

HP OpenView Network Node Manager User's Guide



**Manual Part Number: J2316-90004
Printed in U.S.A., December 1993**

Notice

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

The specific warranty information for the product as to which this material relates is available in Hewlett-Packard's purchasing and licensing terms and conditions.

© Copyright 1992, 1993 Hewlett-Packard Company.

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

Restricted Rights Legend

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

© Copyright 1980, 1984, AT&T, Inc.

© Copyright 1988, 1989, Carnegie Mellon University.

© Copyright 1988, 1989, Massachusetts Institute of Technology.

© Copyright 1979, 1980, 1983, 1985-1988 The Regents of the University of California.

© Copyright 1986, 1987, 1988 Sun Microsystems, Inc.

This software and documentation is based in part on the Fourth Berkeley Software Distribution under license from the Regents of the University of California.

OSF/Motif is a trademark of the Open Software Foundation.

UNIX® is a registered trademark of UNIX System Laboratories Inc. in the U.S.A. and other countries.

Hewlett-Packard Company
3404 East Harmony Road
Fort Collins, CO 80525, U.S.A.

Printing History

First Edition

December 1993

Contents

Chapter 1: Introduction to Using HP OpenView Network Node Manager

Introduction	1-1
General Capabilities of Network Node Manager	1-2
Definitions and Concepts	1-3
Managers and Agents	1-3
MIBs	1-5
How MIBs are Organized	1-6
Unique Properties of the MIB Object sysObjectID	1-7
IP Map	1-8
Submaps	1-8
OVW Root Submap and Home Submap	1-8
IP Map Submaps	1-10
Internet Submap	1-11
Network Submaps	1-12
Segment Submaps	1-14
Node Submaps	1-16
Layout Algorithms	1-17
Map Objects and Symbols	1-17
Symbol Varieties	1-17
Symbol Types (Class and Subclass)	1-18
The Connection Symbol	1-18
Symbol Status	1-19
How IP Map Conveys Status	1-19
Compound Status	1-19
Events	1-21
How Events are Generated	1-21
Traps	1-21
Where to Go for Help	1-23

Chapter 2: Getting Started

Starting HP OpenView Network Node Manager	2-2
Starting NNM	2-2
Prerequisites for this Task	2-2
Procedure	2-2
The ovw Command	2-3
Options	2-3
Examples	2-4
The Submap Window	2-4
The Menu Bar	2-5
The Viewing Area	2-5
The Status Line	2-5
The Button Box	2-5
Map Synchronization	2-6
Exiting HP Network Node Manager	2-7
Understanding IP Map Configuration	2-8
Customizing IP Map for a New Map	2-9
Disabling IP Map Functionality	2-9
Purpose for This Task	2-9
Prerequisites for This Task	2-9
Procedure	2-9
IP Map Configuration Settings and Their Meaning	2-10
Customizing IP Map for an Existing Map	2-12
Purpose for This Task	2-12
Prerequisites for This Task	2-12
Procedure	2-12
Disabling IP-Only Status	2-13
Purpose for This Task	2-13
Prerequisites for This Task	2-13
Procedure	2-13

Chapter 3: Managing Network and System Configuration

Expanding Higher Levels of Your Network Map	3-2
Container Objects	3-2
Partitioned Internet Submaps	3-2
Creating a Partitioned Internet Submap	3-3
Purpose of this Task	3-3
Prerequisites for this Task	3-3
Procedure	3-3
The Containment Realm	3-4
Editing Guidelines	3-4
Example of Internet Submap	3-5
Example of Partitioned Internet Submap	3-6
Maintaining the Containment Realm	3-7
Expanding Lower Levels of Your Network Map	3-8
Adding a Network Object	3-8
Prerequisites for this Task	3-9
Procedure	3-9
Adding a Segment Object	3-10
Prerequisites for this Task	3-11
Procedure	3-11
Adding a Node Object	3-13
Prerequisites for this Task	3-14
Procedure	3-14
Adding an IP Interface Object	3-15
Prerequisites for this Task	3-15
Procedure	3-15
Automatic Layout	3-17
Purpose of this Task	3-17
Prerequisites for this Task	3-18
Procedure 1: For Specific Submaps	3-18
Procedure 2: For All Submaps	3-18
Updating a Map Open with Read-Only Access	3-19
Purpose of this Task	3-19

Prerequisites for this Task	3-19
Procedure	3-19
Taking a Snapshot of Your Network	3-20
Purpose of this Task.	3-20
Prerequisites for this Task	3-20
Procedure	3-20
Viewing Your Current Network and System Configuration	3-21
Viewing Object Descriptions	3-21
Prerequisites for this Task	3-21
Procedure	3-21
Description of an IP Internet Object	3-22
Description of a Network Object.	3-23
Description of a Segment Object.	3-24
Description of a Node Object	3-25
Description of an Interface Object.	3-26
Viewing Network Address Information	3-27
Prerequisites for this Task	3-27
Procedure	3-27
Viewing How Traffic is Routed on a Network	3-28
Prerequisites for this Task	3-28
Procedure	3-28
Viewing the Address Translation Table.	3-29
Prerequisites for this Task	3-29
Procedure	3-29
Viewing the Services Available on a Node	3-30
Prerequisites for this Task	3-30
Procedure	3-30
Viewing Disk Space	3-31
Prerequisites for this Task	3-31
Procedure	3-31
Controlling Network and System Configuration.	3-32
Using SAM to View or Modify HP-UX Network and System Configuration	3-32
Prerequisites for this Task	3-32
Procedure	3-32

Using the Terminal Emulator to Access Other Systems	3-33
Prerequisites for this Task	3-33
Procedure 1: Using Telnet (hpterm)	3-34
Procedure 2: Using Telnet (xterm)	3-34
Procedure 3: Using Vt3k (hp3000)	3-34
Chapter 4: Monitoring Your Network	
Checking the Health and Status of Your Network	4-2
Looking at Maps for Color Alerts	4-2
Purpose of this Task	4-2
Prerequisites for this Task	4-3
Procedure	4-4
Looking at Maps for New Nodes	4-4
Purpose of this Task	4-4
Prerequisites for this Task	4-5
Procedure	4-5
Creating Special Submaps for Monitoring Status	4-5
Purpose of this Task	4-5
Prerequisites for this Task	4-5
Procedure	4-6
Checking for Event Notifications	4-7
Purpose of this Task	4-7
Prerequisites for this Task	4-8
Procedure	4-8
Monitoring for Proactive Fault Diagnosis	4-10
Establishing Baselines for Normal Network Performance	4-10
Prerequisites for this Task	4-11
Procedure	4-11
Building an Application to Monitor Trends	4-12
Prerequisites for this Task	4-12
Procedure	4-12
Setting Up Thresholds for Monitored MIB Values	4-14
Prerequisites for this Task	4-14
Procedure	4-14
Fine Tuning Threshold Monitoring	4-18

Prerequisites for this Task	4-18
Procedure	4-18
Setting Up Event-Triggered Actions	4-18
Prerequisites for this Task	4-19
Procedure	4-19
Chapter 5: Diagnosing Network Communication Problems	
Approach to Problem Diagnosis	5-2
Symptoms of Network Communication Problems	5-3
Diagnosing Network Connectivity Problems	5-4
Purpose of this Task	5-4
Diagnosing Connectivity within the Same Network	5-4
Prerequisites for this Task	5-4
Procedure	5-5
Diagnosing Connectivity across Networks	5-6
Prerequisites for this Task	5-6
Procedure	5-7
Diagnosing Network Performance Problems	5-9
Purpose	5-9
Prerequisites for this Task	5-9
Procedure	5-10
Diagnosing Network Service Problems	5-12
Purpose of this Task	5-12
Prerequisites for this Task	5-12
Procedure	5-13
Chapter 6: Using Network Node Manager Operations	
Loading MIBs	6-2
Purpose of this Operation	6-2
Prerequisites for this Operation	6-2
Procedure	6-3
Viewing MIB Values	6-4
Prerequisites for this Operation	6-4
Procedure	6-4
Related Topics	6-5
Setting MIB Values	6-6
Prerequisites for this Operation	6-6

Procedure 1: Setting Values Using the Query Function.	6-6
Procedure 2: Setting Values Directly (Without Querying)	6-7
Related Topics	6-8
Collecting MIB Data	6-9
Prerequisites for this Operation	6-9
Procedure	6-9
Related Topics	6-12
Defining Thresholds	6-13
Prerequisites for this Operation	6-13
Procedure	6-13
Related Topics	6-15
Viewing Historical Trends.	6-16
Prerequisites for this Operation	6-16
Procedure	6-16
Related Topics	6-17
Building MIB Applications.	6-18
Prerequisites for this Operation	6-18
Procedure	6-19
Related Topics	6-21
Defining Actions for Events	6-22
Conceptual Information about Configuring Events	6-22
Prerequisites for this Operation	6-23
Procedure	6-23
Related Topics	6-24
Taking Snapshots of the Map	6-25

Index

Introduction to Using HP OpenView Network Node Manager

Introduction

Welcome to the HP OpenView Network Node Manager (NNM) product. NNM is a multivendor network management application for use in managing TCP/IP networks and network devices that support the Simple Network Management Protocol (SNMP). NNM is an HP OpenView SNMP-based application running under the HP OpenView Windows (OVW) graphical user interface. General capabilities of the HP OpenView Network Node Manager product are covered in the next section of this chapter.

This user's guide provides you with some concepts of how NNM works, plus steps on how to get started in NNM, how to manage your network and system configuration, how to monitor and diagnose your network, and how to use the NNM operations.

The online help provided in NNM is thorough. Therefore, this guide focuses on examples that tie the network management tasks together. In turn, you can use these examples as a reference for configuring NNM, so you can proactively manage your network and quickly diagnose problems that occur.

This guide does not cover the general concepts and operation of HP OpenView Windows. For this information, see the *HP OpenView Windows User's Guide*. Also, this guide does not cover installation, administration, configuration, troubleshooting, or concepts on background processes of the HP OpenView Network Node Manager product. For information about installation refer to the *Installation Guide*. For information about the other topics, see the *HP OpenView Network Node Manager Administrator's Reference*.

General Capabilities of Network Node Manager

The NNM product is a configuration, performance, and fault management application for multivendor TCP/IP (Transmission Control Protocol/Internet Protocol) networks. NNM enables you to

- Automatically discover the devices on the TCP/IP network and monitor the status of those devices.
- Automatically draw the Internet Protocol (IP) topology maps based on discovered information. A map is a graphical and hierarchical representation of your network and its systems. Discovered devices are placed in appropriate segments, networks, or internets based on the topology of the IP network.
- Manage any vendor devices that support the Simple Network Management Protocol (SNMP). NNM can manage standard MIB objects, as well as, enterprise-specific MIB objects.
- Include new enterprise-specific MIBs into the NNM Management Information Base (MIB). Once you have loaded the new MIB module on the management station, you can manage any of the MIB objects defined in that MIB module.
- Get and set values of MIB objects using a point-and-click "Browse MIB" operation.
- Build new MIB applications, without programming, for Internet-standard and enterprise-specific MIBs. Once you have built your MIB application, you can monitor the objects through the HP OpenView Windows menu bar.
- Collect historical MIB information about the MIB objects, store MIB data for trend analysis, and graph collected data.
- Define event thresholds for MIB objects, for example, when the disk usage on a particular device exceeds a limit.
- Define actions to be taken upon receipt of an SNMP (Simple Network Management Protocol) trap.
- Integrate existing applications with the HP OpenView Windows menu bar to yield an integrated management solution.
- Diagnose network faults and performance problems from one location, and diagnose problems by looking at trends over time. This includes customizing and automating the monitoring of your network and the management station's response to events.

Definitions and Concepts

To understand how HP OpenView Network Node Manager (NNM) manages a network, you need to become familiar with some concepts and terms. This section covers such concepts as the manager system versus the agent system, the Management Information Base (MIB), the Internet Protocol (IP) discovery and layout process, and event generation.

Managers and Agents

A manageable network consists of one or more manager systems, or network management stations, and a collection of agent systems, or network elements.

- A **manager system** executes network management operations which monitor and control agent systems. The implementation of these network management operations is called the **manager**.
- An **agent system** is a device, such as a host, gateway (router), terminal server, hub, or bridge, that has an **SNMP agent** responsible for performing the network management operations requested by the manager.

A manager and agent may exist on the same system.

The Simple Network Management Protocol (SNMP) communicates management information between a manager and an agent. SNMP allows

- A manager to retrieve (**get**) management information from an agent. The manager sends requests for information to the agent, and the agent sends back replies containing the information requested.
- A manager to alter (**set**) management information on an agent.
- An agent to send information to the manager without an explicit request from the manager. Such an operation is called a **trap**. Traps proactively alert the manager of changes that occur on the agent system, such as a reboot. The agent knows which manager system to send traps to through a configurable trap destination.

Requests for information on an agent are accompanied by a **community name**, which enables the manager to access the agent information. Figure 1-1 shows a simplified diagram of the manager-agent interactions.

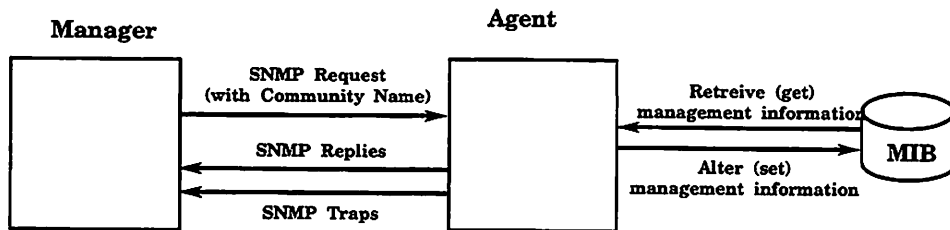


Figure 1-1. Manager-Agent communication through SNMP

MIBs

Conceptually, the information on the agent is known as the **Management Information Base (MIB)**. The **MIB** is not a physically distinct database, but rather, logically encompasses configuration and status values normally available on the agent system. A specific type or class of management information is called a **MIB object** (for example, a system description or an interface status). The existence of a particular value for a MIB object in the agent database is called an **instance**. Some MIB objects have only a single instance for a given agent system (for example, system description). Other MIB objects have multiple instances for a given agent system (for example, interface status for each interface on the system).

The MIB objects are defined using the Internet-standard structure of management information (**SMI**) and compose a virtual data store on the agent system. This structure is defined by *RFC 1155: Structure and Identification of Management Information for TCP/IP-based Internets* and amended by *RFC 1212: Concise MIB Definitions*. Together RFCs 1155 and 1212 define the structure of management information for SNMP based management. SNMP agents contain the “intelligence” required to access MIB values.

MIBs are organized into MIB modules. A **MIB module** is a file defining all the MIB objects under a subtree. The foundation module is the standards-based MIB-II module defined by *RFC 1213: Management Information Base of Network Management of TCP/IP internets: MIB-II*. In addition to the Internet-standard MIB-II objects defined in RFC 1213, many hardware vendors, such as Hewlett-Packard, Cisco Systems, Wellfleet, and Novell, have developed MIB extensions for their own products. The MIBs defined by these various hardware vendors are referred to as **enterprise-specific MIBs** in this manual.

Many additional standard MIBs are under development (for example, LAN Ethernet-like links, remote LAN monitoring, bridges, hubs, and routers). These emerging standard MIBs are based upon a collaboration between vendors, academia, and standards organizations. The intent is to consolidate common management information from enterprise MIBs into standard definitions, yielding consistent access to the management information across multivendor equipment.

How MIBs are Organized

Conceptually, the **MIB objects** are organized in a hierarchical tree structure. Each branch in the tree has a unique name and numeric identifier (see Figure 1-1). Intermediate branches of the tree serve as a way to group related MIB objects together. The "leaves" of the tree represent the actual MIB object. A subtree is used to refer to the entire group of branches and leaves under a particular intermediate branch. Figure 1-2 illustrates the tree structure.

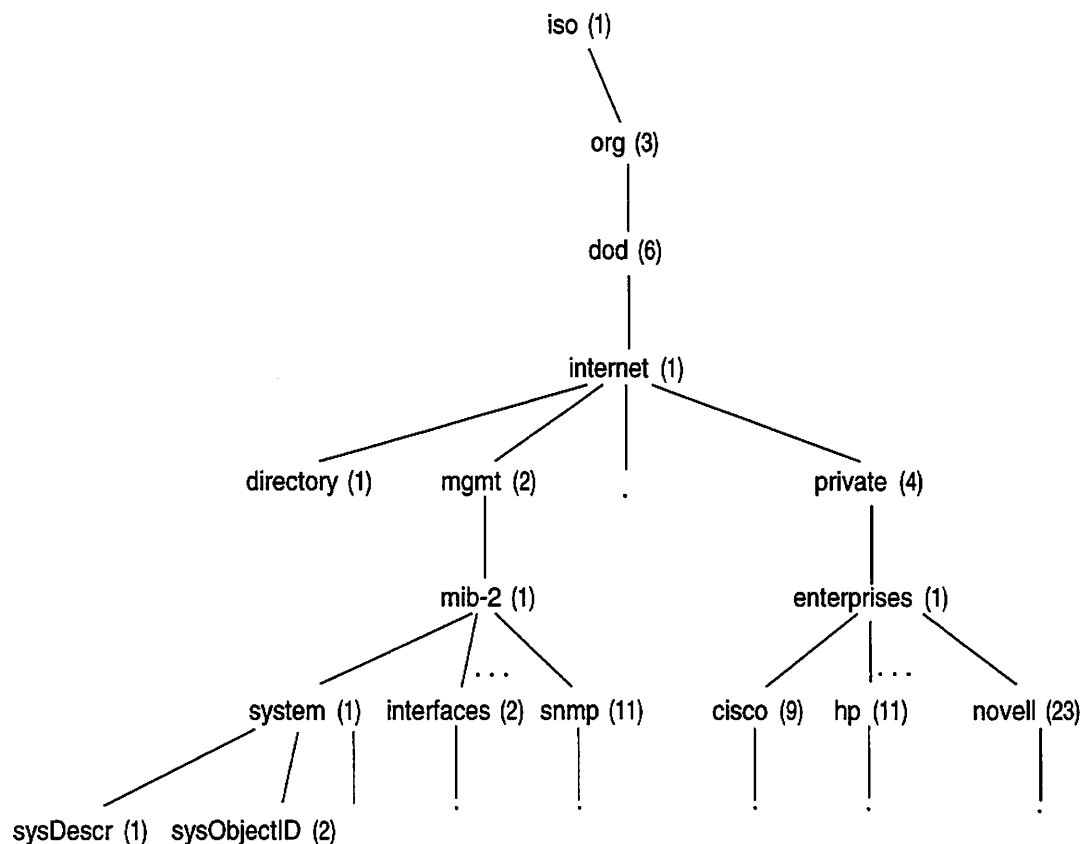


Figure 1-2. MIB Organization

A MIB object is uniquely identified (named) by its place in the tree. A full object identifier consists of the identifier of each branch along the path through the tree hierarchy, from the top of the tree (**iso**) down to the leaf (for example, **sysObjectID**). The object identifier is expressed in "dotted notation," by separating each branch identifier along the path with a period. For example, the **mib-2** subtree is **iso.org.dod.internet.mgmt.mib-2** and its numeric identifier is **1.3.6.1.2.1**. As another example, the full MIB object identifier for **sysObjectID** is **iso.org.dod.internet.mgmt.mib-2.system.sysObjectID** and its numeric identifier is **1.3.6.1.2.1.1.2**. The instance identifier on a MIB object with only one instance is zero. The instance identifier on a MIB object with more than one instance is one or greater. These MIB object notations follow the standard notation defined in Abstract Syntax Notation One (ASN.1); the ASN.1 standard notation definition can be considered the "template" for MIBs.

To avoid conflicts of object IDs, each branch of the tree must be registered (that is, defined), through a designated organization. For example, the Internet Activities Board (IAB) has authority over the **internet** subtree, which includes the MIB-II Internet standard registered under the **mib-2** subtree. In turn, the IAB gives vendors authority over enterprise-specific subtrees. Enterprise-specific MIB objects are registered under the designated authority for that enterprise. To clarify this point, HP registers its enterprise-specific MIBs under **1.3.6.1.4.1.11**, having authority over the **enterprises.hp** subtree; and, Cisco registers its enterprise-specific MIBs under **1.3.6.1.4.1.9**, having authority over the **enterprises.cisco** subtree.

Unique Properties of the MIB Object **sysObjectID**

The **sysObjectID** is an important MIB object to HP OpenView network management operations. This section describes

- what the **sysObjectID** is
- how HP OpenView network management operations use the **sysObjectID**

The **sysObjectID** is registered in the Internet-standard MIB-II module as **iso.org.dod.internet.mgmt.mib-2.system.sysObjectID (1.3.6.1.2.1.1.2)**. The **sysObjectID** is used for administrative purposes to uniquely identify the type of agent software that is running on a given vendor's hardware. This object is different from most other MIB objects. When you query this object, you get back an object identifier that describes the product. For example, when you query the **iso.org.dod.internet.mgmt.mib-2.system.sysObjectID** using the MIB Browser on an HP OpenView SNMP Agent running on an HP 9000 Series 300 system, SNMP returns the object identifier **iso.org.dod.internet.private.enterprises.hp.nm.system.hpux.hp9000s300**

This result tells you how the HP 9000 Series 300 agent is registered in the MIB. Its numeric identifier is **1.3.6.1.4.1.11.2.3.2.2**. Note that there is no value associated with the object ID returned in **sysObjectID**. It is a unique identifier.

The **sysObjectID** includes both hardware and software information and will vary based on the type of hardware and agent software. Some vendors have a different **sysObjectID** for every version of their agents. For example, Hewlett-Packard sells several SNMP agents, each uniquely identified. To distinguish the HP 9000 Series 800 agent from the HP 9000 Series 300 agent, HP registered the HP 9000 Series 800

agent as **iso.org.dod.internet.private.enterprises.hp.nm.system.hpux.hp9000s800**. For more information about **SysObjectID**, see the *HP OpenView Network Node Manager Administrator's Reference*.

IP Map

IP Map is an application that is installed and registered with the HP OpenView Windows (OVW) platform. When you start OVW, IP Map is started automatically. IP Map discovers all IP-addressable nodes on your network, creates a map object for each discovered node, and creates and displays symbols on your network map that represent those map objects.

IP Map uses two background processes, the network monitor process (**netmon**) and the IP Topology Manager (**ovtopmd**) to discover and update the map. The network monitor discovers resources on your network, and the IP Topology Manager continually accesses stored semantic information about IP networks, segments, nodes, and interfaces in the map database. As information in the map database changes, and as events take place with systems or connections on the network, IP Map updates your network map.

Submaps

A submap is a collection of related or connected symbols that are displayed in a single window of the HP OpenView Windows platform. A collection of submaps comprise a map. When you open a map, you actually view one or more submaps of the map. Multiple submaps enable you to see different views of your network map. For example, you can have submaps that consist only of your most critical gateways or routers.

OVW Root Submap and Home Submap

HP OpenView Windows creates a Root submap (see figure 1-3) that network and systems management applications may use to build hierarchies of submaps. The Root submap serves as an anchor on which applications can place a "root" symbol. Symbols on the Root submap can open submaps that are the top level view of a specific application, such as an IP Internet or an OSI network.

Each map has a submap designated as the home submap, which is the submap that OVW displays when the map is opened. By default, when a map is created, the Root submap is designated as the home submap. You can assign any submap in the map as the home submap.

When a map is created, the IP Map application is enabled by default. As soon as the map is created, IP Map begins discovering objects across the network. During the initial discovery process, IP Map places a single Internet symbol on the Root submap. The following figure shows you the Root submap:

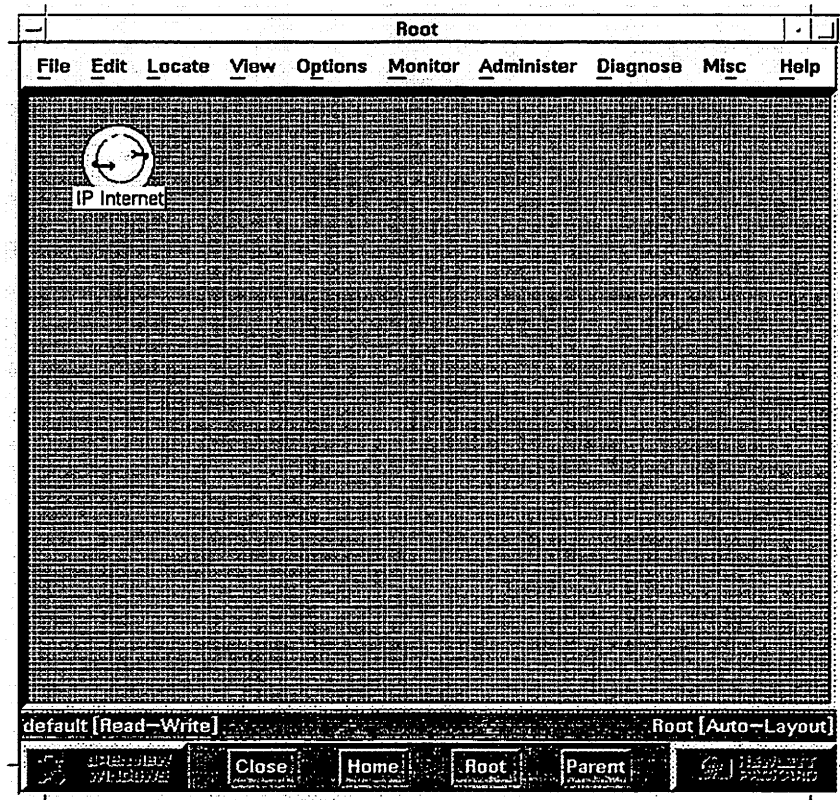


Figure 1-3. Root Submap

The Internet symbol graphically represents all IP-addressable objects on your network. You can enter the realm of IP network management by double-clicking on the Internet symbol in the Root submap.

IP Map Submaps

When a map is created, IP Map creates a hierarchy of submaps that displays your network in increasing detail. From the Internet symbol on the Root submap, you can open and display the Internet submap. You can reorganize and expand the hierarchy of submaps.

IP Map initially creates the following submap hierarchy:

- Internet submap
- Network submaps
- Segment submaps
- Node submaps

IP Map will manage only objects that exist within this hierarchy of submaps. The objects of symbols added to the Root submap, or added outside the realm of the IP submap hierarchy, will not be managed by IP Map.

Internet Submap

The Internet submap (see figure 1-4) displays the logical partitioning of IP networks and gateways into connected network and gateway symbols.

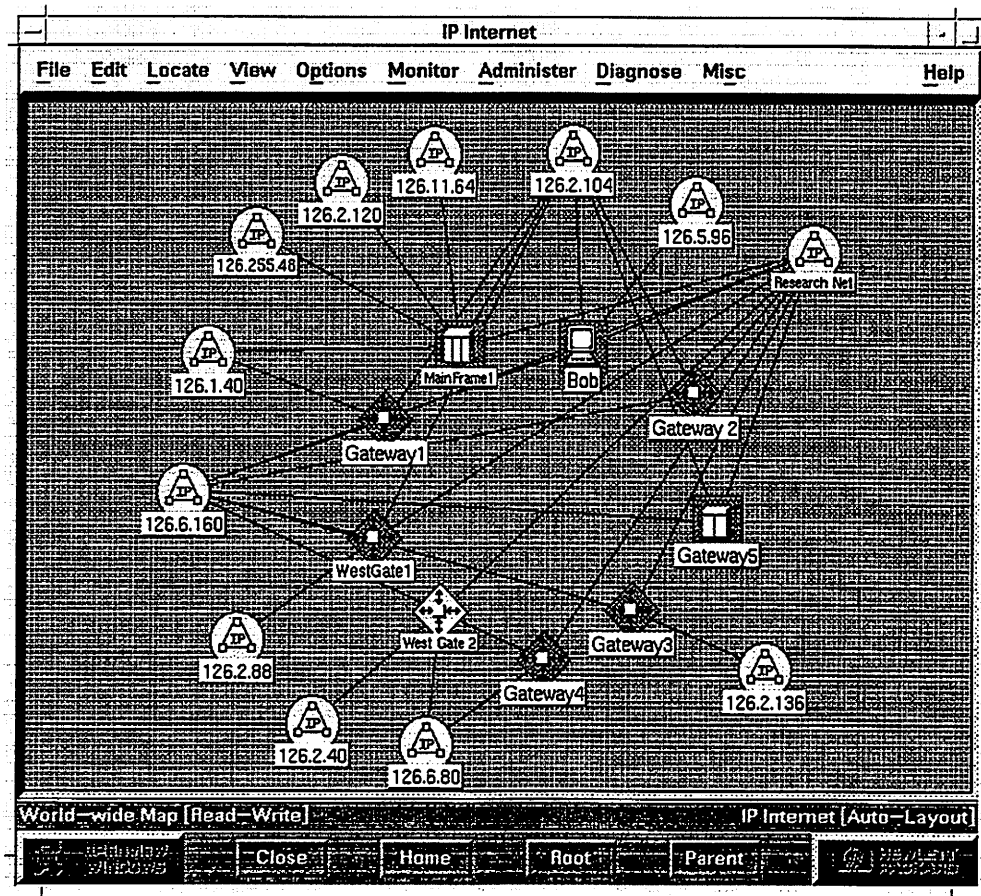


Figure 1-4. Internet Submap

Some of the symbols that IP Map displays in the Internet submap may be computers. IP Map displays these computers on the Internet submap because they function as a gateway or router on the network. If you are only interested in the IP topology and characteristics of your network (and therefore, running only IP Map), you may want to set the Internet submap as the home submap so that is displayed each time the map is opened.

To display a more detailed view of the network map, you can open a Network submap by double-clicking on one of the Network symbols. If you double-click on a gateway (router), IP Map opens a Node submap

that displays the components of the node, such as the IP Interfaces.

Network Submaps

The Network submap (see figure 1-5) represents the physical topology of a network at the level of network segments (subnetworks) and the gateways (routers), repeaters, multi-port repeaters (hubs), and bridges that are attached to those segments. In a Network submap, IP Map discovers and displays IP-addressable segments, gateways (routers), repeaters, multi-ports (hubs), bridges, and the connections between them on the Network submap.

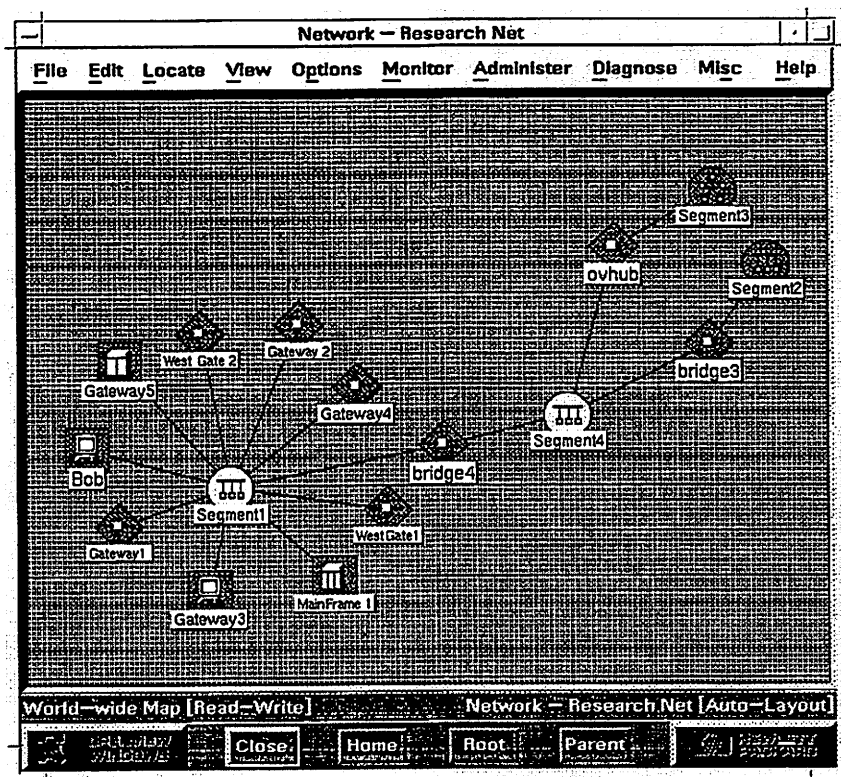


Figure 1-5. Internet Submap

Each segment symbol represents a physical network topology. IP Map may discover and display any of the following segment submaps. Each segment topology is discussed in more detail in the following sections.

- Bus -- Represents nodes attached to a single linear cable that transmits data (for example, Ethernet or IEEE 802.3).
- Token Ring -- Represents nodes attached to an SNMP, IP-addressable token ring central wiring MAU via twisted pair wiring, which conforms to IEEE 802.5 standard.
- Star -- Represents all nodes attached to an SNMP central multi-port repeater (a hub).
- FDDI Ring -- Represents nodes attached to an SNMP, IP-addressable Fiber Optic Data Distribution Interface (FDDI).

One way IP Map can discover a segment is by querying a "smart" gateway (router). Such a device can identify a bus cable, star cable, a Token Ring, and an FDDI ring. On the Network submap, IP Map displays a segment symbol attached to the gateway (router), hub, or bridge for each discovered segment, and displays a Segment submap for each discovered segment. IP Map discovers the nodes on each segment, and displays these nodes in the Segment submap based on the given topological information.

If the gateway (router) does not identify each specific segment and the topology of the segment, IP Map represents the segments as a bus segment and displays a single bus segment symbol. When you open the Segment submap, a bus topology is displayed.

To display a more detailed view of your network map, you can open a Segment submap by double-clicking on one of the segment symbols in the Network submap.

As with the Internet submap, double-clicking on a symbol of the Connector class (for example, a gateway or bridge) opens a Node submap, which displays interface symbols of installed interfaces in the node (the gateway (router), bridge, or computer).

Segment Submaps

A Segment submap represents the physical topology of a segment of your network at the level of nodes and connectors. A Segment submap may contain symbols in the computer class, connector class, or network device class.

In IP networks, a segment is a group of data communication objects, with varying degrees of intelligence, that are interconnected via a common transmission medium. Nodes belonging to the same segment typically use a common physical medium to communicate with each other (for example, Ethernet, Token Ring, telephone lines, and satellite links).

Bus Segment Submaps. A Segment submap with a bus layout displays symbols that represent nodes that are connected via a bus. The bus represents the part of a network that contains a single linear cable that transmits data (for example, Ethernet or IEEE 802.3). Every node on a bus network reads each message transmitted over the network.

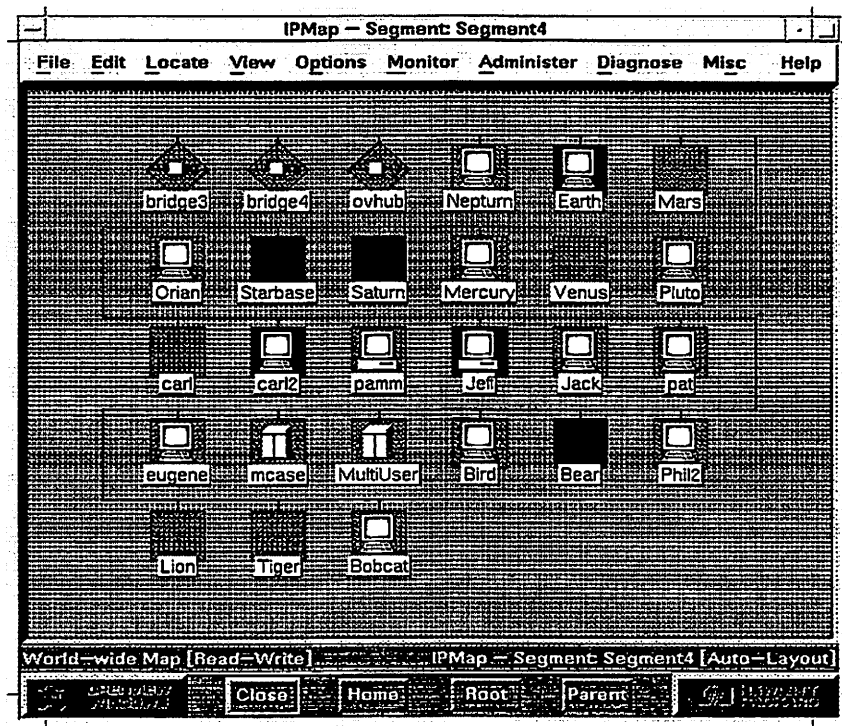


Figure 1-6. Bus Segment Submap

One default bus segment automatically appears. Other bus segments appear only if they are attached to IP-addressable bridges or multi-port repeaters (hubs), or if you manually add them. When IP Map discovers new nodes on a bus Segment submap, it places them on the end of the bus segment.

Star Segment Submaps. A Segment submap with a star layout, represents all nodes attached to a central multi-port repeater (hub). IP Map displays a Star Segment if your network has a multi-port repeater (hub) that is IP-addressable.

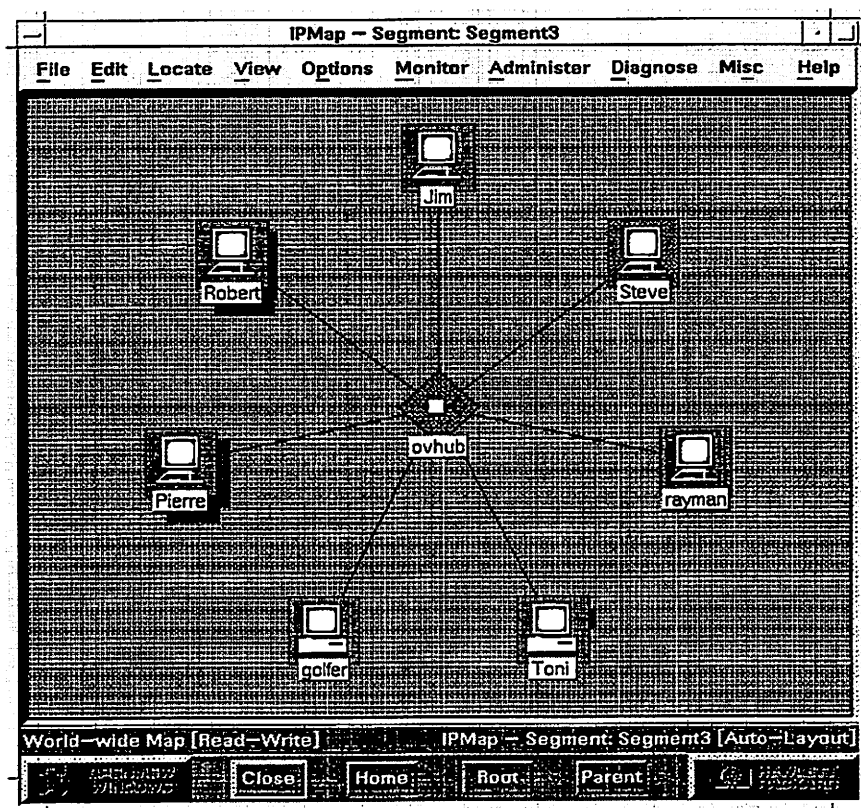


Figure 1-7. Star Segment Submap

Token Ring Segment Submaps. A Segment submap with a token ring layout represents nodes attached to an SNMP, IP-addressable token ring central wiring MAU via twisted pair wiring, which conforms to IEEE 802.5 standard. A token ring segment may have multiple MAUs.

FDDI Ring Segment Submaps. Represents nodes attached to an SNMP, IP-addressable Fiber Optic Data Distribution Interface (FDDI). A symbol of an FDDI segment appears only on a Network submap.

Node Submaps

The Node submap displays symbols that represent the components of a node, such as interfaces. This submap has a row-column layout. You can display a Node submap by double-clicking on a computer or any device in any of the higher level submaps. For example, a gateway (router) may be displayed in the Internet, Network, and Segment submap. You can display a Node submap of the gateway (router) from any of the gateway symbols.

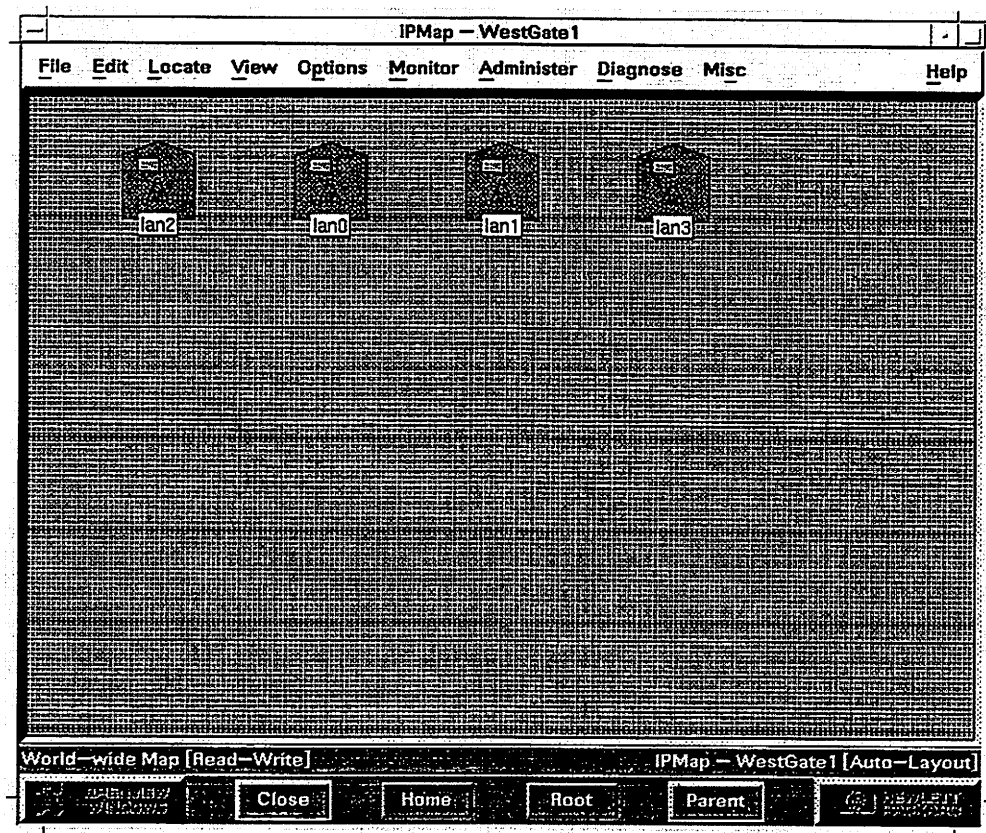


Figure 1-8. Node Submap

Layout Algorithms

Each submap created by IP Map has a layout algorithm that determines how symbols are placed on the submap. Each submap uses one of the following layout algorithms:

- Point-to-point
- Star
- Bus
- Ring
- Row/Column

IP Map arranges symbols on submaps according to the layout algorithm that makes sense for the topology discovered. You can disable the layout algorithm and use the mouse to place symbols where you want. You can enable or disable the layout algorithm for all submaps in the open map or for specific submaps by using the **View: Automatic Laygout** menu item.

Map Objects and Symbols

This section discusses map objects, symbols, and how they work together to give you real-time information about your network map. In its simplest form, a map object is represented by a symbol on a submap. However, a map object may also be graphically represented by more than one symbol in various submaps. For example, IP Map may discover a node that serves as a gateway (router). This node will appear on both a Network submap and a Segment submap. By default, IP Map displays this node as a computer (a workstation, mini or main frame if it can identify it more specifically). You may want to display the node as a gateway (router) on the Network submap and as a computer in the Segment submap. You can do that by changing the symbol type.

Symbol Varieties

OVW uses two varieties of symbols for display on the map. A icon symbol, usually referred to as simply a symbol, consists of a geometric shape. A symbol graphic, or icon, usually appears inside the shape. A connection symbol connects two icon symbols or an icon symbol and a backbone. On a submap, connection symbols appear as the lines. However, connection symbols are not merely lines. They represent objects and can display status. IP Map uses connection symbols to show the current state of connections between resources on your network.

Symbol Types (Class and Subclass)

A symbol consists of a “class” and a “subclass”. The symbol class is simply the outside shape of the symbol. Each symbol class is further divided into subclasses. For example, the computer symbol class is comprised of the PC, Workstation, Mini, and Main Frame subclasses. Together, the symbol class and subclass comprise the symbol type. You can view all the registered symbol types by selecting the **Help: Display Legend** menu item.

The Connection Symbol

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

- A connection symbol represents an object, just like an icon symbol.
- Connection symbols may reside on the application plane or the user plane.
- You can display a symbol pop-up menu for the connection, and open the Symbol Description dialog box to view symbol characteristics.
- You can assign a label to the connection symbol.
- The connection symbol is either explodable or executable.

IP Map often displays an interface symbol in the node submap and a connection symbol in higher level submaps that represent the same object. For example, the Node submap of a gateway (router) may display two interface symbols. In the Segment, Network, and Internet (or Partitioned Internet) submaps, the connection symbols attached to the symbol of the gateway (router) represent the same object as the interface symbol in the gateway's node submap. If the interface goes down, the status is reflected in both the interface symbol (in the Node submap) and the connection symbols (in the higher level submaps).

Symbol Status

Both icon symbols and connection symbols convey status. NNM uses the following status conditions:

Default Status Colors		
Status Condition	Symbol Color	Connection Color
Unknown -- status information unavailable	Blue	Black
Normal -- fully functional	Green	Black
Warning -- potential fault or problem	Cyan	Black
Marginal -- at least one attribute is impaired	Yellow	Yellow
Major -- major fault or problem	Orange	Black
Critical -- nonfunctional	Red	Red
Unmanaged -- resource unused, status unknown	Tan	Black

How IP Map Conveys Status

IP Map displays status of IP-addressable interface objects directly. By default, IP Map also sets the status of node objects directly. The IP Map Configuration section shows you how you can configure how IP Map sets status on node objects. The status of segment, network, and internet symbols is propagated by the compound status scheme set for the map as described in the next section.

Compound Status

When a map is created, HP OpenView Windows uses a scheme to determine how status in a child submap propagates to symbols of the parent object. This enables you to see a summary of the status of symbols in a child submap. HP OpenView Windows offers you compound status rules to choose from. An application can also choose to do its own compound status if it wishes to propagate status according to special rules.

The default compound status scheme determines compound status in the following manner:

HP OpenView Windows Default Compound Status	
Condition of Symbols in the Child Submap	Status of Symbols Representing Parent Object
All symbols are normal.	Normal
Only one symbol is abnormal; the other symbols are normal.	Warning
At least two of the symbols are abnormal and at least two of the symbols are normal.	Marginal
At least one symbol is normal; the other symbols are abnormal.	Major
At least one symbol is abnormal and no symbols are normal.	Critical
No symbols with a status of either normal, warning, marginal, major, or critical.	Unknown

The other compound status schemes allow you to propagate the most critical status and to propagate status according to percentages of malfunctioning object in the child submap.

Events

An event is an unsolicited notification from a manager or agent where possibly one of the following conditions occurred:

- A threshold limit was exceeded.
- The network topology changed.
- An informational message or an error occurred.
- An object's IP status changed.
- A node's configuration changed.
- An application alert occurred.

How Events are Generated

Events are generated; they are not messages that are requested. The sources that generate events are agents on managed systems and monitoring applications residing on the management station; for example, IP discovery (SNMP) and layout (`netmon`, `ipmap`, and `ovtopmd`), data collector (`snmpCollect`), and the SNMP agent. Events can also be generated by a user-written application or shell script.

All events go to the `trapd` process, which then writes notification events in the `/usr/ov/log/trapd.log` file and forwards a subset of these events to the various **Event Browser** windows. If configured to do so, the events could also be forwarded to the `ovactiond` background process to perform a specified action. You can access these **Event Browser** windows via the **Event Categories** window that appears when you start HP OpenView Windows. Events will not be received or displayed if the `trapd` process is not executing. For more information about these processes, refer to the *HP OpenView Network Node Manager Administrator's Reference*.

Traps

A trap is the SNMP term for an event. A trap is a message sent from an SNMP agent to a manager without an explicit request from the manager. Agents send traps to the manager to indicate that a particular condition exists on the agent system, such as an error has occurred or an event has happened.

A core set of SNMP traps are defined in *RFC 1157: A Simple Network Management Protocol (SNMP)*. Each SNMP trap contains a *generic* trap number and a *specific* trap number. The *generic* trap numbers range from 0 to 6.

- ColdStart(0)
- WarmStart(1)
- LinkDown(2)
- LinkUp(3)
- AuthenticationFailure(4)
- EgpNeighborLoss(5)
- EnterpriseSpecific(6)

The *generic* traps 0 through 5 are defined by SNMP and assume a *specific* trap of 0. Additionally, many equipment vendors have defined traps specific to their own equipment. These traps are defined using the *generic* trap **EnterpriseSpecific (6)**, and are referred to as **enterprise-specific traps**. The enterprise-specific traps are uniquely identified by the

- Vendor's enterprise ID (that is, the **sysObjectID** of the vendor's equipment). For example, the enterprise ID for an HP 9000 Series 700 agent is **1.3.6.1.4.1.11.2.3.2.5**. **OpenView** generates traps with enterprise ID **1.3.6.1.4.1.11.2.17.1**.
- *Generic* trap, for example, **EnterpriseSpecific (6)**.
- *Specific* trap ID assigned by the vendor. In the **OpenView** example, one of the specific trap ID's is **58916865**, which is the specific trap ID for **OV_Node_Down**.

Where to Go for Help

HP OpenView Network Node Manager (NNM) has four sources of help:

- The *HP OpenView Network Node Manager Administrator's Reference*
- The *Installation Guide*:
 - HP OpenView Network Node Manager*
 - HP OpenView SNMP Management Platform/Developer's Kit*
 - HP OpenView Distributed Management Platform/Developer's Kit*
- The online **Help** menu
- The online dialog box **Help**

The type of information covered in the *HP OpenView Network Node Manager Administrator's Reference* includes:

- documentation guide and references
- product overview of the background processes in NNM
- configuration information for NNM
- access and security information for NNM
- troubleshooting procedures for diagnosing problems with NNM
- HP OpenView Network Node Manager reference pages (man pages)

The type of information covered in the *Installation Guide* includes:

- required configuration for NNM
- initial installation information for NNM
- updating NNM from a previous NNM release
- access and security information for NNM

The type of information covered in the online menu bar **Help** includes:

- **Help: Index -> Functions** which alphabetically lists help entries for each operation you can perform from the HP OpenView Windows graphical map interface. Each entry describes the purpose of the operation, how to initiate the operation, and an overview of what the operation does.
- **Help: Index -> Tasks** which alphabetically lists help entries for common tasks that can be performed using NNM. Each entry describes the purpose of the task and how to perform the task. Often times, task help provides a higher level view of how to combine various functional operations together to get a particular job done.
- **Help: On Version** which provides product version information.

The type of information provided when you click on the dialog box **Help** button includes

- specific details on how to use the operation or application in the selected dialog box
- specific details on the fields in the dialog box (such as what information is required, where to get this information)
- specific details on the buttons in the dialog box (such as what they do, when to use them)

Since NNM is based on HP OpenView Windows, and uses X Window and various window managers, remember to consult the appropriate documentation for these topics. For information about HP OpenView Windows, see the *HP OpenView Windows User's Guide*.

Getting Started

This chapter discusses topics useful for your first few sessions with HP OpenView Network Node Manager (NNM). The topics include

- starting NNM
- exiting NNM
- understanding IP Map configuration
- customizing IP Map for a new map
- customizing IP Map for an existing map
- disabling IP-only status

Starting HP OpenView Network Node Manager

HP OpenView Network Node Manager is a set of applications that are integrated with HP OpenView Windows (OVW). To start NNM, you start HP OpenView Windows (OVW); OVW automatically starts NNM. OVW automatically starts the applications that are installed and registered.

Starting NNM

This task explains how to start the OVW platform and the applications supplied with NNM.

Prerequisites for this Task

- The network management processes that work with OVW and NNM must be running. The network management processes consist of the following HP OpenView background processes: **ovwdb**, **trapd**, **ovtopmd**, **ovactiond**, **snmpCollect**, and **netmon**. You can check to see if these processes are running with **/usr/OV/bin/ovstatus** command.

If the network management processes are not running, you can start them by executing the **/usr/OV/bin/ovstart** command. These processes run in background mode.

- The workstation must be running X Window to start OVW. You can start X Window by typing **x11start**.
- The **/usr/OV/bin** directory must be in your path.

Procedure

To start OVW

1. Type **ovw**.
2. Press [Return].

The first time you run OVW, a default map is created and opened. When OVW is running, one map is always open. After you run OVW, you can create additional maps and specify any of them as the map that OVW opens during startup in the OVW Graphical User Interface. When a map is opened, OVW displays a submap window of the map. You never need to close a map (in fact, no **Close Map** operation is displayed) because OVW closes a map automatically when you open another map or exit OVW.

The ovw Command

When you run HP OpenView Windows on your workstation (also referred to as your network management station), you start an OVW session. The OVW session remains running until you exit HP OpenView Windows or shutdown your workstation. You can start a new OVW session by running OVW again. You can vary how OVW starts up a session. This section discusses the **ovw** command and gives you examples of how to use it.

Options

The **ovw** command contains the following options:

```
ovw [-ro | -rw] [-map map_name]
```

Option	Meaning
-ro	Each map opened during this OVW session is opened with read-only access.
-rw	Each map opened during this OVW session is opened with read-write access if possible. This is the default. It is necessary only if the X-Resources specify read-only as a default behavior.
-map <i>map_name</i>	Open map <i>map_name</i> . Create the map, <i>map_name</i> , if it does not exist.

Examples

The following table provides examples that show you various ways to start HP OpenView Windows.

Command Entered	Effects
<code>ovw</code>	Runs OVW and all NNM applications, and opens the map assigned as the user default map.
<code>ovw -map AdminMap1</code>	Runs OVW and all NNM applications, and opens the map, AdminMap1 . AdminMap1 does not need to be the user default map.
<code>ovw -ro</code>	Runs OVW and all NNM applications, and opens the map assigned as the user default map. The user default map and all maps subsequently opened during this session are opened with read-only access.
<code>ovw -ro -map Europe2</code>	Runs OVW and all NNM applications, and opens the map called Europe2 . All maps during this session of OVW are opened with read-only access.
<code>ovw -rw</code>	Runs OVW and all NNM applications, and opens the map assigned as the user default map. Maps can be opened with read-write access if permissions allow. The -rw option is the default and is necessary only if X-Resources specify read-only as the default behavior.

The Submap Window

A submap window appears each time you run OVW. OVW always displays at least one submap window. You can open multiple submap windows to view a map of your network from different perspectives. A submap window consists of the following parts:

- menu bar
- viewing area
- status line
- button box

The Menu Bar

The menu bar contains OVW menu items that allow you to access and control the operation of the management station. The menu items are located along the top of the submap window. From the menu bar you can pull down a menu. A pull-down menu contains menu items of similar functionality.

Items in the menu bar are organized according to the type of functionality provided. Because applications can register new menu items on the menu bar, the specific items on your menu bar may vary.

The Viewing Area

The area where OVW displays the submap. The submap displays symbols and graphics that convey information about systems, connections, and other parts of your network.

The Status Line

The status line is under the viewing area. The status line displays the following information:

- The name of the open map and whether it is open with read-only access or read-write access.
- The name of the submap.
- Whether autolayout is on or off.
- Whether the open map is in the process of being updated. In this case, **[Synchronizing]** will appear after the map name.

The Button Box

The button box is below the status bar. This box contains a series of buttons. The following table describes each button.

Button	Action
Close	Close this submap.
Home	Open the home submap.
Root	Open the root submap.
Parent	Open the parent of this submap.

Map Synchronization

When a map that uses IP Map is opened, IP Map starts its synchronization phase. While IP Map is synchronizing, OVW displays the **[synchronizing]** message on the status line of all displayed submaps of the open map. During this phase, IP Map requests information about changes to the IP topology database since the map was last open. This information is constantly updated by the HP OpenView IP Topology Manager (**ovtopmd**). If new objects are discovered, IP Map brings the map up-to-date by drawing new symbols.

While IP Map is synchronizing, the following functionality is *not* available:

- OVW restricts users from deleting symbols, objects, or submaps.
- You can add location symbols and objects, but IP Map will not process additional symbols and objects until the synchronization phase is finished.
- IP Map will not appear in the **Configurable Applications** list on dialog boxes (**Object Description**) until it has completed synchronization.
- You cannot perform the **Manage Object** and **Unmanage Object** operations.

When the synchronization phase is over, IP Map returns to fully configured functionality.

Exiting HP Network Node Manager

To exit NNM and all other integrated applications, you must exit OVW. You can exit OVW in *one* of the following ways:

- Select **File: Exit** from the menu bar of any submap window.
- Click on the **Close** button on all open submap windows until a blank submap window is displayed. When the blank submap window is displayed, click on the **Close** button.

The open map is saved, and all the submap windows and dialog boxes of the map are closed. OVW, all NNM applications, and all other integrated applications exit.

Understanding IP Map Configuration

Network applications and system applications are listed in the **Configurable Applications** list in the **File: New Map** dialog box and the **File: Describe/Modify Map** dialog box. Selecting IP Map and clicking on the **Configure For This Map** button displays the **Configuration** dialog box for IP Map.

IP Map contains four configuration settings that determine how IP Map functions with the open map. You can configure IP Map differently for each map. When you create a new map, the following configuration settings are the defaults:

- IP Map is enabled. When enabled, IP Map displays discovered nodes on the network.
- IP Map displays the status of IP objects.
- IP Map displays the status of interface objects on connection symbols. When enabled, this displays the status of interface objects on connections, in a higher-level submap, in addition to the interface objects.
- IP Map displays the IP status for node objects. This setting means that only IP interfaces in a Node submap contribute to the status of the node object.

When a map is created, the above settings are set to **True**. All of the functionality of IP Map is enabled.



Customizing IP Map for a New Map

You can enable or disable the configuration settings for IP Map. When a new map is created, all configuration settings are enabled; IP Map defaults to full functionality each time a new map is created. Therefore, if you want all settings to be enabled (often a good choice), you can skip this procedure.

Disabling IP Map Functionality

You may want to disable a part or all of the functionality of IP Map. This section explains why and how you disable IP Map functionality when creating a new map.

Purpose for This Task

- 
- Customize a network map so that part or all of IP Map functionality is disabled. This may be desirable if you have installed an application that conveys status of objects in some other way.
 - You may want to create a network map in which another application creates all the submaps, or you may want to create all submaps manually. Disabling IP Map means that it will not create any submaps for that map. Essentially, IP Map will remain dormant.

Prerequisites for This Task

You must be creating a new map to disable IP Map functionality entirely.

Procedure

To change the configuration of IP Map, follow these steps:

- 
1. Select **File: New Map...** The **New Map** dialog box appears.
 2. From the **New Map** dialog box, select the **IP Map** application in the **Configurable Applications** list box.
 3. Click on the **Configure For This Map...** button. The **IP Map Configuration** dialog box appears. From this box, you can disable part or all of IP Map functionality.
 4. When you are finished resetting the configuration of IP Map for this map, click on **Verify** in the **Configuration** dialog box.
 5. Click on **OK**. You are returned to the **New Map** dialog box.

6. Proceed filling in fields in the **New Map** dialog box. You must enter a name for the map. Other fields are optional.
7. Click on **OK**. The new map is created. The currently open map is saved and closed, and the new map is opened.

IP Map Configuration Settings and Their Meaning

Figure 2-1 shows the IP Map Configuration settings. Following the figure is a list explaining the different settings.

Configuration

IP Map

IPMap enabled for this map?
☒ True ☐ False

Should IP status be shown on this map?
☒ True ☐ False

Should status of interfaces be shown on connections?
☒ True ☐ False

Should status of nodes be IP only?
☒ True ☐ False

Messages:

OK Verify Cancel Help

Figure 2-1. IP Map Configuration

- IP Map is enabled when you create a new map. To disable the IP Map application for a map, select the **False** radio button when you create the map. After the map is created, this setting cannot be changed for the map. Disabling IP Map only affects the map you are creating. Each map can have its own setting. If IP Map is disabled, IP Map does not display discovered nodes on the network, and all functionality described in the following bullets is also disabled.
- IP Map displays the status of IP objects. To change this setting, select the **False** radio button. If you change this setting to **False**, IP Map still discovers SNMP objects on the network, but it does not convey IP status of these objects. This enables you to use other methods or applications to convey the status of IP objects. If you change this setting to **False**, the following two settings are also **False**.
- IP Map displays the status of interface objects on connection symbols. When enabled, this displays the status of interface objects on connections, in a higher level submap, in addition to the interface objects. You may choose to disable this feature if you have another network or systems management application that conveys status of connection symbols.
- IP Map displays the IP status for node objects. This setting means that only IP interfaces in a Node submap contribute to the status of the node object. This setting provides a more precise status propagation of IP objects. Change this setting by selecting the **False** radio button. Selecting **False** causes IP Map to allow OVW to propagate the status of all objects, not just IP objects, in a Node submap to the node object.

Setting this to **False** is useful if you have other applications that add symbols to Node submaps and set status for those symbols. In this case, the status of the node is determined by the status of IP Map and non-IP Map objects in the Node submap.

Customizing IP Map for an Existing Map

You can reconfigure some IP Map settings on an existing map. Reconfiguring IP Map for the open map does not affect the IP Map configuration for other maps. You cannot disable IP Map entirely after the map has been created. You can disable IP Map during map creation. However, you can change all other configuration settings of IP Map at any time. Changing IP Map settings causes your network to be polled again. This requires some time.

Purpose for This Task

This task explains how to customize a Network map so that part or all of IP Map functionality is disabled.

Prerequisites for This Task

The map must be open with read-write access.

Procedure

To change the configuration of IP Map, follow these steps:

1. Select **File: Describe/Modify Map...**. The **Map Description** dialog box appears.
2. From the **Map Description** dialog box, select the **IP Map** application in the **Configurable Applications** list box.
3. Click on the **Configure For This Map...** button. The **IP Map Configuration** dialog box appears. From this box you can toggle any of the following settings:
 - Display the status of IP objects.
 - Display the status of interface objects on connection symbols.
 - Display IP status for node objects.
4. When you are finished resetting the configuration of IP Map for this map, invoke your changes by clicking on **Verify**.
5. Click on **OK**. You are returned to the **Map Description** dialog box.
6. Click on **OK**. IP Map requires some time to read the Network map. More time is required in very large networks.

Disabling IP-Only Status

If you add another application that displays symbols on the Node submap, you may want to modify the IP-only status setting of IP Map so that symbols from other applications can contribute to the compound status of the parent object. Reconfiguring IP Map for the open map does not affect the IP Map configuration for other maps.

Purpose for This Task

After completing this task, IP Map allows other applications to place symbols on the Node submap that contribute to compound status.

Prerequisites for This Task

The map must be open with read-write access.

Procedure

To change the IP-only configuration of IP Map for the open map, follow these steps:

1. Select **File: Describe/Modify Map...**. The **Map Description** dialog box appears.
2. From the **Map Description** dialog box, select the **IP Map** application in the **Configurable Applications** list box.
3. Click on the **Configure For This Map...** button. The **IP Map Configuration** dialog box appears.
4. Click on **False** for **Should status of nodes be IP only?**

When this setting is **True**, only IP interfaces in a Node submap contribute to the status of the node object.

When this setting is **False**, IP Map allows OVW to propagate the status of all objects, not just IP objects, in a Node submap to the node object.

5. Click on **Verify**.
6. Click on **OK**. You are returned to the **Map Description** dialog box.
7. Click on **OK**. IP Map requires some time to read the Network map. More time is required in very large networks.

Managing Network and System Configuration

The HP OpenView Network Node Manager (NNM) product provides tools that allow you to customize your network map, document the state of your network, check network configurations, and control system and network configurations.

In this chapter you will learn how to

- Customize your network map to reflect the organization of your company and the physical connectivity of network elements. A network map that matches the physical links of your network enables you to more easily troubleshoot problems when they arise on your network. You can customize your network map in the following ways:
 - Expand the higher levels of your network map by creating container objects that open Partitioned Internet submaps. You can distribute symbols of your IP networks across multiple Partitioned Internet submaps, by cutting symbols of networks and gateways from the Internet submap and pasting them to a Partitioned Internet submap.
 - Expand the lower levels of your network map by creating additional network, segment, and node objects, each of which can open into a submap that displays its contents.
- Use the automatic layout capabilities on maps.
- Update a map that has been opened with read-only access.
- Document your network by taking snapshots of its current state. Snapshots are one way of tracking the evolution of your network. The snapshots enable you to keep track of what you have on the network, where it is located, and what its configuration is.
- View network and system configurations for auditing purposes. You can generate printouts of this information, as well.
- Control network and system configurations from NNM, via HP-UX SAM (the HP-UX System Administration Manager tool), `telnet` (ARPA Services), and `vt3k` (HP Network Services).

Expanding Higher Levels of Your Network Map

To expand your map, you need to understand a few concepts and procedures. This section discusses:

- What container objects are.
- What Partitioned Internet submaps are.
- How to expand the upper levels of your network map from a single Internet submap to include multiple Partitioned Internet submaps.
- What the containment realm is, and how to edit and maintain expanded maps within it.

Container Objects

As a result of the initial discovery process, IP Map displays one IP Internet symbol on the root submap, and creates one Internet submap. The Internet submap displays symbols representing IP networks and IP-addressable gateways (routers). You can expand this single Internet submap by manually adding symbols that represent container objects to the Internet. The container object is represented by a symbol from the Location class or the Internet symbol. You can add container objects to the Internet submap by using either the Internet symbol (in the Network class) or any of the symbols in the Location class.

Partitioned Internet Submaps

A symbol of a container object opens into a special submap called the Partitioned Internet submap. You can add symbols from the Location class and the internet symbol from the Network class to any Partitioned Internet submap as well as the Internet submap. Thus, you can create a hierarchy of Partitioned Internet submaps as many levels deep as you wish.

You can create multiple Partitioned Internet submaps to rearrange how your network map is displayed. However, the Internet submap is always the submap that is opened from the Internet symbol in the root submap. For the submap to function as a Partitioned Internet submap, you must place the symbol that opens the submap onto the Internet submap or a previously created Partitioned Internet submap. You cannot place a symbol on a root submap that opens into a Partitioned Internet submap. Top level Partitioned Internet submaps are created from the Internet submap. Thus, the Internet submap is always at the top of a hierarchy of Partitioned Internet submaps. Container objects and Partitioned Internet submaps enable you to partition the IP networks and gateways (routers) from the original Internet submap to multiple Partitioned Internet submaps.

Creating a Partitioned Internet Submap

To create a Partitioned Internet submap, add the Internet symbol from the Network class or any of the symbols from the Location class to the Internet (or a Partitioned Internet) submap. The new symbol represents a special object, called a container object. Symbols of container objects open into a Partitioned Internet submap. You can cut and paste IP network and gateway (router) objects from your Internet submap to the Partitioned Internet submap, and IP Map will move all objects contained in child submaps and maintain all connections.

Purpose of this Task

Expand your network map so you can distribute symbols of IP networks and gateways across multiple submaps. This enables you to customize the organization of your network map.

Prerequisites for this Task

- The map must be open with read/write access.
- For IP Map to manage the object, you must use one of the supported symbols to represent the Partitioned Internet submap.

Procedure

To add a container object to an Internet or Partitioned Internet submap:

1. Select **Edit: Add Object...** from the OVW menu bar. The **Add Object Palette** appears.
2. From the **Add Object Palette**, select either the **Network Class** or the **Location Class**. The subclasses for the selected class appear.
3. Select a supported symbol, and use mouse button 2 to drag the symbol to the Internet submap or the Partitioned Internet submap of your choice. The **Add Object** dialog box appears.
4. Enter a name for the object in the **Selection Name** field of the **Add Object** dialog box. You may also enter text for other optional fields in the **Add Object** dialog box.
5. Click on **OK**. The newly added symbol resides on the submap, and an empty child submap for that symbol is automatically created. To open the child submap, double-click on the new symbol.

When you add a symbol representing a container object to an Internet submap or a Partitioned Internet submap, IP Map is not listed as a configurable application because IP Map requires no information about the container object.

The Containment Realm

The Internet submap and the hierarchy of Partitioned Internet submaps make up the containment realm. You can populate your manually created Partitioned Internet submap by cutting and pasting IP network and gateway (router) symbols from the Internet submap to a Partitioned Internet submap.

Within the containment realm, cutting and pasting these symbols maintains the hierarchical and topological relationship between the symbols. When you cut these symbols from the Internet submap, and paste them on a Partitioned Internet submap, the child submap, all included symbols and objects, are also moved. Thus, the hierarchical relationship is maintained.

All submaps, objects, symbols, and connections that are contained under the cut and pasted symbol remain intact. Symbol behavior and symbol status are also maintained. If the symbol you paste onto a map explodes into a child submap, that capability exists for the new symbol. In addition to the hierarchical relationship, all the topological relationships between symbols are also maintained. IP Map maintains the connections between symbols after these objects are pasted onto a Partitioned Internet submap, by redrawing connections to the symbol of the container object.

To understand how to expand the containment realm, the following topics are provided:

- editing guidelines in a containment realm
- example of an internet submap
- example of a Partitioned Internet submap
- maintaining the containment realm

Editing Guidelines

This section discusses the types of editing operations you can perform in the containment realm while maintaining the connections between symbols. OVW allows you to cut and paste any symbol in the map from any submap to any other submap. This is done from the OVW **Edit: Cut** and **Edit: Paste** operations.

However, to maintain connections between symbols in the containment realm, you must follow several editing guidelines.

- You can cut and paste symbols between the Internet submap and any Partitioned Internet submap.
- You *cannot* cut and/or paste symbols onto the Root submap or Network, Segment, and Node submaps.
- You cannot cut and paste container symbols.

If you paste a container object on one of these submaps, the containment information is broken; that is, the symbol will no longer maintain its relationship to other symbols. Connections between that symbol and other symbols are also broken.

For more information about the cut and paste operations, see the *HP OpenView Windows User's Guide*.

Example of Internet Submap

On the Internet submap, you can place a map of the world and add symbols that represent container objects of countries or continents. Each container object opens into its own submap. Then, you can cut symbols that represent your resources in a particular country from the Internet submap to any of the Partitioned Internet submap.

The following figure shows an Internet submap in which four container objects were added. The symbols of the container objects represents Asia, U.S.A., South America, and Europe. In addition, all symbols of objects discovered by IP Map have been cut from the Internet submap and placed in lower-level Partitioned Internet submaps. IP Map maintains the connections between the symbols of discovered objects in the lower level submaps. Also, IP Map creates the proper connections between the symbols of the container objects.

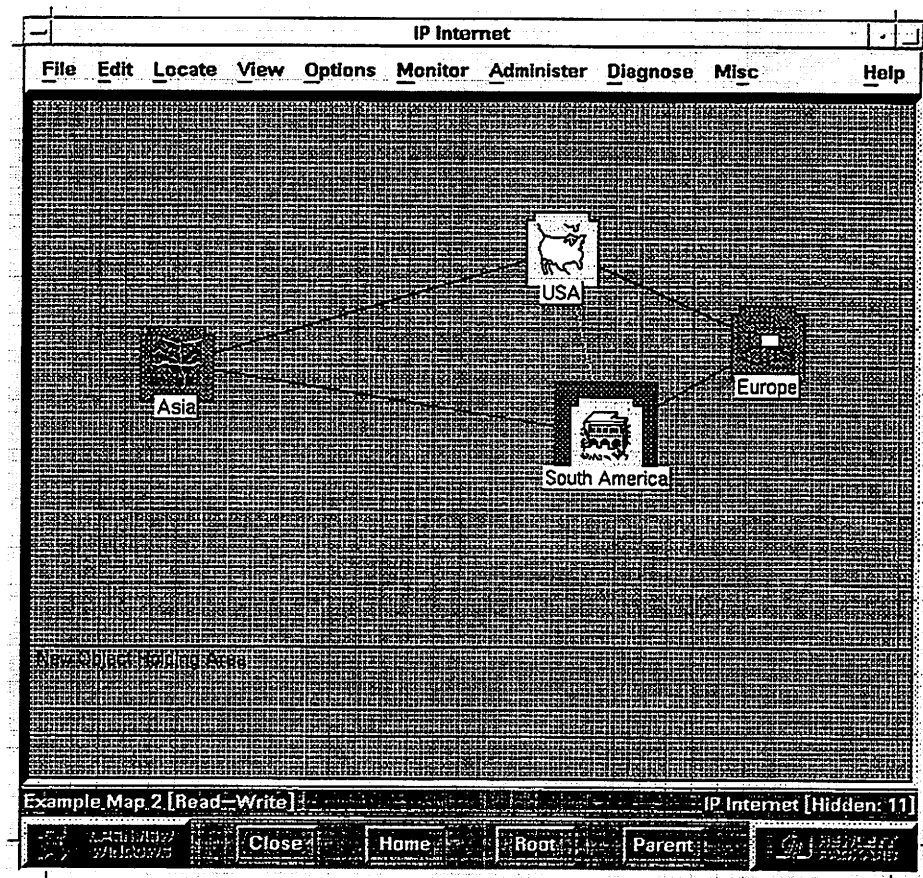


Figure 3-1. Internet Submap

Example of Partitioned Internet Submap

The following figure shows the U.S.A. submap. Six container objects have been created in this submap. This submap may also contain symbols representing IP networks or gateways. From this submap, you can double-click on any of the symbols and open a child submap, which may display other container objects or symbols that represent IP networks and gateways.

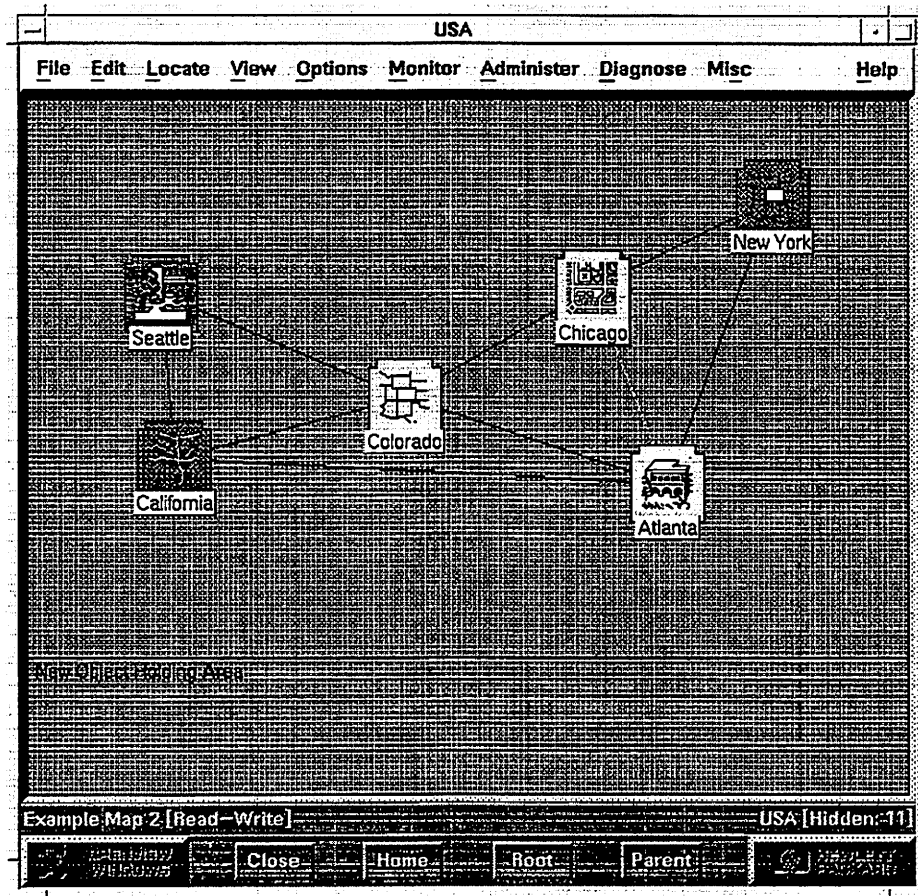


Figure 3-2. Partitioned Internet Submap of the USA

Maintaining the Containment Realm

As you customize your network map, IP Map tracks any editing changes you make to the open map. The Internet submap and all Partitioned Internet submaps make up the containment realm. IP Map continues to manage objects that have been moved within the containment realm with the network monitoring process (**netmon**).

As new IP-addressable resources are added to the network, IP Map may discover these resources, create objects of these resources, and add one or more symbols of the object to a submap. IP Map always places discovered IP-addressable gateways (routers) and networks on the original, highest-level Internet submap.

You can maintain the customized organization of your network map by distributing these symbols (using the cut and paste operation) to the Partitioned Internet submap of your choice. See the *HP OpenView Windows User's Guide*.

Expanding Lower Levels of Your Network Map

Expand the lower levels of your network map by creating additional network, segment, and node objects. This enables you to complete the distribution of resources over your map to better match how your network is organized. IP Map does not maintain connections between symbols at the network, segment, and node level after cut and paste operations on these symbols. You must add a connection between desired symbols after cut and paste operations. You can do this by selecting **Edit: Add Connection...** from the OVW menu bar.

The following sections show you how to add network, segment, node, and interface objects to your network map so that IP Map will manage them.

Adding a Network Object

IP Map discovers the IP networks on your network and creates Network submaps to display segments and gateways of the IP network. IP Map places a symbol of the IP network on the Internet submap. You can create additional Network submaps. In addition to the symbols that represent container objects, you can add an IP network symbol, which represents an IP Network object, to the Internet or a Partitioned Internet submap. The IP network symbol opens into a Network submap. To create an additional Network submap, add a network symbol to the Internet or a Partitioned Internet submap. When you add an IP network symbol to the Internet or a Partitioned Internet submap, an empty Network submap is created. Double-clicking on the network symbol opens the Network submap. IP Map recognizes any of the following symbols when added to an Internet or Partitioned Internet submap:

Symbol	Class
IP Network	Network
Gateway (Router)	Connector

Prerequisites for this Task

The map must be opened with read-write access.

Procedure

1. Select **Edit: Add Object...**
2. From the symbol palette, choose the desired symbol type for the network object by selecting the desired class, then the desired subclass, and use button 2 to drag the symbol to the submap. The **Add Object** dialog box appears.
3. Enter a selection name for the object in the **Selection Name** field of the **Add Object** dialog box.
4. In the **Object Attributes** list, select **IP Map**, and click **Set Object Attributes...** The **IP Map Set Attributes** dialog box for a network object appears.
5. Enter a **Network Name**.
6. Enter a **Network Address**.
7. Optionally, you may enter a **Network Subnet Mask**.
8. Click **Verify** to check for valid entries.
9. Click on **OK** to close the **Set Attributes** dialog box.
10. Click on **OK** in the **Add Object** dialog box to complete the operation.

Adding a Segment Object

If IP Map can identify which segment the node is on, it places it there. If IP Map cannot, IP Map places it on the default segment submap. The default segment submap is the submap created by IP Map when OVW was first run. If that submap has been deleted, the default segment submap is the oldest segment submap. IP Map discovers new nodes on segments attached to SNMP, IP-addressable bridges and multi-port repeaters (hubs).

A Network submap may contain symbols in the Network and Connector classes. IP Map recognizes the following symbols on a Network submap.

Class	Symbol
Network	Bus
Network	Star
Network	Token Ring
Network	FDDI Ring
Connector	Gateway (Router)
Connector	Bridge
Connector	Repeater
Connector	Multi-Port (Hub)

You can add a segment object to a Network submap. When you add a segment, an empty Segment submap is created. Double-clicking on the symbol opens the Segment submap.

Prerequisites for this Task

The map must be opened with read-write access.

Procedure

1. Select **Edit: Add Object....**
2. From the symbol palette, choose the desired symbol type for the segment object by selecting the desired class, then the desired subclass, and drag the symbol to the submap. The **Add Object** dialog box appears.
3. Enter a selection name for the object in the **Selection Name** field of the **Add Object** dialog box.
4. In the **Object Attributes** list, select **IP Map**, and click **Set Object Attributes....** The **IP Map Set Attributes** dialog box for a segment object appears. A figure of the dialog box follows this procedure.
5. Enter a name for the segment. It must be unique to other segment names in the submap.
6. Click **Verify** to check for valid entries.
7. Click on **OK** to close the **Set Attributes** dialog box.
8. Click on **OK** in the **Add Object** dialog box to complete the operation.

When adding a segment, the IP Map Attributes dialog box appears as follows:

Attributes

IP Map

Name :

192.168.1.1

Messages:

Fill in a segment name that is unique in this network.

OK **Verify** **Cancel** **Help**

Figure 3-3. Adding a Segment

Adding a Node Object

You can add an object that represents a node or a network device to your Segment submap by placing one of the supported symbols on a Segment submap. Double-clicking on the node symbol opens a Node submap. IP Map discovers and manages the following symbols from the Computer, Connector, and Net Device classes in a Node submap:

Class	Symbol
Computer	PC
Computer	Workstation
Computer	Mini
Computer	Main Frame
Connector	Bridge
Connector	Gateway (Router)
Connector	Repeater
Connector	Multi-port (Hub)
Net Device	Analyzer
Net Device	Modem
Net Device	X.25
Net Device	PBX

Prerequisites for this Task

The map must be opened with read-write access.

Procedure

1. Select **Edit: Add Object....**
2. From the symbol palette, choose the desired symbol type for the node object by selecting the desired class, then the desired subclass, and drag the symbol to the submap. The **Add Object** dialog box appears.
3. Enter a selection name for the object in the **Selection Name** field of the **Add Object** dialog box.
4. In the **Object Attributes** list, select **IP Map**, and click **Set Object Attributes....** The **IP Map Set Attributes** dialog box for a node object appears:
5. Enter the hostname of the node.
6. Enter the IP address of the node.
7. Click **Verify** to check for valid entries.
8. Click on **OK** to close the **Set Attributes** dialog box.
9. Click on **OK** in the **Add Object** dialog box to complete the operation.

Adding an IP Interface Object

You can add an IP interface to a Node submap by placing an IP Interface symbol on an Node submap. You can do this by entering the IP address of the interface.

Class	Symbol
Cards	IP Interface

Prerequisites for this Task

The map must be opened with read-write access.

Procedure

1. Select **Edit: Add Object....**
2. From the symbol palette, select the IP Interface symbol in the Cards class. The **Add Object** dialog box appears.
3. Enter a selection name for the object in the **Selection Name** field of the **Add Object** dialog box.
4. In the **Object Attributes** list, select **IP Map**, and click **Set Object Attributes...** The **IP Map Set Attributes** dialog box for an IP interface object appears. A figure of the dialog box follows this procedure.
5. Enter the IP Address for the IP interface. The subnet mask is added for you.
6. Click **verify** to check for valid entries.
7. Click on **OK** to close the **Set Attributes** dialog box.
8. Click on **OK** in the **Add Object** dialog box to complete the operation.

When adding an IP Interface to a Node submap, the IP Map Attributes dialog box appears as follows:

Add Object - Set Attributes

IP Map

IP Address :

Subnet Mask :

Messages:

Figure 3-4. Adding an Interface Object



Automatic Layout

Each submap has a layout algorithm that determines how symbols are placed on the submap. When automatic layout is enabled, items discovered by IP Map are automatically placed on the submap according to the submap's layout algorithm. Each submap is assigned one of the following layout algorithms during submap creation:

- bus
- ring
- star
- row/column
- point to point
- none



The following lists describe the behavior of symbols in a submap depending on whether autolayout is enabled or disabled. When autolayout is enabled:

- If you add a new symbol to a submap with the **Edit: Paste** operation or if an application adds a new symbol to a submap, the symbol is placed within the submap according to the configured layout algorithm for that submap.
- To reposition all symbols in a submap according to the layout algorithm, select **View: Redo Layout**.
- If you move a symbol in the submap, it snaps back into the original place.

When autolayout is disabled:

- A **New Object Holding Area** appears in the lower portion of the submap window.
- Symbols added to the submap are placed into the **New Object Holding Area**.
- If you move a symbol from the **New Object Holding Area**, the symbol is placed where you designate.
- If you move a symbol in the submap, the symbol will stay where you designate.



You can enable or disable the autolayout algorithm for the current submap in the open map, or for all submaps in the open map. After enabling or disabling autolayout for all submaps in the open map, you can change the enable or disable setting for specific submaps.

Purpose of this Task

This task explains how to disable or enable the layout algorithm for a submap so you can rearrange symbols in a submap or submaps.

Prerequisites for this Task

The map must be opened with read-write access.

Procedure 1: For Specific Submaps

To disable automatic layout for a specific submap

1. Move the mouse cursor to the menu bar of the submap for which you want to disable automatic layout.
2. Select **View: Automatic Layout -> For This Submap -> Off For This Submap**. The autolayout algorithm for the submap is disabled. **[Auto-Layout]** no longer appears in the status bar of the submap.

Procedure 2: For All Submaps

To disable automatic layout for all submaps in the open map:

1. Move the mouse cursor to the menu bar of any displayed submap window.
2. Select **View: Automatic Layout -> For All Submaps -> Off For All Submaps**. The autolayout algorithm for all submaps in the open map is disabled. **[Auto-Layout]** no longer appears in the status bar of any of the submaps.

You can enable the layout algorithm for a specific submap, or all submaps, of the open map in the same manner. Select **View: Automatic Layout -> For This Submap -> On For This Submap** or **View: Automatic Layout -> For All Submaps -> On For All Submaps**.

Updating a Map Open with Read-Only Access

Maps open with read-only access do not automatically receive updates on topological events such as the addition or deletion of symbols, objects, or submaps, or the relocation of symbols by applications or other users. You can update the topology of a map open with read-only access.

Purpose of this Task

This task explains how to update the topology of a map open with read-only access.

Prerequisites for this Task

- The map must be open with read-only access.
- If another user has the map open with read-write access, you can obtain read-write access to a map, if you have permission, after that user closes the map.

Procedure

1. Make sure the map is open with read-only access.
2. Select **File: Refresh Map**.

Note

The **File: Refresh Map** menu item is greyed on submap windows of maps open with read-write access. The **Refresh Map** operation is not required to update status on maps open with read-write access.

Limited Read-Write Access. Only one user can have a specific map open with read-write access at any one time. If another user has the map open with read-write access, when you open the same map, you have read-only access to it. This is the case even if you have read-write permission for the map from the operating system.

Obtaining Read-Write Access. If the user with read-write access to the map closes the map, the user with read-only access can obtain read-write access by choosing the **File: Refresh Map** menu item. This causes all submap windows and dialog boxes of the map to be closed. OVW reopens the map with read-write access, providing the operating system allows you read-write permission.

Taking a Snapshot of Your Network

You can document your network by creating a snapshot of the open map. A snapshot gives you a static picture of your network map at the time the snapshot was created. Snapshots are useful as a past record of the configuration of systems on the network, which you can use as a troubleshooting tool. Snapshots are read-only. You can perform locate operations in snapshots, but you cannot edit the map. That is, you cannot add, delete, or modify symbols, objects, submaps, or the map.

A snapshot preserves the status of all symbols, and contains all the submaps that existed in the map at the time the snapshot was taken. You can create multiple snapshots of a map, giving you a display of the state of your network at different times. You can open a snapshot and display it alongside the map from which it was taken. You can have only one snapshot open at a given time.

Purpose of this Task

In NNM, maps are continually updated with information from systems, software, and processes in your network. You may want to "freeze" the state of your map at a certain point in time for comparison with the map as it evolves later on. A map snapshot gives you this capability.

Prerequisites for this Task

The map must be open with read-write access.

Procedure

To create a snapshot:

1. Select **File: Map Snapshot -> Create...** The **Create Snapshot** dialog box appears.
2. Change the name of the snapshot, if desired, or leave the default name, and enter comments if desired.
3. Click on **OK** at the bottom of the dialog box. HP OpenView Windows creates the snapshot and closes the **Create Snapshot** dialog box.
4. You can open the snapshot and list all snapshots created for the open map by selecting **File: Map Snapshot -> Open/List...** The status line indicates the name of the snapshot on all submap windows of an open snapshot. The home submap for the snapshot is the home submap of the open map at the time the snapshot was created. Only one snapshot may be open at a time. If a snapshot is already opened when you choose to open another snapshot, the previously opened snapshot is closed.

Viewing Your Current Network and System Configuration

NNM provides quick access to information about your network and system configurations. This section points you to the menu items available to access this information.

Viewing Object Descriptions

You can view a description of the objects that IP Map manages, such as an internet, network, segment, node, or IP interface object. This task is useful when you need to see a full description of an object on the map. The information you see is from the NNM database. Therefore, the descriptions are as current as the last poll.

Prerequisites for this Task

One or more nodes must be selected from the map. If you select more than one node, you receive a dialog box for each selected node.

Procedure

1. Select the object for which you want a description.
2. Select **Monitor: Description -> Selected Objects...** The **Object Description** dialog box appears.
3. In the **Object Description** dialog box, select **IP Map** and select **View/Modify Object Attributes**. The **Set Attributes** dialog box appears.

The following sections (object descriptions of an IP internet, network, segment, node, and interface) list the information included in the **Attributes** dialog box, depending on which object you selected on the map.

Description of an IP Internet Object

When you select the IP Internet symbol on the root submap, IP Map provides the following information:

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

Attributes for Object IP Internet

IP Map:

Number of IP networks :
12

Number of segments :
15

Number of nodes :
113

Number of interfaces :
144

Number of IP Gateways/Routers :
12

Messages:
The fields in this box are read-only. Press OK or Cancel to continue.

OK **Verify** **Cancel** **Help**

Figure 3-5. Internet Description

Description of a Network Object

When you select a network, NNM provides the following information:

- network name as it appears on the map
- network IP address
- subnet mask associated with the network number
- IP Status of the network
- number of segments on the network
- number of nodes contained within the network
- status or error messages may appear in the **Messages** field.

The screenshot shows a dialog box titled "Attributes for Object network object". It contains several input fields and a list box. The fields are labeled as follows:

- IP Map**
- Network Name :** 192.4.35
- Network Address :** 192.4.35.214
- Subnet Mask :** 255.255.255.0
- IP Status :** Unknown (with a dropdown arrow)
- Number of segments :** 1
- Number of nodes :** 0
- Messages:** (empty list box with a vertical scrollbar)

At the bottom of the dialog box, there are four buttons: **OK**, **Verify**, **Cancel**, and **Help**.

Figure 3-6. Network Description

Description of a Segment Object

When you select a segment, NNM provides the following information:

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

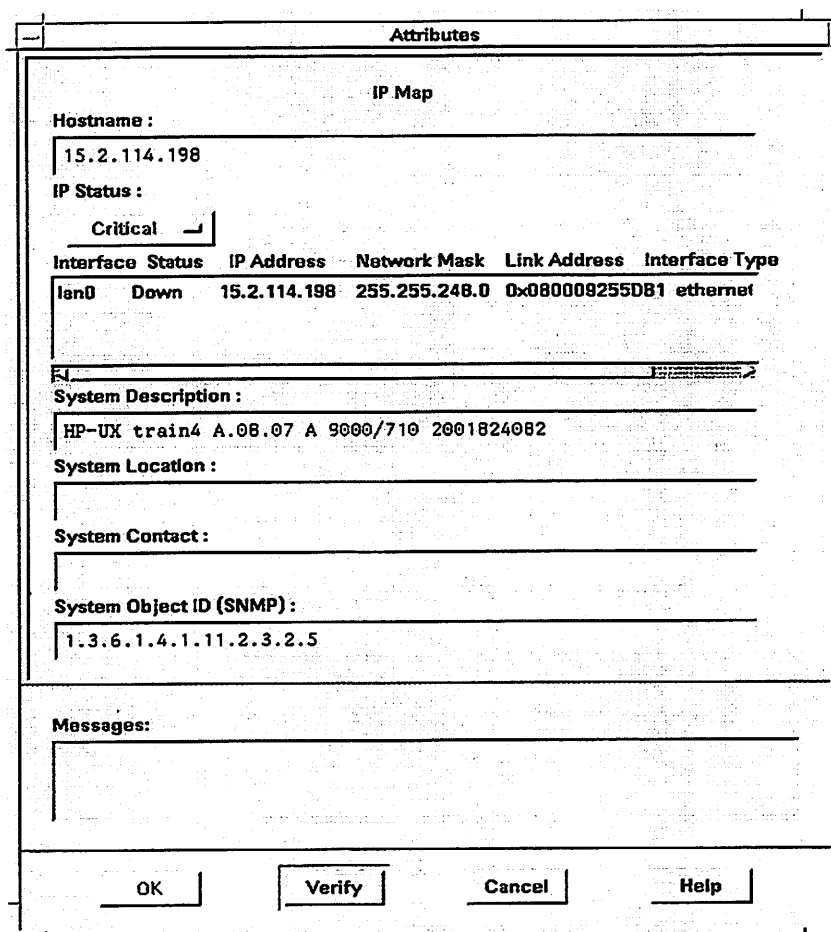
The screenshot shows a window titled "Attributes for Object Example segment". Inside the window, there is a section labeled "IP Map". Under "IP Map", there are two labels: "IP Status :" followed by a dropdown menu showing "Unknown", and "Number of nodes :" followed by a text box containing the number "0". Below the "IP Map" section is a "Messages:" label followed by a large empty text area. At the bottom of the window, there are four buttons: "OK", "Verify", "Cancel", and "Help".

Figure 3-7. Segment Description

Description of a Node Object

When you select a node, NNM provides the following information:

- Host name that was assigned when the node was created.
- IP status of the node.
- Information and status about each IP interface installed on the node.
- System description as returned by the SNMP agent.
- System location and system contact as returned by the SNMP agent.
- System object ID of the node. This field indicates whether or not the node supports SNMP.
- Status or error messages may appear in the **Messages** field.



Attributes

Hostname : 15.2.114.198

IP Status : Critical

IP Map

Interface	Status	IP Address	Network Mask	Link Address	Interface Type
lan0	Down	15.2.114.198	255.255.248.0	0x080009255D81	ethernet

System Description : HP-UX train4 A.08.07 A 9000/710 2001824082

System Location :

System Contact :

System Object ID (SNMP) : 1.3.6.1.4.1.11.2.3.2.5

Messages:

OK Verify Cancel Help

Figure 3-8. Description of a Node Object

Description of an Interface Object

When you select an interface, NNM provides the following information:

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

Attributes for Object Interface: 15.2.113.1

IP Map

IP Address :
15.2.113.1

Subnet Mask :
255.255.248.0

Physical Address (LLA):
0x000000C005484

Interface Type :
Ethernet CMSACD

IP Status :
Normal

Messages:

OK Verify Cancel Help

Figure 3-9. Interface Description

Viewing Network Address Information

This task is useful for determining the addresses associated with a node, without looking through configuration files. The information you see is real-time data taken from the node versus static information taken from a database.

Prerequisites for this Task

- The node must support SNMP.
- One or more SNMP nodes must be selected from the map. If you select more than one node, you receive a dialog box for each selected node.

Procedure

1. Select a node on the map.
2. Use the **Monitor: Network Configuration -> Addresses...** operation to view the following information about each interface on the node:

- interface index
- interface name
- IP address
- network mask
- network address
- link-level address (physical address)

For example:

Index	Interface	IP address	Network Mask	Network Address	Link Address
4	lan1	126.1.0.2	255.255.0.0	126.1.0.0	0x010002033333
3	lan0	126.1.0.3	255.255.0.0	126.1.0.0	0x010002022222
2	lo0	222.0.0.1	255.0.0.0	222.0.0.0	<none>

Viewing How Traffic is Routed on a Network

This task lists the routing table information for a remote SNMP node. It can be useful in determining more efficient routes on the network, assessing the need for explicit routes, and diagnosing connectivity problems. The information you see is real-time data taken from the node versus static information taken from a database.

If you want to reroute traffic on the network, you can either temporarily change the routing using the `route` command or permanently change the routing by editing the `netlinkrc` file and rebooting the system. (Routing commands may vary across vendor systems.)

Prerequisites for this Task

- The node must support SNMP.
- One or more SNMP nodes must be selected from the map. If you select more than one node, you receive a dialog box for each selected node.

Procedure

1. Select a node on the map.
2. Use the **Monitor: Network Configuration -> Routing Table...** operation to view the following information about each destination node with which the selected node communicates:
 - destination name (default is a route that the system uses when it cannot find a specific route)
 - name of the gateway (router) between the selected node and the destination
 - type of route (for example, directly connected to a LAN, through a remote gateway, or route currently not available)
 - network subnet mask associated with the route
 - name of the interface that is used to reach the destination

For example:

Destination	Gateway	Type	Mask	Interface
default	gateway1.grp.org.com	remote	0.0.0.0	lan1
126.1.0.111	sys1.grp.org.com	direct	255.255.0.0	lan1
deptka.grp.org.com	sys2.grp.org.com	remote	255.255.0.0	lan1
deptmd.grp.org.com	sys2.grp.org.com	remote	255.255.0.0	lan1
126.3.0.222	sys1.grp.org.com	direct	255.255.0.0	lan0
localhost	localhost	direct	255.0.0.0	lo0

Viewing the Address Translation Table

This task lists the address translation table for a remote SNMP node using the ARP (Address Resolution Protocol) Cache. It can be useful for diagnosing connectivity problems, since it can tell you if two nodes have a different address for a third node. The information you see is real-time data taken from the node versus static information taken from the database.

Prerequisites for this Task

- The node must support SNMP.
- One or more SNMP nodes must be selected from the map. If you select more than one node, you receive a dialog box for each selected node.

Procedure

1. Select a node on the map.
2. Use the **Monitor: Network Configuration -> ARP Cache...** operation to view the following information about each node listed in the selected node's address translation table:
 - node name or IP address
 - link-level address (physical address) associated with the node name
 - how this specific entry was placed in the table
 - interface name (of the selected node) that is associated with the node and the physical address

For example:

Node	Link Address	Entry Type	Interface
126.1.77.22	0x01000205522	dynamic	lan1
deptmd.grp.org.com	0x01000204444	dynamic	lan2
deptar.grp.org.com	0x01000202323	dynamic	lan2

Viewing the Services Available on a Node

This task lists the IP networking services for which a remote SNMP node is listening. It is useful for determining what configured services a node is currently running. The information you see is real-time data taken from the node versus static information taken from the database.

Prerequisites for this Task

- The node must support SNMP.
- One or more SNMP nodes must be selected from the map. If you select more than one node, you receive a dialog box for each selected node.

Procedure

1. Select a node on the map.
2. Use the **Monitor: Network Configuration -> Services...** operation, to view the following information about the selected node:
 - service protocol: either TCP (Transmission Control Protocol) or UDP (User Datagram Protocol).
 - port to which the service is bound.
 - service for which the node is listening (for example, **telnet**, **nfs**). If no service is listed, the service is either unavailable or unknown.

For example:

Protocol	Port	Service
tcp	512	ftp
tcp	10	telnet
tcp	20	smtp
tcp	333	portmap
udp	333	portmap
udp	200	snmpd
udp	202	who
udp	203	syslog

Viewing Disk Space

This task lists the available file system space on a node. The information you see is real-time data taken from the node versus static information taken from the database.

Prerequisites for this Task

This information is generated by an HP enterprise-specific MIB; therefore, it is only available from an HP 9000 or Sun system running the HP OpenView SNMP Agent software.

Note

If you have another file system utility that is not dependent on the HP OpenView SNMP Agent software, you can integrate the utility to the OVW menu bar. For more information, see the "Integrating Existing Applications" section in chapter 3 of the *HP OpenView Network Node Manager Administrator's Reference*.

If the vendor has provided enterprise-specific MIBs for the file system, you can build an application to do this operation. For information about building MIB applications, see chapter 6.

Procedure

1. Select a node on the map.
2. Use the **Monitor: System Activity -> Disk Space...** operation to view the following information about each file system on the selected node:
 - file system name
 - total kilobytes of disk space
 - number of kilobytes used
 - number of kilobytes available
 - percent of total capacity being used
 - directory name on which the disk is mounted

For example:

Filesystem	kbytes	used	avail	capacity	Mounted on
/dev/dsk/0s0	439998	248720	186878	57%	/
/dev/dsk/0s1	534046	80280	448425	15%	/users/other
/dev/dsk/0s2	534046	413047	115658	78%	/backup1
/dev/dsk/0s3	534046	290003	237712	55%	/backup2

Controlling Network and System Configuration

The task of managing your network can require an investigation or modification of certain network and system configurations. NNM provides access to the system that you want to administer via

- The System Administration Manager (SAM) tool. This tool is only available on HP 9000 systems.
- A terminal emulator.

Using SAM to View or Modify HP-UX Network and System Configuration

If you have an HP 9000 system on your network, you can view and modify network and system configurations using the System Administration Manager (SAM).

Prerequisites for this Task

The selected node must be an HP 9000 system and have the `/usr/bin/sam` application installed for the SAM operation to work.

Procedure

1. Select an HP 9000 system.
2. Using the **Administer: System Management** -> **HP-UX SAM...** operation, you can access the SAM tool to view or modify
 - user accounts
 - group memberships
 - file systems
 - disk space
 - printer status
 - print requests
 - networking services
 - kernel configurations

If SAM is not available on your system, then go to the next section, "Using the Terminal Emulator to Access Other Systems," to view or modify your network and system configurations.

Note

If other vendors provide network and system configuration utilities such as SAM, you can add them to the NNM menu bar. For information about this, see the "Integrating Existing Applications" section in chapter 3 of the *HP OpenView Network Node Manager Administration Reference*.

Using the Terminal Emulator to Access Other Systems

NNM provides three options that enable you to create a terminal emulator window on your management station that is connected to a remote system via a network virtual terminal protocol. Once you connect to the remote system, you can either view or modify network and system configurations. The three options are

- **Telnet (hpterm)**, which allows you to log into a remote UNIX or non-UNIX system from an HP 9000 management station
- **Telnet (xterm)**, which allows you to log into a remote UNIX or non-UNIX system from an HP 9000 or SUN management station
- **vt3k (hp3000)**, which allows you to log into a remote MPE (HP 3000) system from an HP 9000 management station

Prerequisites for this Task

- To use the **Telnet (hpterm)** option
 - The management station should be an HP 9000 system, must have the ARPA Services software installed and configured, and must support the **telnet** protocol.
 - The remote system you want to access should support the HP terminal, must have the ARPA Services software installed and configured, and must support the **telnet** protocol.
- To use the **Telnet (xterm)** option
 - The management station must have the ARPA Services software installed and configured, and must support the **telnet** protocol.
 - The remote system you want to access should support the DEC VT102 terminal, must have the ARPA Services software installed and configured, and must support the **telnet** protocol.
- To use the **vt3k (hp3000)** option
 - The local system must be an HP 9000 and must have the HP Network Services (NS) software installed and configured.
 - The remote system you want to access must be an HP3000, must have the HP NS Virtual Terminal Services running, and must support the **vt3k** network protocol.

Procedure 1: Using Telnet (hpterm)

1. Select the remote system.
2. Select **Misc: Terminal Connect -> Telnet (hpterm)**.
3. Perform your operations on the remote system.
4. Close the window.

For information about the **telnet** service, see the *HP 9000 Using ARPA Services* manual.

Procedure 2: Using Telnet (xterm)

1. Select the remote system.
2. Select **Misc: Terminal Connect -> Telnet (xterm)**.
3. Perform your operations on the remote system.
4. Close the window.

For information about the **telnet** service, see the *HP 9000 Using ARPA Services* manual.

Procedure 3: Using Vt3k (hp3000)

1. Select one of the following modes:
 - **Block Mode...**, which enables you to run a block mode application on the remote system.
 - **Type Ahead...**, which provides you with keyboard input buffering. This mode will not work with block mode applications.
2. Perform your operations on the remote system.
3. Close the window.

For information about **vt3k** service, see the *HP 9000 Using Network Services* manual.

Monitoring Your Network

To manage a network effectively, you need access to information about the health of your network (for example, what is up or down), the state of your network (for example, what errors are being generated, what thresholds are exceeding their limits), and the trends occurring on your network (for example, where is the traffic increasing, which devices are generating recurring errors). HP OpenView Network Node Manager (NNM) provides you with the tools to access this information. However, to obtain some of this information, you will need to tailor NNM to your network environment.

Network management is unique to each administrator's environment. It would be impossible to provide examples of each network environment. The examples in this chapter tie together the NNM tools (for example, Data Collector, Event Configuration, and Application Builder). They are meant to serve as models for you to use when you configure NNM for your network environment.

In this chapter, you will learn how to

- Check the health and status of your network. Checking the health and status involves looking for color alerts on the Internet map, creating submaps for special monitoring needs, and looking for changes on the network.
- Monitor your network for proactive fault diagnosis. By customizing the tools in NNM, you can establish baselines for normal network performance, monitor trends, set thresholds, and invoke customized event notifications.

Checking the Health and Status of Your Network

Once your network has been discovered by HP OpenView IP discovery and layout, you can begin to monitor the state of your network. Monitoring includes tasks such as, checking the map for color alerts which indicate problems, creating submaps that need special monitoring, and checking for network changes. This section provides procedures and examples of how to

- look at maps for color alerts
- look at maps for new nodes
- create special submaps for monitoring status
- check the **Events Browser** window

Looking at Maps for Color Alerts

You can identify the objects that have an abnormal condition without having to look at every object on your network map. A color alert on a symbol indicates that some part of that object may have problems. To isolate a fault somewhere on your network, follow the color alerts to increasingly more specific submaps until you reach the specific object that is not functioning. You follow color alerts by opening child submaps of objects that contain a color alert.

If you need to verify that an object is not functioning, you can select that object and perform some of the following operations:

- **Monitor -> Device Configuration -> System Information...**
- **Diagnose -> Network Connectivity -> Demand Poll...**
- **Diagnose -> Network Connectivity -> Ping...**
- **Diagnose -> Network Connectivity -> IP / TCP / SNMP...**

If these operations do not produce any responses or they time out, then the node is probably down or otherwise unreachable over the network.

Purpose of this Task

- Looking for color alerts enables you to quickly identify specific objects on the network that are not working.
- You can scan your Network map for a high level view of its status if the map uses the OVW default compound status.

Prerequisites for this Task

- Network map must be read-write.
- IP Map must be enabled for the map and it must be configured to display status. These are the default settings for IP Map when a map is created.
- To interpret the meaning of status colors correctly, you should know the compound status scheme of the open map. This tells you how status propagates from objects in a submap to the parent object. You can identify the compound status scheme for the map from the **Map Description** dialog box by selecting **File: Describe/Modify Map....**

Procedure

In this example, the Root submap is displayed, and an Internet symbol is displayed on the Root submap. It is yellow. Compound status for the open map is set to HP OpenView Windows Default.

1. Double-click on the yellow Internet symbol.

The Internet submap opens and displays three IP networks attached to two gateways. One IP network symbol is yellow. This indicates a marginal problem with the network.

2. Double-click on the yellow IP network symbol.

A Network submap opens and displays three segments attached to two gateways. One segment symbol is yellow. This indicates a problem somewhere on the segment.

3. Double-click on the yellow segment symbol.

A Segment submap opens and displays the nodes attached to that segment. Of all the nodes in the segment, one node is red, a workstation. The problem is isolated to that workstation.

4. Double-click on the red workstation symbol.

A Node submap opens and displays two interface symbols, which indicates that two interfaces are installed in the workstation. One of them is red.

You have isolated the fault to a single interface card of a single node on your internet.

Looking at Maps for New Nodes

IP Map will automatically discover new IP-addressable nodes for the open map. Some gateways (hubs), HP gateways (hubs) for example, are able to identify the location of a node and tell IP Map where to place a symbol of the node in the proper Segment submap. However, some gateways (hubs) cannot tell where a node should be placed. In this case, IP Map places symbols of newly discovered nodes in the default Segment submap. The default Segment submap is the oldest of all the Segment submaps in the open map. You may want to occasionally check the default Segment submap for new nodes that may have been discovered.

Purpose of this Task

The purpose of this task is to identify new objects that have been discovered and added to the open map. Because discovery is automated, you will see additional symbols of objects on your network map.

Prerequisites for this Task

IP Map must be enabled for the map. This is the default.

Procedure

IP Map places new symbols directly on the submap if autolayout is enabled. IP Map places new symbols in the **New Object Holding Area** if autolayout is disabled for the submap.

1. To check the default Segment submap for any new nodes that may have been discovered, open the default Segment submap from the segment symbol in the Network submap. View the submap for any new symbols.
2. To easily see new symbols in the submap, disable autolayout for the submap. When autolayout is disabled, a **New Object Holding Area** appears at the bottom of the submap. All newly added symbols are placed in the **New Object Holding Area**.

You can move newly discovered objects from the **New Object Holding Area**, and add (move) them to a specific location on the map by pressing the middle mouse button while the pointer is on an object in the **New Object Holding Area**. Drag the object to the desired location on the map. If using a two-button mouse, press both buttons.

Creating Special Submaps for Monitoring Status

You can create submaps that are logically organized instead of physically organized. For example, you may want to have a submap that contains all the gateways for a particular location.

Purpose of this Task

This task will help you create logical submaps for specialized monitoring.

Prerequisites for this Task

- The map must be open with read-write access.
- You should consider what relationship the submap has with other submaps in the open map. The submap may be independent, or a child submap of an object in the network map.

Procedure

In this example, you want to create a submap that displays all the gateways on your site, and you want to be able to open the submap from a symbol in the Internet submap.

1. Decide where to locate your submap and whether it will have a parent object or not. A submap without a parent object is independent of other existing submap hierarchies in the open map. This submap can be opened only from the **Available Submaps** dialog box. You can create child submaps of this submap, thereby creating a new submap hierarchy in the map.

A submap that has a parent object can be opened from an explodable symbol of the parent object. If you want the new submap to exist within an existing submap hierarchy, you should create this submap from an explodable symbol.

2. To create a submap within an existing submap hierarchy, decide which symbol to use to open the new submap. Do you want to create a new symbol to open the submap or use an existing explodable symbol? If other symbols on the parent submap already open into child submaps or execute applications, you must create a new symbol to open the submap.
3. If you decide to create a new symbol, add a symbol (for an existing object) or a new symbol and object to the submap of your choice selecting the **Edit: Add Object...** item from the HP OpenView Windows menu bar. You may add either of the IP Internet symbols or any of the symbols in the Location class.
4. Open the new submap by double-clicking on the newly created symbol. Copy gateway objects from other submaps into the newly created map, using the OVW **Edit: Copy** and **Edit: Paste** operations. For more information about these operations, see the *HP OpenView Windows User's Guide*.
5. You can add a background graphic to the new submap from the **New Submap** dialog box by selecting **Edit: Submaps - Describe/Modify...** Sample background graphics are supplied with OVW in the `/usr/OV/backgrounds` directory.

Checking for Event Notifications

Anytime a change occurs on the network (for example, a new node was added, a node went down, a threshold was exceeded), an event is generated. Through NNM internal processes, the event is sent to a predefined category in the **Events Browser** window. The **Events Categories** window provides a notification of when new events occur. This window has a button corresponding to each of the event categories (see figure 4-1). When you click on the button that corresponds to a specific event category, a window listing the events for that specific category appears. These windows are **Event Browser** windows.

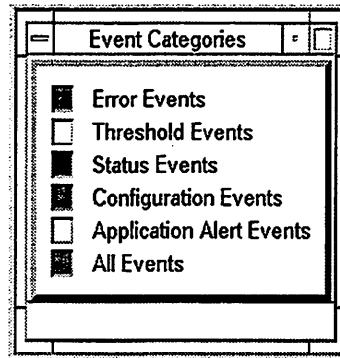


Figure 4-1. Event Categories Window

Purpose of this Task

When a button in the **Event Categories** window changes color, it is an indication that an event occurred on the network which relates to that category. The color of the button indicates the highest severity event in the category. This task provides steps on how to view and delete events from this window. The default categories included in the **Event Categories** window are

- **Error Events.** This indicates an inconsistent or unexpected behavior occurred.
- **Threshold Events.** This indicates that a threshold was exceeded.
- **Status Events.** This indicates an object or interface status changed to up or down, or an object or interface started or stopped responding to ICMP echo requests.
- **Configuration Events.** This indicates a node's configuration changed.
- **Application Alert Events.** This indicates an HP OpenView Windows application generated an alarm or alert.
- **All Events.** This lists all the above events and other events in one dialog box.

Prerequisites for this Task

- In order for a node to send an event, it must support SNMP.
- In order for the "manager" to receive events, the "agent" must be configured to send the events to the designated manager.

Procedure

In this example, you are only going to look at one event category. You notice that the **Threshold Events** button is red, which indicates that a critical threshold was exceeded somewhere on the network. The following steps explain how to view and delete the events that occurred.

1. Click on the **Threshold Events** button in the **Event Categories** window. The **Threshold Events Browser** dialog box appears with a chronological listing of the threshold events that have occurred, with the most recent events at the bottom of the list. Here is an example of the listing:

```
Minor Fri Feb 28 14:12:38 busynode ifInOctets 1 threshold exceeded (>20.00): 25.00
```

Each event listed includes the severity, time the event occurred, node on which the event occurred, and a brief event message. In this example, the threshold of 20 for **ifInOctets** was exceeded. Twenty-five octets per second were measured on this node.

2. To view the node that generated the event shown in this example, select the event from the list and click on **Action-> Highlight Source on Map**.

A map will appear with the **busynode** node highlighted. At this point, you may want to select the highlighted node by clicking on it, and invoke appropriate operations from the menu bar to further diagnose and correct the situation which caused the threshold to be exceeded.

3. To delete the event, select the event (as you did in step 2) and click on **Action-> Delete-> Selected Event**. This will delete only the selected event.

If you have looked at and want to delete all events in the list, you can click on **Action-> Delete-> All Events**. This will delete all events in the list, even if they are not selected. The main reason to delete *all* events is to clear the **Threshold Events** button, so you are notified when new threshold events occur.

Once you delete an event, it does not re-appear in the **Events Browser** window. An event will appear in the **Events Browser** window of the **All Events** category and one of the other categories (for example, **Threshold Events** and **All Events**). When you delete an event in one of the **Events Browser** windows (for example, **Threshold Events**), it disappears from the **all Events Browser** window also. Even though events disappear from the **Event Browser** window, they are still stored in the **/usr/OV/log/trapd.log** or the **/usr/OV/log/trapd.log.old** files.

When you exit HP OpenView Windows (OVW), all the events that have not been deleted are saved. When you re-enter OVW

- The events that have not been deleted appear.
- All events that occurred since exiting OVW appear. For example, if a node's link address changes while OVW is not running, you will receive a configuration event for that node when you re-enter OVW.

For more information about event notification, either click on the **Help** button in the dialog box for the event that you are viewing or select **View SNMP Events** from the **Help: Index -> Task** menu item.

Monitoring for Proactive Fault Diagnosis

In monitoring a network, it is necessary to know when the health of the network is in jeopardy. Devices on the network vary in their importance to network operations, so the need and method for monitoring these devices will vary. For example, say you are managing a gateway on the network that supports communications across several networks. If the error rate of packets passing through the gateway begins to rise, you want to be notified so that you can troubleshoot the problem before it reaches a critical state.

Through the combined use of the NNM tools, such as data collection, event configuration, and application builder, you can proactively monitor your network. While the actual administration effort is minimal, the process to set up your network for proactive monitoring is dynamic and initially takes about one month to do. The setup time will vary depending on how long it takes to establish meaningful network performance data. To achieve a proactive monitoring state on your network, you need to

1. Establish baselines for normal network performance.
2. Build applications to monitor trends.
3. Set up thresholds for monitored MIB values.
4. Fine tune the thresholds.
5. Set up event-triggered actions.

The sections that follow take a closer look at each of these steps. Operation instructions for the NNM tools discussed in the following steps are provided in chapter 6, "Using Network Node Manager Operations."

Establishing Baselines for Normal Network Performance

To establish a baseline, you need to check the condition of your network over a period of time. To do this, you need to decide what it is you want to look at, then monitor it over the course of one or two weeks.

Prerequisites for this Task

The prerequisites differ depending on which NNM tool you use.

- To use the Browse MIB operation
 - You must select a node on the map before you can access the **Browse MIB** dialog box.
 - Only one device can be selected.
 - The MIB you want to browse must be preloaded into the Loaded MIB database. This is done using the **Options: Load/Unload MIBs -> SNMP...** operation.
 - The community names configured on the management station must match the community names that are configured on the agents themselves. If the community names do not match, use the **Options: SNMP Configuration...** operation to change the configuration so the manager can access agent MIB values using the correct community name.
 - If the agent is an HP OpenView SNMP Agent, you must configure the HP OpenView SNMP Agent with a specific community name before the agent can respond to SNMP SetRequests. See the *HP OpenView SNMP Agent Administrator's Reference* manual.
- To use the Data Collection operation, see the prerequisites in chapter 6, "Collecting MIB Data."

Procedure

1. Determine which system or systems you want to monitor.

For this example, you want to monitor performance on a gateway labeled **gateway1**, which has a heavy traffic load and is critical to your network.

2. Determine what data you want to monitor. Highlight the system and use the **Monitor: MIB Values -> Browse MIB: SNMP...** operation to query for the available MIB objects on the system.

After browsing the MIB tree, you decide that the information you want to monitor for **gateway1**'s performance includes inbound octets (**ifInOctets**), outbound octets (**ifOutOctets**), input errors (**ifInErrors**), and output errors (**ifOutErrors**). As shown in the following example, these MIB objects are located under the standard **mib-2** subtree.

```
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutOctets
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInErrors
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutErrors
```

3. Set up a data collection on each MIB object that you determined in step 2, for the purpose of establishing a baseline of what is normal and abnormal performance. To set up the data collection, use the **Options: Data Collection & Thresholds: SNMP...** operation.

In the **MIB Data Collection** dialog box, click on the **Add...** button. For each MIB object in the **gateway1** example, set up the data collection as follows:

- a. Click on **Apply** to save your entry and to re-enter your next selection. When you are done, click on **OK** to save the final entry and the **MIB Data Collection/Add Collection** dialog box appears.
- b. Enter **gateway1** in the **Source Name** field, and click on **Add**.
- c. Select **Store, No Threshold** as the **Collection Mode**. This allows you to collect data without setting a threshold.
- d. Set the **Polling Interval** to one hour (**1h**). More frequent polling intervals will increase the network management traffic on the network.
- e. Set the instances to **All**.

Building an Application to Monitor Trends

Build an application that will show a graph of the data being collected.

Note

An application screen for the MIB variables shown in the following example is already included in the NNM product. In this case, there is no need for you to build an application. You can use the application by selecting the **Monitor: Network Activity -> Interface: Traffic...** menu item.

Use the process provided in this section as a model to follow when you build your own application to monitor other information on the network.

Prerequisites for this Task

To use the MIB Application Builder, see the prerequisites in chapter 6, "Building MIB Applications."

Procedure

1. To build an application, use the **Options: Application Builder: SNMP...** operation.

In the **gateway1** example, set up the application as follows:

- a. In the **MIB Application Builder** dialog box, click on the **Add...** button.
- b. Enter **gateway1** in the **Application ID** field. The name you enter here must be unique.

- c. Select **Graph** for the type of application you want to build.

Note that the **Form** and **Table** options in the MIB Application Builder would not be useful in this example.

- d. Add the following MIB object identifications to the display field:

```
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInOctets  
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutOctets  
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifInErrors  
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutErrors
```

- e. Enter **Monitor: Network Activity -> Interface: Performance** as the HP OpenView Windows menu path for this application.

As a reminder, an application for the MIB objects in step d already exist under the **Monitor: Network Activity -> Interface: Traffic ...** menu item.

For more information about the MIB Application Builder, see "Building MIB Applications" in chapter 6 or click on the **Help** button in the **Add MIB Application** dialog box.

2. Using the application you built, monitor the data for a period of time. Two weeks may provide you with the data you need for trend analysis.

To monitor the data on **gateway1**, do the following:

- a. Select **gateway1** on the map.
- b. Pull down the **Monitor: Network Activity -> Interface: Performance...** menu item. A graph of the data stored for **ifInOctets**, **ifOutOctets**, **ifInErrors**, and **ifOutErrors** will appear.

You could also use the **Monitor: Network Activity -> Interface: Traffic...** operation, which already exists.

- c. Page forward and backward through the collected data over time, and analyze the patterns.

- d. Change the resolution of the data to see a more normalized trend represented. For instance, the trend for the data collected on **ifOutOctets** over an 18 hour period at five minute intervals is difficult to see because of the number of data points shown on the graph. If you change the time intervals under the **View** menu to four hours, you will see a resolution that helps to identify trends and choose appropriate thresholds.

Note

You can print copies of the graphs by selecting the HP OpenView Graph's **File: Print** menu item.

Setting Up Thresholds for Monitored MIB Values

After analyzing the trends, set a threshold on each MIB object. Once a threshold is set, an event is generated and sent to the **Event Browser** window every time the threshold is exceeded.

Prerequisites for this Task

- To use the Data Collection operation, see the prerequisites in chapter 6, "Collecting MIB Data."
- To use the Event Configuration operation, see the prerequisites in chapter 6, "Defining Actions for Events."

Procedure

1. To set up a threshold, use the **Options: Data Collection & Thresholds: SNMP...** operation.

For **gateway1**, set the thresholds as follows:

- a. Select the MIB object that you are modifying, then select **gateway1** from the collection summary.
- b. Select **Store, Check Threshold** as the **Collection Mode**. This mode continues the data collection, as well as generates an event when a threshold is exceeded.
- c. Keep the **Polling Interval** at one hour (**1h**).

- d. Use the **Trap Number 1005**.

The default trap number is **58720263**, which pertains to all threshold events that occur. If you want to customize a data collection, you can assign your own trap number, using an odd number anywhere between 1001 to 1999, as in this example. (The even numbers 1002 to 2000 are reserved for the respective rearm trap ID's, which are generated automatically.) This enables you to set up special event notifications on specific data collections.

If you do this, you must keep records of which customized trap ID's are assigned to which data collections. Also, it is important that you format an event for both the customized trap ID and the rearm trap ID, or the messages you receive in the **Events Browser** window will not be useful. This is done using the **Options: Event Configuration: SNMP...** operation.

Note that the actions you configure for a trap ID will affect all other events registered under that same trap ID.

- e. For **ifInOctets** and **ifOutOctets**, set the **Threshold** to **40** and the **Rearm** to **10**, and select **Percent**. For **ifInErrors** and **ifOutErrors**, set the **Threshold** to **60** and the **Rearm** to **30**, and select **Absolute**.

To explain the **percent** radio button using **ifInOctets** as the example, setting the threshold to 40 and the rearm to 10 *Percent* means that you will receive an event when the number of inbound octets to **gateway1** exceeds 40, during a given polling interval. A rearm event will be generated if the value drops below 10 percent of 40 (that is, 4), at a subsequent polling interval. Another threshold event will not be generated until the rearm event occurs and the collected value again exceeds the **Threshold** value.

If you select the **Absolute** radio button and use **ifInOctets** as the example, setting the threshold to 40 and the rearm to an *Absolute* value of 10 means that you will receive an event when the number of inbound octets that contained errors on **gateway1** exceeds 40. A rearm event will be generated if the value drops below 10. Another threshold event will not be generated until the rearm event occurs and the collected value again exceeds the **Threshold** value.

Counters are computed by calculating the change per second in the sampled values. The data stored for Gauge, INTEGER, IPAddress, and TimeTicks are the actual sampled values. MIB Expressions are computed by rate of change when the Expression includes a counter. Otherwise, MIB Expressions are computed by sampled values. For more information, see chapter 6, "Defining Thresholds."

f. Figure 4-4 shows how the rearm value affects event generation.

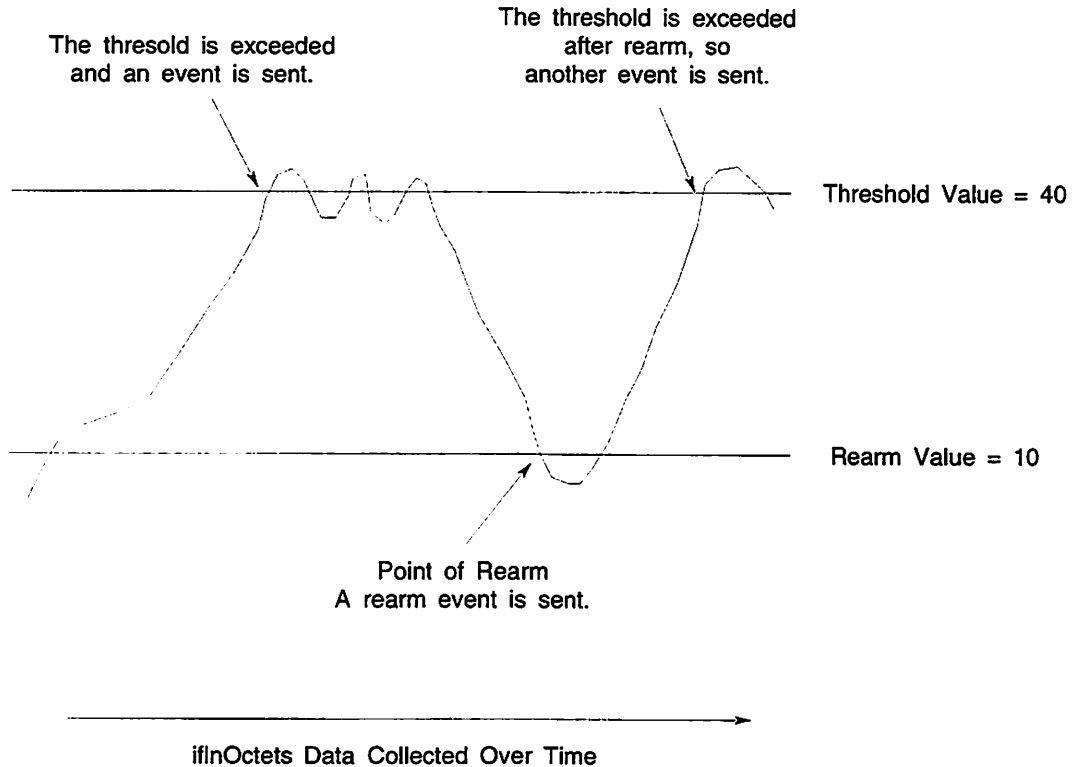


Figure 4-4. Affects of Rearm in Event Generation

2. To format the event notification message for this threshold, use the **Options: Event Configuration: SNMP...** operation. Whenever the threshold is exceeded, this message appears in the **Events Browser** window and is stored in the `/usr/OV/log/trapd.log` file or the `/usr/OV/log/trapd.log.old` file.

In the **gateway1** example, format the message for the **1005** trap number as follows:

- a. Select **OpenView** under the **Enterprise Name**.

You select **OpenView** because all data collection trap identifications are registered under and generated by **OpenView** from the management station.

- b. Click on **Add** from the Event Identification section (second section).

- c. Type in the name of the event in the **Event Name** field.
- d. Make sure the **Generic Trap** is set to **Enterprise Specific**.
- e. Enter a **Specific Trap Number** of 1005.
- f. Leave the **Source** field blank to indicate all sources.
- g. Select **Threshold Events** under **Event Category**.
- h. Set the **Severity** to **Major**.
- i. Enter the message **Specific trap #\$\$ received** in the **Event Log Message** field.

When an event is generated for **gateway1** under the 1005 trap identification, the following message will be sent to the **Event Browser** dialog box:

Specific trap #1005 received.

For information about other possible formats, click on the dialog box **Help** button.

- j. Click on **OK**, to enter the new event log format.
 - k. Click on **OK**, to apply the new event log format.
 - l. Format the rearm event notification message by repeating step a through step f, only enter 1006 for the **Specific Trap Number**.
3. Periodically check the **Events Browser** window to see if the threshold is exceeded. Also, use the application you built to monitor the trends of the MIB objects on which you are collecting data.

When the threshold is exceeded, you may need to take action regarding the problem, as described in the **Events Browser** window. You may discover that no problem exists, because the threshold was not set to a value that provides good feedback for fault diagnosis. See "Fine Tuning Threshold Monitoring."

Fine Tuning Threshold Monitoring

You need to monitor the threshold for a period of time to ensure you set up the appropriate values. If you are receiving several threshold events a day without any loss in the network performance, then you may want to reset the threshold and rearm values.

Prerequisites for this Task

To use the Data Collection operation, see the prerequisites in chapter 6, "Collecting MIB Data."

Procedure

1. On the map, select **gateway1**.
2. Pull down the **Monitor: Network Activity -> Interface -> Performance** menu item, and analyze the trends.
3. Determine if you need to adjust the threshold and rearm values. If so, go to the **Options: Data Collection & Thresholds -> SNMP** operation to adjust the values.
4. Optionally, once you have fine tuned the threshold settings, you may want to turn off the data storage function, but continue to check for thresholds. To do this, set the data collection mode to **Don't Store, Check Thresholds**.

Setting Up Event-Triggered Actions

When threshold settings are stable, you can set up an action to occur when one of the threshold values is exceeded. Setting up an action can range from having a message appear in a pop-up window to having a hand-held beeper alert you about the exceeded threshold. Also, you can set up an action that invokes a script which performs automatic fault recovery. This is how you can take advantage of HP OpenView Network Node Manager's proactive monitoring capabilities.

The example provided in this section is a simple **mail** command to illustrate this concept.

Prerequisites for this Task

To use the Event Configuration operation, see the prerequisites in chapter 6, "Defining Actions for Events."

Procedure

1. To set up an action to an event, use the **Options: Event Configuration -> SNMP...** operation.

In the **gateway1** example, cause a pop-up window to appear as follows:

- a. Select the **OpenView** enterprise name and the specific trap identification **1005**. The trap ID that you choose here must be the same trap ID that you set up in data collection. The trap ID **1005**, which you set up in the data collection, is registered under the **OpenView** enterprise name.
- b. Click on **Add** from the **Eventification Identification** section (second section).
- c. In the optional **Popup Notification** field, type the following:

A performance value on \$3 has been exceeded.

- d. Create the following script in **/usr/local/bin/mailevent**, which will send a message to root at the corporate office:

```
MSG=$1
TO=$2
echo "${MSG}" | /usr/lib/sendmail "${TO}"
```

Type the following command in the optional **Command** field:

```
/usr/local/bin/mailevent "A trap received from $E with $# args:\n$" "root@corp"
```

Note that the actions that you configure in the optional **Command** field will affect all events registered under the same trap ID number (in this case, **Generic 6** and **Specific 1005**). The four MIB objects that you set up with the **1005** trap ID will invoke the same actions defined here. If you want to set up a different action for a MIB object, you need to specify a different trap ID in the Data Collector and use that trap ID here in the Event Configuration operation or set the source to match that node.

2. When you receive notification about an exceeded threshold, you can use the application you built, as well as other applications in NNM, to view the trend and diagnose the problem. At this point, it may be necessary to make changes to the network to improve performance, such as rerouting traffic through a different gateway.

Note that you may also set up an action for the rearm event (in this example, **1006**).

Diagnosing Network Communication Problems

Diagnosing network problems can be time consuming and difficult, especially in complex network environments. Many variables affect the process used to diagnose problems on the network. For example:

- How large is the network?
- What type of systems are on the network?
- Where do the systems reside?
- Are there bridges on the network?
- Are there gateways and routers involved?

Diagnosing Network Connectivity Problems

In the situation of a network connectivity problem, a user is unable to contact a system on the local network or on another network.

Purpose of this Task

In this task, a process for isolating network connectivity problems is provided, along with the NNM tools that can help you at each step along the way. The process you use in your particular environment will most likely be different than the one shown here. This is only a guideline showing you which NNM tools you can use to troubleshoot connectivity problems. The procedures included in this section include:

- diagnosing connectivity within the same network
- diagnosing connectivity across networks

Diagnosing Connectivity within the Same Network

Use this procedure when a user is having problems connecting from one system to another system within the same network.

Prerequisites for this Task

- To do a **Ping**, select only one node on the map.
- To do a **Remote Ping**
 - Select two nodes, a source node and a destination node.
 - The source node selected must be an HP-UX, SunOS, or Solaris system running the HP OpenView SNMP Agent software.
- To connect to a node via **telnet**, the remote node must have ARPA Services running.
- To do an **ARP Cache**, the selected node must support SNMP.

Procedure

In this example, a user cannot connect from System A to System B on the same network.
See figure 5-1.

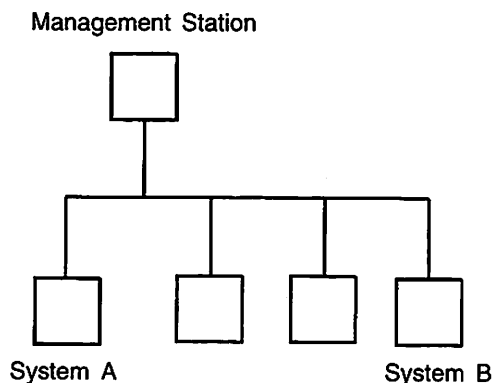


Figure 5-1. Connectivity within the Same Network

1. Look at the color status of System B on the map. If it is red, System B is down. If it is not red, go to step 2.
2. Check to see if System A and System B are operational.

Use the **Diagnose: Network Connectivity -> Ping...** operation to do a ping from the management station to System A and System B.

If the ping to either system fails, check to see if the system is down. If the ping to both systems is successful, go to step 3.

3. Rule out a hostname-to-IP address mapping problem.

On the map, select System A then System B. Use the **Diagnose: Network Connectivity -> Remote Ping...** operation to do a remote ping, from System A to System B. If it fails, go to step 4. If it passes, you may have a hostname-to-IP address mapping problem. To verify and fix the problem, do the following:

- a. Select System A, and connect to it using the **Misc: Terminal Connect -> Telnet (xterm)** operation. Type in `nslookup` with System B's host name to see which IP address-to-hostname mapping service System B is using and what System B's IP address is, according to System A. If the BIND name server is not running on the network, enter full domain name. For example:
`nslookup systemB.dept.site.com`

- b. On the management station, open a terminal window and do an **nslookup** with System B's host name. The response should be the same as the response you received in the previous step.
4. Rule out an IP address-to-link address mapping problem.

On the map, select the management station and System A. Use the **Monitor: Network Configuration -> ARP Cache...** operation to view the ARP Cache tables for the management station and for System A. Do the following:

- a. Locate System B's IP address in both tables, then compare the **Link Address** for System B.
- b. If System A's link address for System B is not the same as the management station, fix System B's link-level address on System A. If they are the same, you may not have a connectivity problem, but rather a performance or network service problems. Go to the appropriate sections to diagnose these problems.

Diagnosing Connectivity across Networks

Use this procedure when a user is having connectivity problems from a system on one network to a system on a different network.

Prerequisites for this Task

- To do a **Ping**, select only one node on the map.
- To do a **Locate Route**
 - Select two nodes, a source node and a destination node.
 - All nodes along the route, except the destination node, must be running SNMP.
 - All gateways between the selected nodes must have their community names correctly set. For information about setting community names, select **Configuring SNMP** from the **Help: Index -> Tasks** menu item or see the *HP OpenView Network Node Manager's Administrator's Reference* manual.

Procedure

In this example, a user is trying to connect from System B on Network 1 to System C on Network 2. The path between the two networks includes two gateways, Gateway 1 and Gateway 2. See figure 5-2.

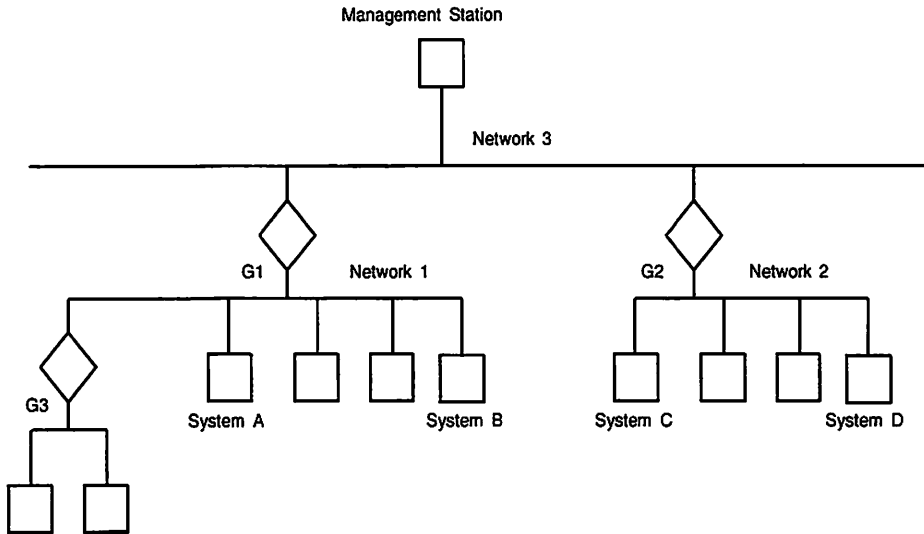


Figure 5-2. Connectivity Across Networks

1. Look at the color status of System C on the map. If it is red, System C is down. If it is not red, go to step 2.
2. Check connectivity to System C.

Use the **Diagnose: Network Connectivity -> Ping...** operation to do a ping from the management station to System C. If the ping is successful, go to step 3. If the ping fails

- a. Do a ping from the management station to G2.
- b. If the ping is successful, go to step 3. If the ping fails, G2 is down.

3. Check connectivity to System B.

Use the **Diagnose: Network Connectivity -> Ping...** operation to do a ping from the management station to System B. If the ping is successful, go to step 4. If the ping fails

- a. Do a ping from the management station to G1.
- b. If the ping is successful, go to step 4. If the ping fails, G1 is down.

4. Find the route between the systems and all intermediate objects between them.

On the map, select System B then System C. Use the **Diagnose: Network Connectivity -> Locate Route: via SNMP...** operation.

5. Look at the map to verify that the highlighted path is correct. For example, in figure 5-2, let us say the route led to G3 rather than G1 and G2. In this case, System B's routing table is incorrect.

If the route is on a single submap, the route should be easy to observe. If the route is not completely visible from a single submap, you can open other submaps along the path. However, it may be easier to use the **Locate Route** dialog box to verify the **Next Hop** host names and IP addresses.

6. Look at the map to verify that all nodes along the correct path are up. A node with a yellow or red status indicates that the node either has a problem or is down. If a node is yellow or red, you need to diagnose the problem on that node.

7. If the route is correct and everything is up along the path, the problem may not be related to connectivity, but rather performance or network services. Go to the appropriate sections to diagnose these problems.

Diagnosing Network Performance Problems

An indication of a network performance problem is slow system response, which could be caused by a traffic overload on the network or an unhealthy device, or lost data during transmission, which could be the result of an overloaded network or device with such slow transmissions that services or applications are timing out.

Purpose

This task provides a process to follow to diagnose problems related to the network performance.

Prerequisites for this Task

- The originating node can reach the destination node without losing a connection.
- To do a **Locate Route**
 - Select two nodes, a source node and a destination node.
 - All gateways between the selected nodes must have their community names correctly set. For information about setting community names, select **Configuring SNMP** from the **Help: Index -> Tasks** menu item or see the *HP OpenView Network Node Manager Administrator's Reference* manual.
- To do a **Remote Ping**
 - Select two nodes, a source node and a destination node.
 - The source node selected must be an HP-UX, SunOS, or Solaris system running the HP OpenView SNMP Agent software.
- To use the **Monitor: System Activity -> CPU Load...** operation, the selected node must be an HP-UX, Sun, or Solaris system running the HP OpenView SNMP Agent software.
- To view **Interfaces or Interface Traffic** on a selected node, the node must support SNMP.

Procedure

In the following example, the user was experiencing unusually slow response time trying to communicate from System B on Network 1 to System C on Network 2. From the Management Station, let us say you know that the response time on Network 3, where System E resides, is normal. In this example, System A and System B are on the same network (Network 1); System D, which has relatively low usage, and System C are on the same network (Network 2); two gateways exist between System B and System C: G1 for Network 1 and G2 for Network 2. Also, in this example, all networks are Ethernet. See figure 5-3.

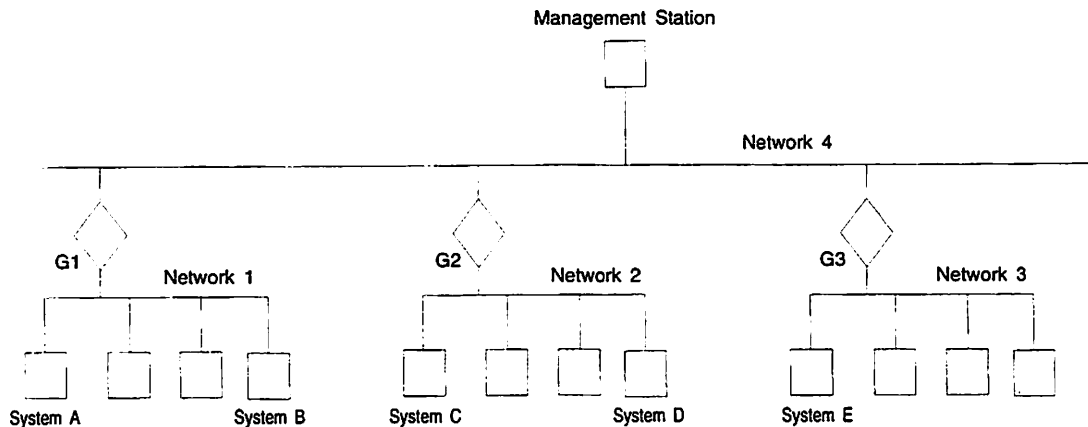


Figure 5-3. Performance Across Networks

1. On the map, select System B then System C. Use the **Diagnose: Network Connectivity -> Locate Route...** operation to find the route between the systems and all intermediate objects between them. In this example, the route is B to G1, G1 to G2, and G2 to C.
2. Use the **Diagnose: Network Connectivity -> Remote Ping...** operation to do remote pings from B to C, B to E, B to D, and A to C. Make a note of the response times on these remote pings, then diagnose the problem as follows:
 - If the response time from B to C, B to D, and A to C is slower than the response time from B to E, then you have a network problem. Go to step 3.
 - If the response time from B to C and A to C is slower than the response time from B to E and B to D, then System C's CPU (Central Processing Unit) is overloaded. Select System C, and use the **Monitor: System Activity -> CPU Load...** operation to verify. If so, reduce System C's CPU load (for example, kill some processes or have users log off the system).

- If the response time from B to C, B to E, and B to D is similar but slower than the response time from A to C, then System B's CPU is overloaded. Select System B, and use the **Monitor: System Activity -> CPU Load...** operation to verify. If so, reduce System B's CPU load (for example, kill some processes or have users log off the system).
3. In this step, you have established that you have a network problem verses a system problem. Use the **Diagnose: Network Connectivity -> Remote Ping...** operation to do remote pings from B to G1, G1 to G2, and G2 to C. Make a note of the response times on these remote pings, then diagnose the problem as follows:
- If the response time from B to G1 is faster than the response time from G1 to G2 and G2 to C, then check the traffic on G2 (step 4).
 - If the response time from G2 to C is faster than the response time from B to G1 and G1 to G2, then check the traffic on G1 (step 4).
 - If the response time from G1 to G2 is slower than the response time from B to G1 and G2 to C, then the problem resides between G1 and G2. You may need to set up a different route, subnet, or gateway on your network.
4. On the map, select the gateway with the problem. Use the **Monitor: Network Activity -> Interface: Traffic ...** operation to see trends of the interface traffic in a graphic presentation. Use the **Monitor: Network Configuration -> Interfaces...** operation to see a snapshot of the interface data in a tabular presentation. If input and output data on interface traffic is abnormally high, you may have a routing problem, an overloaded interface, or an overloaded gateway.

Diagnosing Network Service Problems

In the situation of a network service problem, you have reached System B from System A, but either the connection from System B is refused or the command you are trying to execute from System A to System B is not accepted.

Purpose of this Task

The task provides a process to follow to diagnose problems related to the network services.

Prerequisites for this Task

- To view the **IP** / **TCP** / **SNMP** protocols and **Services** available on a selected node, the node must support SNMP.
- The originating node can reach the destination node without losing a connection.
- You must be superuser of a node to install to it, configure it, or change its permissions.
- To use **HP-UX SAM** on a selected node, the node must be a HP-UX system, version 7.0 or later, and have the `/usr/bin/sam` application installed.

Procedure

In the following example, a user was trying to use a network service (for example, **ftp**, **rcp**, or **nfs**) from System A to System B and received an error message. See figure 5-4.

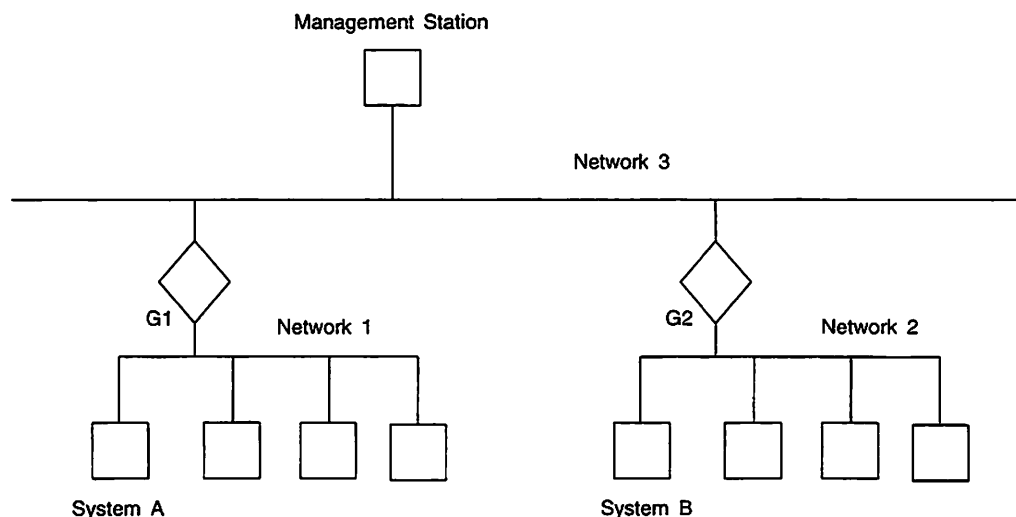


Figure 5-4. Diagnosing Network Services

1. Use the **Diagnose: Network Connectivity -> IP / TCP / SNMP...** operation on both System A and System B to make sure they both support the network protocols and that the protocols are working.

If there are problems with the protocol, an error will appear in the messages field.

2. Use the **Monitor: Network Configuration -> Services...** operation on both System A and System B to make sure they both support the service in question (for example, **ftp**). If they do, go to step 3. If not, do the following:
 - a. Check the file system on the two systems to see if the software for the service (for example, ARPA Services) is installed. If not, you will have to install the software on the system. If the service software is installed, go to step b.
 - b. Configure the service (for example, ARPA Services) on the system.

For HP-UX systems using SAM (System Administration Manager), use the **Administer: System Management -> HP-UX SAM...** menu item to access the SAM tool to configure the service. In SAM, this is located under **Networks and Communications**.

- c. Skip step 3 and go to step 4.
3. Check service security on System B. Make sure the IP address of System A is set for "allow access" and not excluded by a "deny access" in the security files for the service in question (for example, `/usr/adm/inetd.sec` and `/etc/ftpusers`).

For HP-UX systems using SAM, use the **Administer: System Management** -> **HP-UX SAM...** menu item to access the SAM tool to configure the service security. In SAM, this is located under **Networks and Communications**.

4. Try to use the service again, from System A to System B, to verify that the problem is fixed.

Using Network Node Manager Operations

The previous chapters in this user's guide provide information about how you apply the HP OpenView Network Node Manager (NNM) product in a network environment. This chapter provides task-oriented operational steps for using NNM. It goes into greater detail about the dialog box fields that you use to accomplish certain tasks.

The tasks covered in this chapter include:

- loading MIBs
- viewing MIB values
- setting MIB values
- collecting MIB data
- defining thresholds
- viewing historical trends
- building MIB applications
- defining actions for events
- taking snapshots of the IP Map

Loading MIBs

In order to manage a device (or agent) with NNM, it must be running the Simple Network Management Protocol (SNMP). If the device has an enterprise-specific MIB, its MIB must be loaded. NNM is shipped with certain MIBs already loaded (for example, **rfc1213-MIB-II** and **hp-unix**). However, NNM provides a tool that enables you to load multivendor enterprise-specific MIBs or newly released standard MIBs into the MIB database.

Purpose of this Operation

This task explains how to set up a new network device in NNM, which involves loading the enterprise-specific MIB into the MIB database. Once the MIB is loaded, you can monitor the state of the device and customize NNM to proactively manage the device.

You can follow the same procedure in this task to load new MIB standards that emerge in the industry.

Prerequisites for this Operation

- A new device must be installed on the network according to the installation instructions provided by the vendor.
- You must obtain a copy of the MIB definition file from the vendor.
- Copy the MIB definition file to a directory on the management system running the HP OpenView software. To make it easy to keep track of your MIB definitions, copy the new MIB to the default MIB directory `/usr/ov/snmp_mibs`.
- If you have unloaded all the MIBs in the MIB description file, it is recommended that you load MIB-I or MIB-II before you load an enterprise-specific MIB.
- The MIB must conform to RFC 1155 or RFC 1212.
- Ensure the MIB for the device is the most current copy.

Note

If the MIB is not the most current copy, contact the device vendor.

Procedure

In the following example, you want to set up a Proteon device to be managed by NNM.

1. Select the **Options: Load/Unload MIBs: SNMP...** menu item; the **MIB Load/Unload MIBs** dialog box appears, listing the MIBs currently loaded.
2. Click on the **Load** button. The **Load MIB From File** dialog box appears, listing the files in the default directory.
3. Select the **/usr/OV/snmp_mibs/proteon** file from the scrollable list, then click on **OK**. The MIB is automatically loaded and the **MIB Load/Unload MIBs** dialog box reappears.

Note

If the enterprise-specific MIB that you want to load is located in a different directory than **/usr/OV/snmp_mibs**, you can enter the full path name of the file containing the enterprise-specific MIB in the field labeled **MIB File to Load**.

4. The **proteon** MIB is now included in the **Loaded MIBs** scrollable list. You can use the **Monitor: MIB Values -> Browse MIB: SNMP...** operation to view the MIB objects provided with the Proteon device.

If a MIB does not load properly, you will receive an error message. The problem could be related to

- The vendor's MIB. For example, the vendor's MIB is not the most current version for the vendor's device that is on the network. In this case, call the vendor to get the most current MIB version for the device.
- The NNM MIB compiler. In this case, call your support representative.

5. Click on the **Close** button to exit this operation.

For more information about this operation, and information about unloading MIBs, click on the dialog box **Help** button.

Viewing MIB Values

This operation allows you to view MIB values for a selected node.

Prerequisites for this Operation

The selected node for which you want to view MIB values must support SNMP.

Procedure

1. Select the desired node in the OVW map.
2. From the menu bar, select **Monitor: MIB Values -> Browse MIB: SNMP...** and the **Browse MIB** dialog box appears.
3. Specify the MIB object for which you want to view the MIB values. You can specify the **MIB Object ID** by doing *one* of the following:
 - Type in or paste the **MIB object ID** in the **MIB Object ID** field.
 - Select the desired MIB object by moving up or down the MIB tree.

To move down the MIB Tree

 - a. Select the desired component from the **MIB Object ID** selection list.
 - b. Click on **Down Tree** or double click on the component; the **MIB Object ID** field is updated with the selected component, and your location in the MIB tree descends to the next lower level.

Continue this sequence of moving down the MIB tree until you have specified the MIB object on which you want to perform your SNMP request.

To move back up the MIB Tree, click on **Up Tree**.

Optionally, you can query specific instances by specifying the full MIB object ID and then specify the instance in the **MIB Instance** field.
4. Query the MIB object by clicking on **Start Query**; the results are displayed in the **MIB Values** area.

To stop a query, click on **Stop Query**.

Related Topics

For more information related to viewing MIBs

- Click on the **Help** button in the dialog box.
- Go to the **Help: Index -> Functions** menu item and select **Monitor: MIB Values -> Browse MIB: SNMP...**
- See the "Setting MIB Values" section in this chapter.

Setting MIB Values

This operation allows you to set MIB values for selected nodes.

Prerequisites for this Operation

- The selected nodes on which you want to set MIB values must support SNMP.
- The agent must be configured to respond to SNMP SetRequests.
- You must know the agent's community name.

Procedure 1: Setting Values Using the Query Function

The following procedure provides an overview of the steps involved in setting MIB values.

1. Select the desired node in the OVW map.
2. From the menu bar, select **Monitor: MIB Values -> Browse MIB: SNMP...** and the **Browse MIB** dialog box appears.
3. Specify the **MIB Object ID** for which you want to set the MIB value.

You can specify the MIB Object ID by doing *one* of the following:

- Type in or paste the MIB object ID in the **MIB Object ID** field.
- Select the desired MIB object by moving up or down the MIB tree. To move down the MIB tree.
 - a. Select the desired component from the **MIB Object ID** selection list.
 - b. Click on **Down Tree** or double-click on the component; the **MIB Object ID** field is updated with the selected component, and your location in the MIB tree descends to the next lower level.

Continue this sequence of moving down the MIB tree until you have specified the MIB object on which you want to perform your SNMP request.

To move back up the MIB tree, click on **Up Tree**.

4. Query the MIB object by clicking on **Start Query**; the results are displayed in the **MIB Values** area.

5. Select the MIB value you want to change from the **MIB Values** area; the current value is displayed in the **SNMP Set Value** field.
6. Type in the new value for the object in the **SNMP Set Value** field.
7. Click on **Set**. Note that the value on the agent changes as soon as you click on **Set**. However, you may not see the changes on the map until the management system has done the appropriate polling. If you want to see the changes on that node right away, select the **Diagnose: Network Connectivity -> Demand Poll...** menu item.

The message area will indicate the success or failure of the operation. Many devices require a different community name for "sets" than for "queries."

Procedure 2: Setting Values Directly (Without Querying)

Alternatively, you can set a MIB object directly without having to first query the object. To modify a MIB value directly, do the following:

1. Select the desired node in the OVW map.
2. From the menu bar, select **Monitor: MIB Values -> Browse MIB: SNMP...** and the **Browse MIB** dialog box appears.
3. Specify the **MIB Object ID** for which you want to set the MIB value.
4. Enter the instance identifier for the object in the **MIB Instance** field.
5. Type in the new value for the object in the **SNMP Set Value** field.
6. Click on **Set**. Note that the value on the agent changes as soon as you click on **Set**. However, you may not see the changes on the map until the management system has done the appropriate polling. If you want to see the changes on that node right away, select the **Diagnose: Network Connectivity -> Demand Poll...** menu item.

The message area will indicate the success or failure of the operation. Many devices require a different community name for "sets" than for "queries."

Related Topics

For more information about setting MIB values

- Click on the **Help** button in the dialog box.
- Go to the **Help: Index -> Functions** menu item and select **Monitor: MIB Values -> Browse MIB: SNMP....**
- See the "Viewing MIB Values" section of this chapter.

Collecting MIB Data

This operation allows you to collect MIB data from network nodes at regular intervals and save the collected MIB data.

Prerequisites for this Operation

- The node for which you want to collect data must support SNMP.
- Make sure the enterprise-specific MIB for which you want to collect data is loaded into the Loaded MIB database. (The **Options: Load/Unload MIBs: SNMP...** operation lists all MIB modules currently in the MIB description file.) If the enterprise-specific MIB is not loaded, see "Loading MIBs" in this chapter.
- You can only collect data or monitor thresholds on numeric MIB values; that is, the MIB objects that are defined Counter, Gauge, INTEGER, IPAddress, and TimeTicks.
- Make sure you understand the definitions of and purpose for the MIBs on which you want to collect data.

Most device vendors include documentation about their enterprise-specific MIB with their product. This documentation typically describes the MIB object and what the objects mean. In addition, some vendors include overview information describing strategies for how to manage their specific device. The vendor documentation can give you the conceptual understanding that you need to configure your system to collect MIB data.

- Ensure there is enough room to store the data in the directory `/usr/OV/databases/snmpCollect`. If necessary, symbolically link it to another file system. The amount of disk space required depends on how much data you collect.

Procedure

The following procedure provides an overview of the steps involved in collecting MIB data.

1. From the menu bar, select **Options: Data Collection & Thresholds: SNMP...** and the **MIB Data Collection** dialog box appears.
2. Click on **Add** from the **MIB Objects Configured for Collection** section (first section); the **MIB Data Collection/MIB Object Selection** dialog box appears.
3. Specify whether you want to collect data on a MIB object or on an expression by clicking on the radio button corresponding to your selection. The default is MIB object.

4. If you are collecting data on a MIB object, specify the **MIB object ID** for which you want to collect data.

If you are collecting data on an expression, select the item from the **Expression ID** selection list.

You can specify the MIB object ID by doing *one* of the following:

- Type in or paste the full MIB object ID in the **MIB Object ID** field.
- Move up and down the MIB tree by selecting items from the list box under **MIB Object ID**.

To move down the MIB tree

- a. Select the desired component from the **MIB Object ID** selection list.
- b. Click on **Down Tree** or double-click on the component; the **MIB Object ID** field is updated with the selected component, and your location in the MIB tree descends to the next lower level.
- c. Continue this sequence of moving down the MIB tree until you have specified the full object ID, that is, a leaf node.

To move back up the MIB tree, click on **Up Tree**.

5. Enter the label. The label defaults to the last component of the MIB mnemonic name. The label is used as the filename with an instance appended to it. This is where the data will be stored and therefore the label must conform to UNIX filename conventions.
6. Click on **OK**; the MIB object ID is added to the list of configured MIBs and the **MIB Data Collection/Add Collection** dialog box appears.

Add the source name. When you add a source name, the name appears in the **List of Collection Sources** selection list area.

7. Specify the collection mode by choosing one option from the **Collection Mode** option menu.
8. Specify the polling interval.

The polling interval determines how often the program will collect data from the source. To specify a polling interval, enter a positive real number followed by an "s," "m," "h," or "w" indicating seconds, minutes, hours, or weeks, respectively. If you do not enter a letter, the data collector uses the default of seconds. For example:

1.5h = one and a half hours
30 = 30 seconds

9. Optionally, if you set the collection mode to check thresholds, enter a **Trap Number**.

The default trap number is **58720263**. Optionally, you can use odd numbers from 1001 to 1999 for the trap ID, which enables you to configure the manager to take special action for a particular threshold. For more information, see "Defining Thresholds" later in this chapter.

10. Optionally, if you set the collection mode to check thresholds, enter **Threshold** and **Rearm** values.

When a collected value exceeds the threshold value, the data collector generates an event. To avoid continuously generating events, specify an appropriate rearm value. When a MIB value drops below or is equal to the rearm value, a rearm event is generated. Another threshold event will not be generated until the rearm event occurs and the value again exceeds the threshold value.

You can specify the rearm value either as a **Percent** of the threshold value or as an **Absolute** number. Counters are computed by calculating the change per second in the sampled values. The data for Gauge, INTEGER, IPAddress, and TimeTicks are the actual sampled values. MIB Expressions are computed by rate of change when the Expression includes a counter. Otherwise, MIB Expressions are computed by sampled values.

For example, suppose you want to monitor CPU load averages on an HP 9000, Sun SPARCstation, or Solaris system running the HP OpenView SNMP Agent software. You can set a **Threshold** of **200** and an **Absolute Rearm** value of **150**. When the data collector detects a value above 200, a threshold event is generated. Another threshold event will be generated only if the reading drops below 150 (sending a rearm event) and then goes above 200 again.

11. Click on **OK**; the **MIB Data Collection/Add Collection** dialog box disappears and the MIB object is added to the **MIB Objects Configured for Collection** selection list in the **MIB Data Collection** dialog box.

12. Specify on which instance of the MIB object you want to collect data.

If you do not know the instance of a MIB object on a device, use the **Browse MIB** operation to find out what the instance is as follows:

13. Click on **Apply** or **OK** for the changes to take effect.

To cancel all changes and exit the dialog box, click on **Cancel**. This will cancel all changes from the last **Apply** or, if you have not applied any changes since entering the dialog box, it cancels all changes from the time you entered the dialog box.

Note

Data collection is restarted each time you click on **Apply**, which means that polling is interrupted. For example, suppose you have set polling intervals to 1 hour on a MIB object. When you click on **Apply**, the data collector starts polling even if the last polling took place only 5 minutes ago. Clicking on **Apply** several times will increase network traffic and store more data than you might have intended.

The procedure to configure your system to collect MIB data is done. The collected data are stored in the `/usr/OV/databases/snmpCollect` directory, in the filenames defined in step 5 of this procedure.

Related Topics

For more information related to collecting data

- Click on the **Help** button in the dialog box.
- Go to the **Help: Index -> Functions** menu item and select **Options: Data Collection & Thresholds: SNMP...**
- See the "Defining Thresholds" section of this chapter.
- See the "MIBs" section in chapter 1.
- See the *RFC 1155: Structure and Identification of Management Information for TCP/IP-based Internets*.
- See the *RFC 1213: Management Information Base for Network Management of TCP/IP-based internets: MIB-II*.



Defining Thresholds

This operation allows you to define thresholds for collected data and generate events when the specified thresholds are exceeded.

Prerequisites for this Operation

- The node for which you want to collect data must support SNMP.
- You can only collect data or monitor thresholds on numeric MIB values; that is, the MIB objects that are defined as INTEGER, IpAddress, Counter, Gauge, and TimeTicks. or the results of an Expression.

Procedure

The following procedure provides an overview of the steps involved in defining thresholds.

- 
1. From the menu bar, select **Options: Data Collection & Thresholds: SNMP...** and the **MIB Data Collection** dialog box appears.
 2. Select the item from the **MIB Objects Configured for Collection** selection list for which you want to set thresholds; the details for that item appear in the middle section of the dialog box, **MIB Object Collection Summary**.
 3. Select the source from the **MIB Object Collection Summary** list; the configuration details for that source appear in the bottom section of the dialog box, **Collection Details**.
 4. Select *one* of the following menu items from the option menu next to the **Collection Mode** label:
 - **Don't Store, Check Thresholds**
 - **Store, Check Thresholds**The **Threshold** and **Rearm** fields are un-greyed.
 5. Specify a **Polling Interval**.
- 

6. Specify a Trap Number.

The default trap number, **58720263**, is the enterprise-specific trap that the Data Collector sends when a threshold or a rearm value is exceeded. The Data Collector sends the trap using the **OpenView** enterprise ID. The default trap is logged in the **Threshold Events Browser** dialog box.

Using the default trap number may not meet all of your data collection needs. For example, maybe some of the threshold values you monitor are more critical than others. In this case, you can configure the manager to take special action on traps for that particular threshold. For example, you may want to configure the manager to send a mail message when it receives the trap.

To configure NNM to take special action when a specific threshold event occurs, use the optional trap numbers which are odd numbers ranging from 1001 to 1999. (The even numbers from 1002 to 2000 are reserved for rearm trap ID's of their respective trap numbers. For example, the threshold trap ID 1005 will have a rearm trap ID of 1006. These rearm trap IDs are automatically assigned in NNM.) If you use one of the optional trap numbers, you must configure events for both the threshold and rearm trap ID's. Configuring events is covered later on in this procedure.

Note

Make sure to write down the trap numbers from 1001 to 1999 that you add. You need to know the trap numbers when you configure the new trap using the Event Configuration operation.

7. Enter the threshold value in the **Threshold** field.

Use this field when you want to be notified of data patterns that are outside the normal expectations. When the threshold value is passed, the specified threshold event is generated, and the **Event Categories** window notifies you accordingly.

8. Optionally, enter a rearm value in the **Rearm** field. You can specify the rearm value as either a **Percent** of the threshold value or an **Absolute** number, using the toggle buttons to the right of the **Rearm** field.

The rearm value controls the frequency of threshold events generated. To avoid continuously generating events, specify an appropriate rearm value. When a MIB value drops below or is equal to the rearm value, a rearm event is generated. Another threshold event will not be generated until the rearm event occurs and the collected value again exceeds the **Threshold** value.

If you selected the **Percent** button, enter a whole or fractional number from 0 to 100.

If you selected the **Absolute** button, enter a whole or fractional number.

9. Click on **Apply** or **OK** to set this threshold and to prepare to set another threshold. Click on **OK** when all thresholds are set.
10. Now that the threshold value is set, and events are being sent to the **Threshold Events Browser** dialog box, you may find that the default event notification message does not give you enough information about the event. If this is the case, you can customize the event notification message using the **Options: Event Configuration: SNMP...** menu item. To customize the default event.

Note

If you assigned a trap number from 1001 to 1999 in the MIB Data Collection operation, then you must configure an event for both the threshold and rearm trap IDs. If you do not do this, the event messages you receive about those traps will not make sense, and the rearm event will generate an error stating that the trap has an undefined format.

- a. In the **Event Configuration** dialog box, select the **OpenView** enterprise; all events defined for the **OpenView** enterprise are displayed in the **Event Identification** selection list.
- b. Scroll through the **Event Identification** selection list until you find the event **Specific 58720263**.
- c. Edit as appropriate by following the help information in the **Event Configuration** dialog box.

Related Topics

For more information related to defining thresholds

- Click on the **Help** button in the dialog box.
- Go to the **Help: Index -> Functions** menu item and select **Options: Data Collection & Thresholds -> SNMP....**
- See the "Collecting MIB Data" section of this chapter.

Viewing Historical Trends

This operation allows you to view previously collected data and manipulate that data to determine trends.

Prerequisites for this Operation

Data collection must have been started on the selected nodes using the **Options: Data Collection & Thresholds: SNMP...** menu item.

Procedure

1. Select the desired nodes in the HP OpenView Windows (OVW) map.
2. From the menu bar, select **Monitor: MIB Values -> Graph Collected Data: SNMP -> Selected Nodes....** The primary window for the HP OpenView Graph tool appears.

When you select this operation, all the collected MIB data from the selected nodes will be read into memory and will be available for you to "browse" by using the HP OpenView Graph's functions.

The HP OpenView Graph's window consists of

- A menu bar with functions to manipulate the data. The menu bar also has help entries explaining how to use HP OpenView Graph tool.
- The actual graph presentation area. Time is shown on the x-axis.
- A legend across the top of the graph that identifies the nodes for which data is being graphed.

Note

If you have collected data for specific MIB variables, you can also view historical trends for the specific MIB variables by selecting the appropriate graph application from the OVW menu bar (for example, an application you built with the MIB Application Builder).

Related Topics

For more information related to viewing historical trends

- Click on the **Help** button in the dialog box.
- Go to the **Help: Index -> Functions** menu item and select **Monitor: MIB Values -> Graph Collected Data....**

Building MIB Applications

This operation allows you to build, without programming, MIB applications for standard and enterprise-specific MIB objects.

Prerequisites for this Operation

- Make sure the enterprise-specific MIB you will use to build your MIB application is loaded into the Loaded MIB database. (The **Options: Load/Unload MIBs: SNMP...** operation lists all MIB modules currently in the Loaded MIB database.) If the enterprise-specific MIB is not loaded, see "Loading MIBs" in this chapter.
- Make sure you understand the enterprise-specific MIB. To build useful applications you need to understand the definitions of the MIB objects and what they do.

Most device vendors include documentation about their enterprise-specific MIB with their product. This documentation typically describes the MIB objects and what the objects do. In addition, some vendors include overview information describing strategies for managing their specific devices. The vendor documentation can give you the conceptual understanding that you need to build an effective application.

- Design your application. For example:
 - Which objects do you want to include in your application?
 - Which objects make sense to group?
 - Should you be graphing this information or should you put it in a table or a form? You can choose from one of three presentation styles -- Form, Table, or Graph.

Note that enterprise-specific MIBs are device-specific. For example, if you build an application for a Cisco router, you cannot use that application on a Wellfleet router.

- Plan the menu structure. For example, if you have multiple devices from different vendors, you may want to organize the menu structure such that you have all MIB applications for routers grouped under one menu.
- Familiarize yourself with the MIBs using the **Monitor: MIB Values -> Browse MIB: SNMP...** operation.

Procedure

1. From the menu bar, select **Options: Application Builder: SNMP...**; the **MIB Application Builder** dialog box appears.
2. Click on **Add...**; the **Add MIB Application** dialog box appears.
3. Type in the name of the application in the **Application ID** field. This is the file where information will be stored.
4. Select the type of application that you want to build. To select the type
 - a. Click on the **Application Type** option button; an option menu appears with the following choices:
 - **Form.** Use this option to display MIB information that is not part of a table and does not change very often (for example, system description).

The information associated with each MIB object is displayed one MIB object per line with the MIB value to the right of the MIB label.
 - **Table.** Use this option to display MIB information that constructs a logical table in the MIB (for example, a routing table).

The MIB objects are laid out horizontally, making up the columns of the table. Each entry in the MIB table makes up the rows of the application table.
 - **Graph.** Use this option to display numeric MIB information that fluctuates over time (for example, interface statistics).
 - b. Make your selection from the option menu.
5. Enter the title you want for your application in the **Application Title** field. This title will appear in the menu bar of the dialog box when you run your application.
6. Click on **Add...**; the **MIB Application Builder/Add MIB Objects** dialog box appears.
7. Specify the MIB object to include in your application.

You can specify the MIB object ID by doing *one* of the following:

- Type in or paste the **MIB object ID** in the **MIB Object ID** field.
- Select the desired MIB object by moving up or down the MIB tree.

To move down the MIB tree

- a. Select the desired component from the **MIB Object ID** selection list.
- b. Click on **Down Tree** or double click on the component; the **MIB Object ID** field is updated with the selected component, and your location in the MIB tree descends to the next lower level.

Continue this sequence of moving down the MIB tree until you have specified the full object ID, that is, a leaf node.

To move back up the MIB Tree, click on **Up Tree**.

Note You *cannot* create table applications which consist of MIB fields from multiple MIB tables.

8. Once you have specified the full object ID, click on **Apply**; the object ID is added to the Display Fields list.

Optionally, you can select multiple objects, and then click on **Apply**.

Note When you select a **Graph**, the **OK** and **Apply** buttons are greyed-out until you have selected a numeric value. When you select a **Form** or a **Table**, the **OK** and **Apply** buttons are active for all leaf nodes, because you can include any type of MIB object in a table or a form.

9. Repeat steps 7 and 8 until you have specified all of the MIB objects you want included in the list.
10. Exit the MIB selection dialog box by clicking on **Cancel**.
11. Optionally, edit the **Label** for each MIB object selected, and if you are building a **Table**, specify the **width** of the column of the table. If you do not edit the **Label**, the label defaults to the last component of the MIB mnemonic name.

To edit the **Label** and, if applicable, the **width** of the column,

- a. Select the **MIB object ID** on which you want to change the label.
- b. Type the name of the label in the **Label** field and, if applicable, the width of the column in the **width** field.

- c. Click on **Replace** for the changes to take effect.

To cancel the changes and use the default **Label**, click on **Reset**.

12. Optionally, change the order of the items in the list, which affects the order the items are displayed when you run the application.

To change the order of the items in the list, select an item (or items) to move and click on the up or down arrows to the right of the **MIB Object** list. Each click moves the item (or items) up or down one position.

13. Enter the menu path. This is the full HP OpenView Windows (OVW) menu path for the application. Use the character sequence -> to separate menu items in the cascaded path.

If the menu path is not specified, the application is created and registered with OVW; however, the application will not appear in the OVW menu bar. This is useful for creating applications to be used as the action for an OVW Executable Symbol.

14. Enter the OVW selection rule. This selection rule is based on defined OVW Capabilities of the nodes for which this application is compatible. If the application is registered in the OVW menu bar, the menu item for this application is only accessible if the capabilities of the selected nodes match those defined in this selection rule.

15. Enter the help text that you want for your application. For example, you may want to give a general description of the MIB operation and how to interpret the information that is obtained. When you create the MIB operation menu item, the program automatically adds an entry in the **Help: Index -> Function** menu item and in the dialog box help.

16. Click on **OK** to create the new MIB application.

To abort the process, click on **Cancel**.

The procedure to build a new MIB application is now complete. To access the new MIB application, select the appropriate menu item.

Related Topics

For more information related to building MIB applications

- Click on the **Help** button in the dialog box.
- Go to the **Help: Index -> Functions** menu item and select **Options: Application Builder: SNMP....**

Defining Actions for Events

This operation allows you to customize the event notification messages and define actions that the application should perform when a trap is received.

Conceptual Information about Configuring Events

A trap is a message sent from an agent to a manager without an explicit request from the manager. Agents send traps to the manager to indicate that a particular condition exists on the agent system, such as an error has occurred or an event has happened.

All SNMP traps are defined in *RFC 1157: A Simple Network Management Protocol (SNMP)*. Each SNMP trap contains a *generic* trap number and a *specific* trap number. The *generic* trap numbers range from 0 to 6.

- ColdStart(0)
- WarmStart(1)
- LinkDown(2)
- LinkUp(3)
- AuthenticationFailure(4)
- EgpNeighborLoss(5)
- EnterpriseSpecific(6)

The *generic* traps 0 through 5 are defined by SNMP and assume a *specific* trap of 0. Additionally, many equipment vendors have defined traps specific to their own equipment. These traps are defined using the *generic* trap **EnterpriseSpecific (6)**, and are referred to as **enterprise-specific traps**. The enterprise-specific traps are uniquely identified by the

- Vendor's enterprise ID (that is, the **sysObjectID** of the vendor's equipment). For example, the enterprise ID for an HP 9000 Series 700 agent is **1.3.6.1.4.1.11.2.3.2.5**. **OpenView** generates traps with enterprise ID **1.3.6.1.4.1.11.2.17.1**.
- *Generic* trap, for example, **EnterpriseSpecific (6)**.
- *Specific* trap ID assigned by the vendor. In the **OpenView** example, one of the specific trap ID's is **58916865**, which is the specific trap ID for **OV_Node_Down**.

The most useful information you can get from a trap are

- the name or IP address of the node the trap came from, also called an agent address
- the trap number
- trap specific variables (or data)

For a list of the *specific* SNMP traps shipped with the NNM product, select **Options -> Event Configuration: SNMP** and click on the **Enterprise Identification OpenView**. The specific SNMP traps will be displayed in the **Event Identification** section.

Prerequisites for this Operation

- The node for which you want to configure an event must support SNMP.
- Make sure the enterprise-specific MIB for which you want to configure events is loaded into the Loaded MIB database. (The **Options: Load/Unload MIBs: SNMP...** operation lists all MIB modules currently in the MIB description file.) If the enterprise-specific MIB is not loaded, see "Loading MIBs" in this chapter.
- The MIB for which you want to configure events must be loaded. To load the MIB, see **Options: Load/Unload MIBs: SNMP...**
- Make sure you understand the definitions of and purpose for the MIBs on which you want to configure events.

Most device vendors include documentation about their enterprise-specific trap with their product. This documentation typically describes the trap and when the trap is generated. In addition, some vendors include overview information describing strategies for how to manage their specific device. The vendor documentation can give you the conceptual understanding that you need to configure effective event formats and actions.

Procedure

1. From the menu bar, select **Options: Event Configuration: SNMP...** menu item, and the **Event Configuration** dialog box appears.
2. Select the enterprise name of the target event from the **Enterprise Identification** section (first section) of the dialog box; the events configured for the selected enterprises appear in the **Event Identification** selection list (second section).

If the enterprise name of the target event does not appear in the **Enterprise Identification** selection list, add the enterprise name. To add an enterprise name, click on **Add...**; the **Add New Enterprise** dialog box appears. For help information about the **Add New Enterprise** dialog box, select the **Help** button within that dialog box.

3. Complete the **Add New Enterprise** dialog box and click on **Add...**

4. Select the specific event from the **Event Identification** section list (second section).

If the event is not listed in selection list, add the event. To add a new event, click on **Add...**; the **Add Event** dialog box appears. If the event already exists, select the event and click on **Modify...**; the **Modify Event** dialog box appears.. For help information about the **Add Event** or **Modify Event** dialog box, select the **Help** button within that dialog box.

5. Optionally, modify the **Event Log Message** field. For detailed help information about valid entries for the **Event Log Message** field, select the **Help** button within the **Event Configuration** dialog box.
6. Optionally, specify the source of the event in the **Source** field. For detailed help information about valid entries for the **Source** field, select the **Help** button within the **Event Configuration** dialog box.
7. Define the **Event Category**.
8. In the **Command** field, specify the action to take when the event is received.
9. To accept the new event definition without closing the dialog box, click on **Apply**. To accept the new event definition and simultaneously close the dialog box, click on **OK**.

All the changes are written to the **trapd.conf** file.

To exit the dialog box without adding a new Enterprise Name, click on **Cancel**.

Related Topics

For more information related to defining actions for events

- Click on the **Help** button in the dialog box.
- Go to the **Help: Index -> Functions** menu item and select **Options: Event Configuration: SNMP....**

Taking Snapshots of the Map

From the HP OpenView Windows menu bar you can create, list, open, close, delete, and get a description of a snapshot.

Selecting **File: Map Snapshot** displays a cascade of menu items that enables you to do any of the following:

- Open a snapshot. Only one snapshot may be open at any time. If you open a snapshot when another snapshot is open, the original snapshot is closed and the new snapshot is open.
- List all snapshots of the open map.
- Create a snapshot. Creating a snapshot defines the state of the network at the moment of creation. This operation does not open the snapshot.
- Delete a snapshot. Deleting an open snapshot causes all the submap windows and dialog boxes of the snapshot to close.
- Get a description of the open snapshot.
- Close the open snapshot. This closes all submap windows and dialog boxes of the open snapshot.

Once you create the snapshot, you can open and display the snapshot from the **Available Snapshots** dialog box as follows:

1. Select **File: Map Snapshots -> Open Snapshot** from the HP OpenView Windows menu bar.
2. From the **Available Snapshots** dialog box select the snapshot entry you want to open, and click on **Open Snapshot**.

The Home submap of the selected snapshot is displayed in a new submap window. You can also open a snapshot by double-clicking on the snapshot entry in the list box.

When you open a snapshot, the Home submap (at the time the snapshot was taken) is displayed. The status line indicates the name of the snapshot. Snapshots are read-only. You cannot edit a snapshot. However, you can traverse submaps, perform location tasks for specific objects, and keep an updated selection list for each submap. You cannot replace the map with a snapshot. Snapshots cannot be restored.

A snapshot is simply a picture of your network at a given time.

You can perform the following operations on a snapshot in the same way that you perform these operations on an open map:

- Select objects in the snapshot. The selection list for a snapshot has the same functionality as a selection list for a map. The snapshot selection list is independent of the selection list for the open map. You can display both map and snapshot selection lists at the same time. You can distinguish the selection list of a map and a snapshot by the map or snapshot name in the title bar.
- Locate objects in the snapshot.
- Navigate among the submaps of the open snapshot. This includes using all buttons in the button box (**C**lose, **H**ome, **R**oot, and **P**arent).

In a submap window of a snapshot, you *cannot*

- Add, delete, or modify objects or symbols.
- Use menu items greyed for read-only maps.
- Update maps.
- Use menu items from registered applications.
- Start an application by double-clicking on an executable symbol.

Index

A

- adding
 - IP interface object 3-15
 - network object 3-8
 - node object 3-13
 - segment object 3-10
- address information, viewing 3-27
- address translation table, viewing 3-29
- agent system, definition of 1-3
- agent, information available from 1-21
- applications, IP Map
 - See IP Map
- applications, MIB
 - building 6-18
 - See Also proactive fault diagnosis
 - viewing trends 6-16
- ARP Cache
 - diagnosing connectivity 5-6
 - prerequisites for using 5-4
 - viewing 3-29
- automatic layout
 - algorithm for 1-17
 - disabling 3-17
 - overview of 3-17
 - symbol behavior 3-17

B

- browsing MIB
 - determining objects for monitoring purposes 4-11
 - setting MIB values 6-6, 6-7
- building MIB applications 6-18
- bus segment 1-13, 1-14

C

class, symbol	1-18
collecting data	
See data collection	
communication problems, symptoms of	5-3
community name	1-4
compound status	1-19, 1-20
connection symbol	1-18
connection symbols	1-17
connectivity problems, diagnosing	5-4
container object	3-2, 3-3
containment realm	
editing guidelines	3-4
example of Internet submap	3-5
example of Partitioned Internet submap	3-6
maintaining	3-7
overview of	3-4
customizing a map	3-1

D

data collection	
determining trap number	4-15
network performance, establishing	4-11
rearm value	4-15
setting thresholds	4-14
using the data collector	6-9
diagnosing problems	
approach to solving	5-1
connectivity, across networks	5-6
connectivity, within the same network	5-4
performance on the network	5-9
See Also proactive fault diagnosis	
services on the network	5-12
symptoms	5-3
discovery, of the map	1-8
disk space, viewing	3-31
documenting the network	3-20

E

enterprise-specific MIB	1-5
enterprise-specific trap	
See trap	
event configuration	
checking Event Browser window	4-17
conceptual information	6-22
defining actions for events	6-22
formatting events	4-16
generic trap ID	4-17
See Also events	
specific trap ID	4-17
events	
acknowledging	4-8
categories window	4-7
definition of	1-21
formatting	4-16
generated by data collector	4-15
how they are generated	1-21
receiving notification of	1-21
See Also trap	
See event configuration	
setting up special actions for	4-18
trap, definition of	1-21
exiting NNM	2-7
expanding maps	
containment realm	3-4
creating Partitioned Internet submap	3-3
higher level maps	3-2
IP interface object, adding	3-15
lower level maps	3-8
network object, adding	3-8
node object, adding	3-13
See Also containment realm	
segment object, adding	3-10
extended MIB objects	1-5

F

FDDI ring segment 1-13, 1-16

G

generic trap numbers 1-22, 4-17, 6-22

get operation, definition of 1-3

H

help

from a dialog box 1-24

from the menu bar 1-23

how to get help 1-23

Home submap 1-8

HP-UX SAM

configuring networks and systems from NNM 3-32

diagnosing network service problems 5-13

prerequisites for using 5-12

I

icon symbols 1-17

instance

definition of 1-5

determining 6-11

query for, in MIB Browser 6-4

setting 6-11

interface object 3-26

Internet-standard MIB 1-5

IP internet object 3-22

IP Map

background processes 1-8

configuration defaults 2-8

conveying status 1-19

creation of submaps	1-10
customizing configuration settings, for a new map	2-9
customizing configuration settings, for an existing map	2-12
definition of	1-8
disabling IP-only status	2-13
explanation of configuration settings	2-11
layout algorithms	1-17
managing objects	3-7
See Also submaps	
synchronization	2-6
taking snapshots, operation for	6-25

L

layout	
algorithms	1-17
automatic	3-17
loading, MIBs	6-2
locating route	
diagnosing performance problems	5-10
prerequisites for	5-9

M

Management Information Base (MIB)	
definition of	1-5
See Also MIB	
manager system, definition of	1-3
managing	
network configuration	3-1
system configuration	3-1
Map	
See Also IP Map	
map	
customizing	3-1
expanding	3-2, 3-8
maintaining an expanding map	3-7

See Also expanding maps	
See Also monitoring the network	
See Also object	
See Also Partitioned Internet submap	
See Also symbol	
taking a snapshot	3-20
updating	3-19
map synchronization	2-6
menu bar	2-5
MIB	
building applications	6-18
defining thresholds, operation for	6-13
definition of	1-5
extended	1-5
loading	6-2
module	1-5
numeric values	6-9, 6-11, 6-13
object, definition of	1-5
object, organization of	1-6
organization	1-6
query function	6-6
See Also browsing MIB	
See Also data collection	
setting MIB values	6-6, 6-7
tree	1-6
viewing MIB values	6-4
MIB-II, definition of	1-5
monitoring the network	
checking for events	4-7
color alerts, watching for	4-2
creating special submap	4-5
new nodes, watching for	4-4
overview of	4-1
See Also proactive fault diagnosis	

N

network configuration	
controlling	3-32
managing	3-1

network map	
See map	
Network Node Manager (NNM)	
capabilities of	1-2
concepts about managing networks using NNM	1-3
exiting	2-7
introduction to	1-1
starting	2-2
using NNM operations	6-1
network object	3-23
network performance	
See proactive fault diagnosis	
network services	
diagnosing problems	5-12
prerequisites for viewing on a node	5-12
viewing on a node	5-13
node	
object	3-25
submap	1-16
Node submap	
disabling IP-only status	2-13
numeric MIB values	6-9, 6-13

O

object	
container	3-2
identifier	1-7
interface, viewing description of	3-26
IP interface, adding	3-15
IP internet, viewing description of	3-22
map, definition of	1-17
MIB, definition of	1-5
network, adding	3-8
network, viewing description of	3-23
node, adding	3-13
node, viewing description of	3-25
segment, adding	3-10
segment, viewing description of	3-24
sysObjectID, unique properties of	1-7

OpenView Windows (OVW)	
concepts about managing networks	1-3
exiting	2-7
starting	2-2
operations, using NNM	6-1
ovw command	
examples of options	2-4
options	2-3
starting OVW	2-2

P

Partitioned Internet submap	
creating	3-3
example of	3-6
how it is managed	3-7
overview of	3-2
See Also containment realm	
performance	
diagnosing	5-9
establishing baselines on a network	4-10
ping	
diagnosing connectivity, across networks	5-7
diagnosing connectivity, within a network	5-5
prerequisites for using	5-4, 5-6
See Also remote ping	
polling interval	
determining frequency	4-12
setting	6-10
proactive fault diagnosis	
building application to monitor trends	4-12
establishing baseline for performance	4-10
fine tuning thresholds	4-18
overview of	4-10
setting thresholds	4-14
setting up event-triggered actions	4-18
problems	
See diagnosing problems	

protocols	
prerequisites for viewing on a node	5-12
viewing on a node	5-13

Q

query, MIB values	6-6
-------------------	-----

R

rearm value	
absolute, setting to	4-15, 6-11, 6-14
percent, setting to	4-15, 6-11, 6-14
See Also thresholds	
setting	6-11
trap numbers	4-15
when to use	6-14
refresh map	3-19
remote ping	
diagnosing connectivity, within a network	5-5
diagnosing network performance	5-10
prerequisites for using	5-4, 5-9
Root submap	1-8
route	
See locating route	
routing table, viewing	3-28

S

SAM

See HP-UX SAM

segment	
object	3-24
submap	1-14
symbol	1-13
services, viewing	3-30
set operation, definition of	1-3

setting	
MIB values, directly	6-7
MIB values, using query	6-6
snapshot	
operation for creating	6-25
snapshot, documenting your network	3-20
SNMP (Simple Network Management Protocol), how it works	1-3
specific trap numbers	1-22, 4-17, 6-22
star segment	1-13, 1-15
starting NNM	2-2
status	
compound	1-19, 1-20
how it is conveyed	1-19
network	4-2
symbol	1-19
subclass, symbol	1-18
submap window	
button box	2-5
menu bar	2-5
status line	2-5
viewing area	2-5
submaps	
definition of	1-8
Home	1-8
Internet	1-11
Network	1-12, 3-8
Node	1-16, 3-13
Partitioned Internet	3-2
Root	1-8
Segment	1-14, 3-13
subtree	1-6
symbol	
definition of	1-17
Internet	1-9
status	1-19
types	1-18
varieties	1-17
symptoms of network communication problems	5-3
synchronization, of the map	2-6
sysObjectID	
unique properties of	1-7
system configuration	

controlling	3-32
managing	3-1

T

telnet	
hpterm	3-33
xterm	3-34
telnet, from NNM	
prerequisites for using	5-4
terminal emulation, from NNM	3-33
thresholds	
fine tuning	4-18
operation for defining	6-13
setting	4-14
Token Ring segment	1-13, 1-16
trap	
assigning trap numbers	4-15, 6-15
conceptual information	6-22
definition of	1-21
enterprise-specific	6-22
enterprise-specific, how they are identified	1-22
generic	6-22
numbers	1-22
setting trap ID's	6-11
specific	6-22
trends	
building applications to monitor	4-12
changing data resolution on the graph	4-14
viewing, historical data	6-16

U

updating a map	3-19
----------------------	------

V

values, MIB

See MIB

viewing

address information	3-27
address translation table	3-29
disk space	3-31
historical trends	6-16
MIB values	6-4
network services	3-30
object descriptions	3-21
traffic route	3-28