin
```

- b. Export the file system with the following command:

```
/usr/sbin/exportfs -a
```

On the target NNM 7.01 management station where you want to install the Multicast SPI product, follow these steps to install all required components of the Multicast SPI product on the remote system.

---

**CAUTION**

---

If you try running `swinstall` instead, several critical steps are excluded.

1. NFS mount the CD-ROM file system (at `/cdrom`, for example). Execute the commands:

```
mkdir /cdrom
```

```
mount marion:/cdrom /cdrom
```

2. Change to the directory where you mounted the CD-ROM file system. Execute

```
cd /cdrom
```

3. Set the `DISPLAY` variable by typing:

```
export DISPLAY=marvin:0.0
```

4. Install your the Multicast SPI product. Execute

```
./install
```

5. An installation program appears on screen.

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. In this case, you must fix the error, then re-run the installation program in order to install the Multicast SPI.

When the installation is finished, check the `/var/adm/sw/swagent.log` file if you want more detailed information about the completed installation steps.

6. See the Multicast SPI release notes located in the root directory of the installation CD.

7. On the *target* system:

- Use the `cd /` command to back out of the `/cdrom` directory.
- Unmount the CD-ROM disk by typing

```
/etc/unmount /dev/dsk/device_name /cdrom
```

where ***device\_name*** is the specific name of your CD drive.

8. On the *source* system:

- Use the `cd /` command to back out of the `/cdrom` directory.
- Unmount the CD-ROM disk by typing

```
/etc/unmount /dev/dsk/device_name /cdrom
```

where ***device\_name*** is the specific name of your CD drive.

9. Remove the Multicast SPI CD from the CD-ROM drive.

10. Go to “Configuring the Multicast SPI” on page 42.

11. Go to “Starting the Multicast SPI” on page 57.

12. Go to “Entering License Information” on page 62.

---

## Installing the Multicast SPI 2.1 on Solaris

---

### NOTE

If you are upgrading from any previous version of Multicast, you must read Appendix E, “Migration to the Multicast Smart Plug-in 2.1,” on page 139 before proceeding. This appendix provides information about migrating from Multicast 2.0.

---

The Multicast SPI comes with a 60-day trial license. After you have installed the Multicast SPI, request a permanent license password. See “Entering License Information” on page 62 for more information.

This section describes the ways you can install your the Multicast SPI product:

- On a local Solaris system (the most common type of installation).
- From a different Solaris machine that has a CD-ROM drive (if your system does not).

For HP-UX systems, see “Installing the Multicast SPI 2.1 on HP-UX” on page 31.

For NNM Advanced Edition remote consoles, see “Installing the Multicast SPI on NNM Advanced Edition Remote Console (Management Console)” on page 40.

### Installing the Multicast SPI on a Local System

To install all required components of the Multicast SPI product on your local system, follow these steps.

---

### CAUTION

If you try running `swinstall` instead, several critical steps are excluded.

1. Log in as `root` to the NNM 7.01 management station where you wish to install the Multicast SPI.
2. Set the `DISPLAY` variable by typing:  

```
export DISPLAY=hostName:0.0
```

3. Insert the Multicast SPI CD into the CD-ROM drive.

4. Mount the CD-ROM disk by typing

```
cd /cdrom/cdrom0
```

5. Type **ls -l** to see a listing of the files in `cdrom0`.

6. Start the installation program by typing **./install**

7. An installation program appears on screen.

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 the Multicast SPI.

When the installation is finished, check the `/var/adm/sw/swagent.log` file if you want more detailed information about the completed installation steps.

8. See the Multicast SPI release notes located in the root directory of the installation CD.

9. Remove the Multicast SPI CD from the CD-ROM drive by typing:

```
cd /
```

```
eject cdrom
```

10. Go to “Configuring the Multicast SPI” on page 42.

11. Go to “Starting the Multicast SPI” on page 57.

12. Go to “Entering License Information” on page 62.

## **Installing the Multicast SPI from a Remote System with a CD-ROM Drive**

If your system (the target system) does not have a CD-ROM drive attached, you can use another system (the source system) with a CD-ROM drive to install the Multicast SPI on your system. The source system must have the same version of the Solaris operating system as the target system.

On the source system where the CD-ROM drive is located, do the following:

1. Log in as root.
2. Insert the Multicast SPI CD into the CD-ROM drive.
3. Mount the CD-ROM disk by typing

```
cd /cdrom/cdrom0
```

4. Type **ls -l** to see a listing of the files in `cdrom0`.

Share the CD-ROM. (In the examples below, `marion` is the name of the source Solaris workstation where the CD-ROM drive is physically mounted, and `marvin` is the name of the target workstation.) Add the following line to the file `/etc/dfs/dfstab` on `marion`:

```
share -F nfs -o ro,nosuid,root=marvin /cdrom/cdrom0
```

5. Verify that the correct NFS services are running on the source workstation by typing:

```
ps -ef | grep nfs
```

You should see the following services:

```
/usr/lib/nfs/statd  
/usr/lib/nfs/lockd  
/usr/lib/nfs/mountd  
/usr/lib/nfs/nfsd -a 16
```

All four services must be present. If `mountd` and `nfsd` are not started then notify any users of the source system that NFS will be momentarily interrupted.

6. As root, type:

```
/etc/rc3.d/S15nfs.server stop  
/etc/rc3.d/S15nfs.server start
```

7. Verify that the `mountd` and `nfsd` services are running by typing:

```
ps -ef | grep nfs
```

8. Verify that the CD-ROM is shared by typing:

```
share
```

You should see a list of all shared directories.

*On the target NNM 7.01 management station* where you want to install the Multicast SPI product, follow these steps to install all required components of the Multicast SPI product on the remote system.

---

**CAUTION**

---

If you try running `swinstall` instead, several critical steps are excluded.

1. NFS mount the CD-ROM file system (at `/cd_mnt`, for example).  
Execute the commands:

```
mkdir /cd_mnt
```

```
mount marion:/cdrom/cdrom0 /cd_mnt
```

Do not use `cdrom` as a directory name.

2. Change to the directory where you mounted the CD-ROM file system. Execute

```
cd /cd_mnt
```

3. Set the `DISPLAY` variable by typing:

```
export DISPLAY=marvin:0.0
```

4. Install your the Multicast SPI product. Execute

```
./install
```

5. An installation program appears on screen.

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. In this case, you must fix the error, then re-run the installation program in order to install the Multicast SPI.

When the installation is finished, check the `/var/adm/sw/swagent.log` file, if you want more detailed information about the completed installation steps.

6. See the Multicast SPI release notes located in the root directory of the installation CD.
7. Unmount the `cd_mnt` directory by typing:  

```
cd /  
umount /cd_mnt
```
8. Go to “Configuring the Multicast SPI” on page 42.
9. Go to “Starting the Multicast SPI” on page 57.
10. Go to “Entering License Information” on page 62.

## Installing the Multicast SPI on NNM Advanced Edition Remote Console (Management Console)

This section describes deploying the Multicast SPI into an NNM Advanced Edition environment where one NNM management station functions as the server machine (housing all of the NNM databases) and other systems are configured as NNM remote consoles (running NNM locally, but using the NNM server's database information). See the NNM manual *A Guide to Scalability and Distribution* and the *ovwsetupclient* manpage for more information.

### Multicast SPI on the NNM Advanced Edition Server

Install the Multicast SPI as described in the section appropriate to your operating system:

- “Installing the Multicast SPI 2.1 on HP-UX” on page 31
- “Installing the Multicast SPI 2.1 on Solaris” on page 35

### Multicast SPI on NNM Advanced Edition Remote Consoles

To install the Multicast SPI on a NNM Advanced Edition remote console, you must temporarily turn off the NNM Advanced Edition client/server relationship, install the Multicast SPI, then reestablish the NNM Advanced Edition client/server relationship.

On the NNM Advanced Edition Remote console:

1. At the command prompt, type:

```
ovwsetupclient -u
```



**Installing the Multicast SPI on NNM Advanced Edition Remote Console (Management Console)**

2. Install the Multicast SPI as described in the section appropriate to your operating system (you do not need an additional license for the console, simply click **Cancel** when the **HP Auto Pass** dialog box appears):
  - “Installing the Multicast SPI 2.1 on HP-UX” on page 31
  - “Installing the Multicast SPI 2.1 on Solaris” on page 35
3. Reestablish the NNM Advanced Edition client/server relationship. At the command prompt, type:

```
ovwsetupclient /opt/OV/nfs/server
```

---

**NOTE**

---

If you have used the NFS automounter, the path may be different.

4. To verify that the configuration is correct, run the following command:

```
ovw -server
```

Look at the return value from the `ovw -server` command on your display. It should look similar to:

```
%ovw -server
```

```
your server name shows up here
```

5. Open NNM Advanced Edition (run **ovw**) on the NNM Advanced Edition remote console.

If you are running on an HP Service Guard cluster, you may run **ovwrs** rather than **ovw**, if NNM Advanced Edition is configured as a package. Refer to the *ovwrs* manpage for more information about restartable **ovw**.

## Configuring the Multicast SPI

This section describes the Multicast SPI configuration files that you must configure *before* starting the Multicast SPI background processes. These configuration files are as follows:

- The `managed.mmon` file configures Multicast SPI's discovery process. This file is required. See “`managed.mmon` Configuration File” on page 43.
- The `unmanaged.mmon` file sets specified multicast-enabled routers to an “unmanaged” state. This file is optional. See “`unmanaged.mmon` Configuration File” on page 45.
- The `mmon.conf` file controls many aspects of how the Multicast SPI works. This file is optional. See “`mmon.conf` Configuration File” on page 47.
- The `mmon_ma.conf` file instructs the Multicast SPI regarding how to treat certain interface types. This file is required, but you probably do not need to modify it. See “`mmon_ma.conf` Configuration File” on page 54.
- The `snmpCollect.lrf` file controls the functions of the `snmpCollect` process. This file is required, but you probably do not need to modify it. See “`snmpCollect.lrf` Configuration File” on page 55.

---

### TIP

If you change the settings in the `managed.mmon`, `unmanaged.mmon`, or `mmon.conf` configuration files while the Multicast SPI is running, you must use one of the following procedures to force the Multicast SPI to reread these files:

- Stop and restart the `mmonitor` process.
- Click `Multicast:Reload Configuration Files` on any submap in the Multicast hierarchy.
- At the command prompt, type:

```
$OV_BIN/mcastreloadconf.ovpl
```

## managed.mmon Configuration File

The Multicast SPI requires at least one fully-qualified IP address for a multicast-enabled router in your management domain to start the Multicast SPI discovery process. Discovery starts with the routers listed in the managed.mmon configuration file and proceeds outward. The managed.mmon file is located in the following directory:

*/etc/opt/OV/share/conf/*

Each line in the managed.mmon file is a distinct entry. It is recommended that you enter one (and only one) line for each multicast-enabled router that to be managed. For example, enter either an IP address or host name, but not both.

There are three benefits to using IP addresses:

- Use a specific IP address to control exactly which interface the Multicast SPI uses for communication and data collection. (With host names, you relinquish control over which router interface the Multicast SPI uses for communication and data collection. The IP address of the first multicast-enabled interface that is discovered is used.)
- Use the loopback address, if available, so that communication with the router automatically rolls to another IP address if the loopback interface goes down.
- Use IP addresses so that the Multicast SPI works successfully even if your name resolution system fails.

---

### CAUTION

If you use HSRP in your environment, do NOT specify an HSRP Standby Address or host name that resolves to an HSRP Standby Address. If you include an HSRP entry in the managed.mmon file, the Multicast SPI fails whenever one of the HSRP-enabled Routers goes down.

---

Entries in the managed.mmon file control the extent of the Multicast SPI discovery process. Two distinct discovery styles can be used in combination:

- **Limited discovery process:** Each multicast-enabled router that needs to be managed (monitored) by the Multicast SPI is explicitly identified with either a fully-qualified router IP address or a fully-qualified host name listed in the managed.mmon file. Routers

discovered through neighboring relationships are not managed by the Multicast SPI; they appear on the Multicast submap as white icons. Discovery does not continue beyond an unmanaged router. In order to discover and manage all multicast-enabled routers in your management domain, you must enter an IP address or host name for each router into the `managed.mmon` file.

To use the limited discovery process, enter at least one fully-qualified IP address or fully-qualified host name for a multicast-enabled router in your management domain. It is recommended that you enter one fully-qualified IP address for each multicast-enabled router.

Optionally, you can enter a fully-qualified router host name that resolves to one, and only one, IP address through your name resolution system, such as DNS, or `/etc/hosts`. (If you use HSRP in your environment, do NOT add to this file a router name that resolves to an HSRP Standby Address.)

- **Least-effort discovery:** Multicast-enabled routers discovered through neighboring relationships are automatically managed by the Multicast SPI, provided that the IP address or name matches a wildcard name entry or IP-address/subnet-mask pair in the `managed.mmon` file.

To use the least-effort discovery process, enter at least one fully-qualified IP address or fully-qualified host name for a multicast-enabled router in your management domain.

Create conditions that allow the Multicast SPI to set all discovered neighboring routers that match these entries to the managed state (monitored by the Multicast SPI):

— Wildcard for router name

During the discovery process the Multicast SPI compares the MIB-II `sysName` object to this wildcard to decide whether or not to manage the newly discovered router.

If during discovery, SNMP communication is unavailable for a newly discovered router, the Multicast SPI compares the wildcard name to the `hostName` (the name returned through your name resolution service) *instead of the MIB-II sysName*. If SNMP communication is *successful*, the `hostName` is not checked.

For example, `*.myDiv.myCompany.com`. In this example, if a Router has the MIB-II `sysName` of `x.myDiv.myCompany.com`, it would be managed by the Multicast SPI. However, if the Multicast SPI cannot obtain the `sysName`, the DNS `hostName` would be checked instead.

— Wildcard for IP address

Specify an IP address that uses one or more wildcards to allow a range of IP addresses.

For example, with the IP address range `10.0.3.*`, the Multicast SPI manages all IP addresses from `10.0.3.0` to `10.0.3.255` upon discovery.

With the IP address range `10.1*.5.*`, the Multicast SPI manages all IP addresses from `10.10.5.0` to `10.10.5.255`, `10.11.5.0` to `10.11.5.255`, and so on, through `10.19.5.0` to `10.19.5.255`.

With the IP address range `10.1*`, the Multicast SPI manages all IP addresses from `10.10.0.0` to `10.19.255.255` upon discovery.

— IP address and subnet mask pair

Specify an IP-address/netmask pair combination that allows a range of IP addresses. Use the format `IP_address IP_mask`; for example,

```
10.20.0.0 255.255.0.0
```

In this example, the Multicast SPI manages all addresses between `10.20.0.0` and `10.20.255.255` upon discovery.

## unmanaged.mmon Configuration File

If you don't want the Multicast SPI to manage certain routers, even though they pass the `managed.mmon` file, create this optional file. You must use this file, rather than NNM's `Edit:Unmanage Object` command because, without the `unmanaged.mmon` file, the symbols revert back to their previous (managed) state the next time that the multicast polling cycle runs.

Use caution when listing routers to be *unmanaged*. The Multicast SPI may not be able to draw accurate forwarding trees or present complete information about all members of a multicast group when participating routers are *unmanaged*.

---

**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 SPI mmonitor process, and set the same router to be “managed” by the NNM netmon process.

---

The unmanaged routers may appear on multicast submaps as neighbors to managed routers, but are not monitored or queried by the Multicast SPI after initial discovery (shown with a white status color).

---

**NOTE**

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

---

To specify routers that should be unmanaged create the `unmanaged.mmon` file in the following directory:

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

Use the format of the `managed.mmon` file. Include one entry per line. The file can contain any or all of the allowed entry types. Each line must contain only one entry type. Your choices are as follows:

- Enter a fully-qualified IP address for a multicast-enabled router in your management domain.
- Enter a fully-qualified router name that resolves to one, and only one, IP address through your name resolution system, such as DNS, or `/etc/hosts`.
- Wildcard for router name:

During the discovery process the Multicast SPI compares the MIB-II `sysName` object to this wildcard to decide whether or not to manage the newly discovered router.

If during discovery, SNMP communication is unavailable with a newly discovered router, the Multicast SPI compares the wildcard name to the `hostName` (the name returned through your name resolution service) *instead of the MIB-II sysName*. If SNMP communication is *successful*, the `hostName` is not checked.

- Wildcard for IP address  
Specify an IP address that uses one or more wildcards to allow a range of IP addresses. For example, 10.0.3.\*, 10.1\*.5.\*, or 10.1\*
- IP address and subnet mask pair  
Specify an IP-address/netmask pair combination that defines a range of IP addresses. Use the format *IP\_address IP\_mask*; for example, 10.20.0.0 255.255.0.0

After creating the unmanaged.mmon 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

The mmon.conf configuration file controls the configuration settings of the mmonitor background process. See the comments within this file for more information. The file is located in the following directory:

*/etc/opt/OV/share/conf/ (\$OV\_CONF/)*

- HOST\_IP  
(Required) An IP address within your NNM management station. The Multicast SPI uses this interface when communicating 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, you were instructed to provide the one you wanted to be entered into this file.

---

### NOTE

In Service Guard environments, if the NNM\_INTERFACE field is specified in the *\$OV\_CONF/ov.conf* file, then it is recommended that HOST\_IP in the *\$OV\_CONF/mmon.conf* file is set to the same address. This is the Service Guard *logical IP address*, and this address is the interface of choice for communications.

For more details on setting up Service Guard with NNM, see the whitepaper */opt/OV/doc/WhitePapers/MCServiceGuard.doc*.

- `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). The Multicast SPI polling includes status checks and discovery cycles. If the `CYCLE_MINUTES` time expires while polling is in progress, the Multicast SPI 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 116.

- `IGMP_PARMS` 1 2 4 10 3

(Required) This series of five parameters controls the following IGMP settings. These settings are used when the Multicast SPI 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 tries

This parameter is sets the minimum number of times that the Multicast SPI attempts to get correct response for Neighbor Query. The value of this parameter must be at least 2.

The protocol for Neighbors query (`IGMP ASK_NEIGHBORS`) can have a response containing multiple packets without a termination indicator. Therefore, the Multicast SPI 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 the Multicast SPI performs the query. If this parameter is set to “*n*”, the Multicast SPI 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, the Multicast SPI uses that response. If they don’t match, the Multicast SPI tries one more time and so on up to the maximum number of tries (described in number 3).

3. maximum number of tries

This parameter sets the maximum number of times that the Multicast SPI 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 multicast-enabled interfaces in two different routers. The Multicast SPI 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 Multicast SPI 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 the Multicast SPI 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 the Multicast SPI 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 6`

(Required) This series of parameters sets the status assigned for certain error conditions that may be encountered during SNMP data collection. These parameters are all required and must be in the order listed here:

- The status when a router no longer responds to IGMP (multicast monitoring).

---

**NOTE**

If a router *never* responds to IGMP, its status is set to “unknown” (dark blue). This behavior is not further configurable if IGMP-based discovery is used. Consider using SNMP-based discovery (see “DISCOVERY\_VIA\_SNMP” on page 52).

- The status when a 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 down link or tunnel 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.

- The impact of inadequate multicast MIB support on the parent router's status.

See the comments within the `mmon.conf` file for specific information about the possible status numbers and each parameter's default value.

- `SNMP_POLL`

(Optional, but recommended) This is the multiplier for spacing the Multicast SPI 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 query 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. This includes checking for any changes in the location of the multicast-related MIB files.

You can manually query a router by right-clicking the router symbol and selecting `Rediscover Routers`.

- `DOMAIN_SUFFIX`

(Optional) The Multicast SPI can automatically trim the domain suffix from router names to minimize the length of labels that appear on the map and in the text of alarm messages. However, if your network is configured to use round-robin DNS servers, the Multicast SPI may not be successful in trimming the domain suffix. Set this parameter to force precise trimming of router names in the round-robin DNS environment. Use only if router names, without the suffix, correctly resolve (via DNS and `/etc/hosts`) to valid IP addresses. For example, if `'myRouter'` resolves to `'myRouter.myCompany.com'`, then set the domain suffix to `'myCompany.com'`.

Multiple domain suffix entries are allowed. The order of these entries affects their impact. For example, the sequence:

```
DOMAIN_SUFFIX myRouter.myCompany.com
DOMAIN_SUFFIX myCompany.com
DOMAIN_SUFFIX com
```

trims 'myInterface.myRouter.myCompany.com' to 'myInterface' and 'thatRouter.myCompany.com' to 'thatRouter'; whereas, the sequence:

```
DOMAIN_SUFFIX com  
DOMAIN_SUFFIX myCompany.com  
DOMAIN_SUFFIX myRouter.myCompany.com
```

trims 'myInterface.myRouter.myCompany.com' to 'myInterface.myRouter.myCompany' and 'thatRouter.myCompany.com' to 'thatRouter.myCompany'.

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

- `NODE_CONTROLS_INTF_STATUS`  
(Optional) Controls the impact on interface status within a router when the router quits responding to IGMP (*mrintfo*) queries, or when the router quits responding to SNMP polls (if the router is discovered by SNMP instead of IGMP).  
  
0 = no change in interface status  
1 = all multicast interfaces changed to “unknown” status
- `TUNING`  
(Optional) Allows you to monitor routers that are responding late or beyond the time-out value established by `IGMP_PARMS` (page 48).  
  
0 = no monitoring  
1 = alarm messages are generated when a router responds late, or beyond the `IGMP_PARMS` time-out value.
- `TRIM_FWD_TREE_STATE`  
(Optional) Controls the display of the multicast forwarding trees.  
  
0 = show the forwarding trees based on each router’s incoming interface report, even if the router is not forwarding the traffic  
1 = only show the forwarding trees if the router is forwarding the traffic
- `DISCOVERY_VIA_SNMP`  
(Optional) Forces the method used to discover and monitor multicast routers.  
  
0 = use *mrintfo* (IGMP) exclusively  
1 = use SNMP exclusively

2 = use *mrinto* except with Cisco Catalyst 6000 routers (because of potential defects in that product's handling of *mrinto*)

4 = use SNMP when possible and *mrinto* when a router has inadequate multicast SNMP MIB support

6 = use SNMP when possible and *mrinto* when a router has inadequate multicast SNMP MIB support, but never use *mrinto* with Cisco Catalyst 6000 routers (6 is the combination of 2 and 4)

- NO\_DISABLED\_INTERFACE\_IN\_SUBNETS

(Optional) Controls the display of disabled interfaces. These interfaces may result in subnets with unknown status (shown in blue). Disabled interfaces are still visible on router submaps and via the Describe Multicast Object menu command on routers, even when the configuration specifies to not display these interfaces in subnet submaps.

0 = allow disabled interfaces to display in subnet submaps and affect the subnet status

1 = do not display disabled interfaces in subnet submaps

- MAX\_SNMP\_GETBULK\_ROWS

(Optional) Limits the number of MIB objects requested in an SNMP v2C getbulk request.

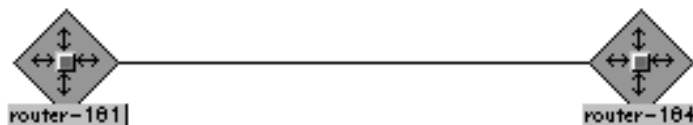
SNMP accesses may use the getbulk request for 1000 or more MIB objects in one call. Some routers are overwhelmed by this number. Setting a value for this parameter works with all routers at the cost of reduced efficiency for more capable routers.

## 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 the Multicast SPI 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 the Multicast SPI background processes have not yet been started. Either select the symbols on the Multicast submap, delete them, and wait for rediscovery, or see “Stopping the Multicast SPI” on page 58.

---

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
53 # propVirtual
59 # aflane8023
60 # aflane8025
62 # fastEther
69 # fastEtherFX
71 # ieee80211
114 # ipOverAtm
117 # gigabitEthernet
135 # l2vlan
136 # l3ipvlan
```

## snmpCollect.lrf Configuration File

The Multicast SPI 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, use the `-c` and `-n` parameters.

- `-c #` (lowercase c)

Frequency (in minutes) with which snmpCollect performs configuration checks. 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, the Multicast SPI 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 #` (lowercase n)

Maximum number of concurrent SNMP requests. When no value is specified, the default value is 80.

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

---

**NOTE**

In the Multicast SPI 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.



## Starting the Multicast SPI

1. The first time that you use the Multicast SPI, log in as `root`, and at the command line, type `ovstart`. This automatically starts all background processes registered with NNM.

At installation, the Multicast SPI receives a 60-day trial license. You can request a permanent password from the Multicast SPI menu. See “Entering License Information” on page 62.

2. To open the software, at the command line, type `ovw&` (you do not need to be logged in as `root`).
3. Select a map to which you have [read-write] access to ensure access to all the Multicast SPI features.
4. Navigate to the `Multicast` submap by double-clicking on the Multicast symbol on the `Root` submap.



## Stopping the Multicast SPI

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 Multicast SPI background processes, at the command prompt, type:

```
ovstop mmonitor mtraffic
```

The multicast submaps are still visible, but none of the menu commands 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
    - mcastIf%inutilStd
  - c. Select Actions:Suspend Collection. Repeat for each of the above.

---

**NOTE**

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/](http://ovweb.external.hp.com/lpe/doc_serv/)
  - From any NNM submap in Adobe Acrobat format (pdf), select Help:Online Manuals:Managing Your Network.
-

## Uninstalling the Multicast SPI

To remove the Multicast SPI from your computer, follow these steps.

1. Log in as `root` or `superuser`.
2. Run the `remove` script. At the command prompt, type  
**`$OV_BIN/remove.mcast`**

---

### NOTE

The `Multicast Alert Alarms` category is not removed from the NNM alarm browser. However, it is no longer used. For information on deleting this alarm category, see the `trapd.conf` manpage.

---

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/](http://ovweb.external.hp.com/lpe/doc_serv/)
- With NNM 7.01, from any NNM submap in Adobe Acrobat format (pdf), select Help:Online Manuals:Managing Your Network.

## Entering License Information

The Multicast SPI comes with a 60-day trial license that allows you to use the product for 60 days after you install it.

A password is required for each the Multicast SPI management station or NNM Advanced Edition collection station where the Multicast SPI is installed. If you are accessing the Multicast SPI from a remote NNM Advanced Edition console, you can simply click `Cancel` and dismiss the licensing dialog box. Remote NNM Advanced Edition consoles use their parent NNM Advanced Edition management station's password.

---

### WARNING

**Do not install a password on a remote NNM Advanced Edition console.**

To obtain a password and permanent license for the Multicast SPI, select `Options:Multicast License Password->Request Password` from the menu bar of either the `Root` submap or any multicast submap. The HP Auto Pass installation program leads you through the licensing process.

Refer to the Multicast SPI online help topic "Multicast License Password" for more information. Refer to the *HP Auto Pass User Guide* (`AutoPass_guide.pdf`) on the installation CD for details about using the licensing program.

To request a permanent password and license, you need the following:

- The HP Purchase Order Number
- The Entitlement Certificate
- The IP Address of the Server
- Your Company Information

---

### TIP

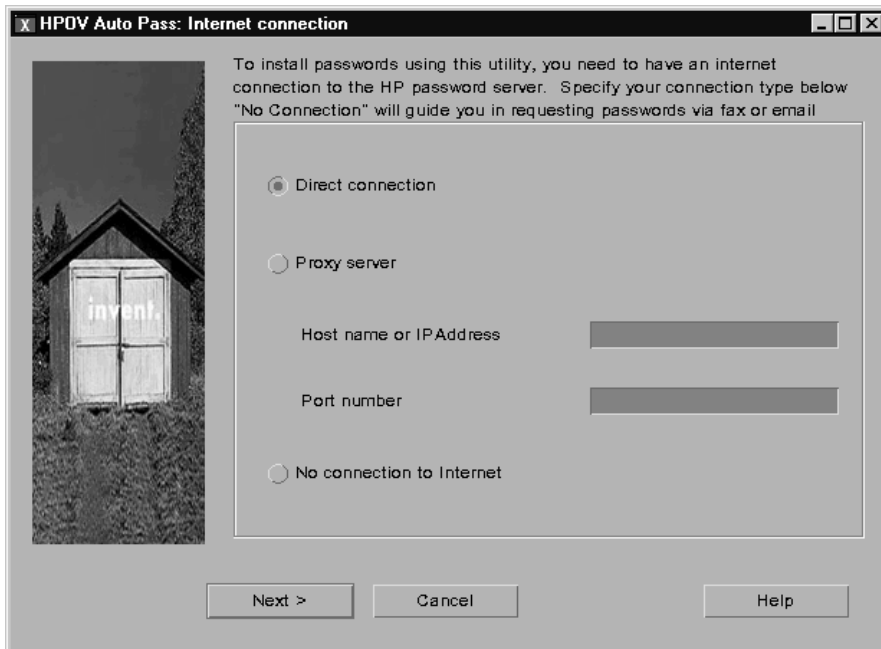
If you have not yet purchased the product, visit `hp.com` to locate an HP OpenView authorized reseller.

---

The HPOV Auto Pass: Internet Connection dialog box appears automatically under the following circumstances. You must take action to continue using the product:

- If the NNM management station on which you installed the Multicast SPI permanent password does not have an NNM *enterprise*-level license, the following dialog box is automatically displayed when NNM is opened. Click **Cancel**. Upgrade the NNM license to meet the minimum system requirements for the Multicast SPI. The next time you open NNM, you won't see this dialog box.
- If the 60-day trial license for the Multicast SPI expires before you upgrade to the permanent password, the following dialog box is automatically displayed when you open NNM. You must request a permanent the Multicast SPI password to continue using the product.

**Figure 2-1** Dialog Box for Entering Password Information



## Troubleshooting for Licensing

If the licensing portion of the Multicast SPI installation procedure is failing.

- Ensure that NNM is running with an *enterprise*-level license. NNM Multicast requires an enterprise-level NNM.
- Check the `/var/admin/sw/swagent.log` file. If you see the following error sequence, during installation, the `DISPLAY` variable was not set correctly. The HP Auto Pass dialog box cannot open:

```
ERROR: Calling AutoPassStartUp failed.  
EXITING the HP Auto Pass installation.
```

If this happens, you need to uninstall the Multicast SPI and reinstall:

1. Set `DISPLAY` variable correctly.
  2. Run `/opt/OV/bin/remove.mcast`
  3. Follow the installation procedure earlier in this chapter.
- Type the following at the command prompt:

```
ovstart -c
```

```
ovstatus -c
```

If you see this error message for `mmonitor` or `mtraffic`, follow the steps below:

```
No valid password exists for the Multicast SPI; Could be  
because of not having NNM Enterprise License (<Error  
Number>)
```

1. Open the NNM interface (`ovw`). The HP Auto Pass dialog box for license password installation should appear before the map opens.
2. Click `Cancel` to use the 60-day Instant-On password or use other buttons to obtain your permanent the Multicast SPI license.
3. Close the map.
4. At the command prompt, type:  
**ovstart mmonitor mtraffic**



5. At the command prompt, type the following to confirm that `mmonitor` and `mtraffic` are running successfully:  
**`ovstatus mmonitor mtraffic`**



---

---

**3****Getting Started with the  
Multicast Smart Plug-in**

## The Multicast SPI Makes Your Job Easier

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

The Multicast Smart Plug-in (SPI) provides a wealth of new tools to help you map out (page 69), monitor (page 75), and troubleshoot (page 78) your multicast environment. The Multicast menu includes:

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

Locate & Highlight IP Address

Highlight PIM Designated Routers

Clear Highlights

Rediscover Routers

Reload Configuration Files

Multicast License Password->

Show Current Password

Show Password

See the Multicast SPI online help for detailed information about each menu command.

## Mapping Your Multicast Environment

- “Which routers within my management domain are configured to handle multicast?”
- “Which multicast groups does this router serve?”
- “Which subnets have subscribers to this group’s traffic?”
- “What path does the routing tree for this group follow?”
- “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?”

After you install the Multicast SPI and supply the IP address of at least one multicast-enabled router, the Multicast SPI 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.



Multicast

To view the Multicast topology, open the NNM interface (ovw) and double-click the Multicast icon. If the Multicast submap is crowded with symbols, select `View:Pan` and `Zoom` to zoom into specific areas on your submap.

Confirm that your topology is properly discovered and drawn on the multicast submaps. If you have questions or concerns, see Appendix A, “Troubleshooting the Multicast Smart Plug-in,” on page 81 and “Configuring the Multicast SPI” on page 42.

The Multicast SPI 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 for polling 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 `Multicast` submap does not support *container* objects to split the map into smaller segments. The Multicast SPI does not support *hidden* symbols within the multicast submap hierarchy.

---

### **“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.

NOTE: A Cisco Router can be configured to bypass the standard IGMP protocol and join multicast groups through the “static group” IOS command. Routers that have joined the multicast group in this manner cannot be detected with the `Group Membership:ShowGroups with Local Subscribers` command.

## “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 salmon:

- 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: A Cisco Router can be configured to bypass the standard IGMP protocol and join multicast groups through the “static group” IOS command. Routers that have joined the multicast group in this manner cannot be detected with the `Group Membership:Highlight Subnets & Routers in a Group` command.

## “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 (shortest-path) trees is shown using *administrative “restricted”* status color (by default salmon).
- Forwarding based upon shared trees is shown using *administrative “testing”* status color (by default orange-brown).
- An interruption to the flow of data in a forwarding tree is shown using *operational “critical”* status color (by default red).

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.
- If an interruption to the flow of data in a forwarding tree is detected, the Multicast SPI displays a message box that identifies the point of interruption.

Click **Help** in the **Highlight Forwarding Tree** dialog box for more information.

### **“Which router or subnet contains the given IP address?”**

When a problem with multicast traffic to or from a specific IP address occurs, you need to know how that IP address fits in to the overall multicast topology.

Select **Multicast:Locate & Highlight IP Address** to quickly identify that symbol representing that IP address.

If the specified IP address belongs to one of the routers that the Multicast SPI manages, that router symbol and the connection that represents the interface are highlighted. If the specified IP address does not belong to one of these routers, the symbol for the containing subnet is highlighted.

### **“Which router is the PIM designated router for this subnet?”**

When a Multicast problem arises on a Host (in a Subnet), the PIM Designated Router is the best place to start looking for answers to the problem. Among other things, this Router is supposed to join the group at the rendezvous point (RP), assuming PIM Sparse Mode is being used.

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 submaps 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 Multicast SPI submaps 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.

## Mapping Your Multicast Environment

- 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 Alert Alarms` category.

## Monitoring Your Multicast Environment

- “How can I collect multicast-specific performance data and set multicast-specific thresholds?”
- “What is the true impact of a specific multimedia data stream 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 multicast 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.

## Monitoring Your Multicast Environment

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.

After 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?”**

To completely block multicast traffic from consuming any bandwidth beyond a specific threshold, your network devices can be configured to establish Quality of Service (QoS) parameters for multicast traffic. Consult with your HP representative about traffic engineering solutions.

## 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 “Monitoring Your Multicast Environment” on page 75), 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. See page 109.

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 request 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 for 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.

NOTE: A Cisco Router can be configured to bypass the standard IGMP protocol and join multicast groups through the “static group” IOS command. Routers that have joined the multicast group in this manner cannot be detected with the `Group Membership:ShowGroups with Local Subscribers` command unless the static group membership uses a software loopback interface.

- 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 graph 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 Multicast SPI online help for more information.

---



---

# **A Troubleshooting the Multicast Smart Plug-in**

## The Multicast SPI 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”

### Multicast menu commands don't work. Why?

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

Many commands depend upon the multicast-related MIB files, that are currently moving out of the experimental branch into the official MIB-II branch. During this transitional period, your routers may have the `igmpMIB` file and `IPRouteMIB` file installed in one of two places. If a multicast command does not work, select the router icon on the map, select `Multicast:Rediscover Routers` so that the Multicast Smart Plug-in (SPI) can test for the actual MIB location. Then try the command again.

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

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

If you know that the objects represented by the blue icons are not managed, you can configure the Multicast SPI to not display these icons. See “`NO_DISABLED_INTERFACE_IN_SUBNETS`” on page 53.

If you believe that the objects represented by the blue icons should be managed by the Multicast SPI, check the following:

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

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

- Signal the Multicast SPI to re-read the configuration files by navigating to the Multicast submap and selecting `Multicast:Reload Configuration Files`.
- Or at the command prompt, type:  
**`$(OV_BIN)/mcastreloadconf.ovpl`**
- Or at the command prompt, type:  
**`ovstop mmonitor`**  
**`ovstart mmonitor`**

2. Verify that the router supports the multicast IGMP protocol, see “Router Requirements” on page 28. Some routers have filters or defective software implementations that prevent them from responding to IGMP queries. See Table 0-1, “Known Problems with Cisco Routers,” on page HIDDEN.
3. Ensure that you can “ping” at least one router specified in your `$(OV_CONF)/managed.mmon` file. If not, the problem is with your network.
4. If the Multicast SPI can’t get a response to *mrinfo*, the router appears blue (unknown) or red (critical status, previously contacted but unreachable now) on the map. Use the public domain utility *mrinfo* to verify that your router responds successfully.

*HP-UX*: The *mrinfo* utility is shipped with HP-UX operating systems, and is typically located at `/usr/sbin/mrinfo`.

*Solaris*: Obtain the *mrinfo* source from the public domain “mrouted” distribution:

`ftp://ftp.parc.xerox.com/pub/net-research/ipmulti/`

Follow the links to the mrouted source. You can download “gzipped” *mrinfo* source that is executable for Solaris SPARC machines (you need gunzip or some other tool to extract).

## The Multicast SPI Submaps

Run the public domain utility *mrinfo* from another router or from the NNM management station where the Multicast SPI is installed:

- To run *mrinfo* from the NNM management station where the Multicast SPI is installed:
  - a. You must be superuser (*root*) to run *mrinfo*.
  - b. Stop `mmonitor` to prevent confusing responses to your *mrinfo* query. (`mmonitor` makes regularly scheduled *mrinfo* queries. When you issue an *mrinfo* query directly from the command line, the next *mrinfo* reply is displayed, whether or not it is the reply you expected. This happens because IGMP protocol operates directly above IP, does not use either TCP nor UDP, and does not have a *socket* concept.) At the command prompt, type:
 

```
ovstop mmonitor (or use ovpause)
```
  - c. Execute the *mrinfo* query, at the command prompt, type one of the following:

```
mrinfo <IP address of destination router>
```

```
mrinfo <name of destination router>
```

```
mrinfo -n <IP address of destination router>
(-n to skip DNS lookup on the address)
```

- d. Restart `mmonitor`, at the command prompt, type the following:

```
ovstart mmonitor (or use ovresume)
```

- To run *mrinfo* from another router, at the router's command prompt, type one of the following:

```
mrinfo <IP address of destination router>
```

```
mrinfo <name of destination router>
```

```
mrinfo -n <IP address of destination router>
(-n to skip DNS lookup on the address)
```

Example of *mrintfo* output, after typing `mrintfo mcrouter81` on an HP-UX machine, the following was displayed:

```
15.2.32.81 (mcrouter81.cnd.hp.com) [version
12.0,prune,mtrace]:
10.0.2.81 -> 10.0.2.84 (10.0.2.84) [1/0/pim]
10.0.2.81 -> 10.0.2.82 (10.0.2.82) [1/0/pim]
10.0.3.81 -> 0.0.0.0 (local) [1/0/pim/querier/leaf]
10.0.10.81 -> 10.0.10.85 (10.0.10.85) [1/0/tunnel/pim]
```

5. If you tried all of the above and still haven't resolved 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. This book is available:

- From the HP Documentation web site in Adobe Acrobat format (pdf): [http://ovweb.external.hp.com/lpe/doc\\_serv/](http://ovweb.external.hp.com/lpe/doc_serv/)
- From any NNM submap in Adobe Acrobat format (pdf), click Help:Online Manuals:Managing Your Network.

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

White icons are *unmanaged*.

Only those routers specifically listed in the managed.mmon file are set to managed during the discovery cycle. If you used wildcards in the managed.mmon file, verify that the wildcard is not too exclusive. If you used host names in the managed.mmon file, verify that each host name can be resolved to an IP address from the NNM management station.

Unmanaged routers are listed in the unmanaged.mmon file.

Unmanaged elements are not polled after initial discovery. They are not included in regular status polling cycles. See "unmanaged.mmon Configuration File" on page 45 for more information. Edit this file if you wish to make changes. After making changes to the file, force the Multicast SPI to acknowledge the changes by selecting Multicast:Reload Configuration Files (or, at the command prompt, type: `$OV_BIN/mcastreloadconf.ovpl`).

---

**NOTE**

Although it is *possible* to use the `Edit:Manage & Unmanage` menu commands to change the management status of the symbols on the multicast submaps, without the `unmanaged.mmon` file, the symbols revert back to their previous state the next time that the multicast polling cycle runs.

---

## How are symbol names (symbol labels) determined by the Multicast SPI?

**Routers:** the Multicast SPI determines a “router name” (and the symbol label on the submap) as follows:

1. The Multicast SPI queries for the SNMP MIB-II `sysName`. If the `sysName` is obtained, a space character is appended.
2. If no `sysName` is identified, the Multicast SPI invokes `gethostbyaddr()`, which uses `/etc/hosts` and the name resolution system to try to find a name. This may be shortened based upon the `DOMAIN_SUFFIX` setting in `$OV_CONF/mmon.conf`. A space character is appended to the host name.

If the resulting `hostName` is not unique, the Multicast SPI appends a random number; for example the router symbol might have the label `myRouter.myDiv.myCompany.com 294`

3. If no name is identified, the IP address (`x.x.x.y`) is used for the router name and label on the map. A space character is appended to the IP address.

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.

If the resulting IP address is not unique, the Multicast SPI appends a random number; for example the router symbol might have the label `x.x.x.y 934`

**Interfaces:** the Multicast SPI determines an “interface name” (and the symbol label on the submap) as follows:

1. The IP address ( $x.x.x.y$ ) is used for the interface name and label on the map. A space character is added to the beginning and end of the IP address.
2. If duplicate IP addresses are encountered, the router name is appended to the duplicates; for example,  $x.x.x.y_{<sysName \text{ or } hostName>}$ .
3. For Cisco and Foundry routers, the standard short form of the interface description is appended to the IP address; for example,  $x.x.x.y_{Et2/0}$  for an Ethernet2/0 router.
4. If the interface is a tunnel, the SNMP `ifDescr` of the interface (typically, Tunnel10, Tunnel11) is appended to the IP Address; for example,  $x.x.x.y_{Tunnel6}$ .
5. If the previous steps do not result in a unique name, a random number is appended.

**Subnets:** the Multicast SPI determines a “subnet name” (and the symbol label on the submap) as follows:

1. Network addresses are used to name Subnets. A space character is appended to the subnet name.
2. If the subnet address is not unique, a number is appended; for example  $x.x.x.y \ 239$ .

**Links:** the Multicast SPI determines a “link name” (and the symbol label on the submap) as follows:

1. Link objects are named `Link: Interface1 - Interface2` with the names of the interfaces that this link connects.
2. If the link is not unique, a number is appended; for example `Link_2: Interface1 - Interface2 259`.

## **A router symbol on the Multicast submap doesn't make sense.**

Select the Router symbol and click `Multicast:Rediscover Routers`.

If the problem is not corrected, delete the Router symbol and click `Multicast:Reload Configuration Files` (or, at the command prompt, type: `$OV_BIN/mcastreloadconf.ovpl`).

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

Green means that everything is working.

Blue means *unknown* status (never responded 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 for the router are controlled by the `NODE_STATUS` settings in the `$OV_CONF/mmon.conf` file. See “`mmon.conf Configuration File`” on page 47 for more information.

It may be useful to review any alarms associated 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 router symbol color keeps switching between green and red. What happened?

Green means that everything is working.

Red means that the status is critical. Critical status is calculated in a number of ways. It may mean that the router no longer responds to *mrinfo* communications (see the resolution steps under “The Multicast submap has blue icons. What's wrong?” on page 82.)

On the Multicast submap, right-click the router symbol and select `Router Health:Explain Status` to see the cause of the critical 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. See “`mmon.conf` Configuration File” on page 47 for more information.

If the router icon keeps switching from green to red and back again, the problem may be caused by too short a time-out setting in the `$OV_CONF/mmon.conf` file. Locate the `IGMP_PARMS` setting and increase the first (time-out) and third (maximum retries) parameters. See “`mmon.conf` Configuration File” on page 47 for more information.

If the `$OV_CONF/mmon.conf` file contains the setting `DISCOVERY_VIA_SNMP 1`, which forces SNMP-based discovery instead of IGMP(*mrinfo*)-based discovery, a router icon can flap in and out of critical status at a seemingly random interval based on the values of the `CYCLE_MINUTES` and `SNMP_POLL` parameters in the `$OV_CONF/mmon.conf` file. This problem arises if routers are running a newer version of IOS (12.3)x that supports the RFC2932 STD ipMRRoute MIB. There is one defect in the “NNM Multicast 2.0+patch” product support of the RFC2932 STD ipMRRoute MIB. This problem is fixed in the Multicast SPI version 2.1.

It may be useful to review any alarms associated 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 router symbol color keeps switching between green and orange. What happened?**

Green means that everything is working.

Orange means that the status is major. Major status may mean that the router no longer responds to *SNMP* communications. You may need to increase the SNMP time out settings (see “Configuring NNM.” on page 30 for more information.)

On the Multicast submap, right-click the router symbol and select `Router Health:Explain Status` to see the cause of the major 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. See “mmon.conf Configuration File” on page 47 for more information.

It may be useful to review any alarms associated 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 connection symbol keeps switching from black to red. What happened?

Black means that everything is working.

Red means that the status is critical. Critical status is calculated in a number of ways. It may mean that the neighboring router no longer responds to *mrinfo* communications. The following reasons may cause a disruption in *mrinfo* communications between neighbors:

- Hardware reconfiguration within one of the routers.
- The Multicast SPI might receive inconsistent neighbor information if it queries in the middle of the routers' protocol data exchanges (3 minute minimum required, two 90-second response time windows) or when there is so much network traffic that the routers' handshake is interrupted or delayed. To eliminate false alarms, it is recommended that the fifth parameter (number of discovery cycles before declaring a link "inconsistent" when the link is reported differently by the neighboring endpoints) of `IGMP_PARMS` be set to 2 or more. (See "mmon.conf Configuration File" on page 47 for more information.)

It may be useful to review any alarms associated with the corresponding routers:

- To review the alarms associated with a 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 a 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 Multicast SPI does not support *hidden* objects on the multicast submaps. If you have hidden any router or subnet objects, the forwarding tree feature draws strange results.

## **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 Multicast submap: right-click Delete, or Edit:Delete.

The Multicast SPI creates only one symbol as it goes through its next discovery cycle. To force the Multicast SPI to immediately run a discovery cycle, select Multicast:Reload Configuration Files (or, at the command prompt, type: `$OV_BIN/mcastreloadconf.ovpl`).

## **Are there any limits to the number of devices that the Multicast SPI can manage?**

There is no limit to the number of routers that the Multicast SPI can manage. However, the following underlying limits do apply:

- `MAX_INTERFACES_PER_NODE = 1000`  
1000 interfaces maximum on any one router
- `MAX_NBRS_PER_INTERFACE=1000`  
1000 neighboring relationships maximum to any one interface

## **Why is a single physical interface appearing in two different routers?**

To correct this problem, delete the two Router symbols and select `Multicast:Reload Configuration Files` to initiate a new discovery cycle. (Or, at the command prompt, type:  
`$OV_BIN/mcastreloadconf.ovpl`)

## **The PIM Designated Router is not highlighted for some of the submaps. Why?**

The routers on this submap correspond to a point-to-point connection. Typically, point-to-point links do not have PIM Designated Routers. You can simplify the multicast topology by changing the `$OV_CONF/mmon_ma.conf` file. See “`mmon_ma.conf` Configuration File” on page 54 for more information.

## The Multicast SPI Data Collection and Alarms

### The network is flooded after installing the Multicast SPI

Do you have Cisco 6500s running in Hybrid mode with the MSFC card running IOS 12.1(6)E? There is a known Cisco bug that causes these devices to loop *mrimfo* packets at Level 3. For information about this problem, contact your vendor's technical support. (The Cisco case number for this problem is CSCdu42068.)

To check for the existence of this problem within your network environment, open the `mmon.conf` file and set the `TUNING` parameter to 1:

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

After a complete the Multicast SPI monitoring cycle has passed (determined by `CYCLE_MINUTES` parameter settings in the `mmon.conf` file), click **Multicast Alert Alarms** in NNM's Alarm Categories window. If you see multiple "IGMP duplicate/late reply from <router-X>" errors, then <router-X> has this problem.

### Alarm: "Router X failed to respond to some SNMP queries."

Increase NNM's SNMP-query time-out and retry settings for the router's monitoring address:

1. On any NNM submap, select **Options:SNMP Configuration** (or at the command prompt, type `xnmssnmpconf`).
2. Create an entry for the parent router's monitoring address that increases the current settings for **Timeout** and **Retry Count** (click **Help** in the **SNMP Configuration** dialog box for more information).

## **Alarm: “Could not find intfciid corresponding to index N:router-A. Please rediscover node.”**

When a router is originally discovered, the Multicast SPI 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 the Multicast SPI runs its next discovery cycle and updates the NNM object database.

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

To control how often the Multicast SPI runs a discovery cycle set the `SNMP_POLL` parameter in `mmon.conf` file. See “`mmon.conf` Configuration File” on page 47 for more information.

## **Multicast Data Collection isn’t happening when it should.**

1. In order for the Multicast SPI to gather SNMP information, verify that the settings for this router’s `community` names are correct in the `Options:SNMP Configuration` dialog box. (See the step about “`Configuring NNM.`” on page 30.)
2. Have you disabled the Multicast SPI’s ability to maintain multicast data collection configurations within NNM’s `Data Collections & Thresholds` feature by disabling the `mtraffic synchronize` attribute (`-s`)? See “`mtraffic`” on page 118. Do you see the following alarm:

```
MIB Location Change with NO SYNC flag: Data Collection not updated for node <IPaddress>.
```

When synchronization is disabled, if the location of the multicast MIB files changes on any router (for example, the operating system is updated on the router and the MIB files are moved from the experimental branch to the MIB-II branch), the multicast data collections are broken until you manually update them.

3. The `snmpCollect` polling queue may be excessive, and the polling may be falling behind. See “`snmpCollect.lrf` Configuration File” on page 55 for more information. See also “`mmon.conf` Configuration File” on page 47.

**When I type “ovstatus mmonitor”, I get the error message “Terminated due to invalid configuration.”**

Verify that the following files are configured correctly:

- “mmon.conf Configuration File” on page 47
- “managed.mmon Configuration File” on page 43



## The Multicast SPI Graphs and Tables

### **Grapher error message, “Counter for <router-a> McastOctets.x.x.x.x.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.

### **I used to see historical data with the Graph Group Traffic. Now I only see live traffic.**

Did the location of the multicast MIBs change on your router or routers (for example, the operating system is updated on the router and the MIB files are moved from the experimental branch to the MIB-II branch)? Moving the MIBs causes the data collection history to restart.

### **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 55 for more information.

### **The traffic collection tables are empty. Why?**

If you start Traffic Collection tables (using the menu commands Multicast:Multicast Data Collection->Monitor ...) when the tables are empty, the tables are not automatically refreshed. After data collection has begun, close the web browser and re-open the traffic collection tables.

## Performance

**The Multicast SPI performance is very slow and/or is using a high percentage of the management station's CPU.**

Is the name resolution service (such as DNS or `/etc/hosts`) in your management domain configured and working properly for your multicast-enabled routers? Name resolution time-outs can cause this problem. Look in the `/etc/opt/OV/share/conf/managed.mmon` file. All entries in this file must successfully resolve through your name resolution service.

If you intentionally wish to avoid *naming* specific devices to resolve through the name resolution service, see “Configuring NNM.” on page 30 for information.

---

## Web Interface

If you encounter problems getting the Multicast Data Collection -> Monitor Group Traffic Collection and Multicast Data Collection -> Monitor Interface Traffic Collection menu commands working on your computer, check the following configuration files:

- `$OV_CONF/ovweb.conf`

Verify that Browser, Host, and Port are set appropriately. Also verify that the browser specified in this file works correctly. Host and Port must match what is specified in `httpd.conf` (explained below). See the manpage of `ovweb.conf` for full details.

- `/opt/OV/httpd/conf/httpd.conf`

Verify that `ServerName` and `Port` match the values specified for `Host` and `Port` in `ovweb.conf` (explained above).

- `/apps/bin/netscape`

Assuming that your preferred browser is Netscape (as specified in `ovweb.conf`), verify that `/apps/bin/netscape` points to the correct version of Netscape that is operational on your computer.

- `$OV_LRF/httpd.lrf`, etc.

Verify that your `httpd` process is started by `ovstart`. Please see `$OV_LRF/httpd.lrf` and the manpages for `lrf` and `ovstart` for more details.

Troubleshooting the Multicast Smart Plug-in  
**Web Interface**

---

## **B** Frequently Asked Questions

## Questions about the Multicast Smart Plug-in Submaps

### Which routers work with the Multicast SPI?

See “Router Requirements” on page 28 for information about routers supported by the Multicast Smart Plug-in (SPI).

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

The Multicast SPI does not support *container* objects on the multicast submaps.

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

The Multicast SPI does not support *hidden* objects on the multicast submaps.

### How are multicast tunnels depicted on the Multicast SPI submaps?

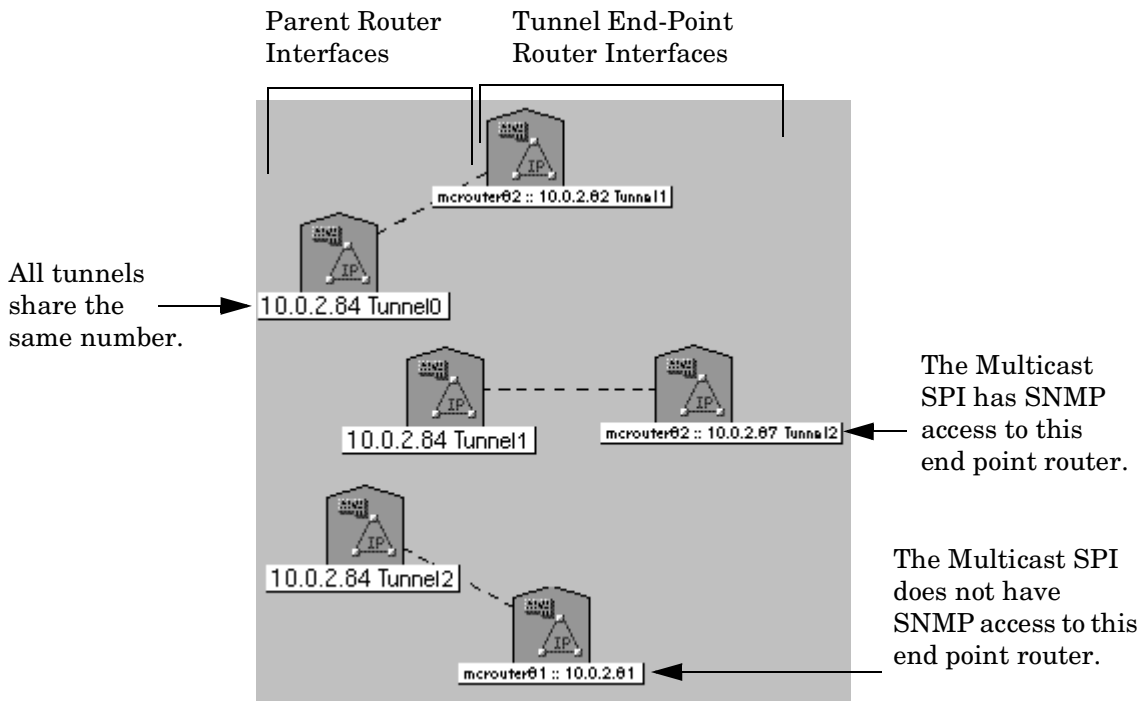
A dashed connecting line on any multicast submap indicates the neighbor relationship between endpoints of a multicast tunnel (instead of the solid line used for all other neighbor relationships). Multicast tunnels encapsulate multicast packets inside unicast packets for transport through networks that are not multicast-enabled; for example, tunneling private multimedia through the Internet. Tunnels can be used to pass information through firewalls.

Navigate to the Interfaces & Neighbors submap for a router. Look at the interface symbol labels. Logical multicast tunnel interfaces are discovered and monitored just like physical multicast-enabled interfaces on a router. If the Multicast SPI has access to SNMP information from the router, the logical multicast tunnel interface symbol's label and

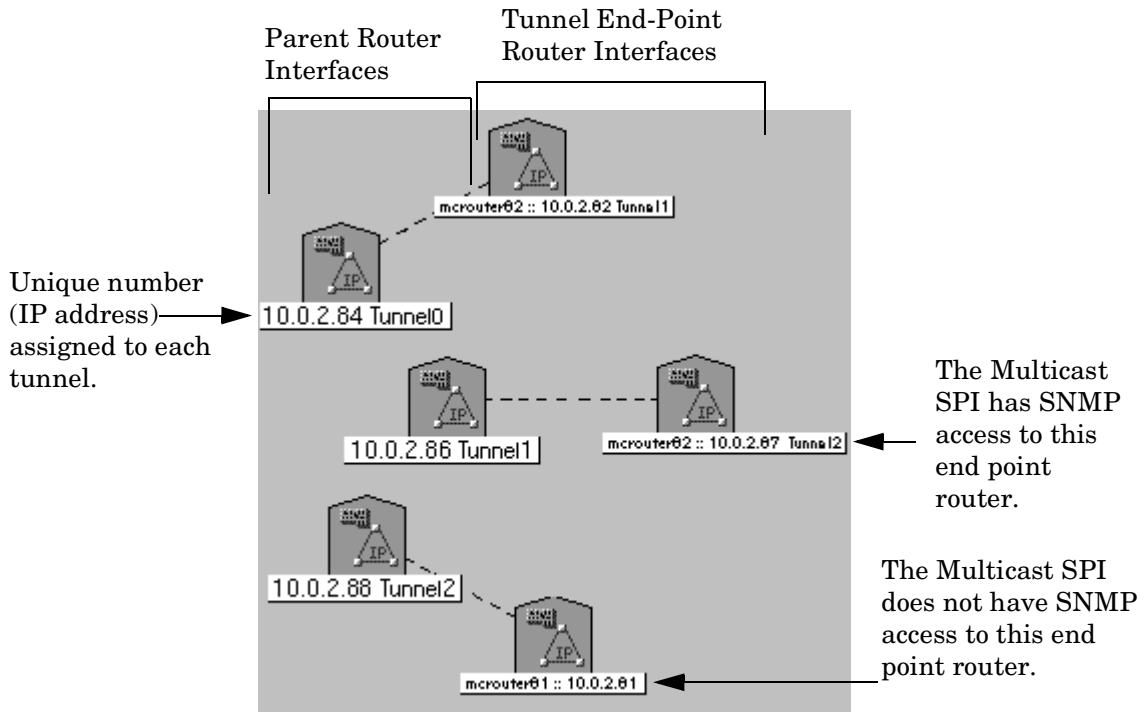
selection name include both the IP address used by the tunnel and the descriptor for the interface (obtained from the MIB-II *ifDescr* element; for example, Tunnel0).

Appending the *ifDescr* is necessary because tunnel interfaces may be configured with unnumbered IP addresses, and multiple such tunnel interfaces may use a single, common IP address as their tunnel source. Since the *ifDescr* is unique for each tunnel interface, appending it to the potentially common IP address results in a unique label and selection name for each tunnel interface. Refer to the following three figures for example snippets from the *Interfaces & Neighbors* submap for a router.

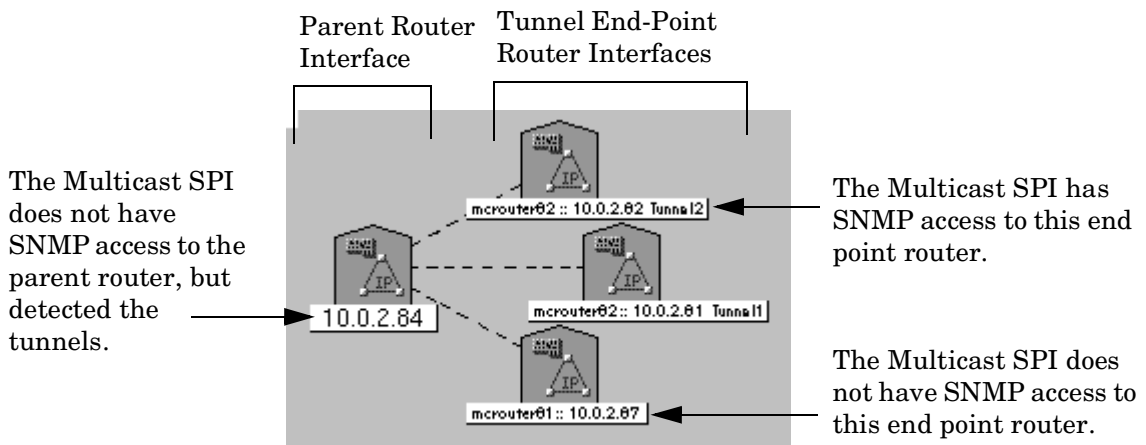
**Figure B-1 Unnumbered Multicast Tunnels with SNMP Read Access to Parent Router**



**Figure B-2**      **Numbered Multicast Tunnels with SNMP Read Access to Parent Router**



**Figure B-3**      **Any Multicast Tunnels without SNMP Read Access to Parent Router**





## The Multicast submap is empty. Why?

Discovery did not happen. Check whether `mmonitor` (the Multicast SPI discovery process) is running correctly. At the command prompt, type:

```
ovstatus mmonitor
```

If the status is not normal, restart the process. At the command prompt, type: `mmonitor`

If any errors are reported, please contact the HP Support and tell them the error reported, see “Support” on page 7.

If no error is displayed, configure `mmonitor` to print debug messages. Please see “mmonitor” on page 116 for more information.

## How does the Multicast SPI discovery process work?

The Multicast SPI background process called `mmonitor` conducts discovery for multicast-enabled routers in the following manner:

1. The Multicast SPI gathers all fully-qualified router IP-host-names/IP-addresses listed in the `managed.mmon` file.
2. Contacts one router using SNMP to gather the `sysName`. If SNMP is not available, contacts the router through your name resolution service to gather the `hostName`. See “How are symbol names (symbol labels) determined by the Multicast SPI?” on page 86 for more information.
3. Determines the router’s status:
  - **Managed** if that router matches the entries in the `managed.mmon` file. If *managed*, continue with next step.
  - **Unmanaged** if that router does not match entries in the `managed.mmon` file or matches entries in the `unmanaged.mmon` file. If *unmanaged*, place the router symbol (white icon) on the Multicast submap and return to step 2 contacting the next router on the list generated.

## Questions about the Multicast Smart Plug-in Submaps

4. Depending on the configuration in the `mmon.conf` file, issues `mrinfo` queries (IGMP protocol) or SNMP queries to:
  - Determine which interfaces within the router are multicast-enabled. Places the symbols on the multicast submaps.
  - Get the list of neighbors from each multicast-enabled interface in this router.
5. Append any reported neighbors to the list in step 1, if they are not already listed. Return to step 2 and choose the next router on the list.
6. This process continues until all of the most-recently-discovered neighboring routers are set to *unmanaged* or report no multicast neighbors (all discovery paths are terminated).
7. The managed routers are periodically queried for configuration and status information using the following:
  - Depending on the configuration in the `mmon.conf` file, either `mrinfo` queries (IGMP protocol) or SNMP queries to update multicast-enabled interfaces and neighboring relationships.
  - SNMP MIB-II (RFC1213.txt, also IETF STD0017) used to gather router and interface information.

The MIB-II object `sysName` must be set, and must be unique for each multicast-enabled router that you wish to manage.
  - If multicast tunnels are detected, the following SNMP MIBs are queried, as needed, to gather the required information:
    - `ipMRouteMIB`
    - `pimMIB`
  - `igmpMIB` and `ipMRoute MIB` used to verify the current location of the MIB files (experimental branch or standardized branch).

## Questions about the Multicast SPI Data Collection and Alarms

### **Multicast data collections are not happening. Why?**

Verify that `mtraffic` is running correctly. At the command prompt, type:

```
ovstatus mtraffic
```

If the status is not normal, restart it. At the command prompt, type:

```
mtraffic
```

If any errors are reported, please contact HP support with the error reported. See “Support” on page 7.

If no error is displayed, configure `mtraffic` to print debug messages. See “`mtraffic`” on page 118 for more information.

### **What are the important SNMP TRAPS that the Multicast SPI generates?**

See “Multicast-Specific SNMP Trap Definitions” on page 127.

### **Why do the Monitor Group Traffic Collection and Monitor Interface Traffic Collection tables open slowly?**

When information is gathered from the NNM `snmpCollect` database, the entire database must be scanned. Trim the data in your `snmpCollect` database to speed up this operation. See *Managing Your Network with NNM* for more information about the NNM `snmpCollect` database and available trimming routines.

### 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 48.

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 116.

### How do I determine the best value for “IGMP\_PARMS” in mmon.conf?

Read about the `TUNING` setting to monitor problems with slow router response times. See “TUNING” on page 52. You may wish to turn off `TUNING` after you establish the ideal settings, in order to reduce the number of multicast alarms being generated.

### How can I get information from the NNM Object Database (ovwdb)?

The `NNM` command `ovobjprint` outputs details of a specific object in the `NNM` object database. See the `ovobjprint` manpage for complete information about the parameters available to control the output.

To output the names of all multicast objects in the database, at the command prompt, type (`-a` specifies the name of the field to print):

```
ovobjprint -a 'Selection Name' 'isMulticast=TRUE'
```

To output the names of all multicast routers in the database, at the command prompt, type:

```
ovobjprint -a 'Selection Name' 'MCAST isRouter=TRUE'
```

To output information about a specific multicast router (`myRouter`) in the database, at the command prompt, type (remember to include the space character at the end of the router “Selection Name”):

```
ovobjprint -s 'myRouter '
```

To output more descriptive information from the database (instead of field name values) about a multicast object, see “mdbprint” on page 113.

## Questions about Accessing the Multicast SPI

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

Traffic data and events collected by the Multicast SPI can be forwarded to another NNM management station in the normal manner. See the NNM documentation for more information.

The Multicast SPI submaps residing on the NNM collection station can be displayed on a remote NNM management station only through NNM's web-based launcher.

### **What Multicast SPI 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:the Multicast SPI->Tasks, Viewing current the Multicast SPI 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 Alert Alarms category list is fully operational through the Launcher interface. Multicast alarms can be acknowledged and deleted over the web.

### **How do I access the web-based Multicast SPI operations apart from the NNM menu commands?**

On any computer from which you can access the computer that hosts the Multicast SPI, use the following URLs:

- For the multicast group traffic collection table:  
`http://<Host>:<Port>/OvCgi/mcastgrptable.ovpl`

**Questions about Accessing the Multicast SPI**

- For the multicast interface traffic collection table:  
**`http://<Host>:<Port>/OvCgi/mcastiftable.ovpl`**

Replace *<Host>* with your Hostname, and replace *<Port>* with the appropriate port number. The default port number is 3443.

---

# **C Command Line Utilities and Multicast Process Options**

Several utilities and process controls are available:

- “mdbprint” on page 113
- “mdbck” on page 114
- “mmonlog” on page 115
- “mmonitor” on page 116
- “mtraffic” on page 118
- “mmap” on page 120
- “Logging and Tracing for the Multicast SPI” on page 121



---

## **mdbprint**

This command displays all of the multicast-related information that the Multicast Smart Plug-in (SPI) 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. If `-a -v` combination is used, the deleted object count is printed in addition to information about current objects.

`-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 (see “How are symbol names (symbol labels) determined by the Multicast SPI?” on page 86):

```
$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
```

### Troubleshooting

Error message: *"No SNMP parameters for Interface 10.0.1.1"* Yet the interface's parent router does respond to SNMP.

Solution: Increase NNM's SNMP-query time-out and retry settings for the parent router's monitoring address:

1. On any NNM submap, select `Options:SNMP Configuration` (or at the command prompt, type `xnmsnmpconf`).
2. Create an entry for the parent router's monitoring address that increases the current settings for `Timeout` and `Retry Count` (click `Help` in the `SNMP Configuration` dialog box for more information).

---

## mmonlog

This command is useful when something unexpected happens and you do not have the multicast-specific logging and tracing enabled (“Logging and Tracing for the Multicast SPI” on page 121). The entries that are displayed when running this command are from the standard NNM *nettl* logging and tracing, with the `OVEXTERNAL` subsystem. You can use the `netfmt` command instead of `mmonlog`, if desired.

This command displays the last *N* entries in the *nettl* tracing and logging facility. It does not actually distinguish between the Multicast SPI and any other NNM process entries, thus it includes entries for NNM mixed in with entries for the Multicast SPI. When executing this command with no argument, the last two entries from *nettl* are displayed; with an optional numeric argument, the specified number of most recent entries are displayed.

---

**TIP**

`mmonlog` is more useful for troubleshooting the Multicast SPI 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 2.

### Example invocations:

```
$OV_BIN/mmonlog (last two entries 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`, and `ovresume`. 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 47.

If you are troubleshooting `mmonitor`, the following switches enable logging and tracing.

`-d -f -k -n` See “Logging and Tracing for the Multicast SPI” on page 121 for more information.

After making changes to the LRF file, execute the following commands to force the Multicast SPI to acknowledge the changes. From the command prompt, type:

1. `ovstop mmonitor`
2. `ovdelobj $OV_LRF/mmonitor.lrf`
3. `ovaddobj $OV_LRF/mmonitor.lrf`
4. `ovstart mmonitor`

If you are trying to fine tune the `CYCLE_MINUTES` setting in the `mmon.conf` file (see “`mmon.conf` Configuration File” on page 47), 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. Review the contents of the `$OV_SHARE_LOG/mmonitor.log` file for 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. 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`, and `ovresume`. 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`
  - `mcastIf%inutilStd`

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 dialog box (`snmpCollect`) are lost.

- d -f -k -n        See "Logging and Tracing for the Multicast SPI" on page 121 for more information.

After making changes to the LRF file, execute the following commands to force the Multicast SPI to acknowledge the changes. From the command prompt, type:

1. **ovstop mtraffic**
2. **ovdelobj \$OV\_LRF/mtraffic.lrf**
3. **ovaddobj \$OV\_LRF/mtraffic.lrf**
4. **ovstart mtraffic**

Review the contents of the `$OV_SHARE_LOG/mtraffic.log` file for the logging and tracing results.

---

## 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.

To establish logging and tracing for one instance of `mmap`, use environment variables (see “Environment Variables” on page 125).

To establish logging and tracing for all instances of this process, use the available switches in the `$OV_REGISTRATION/C/mmap` file. These switches can be inserted into the `mmap` registration file that launches `mmap`:

`-d -f -k -n` See “Logging and Tracing for the Multicast SPI” on page 121 for more information.

For example, in the `mmap` registration file, search for `$OV_BIN/mmap` and add `-d4` before the ending quote:

**Command** `-Shared -Initial "$OV_BIN/mmap -d4";`

Review the contents of the following files for `mmap` logging and tracing results:

`$OV_SHARE_LOG/mmap_<loginName>.log`

`$OV_SHARE_LOG/mcdialog_<loginName>.log` to view logging and tracing information about the Java Virtual Machine. The `mmap` process launches this Java Virtual Machine to perform user-interface interactions.

The behavior of the `mcdialog_<loginName>.log` file is inherited from any `mmap` logging and tracing settings; however, the `mcdialog` prefix to the *filename* cannot be changed.

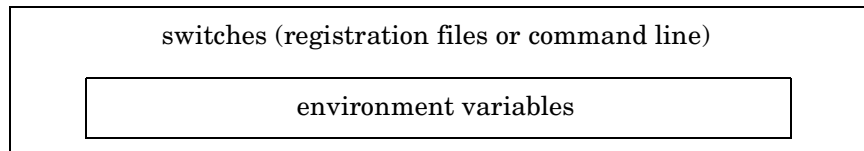


---

## Logging and Tracing for the Multicast SPI

Logging and tracing is available for the Multicast SPI processes.

The multicast logging and tracing levels can be specified in any combination of environment variable entries and registration-file/command-line switches. Switches override environment variable settings.



- Environment variables can define global default the Multicast SPI process behavior. `root` access is not required to change environment variables. (see “Environment Variables” on page 125).
- Switches that are in an individual process’s registration file or entered at the command prompt. `root` access is required. The switches override any environment variable settings (see “Switch Options” on page 122):
  - Customized logging and tracing settings for an individual Multicast SPI *foreground process* can be specified in the process’s registration file (`$OV_REGISTRATION/C/mmap`). For example (excerpt from the `mmap` registration file):

```
Command -Shared -Initial "$OV_BIN/mmap -d 3 -k 10240 -n 4"
```

- Customized log settings for an individual Multicast SPI *background process* can be specified in the process’s local registration file (`$OV_LRF/mmonitor.lrf` and `$OV_LRF/mtraffic.lrf`). For example (excerpt from the `mtraffic` registration file):

```
mtraffic:mtraffic:
OVs_YES_START:pmD,ovwdb,snmpCollect:-d 3 -n 4:OVs_WELL_BEHAVED:15:PAUSE:::
```

### SYNOPSIS

```
<multicastProcess> [-d <#loggingLevel>] [-f <path/filename>]
[-k <#fileSize(kbs)>] [-n <numberOfFiles>]
```

## Switch Options

`-d <#loggingLevel>`

Specifies the extent of logging and tracing desired. The `-d` switch within an individual process's registration file or at the command line, overrides any global setting. (A global multicast logging level can be specified via the environment variable `MC_DLEVEL=<integer>`. The default is 7 (MC\_NONE), if not otherwise specified.)

- |   |  |
|---|--|
| 7 | (MC_NONE) No logging.  |
| 6 | (MC_CRITICAL) An error in an application occurred, rendering continuation impossible.  |
| 5 | (MC_MAJOR) An event in an application occurred that has produced invalid results based on the functionality of the application.  |
| 4 | (MC_MINOR) An event occurred that should be relayed to the user for correction, but does not have adverse affect on the application or the functionality.                      |
| 3 | (MC_INFO) An event occurred that reflects import data for the specific application, and may be useful in debugging future problems without producing significant data.         |
| 2 | (MC_TRACE_L1) Tracing capability at a high level.  |
| 1 | (MC_TRACE_L2) Tracing capability at a medium level.  |
| 0 | (MC_VERBOSE) Tracing and informational information at the most verbose level. Data information in loops and frequent low level function calls may cause performance slow-down. |

`-f <path/filename>`

Controls the location and name of the logging file or files for a specific process.

`path`: by default, the path is assumed to be `$OV_SHARE_LOG` (which is an environment variable that is set by NNM during installation). The NNM environment variable `$OV_SHARE_LOG` must be set. An alternative path can be specified using the `-f` switch.

`filename`:

- Background processes (`mmonitor` or `mtraffic`) by default the filename equals the name of the process being monitored with a “.log” extension. For example, `mmonitor.log`. (See “mmonitor” on page 116 and “mtraffic” on page 118 for more information.)

A unique alternative name can be specified with the `-f` switch.

- A foreground process (`mmap`) potentially runs in multiple instances; therefore, by default the log file name equals the name of the process being monitored with the user’s login name appended and a “.log” extension. (If the user’s login name is unavailable, the `userID` is used instead.) For example, `mmap_samantha.log`. (See “mmap” on page 120 for more information.)

A unique alternative to the process’s name can be specified using the `-f` switch. Also, a unique alternative to the login name can be specified with the environment variable `MC_DUSER`.

`-k <#fileSize(kbs)>`

Specifies the *relative* maximum size of logging files in kilobytes. *Relative* means that a log file, on its last log entry, may go beyond the specified size. Log entries are truncated to the existing file until the limit is reached, then log entries overwrite a different version of the file determined by the `-n` setting.

Default log file size is 5 Megabytes (5120 kbs), if not otherwise specified.

A global multicast log file size can be specified through the environment variable `MC_DFILESIZE`.

Log file size can be specified within an individual process's registration file or the command line, overriding the global setting and the default setting.

`-n <numberOfFiles>`

Specifies the number of concurrent multicast log files allowed per process instance. If specified, each log file has a number appended to the file name, for example `mmonitor_3.log`, `mmonitor_4.log` or `mmap_samantha_1.log`, `mmap_samantha_2.log` After the maximum specified number of log files are filled, the oldest one is overwritten.

The default number of log files per process instance is one, if not otherwise specified.

A global number of persistent multicast logging files can be specified through the environment variable `MC_DFILES`.

The number of log files allowed can be specified within each individual process's registration file or at the command prompt, overriding the default and global settings.

## TROUBLESHOOTING

After making changes to any LRF file, execute the following commands to force the Multicast SPI to acknowledge the changes. From the command prompt, type:

```
ovstop <processName>  
ovdelobj $OV_LRF/<processName.lrf>  
ovaddobj $OV_LRF/<processName.lrf>  
ovstart <processName>
```

See also the *lrf* and *OVwRegIntro* manpages for more information.

## RELATED FILES

### UNIX:

```
$OV_REGISTRATION/C/mmap  
$OV_LRF/mmonitor.lrf  
$OV_LRF/mtraffic.lrf  
$OV_SHARE_LOG/mmap_<loginName>.log  
$OV_SHARE_LOG/mcdialog_<loginName>.log  
$OV_SHARE_LOG/mmonitor.log  
$OV_SHARE_LOG/mtraffic.log
```

## Environment Variables

Environment variables can define global default logging and tracing behavior for the Multicast SPI background processes and foreground processes. `root` access is not required to change environment variables.

---

### TIP

If you are using switches for a particular process, the environment variables are ignored (see “Switch Options” on page 122).

---

**Table C-1 Environment Variables for Multicast Logging and Tracing**

Environment Variable	Usage
MC_DLEVEL	Sets a global logging and tracing level for the Multicast SPI background and foreground processes.  The <code>-d</code> switch overrides this environment variable. See “Switch Options” on page 122 for more information.
OV_SHARE_LOG	This variable is set during NNM installation. Designates default <code>PATH</code> for storing NNM log files.  The <code>-f &lt;*path*/filename&gt;</code> switch overrides this environment variable.

**Logging and Tracing for the Multicast SPI****Table C-1 Environment Variables for Multicast Logging and Tracing**

<b>Environment Variable</b>	<b>Usage</b>
MC_DUSER	<p>For the Multicast SPI foreground process's log files, used to override the use of <code>loginName</code> in the log file naming convention:</p> <pre>mmap_&lt;loginName&gt;.log</pre> <pre>mcdialog_&lt;loginName&gt;.log</pre>
MC_FILESIZE	<p>Specifies global relative file size for the Multicast SPI logging and tracing files. For example, <code>MC_DFILESIZE=5120</code> sets the maximum relative log file size to 5 megabytes.</p> <p>The <code>-k</code> switch overrides this environment variable.</p>
MC_DFILES	<p>Specifies the number of concurrent log files allowed per the Multicast SPI process instance.</p> <p>The <code>-n</code> switch overrides this environment variable.</p>

---

# **D Multicast-Specific SNMP Trap Definitions**

## Harnessing the power of SNMP traps

The Multicast Smart Plug-in (SPI) 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 OpenView multicast-specific traps. The Multicast SPI has also added two new traps in the 0.0000 - 0.9999 range:

- The multicast threshold event uses the OpenView event number:  
.1.3.6.1.4.1.11.2.17.1.0.5369
- The multicast rearm event uses the OpenView event number:  
.1.3.6.1.4.1.11.2.17.1.0.5370

You can control NNM's response to any of these traps:

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 the Multicast SPI. 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 alarm browser under the `Multicast Alert Alarms` category.

You can customize NNM's response to any of these traps, 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.

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

Click `Help` for further instructions about using the NNM Event Configuration feature.



See *Managing Your Network with NNM* for more information about working with events.

---

## Public Trap Definitions

The important traps occur when the Multicast SPI 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)
- OV\_MCAST\_DataCollectThresh (1,3,6,1,4,1,11,2,17,1,0,5369)
- OV\_MCAST\_DataCollectRearm (1,3,6,1,4,1,11,2,17,1,0,5370)
- EVENT\_DATA\_COL\_AGENT\_DOWN a.k.a.  
OV\_MCAST\_DataColl\_AgentDn (1,3,6,1,4,1,11,2,17,1,0,30000049)

The following is a list of the var-binds in the Multicast SPI traps. Each var-bind is a triple.

```
/* 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)`

**Public Trap Definitions**

- 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)
```

**Public Trap Definitions**

```
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

\*/

**Public Trap Definitions**

```
/* OV_MCAST_DataCollectThresh */
```

```
{1,3,6,1,4,1,11,2,17,1,0,5369}
```

```
/* This event is generated by HP OpenView data collector when a  
sampled multicast traffic rate on an interface exceeds a preconfigured  
level. This is a mirror event of the regular threshold event:  
OV_DataCollectThresh and identifier: 58720263 */
```

```
/* 1) The ID of application sending the event
```

```
2) The name of the host that caused the threshold event
```

```
3) The HP OpenView object identifier, if available
```

```
4) The MIB variable in dotted numeric format
```

```
5) The name of the collection
```

```
6) The MIB instance
```

```
7) The threshold value
```

```
8) The sampled value
```

```
9) The highest sampled (peak) value
```

```
10) The time the highest value was sampled
```

```
11) The lowest sampled (trough) value
```

```
12) The time the lowest value was sampled
```

```
13) The threshold operator
```

```
14) The threshold count
```

```
*/
```

```
/* OV_MCAST_DataCollect_Rearm */
```

```
{1,3,6,1,4,1,11,2,17,1,0,5370}
```

```
/* This event is generated by HP OpenView data collector when a  
sampled multicast traffic rate on an interface drops below a  
preconfigured level, after generating an event for exceeding a value. This  
is a mirror of the regular NNM event: OV_DataCollect_Rearm :  
58720264 */
```

```
/* 1) The ID of application sending the event
```

```
2) The name of the host that caused the rearm event
```



```
3) The HP OpenView object identifier, if available
4) The MIB variable in dotted numeric format
5) The name of the collection
6) The instance
7) The rearm value
8) The sample value
9) The highest sampled (peak) value
10) The time the highest value was sampled
11) The lowest sampled (trough) value
12) The time the lowest value was sampled
13) The rearm operator
14) The rearm count
*/

/* EVENT OV_MCAST_DataColl_AgentDn */
{1,3,6,1,4,1,11,2,17,1,0,30000049}

/* This event is generated by HP OpenView data collector when it is no
longer able to collect a variable from an agent. This could be caused by
the node being unreachable or the agent no longer executing. */

/* 1) The ID of application sending the event
2) The name of the host that is no longer responding
3) The HP OpenView object identifier, if available
4) The MIB variable in dotted numeric format
5) The name of the collection
6) The MIB instance
7) The time since last successful collection or
"Unknown" if no successful collection since data
collector last started.
*/
```

Multicast-Specific SNMP Trap Definitions  
**Public Trap Definitions**

---

---

## **E Migration to the Multicast Smart Plug-in 2.1**

## What's New?

### **Multicast 2.0 to Multicast 2.0 with the Consolidated Patch Number PHSS\_28159/PSOV03228**

The following changes to the product were made in the consolidated patch for Multicast 2.0:

- Support for different versions of Cisco IOS and MIBs

Cisco's new router IOS versions support the IGMP and ipMRout MIBs in the standard MIB-II branch.

The consolidated patch allows management of routers running IOS versions 12.2(4)T and later, as well as, the already supported older versions. In the NNM MIB Browser, you will see IGMP-MIB referenced in two MIB branches. To use the NNM MIB Browser for gathering information, use:

- .iso.org.dod.internet.mgmt.mib-2.igmpStdMIB (for newer IOS versions i.e., 12.2(4)T or later)
- .iso.org.dod.internet.experimental.igmpMIB (for older IOS versions)

- Changes to Monitor Traffic Collection

The two menu commands under the Multicast menu, Multicast Data Collection -> Monitor Group Traffic Collection and Multicast Data Collection -> Monitor Interface Traffic Collection now use a web interface. The web interfaces provide a Pause button. To sort by a column of your choice, click on the column title.

Prior to this patch, the native NNM user interface-based table had to be running in order to be able to use the web interface. That requirement does not exist anymore with the patch.

If you encounter problems getting these menu commands working on your computer, check the following configuration files:

— `$OV_CONF/ovweb.conf`

Verify that Browser, Host, and Port are set appropriately. Also verify that the browser specified in this file works correctly. Host and Port must match what is specified in `httpd.conf` (explained below). See the manpage of `ovweb.conf` for full details.

— `/opt/OV/httpd/conf/httpd.conf`

Verify that `ServerName` and `Port` match the values specified for Host and Port in `ovweb.conf`.

— `/apps/bin/netscape`

Assuming that your preferred browser is Netscape (as specified in `ovweb.conf`), verify that `/apps/bin/netscape` points to the correct version of Netscape that is operational on your computer.

— `$OV_LRF/httpd.lrf`, etc.

Verify that your `httpd` process is started by `ovstart`. Please see `$OV_LRF/httpd.lrf` and the manpages for `lrf` and `ovstart` for more details.

Optionally, you can ignore these two menu commands and bookmark the following URLs on any computer from which you can access the computer that hosts the Multicast product:

— Group: `http://<Host>:<Port>/OvCgi/mcastgrptable.ovpl`

— Interface: `http://<Host>:<Port>/OvCgi/mcastiftable.ovpl`

Replace `<Host>` with your Hostname, and replace `<Port>` with the appropriate port number. In NNM, the default port number is 3443.

- New menu command for locating an IP Address

A new menu command, `Locate & Highlight IP Address` has been added under the Multicast menu.

With this menu command, you can locate the Subnet or Router object in the Multicast submap that contains the specified IP Address. This menu command is useful for identifying where an IP Address belongs in the map (i.e., which subnet or router) and can be used as part of troubleshooting multicast traffic to/from a specific IP Address.

## What's New?

If the specified IP address belongs to one of the Routers managed by the Multicast product, that Router symbol and the connection-line (representing the Interface) is highlighted.

Otherwise, the Subnet symbol where the IP address exists is highlighted.

- Change to the menu command for clearing highlights

The Multicast:Clear Highlights menu command clears the highlights created by either Highlight PIM Designated Routers or Locate & Highlight IP Address.

This replaces the earlier menu command Clear PIM Highlights.

- Enhancements to Describe Multicast Object operation

The Describe Multicast Object menu command now shows an enhanced structure for better readability.

- Changes to menu accelerator keys

Due to some changes in the Multicast menu, the accelerator keys for the menu commands have been changed.

- IP Address wildcards in managed.mmon and unmanaged.mmon

It is now possible to specify IP Address ranges using wildcards in the `$OV_CONF/managed.mmon` and `$OV_CONF/unmanaged.mmon` files.

By default, you continue using your current version of these files. If you wish to take advantage of the IP Address wildcards, please see the comments section of `/usr/newconfig/etc/opt/OV/share/conf/managed.mmon` for more details.

We recommend that you replace the comments in your `$OV_CONF/managed.mmon` with those from the new file, `/usr/newconfig/etc/opt/OV/share/conf/managed.mmon`, so that you have this information for future reference.

- New/modified configuration parameters in `mmon.conf`

A few configuration options have been added/modified.

By default, you continue using your current version of this configuration file, `$OV_CONF/mmon.conf`. Changes to the configuration options are explained as comments in the new version of the configuration file:

`/usr/newconfig/etc/opt/OV/share/conf/mmon.conf`.

**DO NOT OVERWRITE YOUR CURRENT `$OV_CONF/mmon.conf` FILE.**

Here is the list of changes:

- `NODE_STATUS`: Has an additional parameter to configure Status if the Multicast MIBs are inadequate.
- `DOMAIN_SUFFIX`: Now, multiple suffixes can be specified.
- `TRIM_FWD_TREE_STATE`: Affects Forwarding Tree display.
- `DISCOVERY_VIA_SNMP`: This allows options for the discovery process (MRINFO versus SNMP).

*Tip:* We recommend that you copy the comments for `NODE_STATUS`, `DOMAIN_SUFFIX`, `TRIM_FWD_TREE_STATE`, and `DISCOVERY_VIA_SNMP` from `/usr/newconfig/etc/opt/OV/share/conf/mmon.conf` to `$OV_CONF/mmon.conf`, so that you have this information for future reference.

## **Multicast 2.0 with the Consolidated Patch Number PHSS\_28159/PSOV03228 to the Multicast Smart Plug-in 2.1**

The following changes to the product were made in the Multicast Smart Plug-in (SPI) 2.1:

- Multicast 2.0 ran with NNM 6.2. The Multicast SPI 2.1 is supported only with NNM Advanced Edition 7.01.
- Forwarding tree display when routers have multiple parallel connections (OpenView "metaconnections")

Previous versions of NNM Multicast failed to display the forwarding tree on the single line used on the network map to represent multiple, parallel connections between routers (known as an

## What's New?

OpenView "metaconnection"). This problem is fixed, and the forwarding tree is also correctly shown on the metaconnection submap.

- Forwarding tree display when no data is flowing on route

Previous versions of NNM Multicast displayed forwarding trees using only two colors (one for shared tree, one for source-specific or shortest-path tree. Now the critical-status color (red) may also be used in a forwarding tree display. This color is used when data is not flowing along a portion of the tree, as reported by the routers. A pop-up message appears when this condition is detected during the display of a forwarding tree. This serves as a visual indication of a multicast fault, and aids in diagnosis of multicast issues.

In addition, the display of a forwarding tree will now correctly follow the shared path for the next hop downstream if the incoming shortest-path route is not receiving data. Prior versions of NNM Multicast did not handle this correctly.

- New configuration parameters in mmon.conf

A few configuration options have been added:

- NO\_DISABLED\_INTERFACE\_IN\_SUBNETS

By default, disabled interfaces may result in "blue subnets" appearing on the map because the disabled interface may be the only multicast-enabled interface in the subnet. With no other object to define the subnet's status, it is unknown (blue).

Setting this parm to 1 disables the display of "blue subnets" that are caused by disabled interfaces, by eliminating all disabled interfaces from subnets. This can greatly reduce the number of objects on a multicast map.

The disabled interfaces will still be seen on router submaps, and via the Describe Multicast Object menu command when one or more routers is selected.

- MAX\_SNMP\_GETBULK\_ROWS

SNMP accesses may try for 1000 or more objects using SNMP v2C get-bulk. Some routers are overwhelmed by this. This parameter determines the maximum number of objects requested with each SNMP get-bulk request. This default value works with all routers, at the cost of reduced efficiency for more capable routers.



- New configuration parameters in `mmon_ma.conf`

Three interface types have been added to `mmon_ma.conf`:

- `propVirtual`
- `l2vlan`
- `l3ipvlan`

For information about using this configuration file, see the Multicast Smart Plug-in Administrator's Guide, Chapter 2 "Installation and Configuration."

- Interface labels

For Cisco and Foundry routers, interface labels will incorporate the standard short-form of the interface description. As examples:

**Table E-1**

**Example Use of Interface Description Short Forms in Labels**

| <b>Interface Description</b> | <b>Submap Label Text</b> |
|------------------------------|--------------------------|
| Ethernet2/0                  | Et2/0                    |
| ATM9/0/0.1-aal5 layer        | AT9/0/0.1                |
| GigabitEthernet4/14          | Gi4/14                   |

## Migration from Multicast 2.0 to the Multicast SPI 2.1

No steps beyond the standard installation of the Multicast SPI 2.1 are required when migrating from NNM Multicast 2.0 with or without consolidated patch PHSS\_28159/PSOV03228.

If your HP customer support for Multicast 2.0 is current, this upgrade to the 2.1 version of the Multicast SPI is free.

Before upgrading to the Multicast SPI 2.1, you must upgrade to NNM Advanced Edition 7.01.

When upgrading from Multicast 2.0 to the Multicast SPI 2.1, all of your customizations to the following files are preserved. None of your settings are changed during installation. The new versions of these files (excluding `unmanaged.mmon`) are installed to the `/usr/newconfig/etc/opt/OV/share/conf/*` directory.

- `mmonitor.lrf`
- `mtraffic.lrf`
- `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`
  - `unmanaged.mmon`

A new version of the `mmap` registration file is installed to provide access to new the Multicast SPI 2.1 menu commands. The old version of the `mmap` registration file is moved to `/tmp/Multicast/mmap.$LANG.save` (for example `/tmp/Multicast/mmap.C.save`). If you customized your

mmap file for Multicast 2.0 (see “mmap” on page 120), review your changes and reproduce those you wish to continue using in the newer version of the mmap file for the Multicast SPI 2.1.

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 the Multicast SPI installation:

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

New `mcast_fields` are added to the NNM object database (`ovwdb`). The new fields are associated with each multicast-enabled router object and are used to record the location of the multicast MIB files, since they may be located either in the experimental branch or the MIB-II branch, depending upon the operating system version on the router.

Migration to the Multicast Smart Plug-in 2.1

**Migration from Multicast 2.0 to the Multicast SPI 2.1**

**A**

alarms  
  automatic actions, 21  
  for slow IGMP response (TUNING), 52  
  multicast, 21, 24, 77  
  rearm for threshold, 21  
  threshold, 21  
  troubleshooting, 94, 97  
anycast, 13  
arrows, 15  
ATM, 54  
Auto Pass, 62  
automatic actions response, 21

**B**

blue symbols, 82

**C**

collection stations, 109  
command line utility  
  mdbck, 114  
  mdbprint, 113  
  mmonlog, 115  
community names, 30  
configuration  
  community names, 29  
  data collection, 21, 55  
  logging and tracing, 121  
  managed.mmon, 43  
  mmap, 120  
  mmon.conf, 47  
  mmon\_ma.conf, 54  
  mmonitor, 116  
  mtraffic, 118  
  overview, 42  
  snmpCollect.lrf, 55  
  unmanaged.mmon, 45  
console (NNM Advanced Edition), 40  
container objects  
  multicast submaps, 102  
CPU overload, 98  
creating  
  multicast tools, 80  
CYCLE\_MINUTES, 48, 108

**D**

data collection  
  configuration, 21, 55, 75  
  configure community names, 29

  configuring (multicast), 21  
  monitoring multicast, 21  
  process, 118  
  stop, 58  
  suspend, 58  
  synchronize with NNM, 95, 118  
  troubleshooting, 55, 94  
Data Collection & Thresholds, 58  
database  
  limits, 92  
  object, 24, 58  
  print out, 108  
discovery  
  controlling file, 43  
  controlling mechanism, 52  
  process, 105, 116  
  restart, 58  
DISCOVERY\_VIA\_SNMP, 52  
displaying  
  current group traffic, 23  
  multicast forwarding tree, 15, 52, 71, 82  
  multicast group membership, 17, 71, 82  
  PIM designated routers, 20, 72  
  specific IP address, 19, 72  
DOMAIN\_SUFFIX, 51

**F**

fault  
  diagnosing multicast, 78  
FILTER  
  managed, 43, 49  
  NNM filters, 24  
  unmanaged, 45, 50  
forwarding tree, 15, 71  
  configuring display, 52  
  troubleshooting, 82  
frequency  
  data collection, 21  
  discovery, 48, 51  
  MIB location check, 51  
  status check, 48, 51  
frequently asked questions, 101  
  accessing the Multicast SPI, 109  
  data collection and alarms, 107  
  submaps, 102

**G**

GET community names, 30  
graph

---

# Index

- create your own, 80
  - Group Traffic (group,\*), 68
  - Group Traffic Over Tree, 15, 68
  - Incoming All Traffic, 68, 76
  - Incoming Multicast, 68, 76
  - Outgoing All Traffic, 68
  - Outgoing Multicast, 68
  - Router Health, 68
  - troubleshooting, 97
  - group (multicast)
    - all known per router, 70
    - data collection, 21
    - forwarding tree, 71
    - highlight members, 17, 71
    - traffic, 23
- ## H
- hidden
    - objects, 102
    - symbols, 92
  - highlight
    - forwarding tree, 15, 71
    - group routers and subnets, 17, 71
    - PIM designated routers, 20, 72
    - PIM designated routers failed, 93
    - specific IP address, 19, 72
    - troubleshooting, 82
  - HOST\_IP, 47
  - HP Auto Pass, 62
  - HSRP, 43
- ## I
- ifType, 54
  - IGMP
    - discovery configuration, 52
    - generate alarm upon late response, 52
    - join, 20
    - mrinfo, 52
    - polling configuration, 48
    - retry setting, 48
    - time-out setting, 48
  - IGMP\_PARMS, 48, 108
  - installing the Multicast SPI
    - configuration, 42
    - HP-UX, 31
    - license, 62
    - on NNM Advanced Edition remote console, 40
    - on NNM Advanced Edition server, 40
    - Solaris, 35
    - upgrade from Multicast 2.0, 140
    - upgrade from Multicast 2.0 with the consolidation patch, 140
  - installing the MulticastSPI MIBs, 28
  - interface
    - controlling display of unknown status, 53
    - names on map, 86
    - status calculation, 52
    - submap, 13
    - wrong symbol, 93
  - interval
    - data collection, 21
    - discovery, 48, 51
    - MIB location check, 51
    - status check, 48, 51
- ## J
- join multicast group, 17
- ## L
- license for the Multicast SPI, 62
  - links
    - names on map, 86
  - list
    - database objects, 108
    - multicast groups, 18, 68, 70
  - local registration file (LRF)
    - mmonitor, 116
    - mtraffic, 118
    - snmpCollect, 55
  - logging
    - multicast-specific, 121
    - tracing through mmonlog, 115
- ## M
- managed routers, 43
  - management console (NNM Advanced Edition), 40
  - management station
    - prerequisites, 28, 29
  - map overlay
    - forwarding tree, 15, 71
    - group members, 17, 71
    - PIM designated routers, 20, 72
    - specific IP address, 19, 72
  - MAX\_SNMP\_GETBULK\_ROWS, 53
  - mdbck, 114
-

- mdbprint, 113
  - menu
    - commands, 68
    - items not functioning, 82
  - MIBs
    - multicast, 28
  - migration
    - from Multicast 2.0, 140
    - from Multicast 2.0 with the consolidated patch, 140
  - mmap, 120
  - mmon.conf
    - CYCLE\_MINUTES, 48, 108
    - DISCOVERY\_VIA\_SNMP, 52
    - DOMAIN\_SUFFIX, 51
    - FILTER (managed), 49
    - FILTER (unmanaged), 50
    - HOST\_IP, 47
    - IGMP\_PARMS, 48, 108
    - MAX\_SNMP\_GETBULK\_ROWS, 53
    - NO\_DISABLED\_INTERFACE\_IN\_SUBNETS, 53
    - NODE\_CONTROLS\_INTF\_STATUS, 52
    - NODE\_STATUS, 50
    - TRIM\_FWD\_TREE\_STATE, 52
    - TUNING, 52
  - mmon\_ma.conf, 54
  - mmonitor
    - optimal settings, 108
    - process configuration, 116
    - start, 57
    - stop, 58
    - vs. netmon, 24
  - mmonlog, 115
  - monitor
    - data collection, 21
  - mrinfo, 52
    - obtaining the software, 83
    - requirements, 28
    - running the software, 84
    - sample output, 85
    - troubleshooting, 89
  - mtraffic
    - process configuration, 118
    - start, 57
    - stop, 58
    - synchronize data collection with NNM, 95, 118
    - vs. netmon, 24
  - multi-access ports, 54
  - multicast
    - creating your own tools, 80
    - diagnosing faults, 78
    - MIBs, 28
    - monitoring performance, 78
    - symbol status, 11, 50
    - traps, 128, 130
    - tunnels, 11, 102
  - Multicast 2.0 migration, 140
  - Multicast 2.0 with the consolidated patch migration, 140
  - multicast group, see group (multicast)
  - Multicast SPI
    - collection stations, 109
    - configuration, 42
    - installation (HP-UX), 31
    - installation (Solaris), 35
    - license, 62
    - menu commands, 68
    - prerequisites, 28, 29
    - read-write access, 82
    - relationship to NNM Advanced Edition, 24
    - uninstall, 60
    - web access, 109
  - multicast submaps, 11, 13, 14, 15, 17, 102
  - multicast traffic
    - current group activity, 23
    - monitor data collection, 21
- ## N
- names
    - of interfaces, 86
    - of links, 86
    - of routers, 51, 86
    - of subnets, 86
  - neighbor relationship, 13
  - netmon, 24
  - NNM
    - object database, 58
    - slow to open, 82
  - NNM Advanced Edition
    - patches required, 29
    - relationship to the Multicast SPI, 24
  - NO\_DISABLED\_INTERFACE\_IN\_SUBNETS, 53
  - NODE\_CONTROLS\_INTF\_STATUS, 52
  - NODE\_STATUS, 50
- ## O
- object
-

---

# Index

- container, 102
- database, 24, 58, 108
- hidden, 102
- names, 86
- status, 73
- status calculation, 50
- troubleshooting, 82, 108
- ovwsetupclient command, 40

## P

- pan and zoom, 69
- password for the Multicast SPI, 62
- patches
  - required software, 28, 29
- performance
  - monitoring multicast, 78
  - slow, 98
- PIM (Protocol-Independent Multicast)
  - designated router not highlighted, 93
  - locate designated router, 20, 72
- pink symbols, 17
- PolicyXpert, 77
- polling
  - discovery frequency, 48, 51
  - for data collection, 21
  - IGMP, 48
  - interface to use, 47
  - interval, 48
  - MIB location frequency, 51
  - process, 118
  - SNMP configuration, 55
  - status frequency, 48, 51
- prerequisites for multicast, 28, 29
- public trap definitions, 130

## R

- read-write access, 13, 82
- rearm
  - alarm for data collection, 21
  - automatic action, 21
- registration file
  - mmap, 120
  - mmonitor.lrf, 116
  - mmtraffic.lrf, 118
  - snmpCollect.lrf, 55
- remote console (NNM Advanced Edition), 40
- retry
  - IGMP setting, 48
  - SNMP setting, 94

- review
  - data collection (multicast), 21
- router
  - all multicast groups, 17
  - avoiding overloading with SNMP getbulk requests, 53
  - data collection (multicast), 21
  - IGMP JOIN, 17
  - known problems, 28
  - locate IP address, 19, 72
  - locate PIM designated, 20
  - locate PIM designated failed, 93
  - managed, 43
  - names on map, 51, 86, 92
  - passive join, 17
  - prerequisites, 28
  - supported, 28
  - unmanaged, 45
  - wrong symbol, 88

## S

- seed file, 43
- self-subscribe join group, 17
- server (NNM Advanced Edition), 40
- Service Guard environment, 41, 47
- shorten router names, 51
- SNMP
  - community names, 30
  - discovery configuration, 52
  - getbulk configuration, 53
  - multicast MIBs, 28
  - multicast traps, 128, 130
  - polling configuration, 55
  - retry setting, 94
  - time-out setting, 94
  - troubleshooting, 90, 94
- snmpCollect.lrf
  - c parameter, 55
  - n parameter, 55
- standby
  - address (HSRP), 43
  - hostname (HSRP), 43
- start
  - Multicast SPI, 57
  - read-write access, 82
- static group IOS command, 17
- status
  - blue symbol, 53, 82
  - calculation configuration, 50, 52
  - keeps changing, 88, 89, 90, 91



- multicast, 73
- polling process, 116
- white symbol, 85
- stop
  - data collections, 58
  - Multicast SPI, 58
- submaps
  - container objects, 102
  - customizing, 69
  - hidden objects, 102
  - interfaces & neighbors, 13
  - multicast, 11, 15, 17
  - process, 120
  - subnet, 14
  - troubleshooting, 82
  - zoom, 69
- subnet
  - names on map, 86
  - submap, 14
- support
  - contacting HP, 7
- suspend
  - multicast data collections, 58
- symbol
  - color meaning, 88
  - container, 102
  - duplicate, 92
  - hidden, 92, 102
  - names, 86
  - odd, 88, 93
  - remove direct connect network, 54
  - status, 11, 73, 82, 88, 89, 90, 91
  - status calculation, 50
  - troubleshooting, 82
- synchronize
  - troubleshooting, 95
  - with NNM data collection, 118
- sysName for routers, 28, 105
- system requirements, 29

**T**

- table, 68
  - create your own, 80
  - Groups with Local Subscribers, 17, 70
  - Monitor Group Traffic Collection, 21
  - Monitor Interface Traffic Collection, 21
  - Show All Group Activity, 23, 76
  - troubleshooting, 94, 97
- thresholds

- alarms, 21
  - automatic actions, 21
  - multicast, 21, 77
- time-out
  - generate alarm for late IGMP response, 52
  - IGMP setting, 48
  - SNMP setting, 94
- tools
  - creating your own multicast, 80
- topology, 11
- tracing
  - multicast-specific, 121
  - through mmonlog, 115
- traffic
  - current group activity, 23
  - multicast, 75
  - over tree, 15
- traps
  - automatic action, 21
  - multicast, 128, 130
- tree (multicast forwarding), 15, 71
- TRIM\_FWD\_TREE\_STATE, 52
- troubleshooting
  - data collection and alarms, 94
  - graphs, 97
  - logging and tracing processes, 121
  - multicast environment, 23
  - NNM Multicast, 81
  - performance, 98
  - submap issues, 82
  - tables, 97
  - web interface, 99
- TUNING, 52
- tunnels, 11, 102

## **U**

- uninstalling
  - Multicast SPI, 60
- unmanaged routers, 45, 85

## **W**

- web access, 109
- web interface
  - accessing, 109
  - troubleshooting, 99
- white symbols, 85

## **X**

- X's, 15

---

## Index

### Z

zoom in on submap, 69