NetView for AIX

SC31-8163-01

Installation and Configuration

Version 4

IBM

NetView for AIX

SC31-8163-01

Installation and Configuration

Version 4

Note

Before using this product, read the general information under “Notices” on page vii.

First Edition (July 1995)

This document applies to IBM NetView for AIX (feature 5608), which is a feature of SystemView for AIX (5765-527). IBM NetView for AIX runs under the AIX Operating System for RISC System/6000 Version 3 Release 2 (5756-030) or Version 4 Release 1 (5765-393). This product is based, in part, on Hewlett-Packard Company's OpenView product.

Publications are not stocked at the address given below. If you want more IBM publications, ask your IBM representative or write to the IBM branch office serving your locality.

A form for your comments is provided at the back of this document. If the form has been removed, you may address comments to:

IBM Corporation
Department CGMD
P.O. Box 12195
Research Triangle Park, North Carolina 27709
U.S.A.

Or, you can send your comments online to CIBMORCF at RALVM13 using IBMLink or to USIB2HPD at IBMMAIL.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Contents

Figures

Tables

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make them available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of the intellectual property rights of IBM may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
USA

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

Site Counsel
IBM Corporation
P.O. Box 12195
3039 Cornwallis Road
Research Triangle Park, NC 27709-2195
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement.

This document is not intended for production use and is furnished as is without any warranty of any kind, and all warranties are hereby disclaimed including the warranties of merchantability and fitness for a particular purpose.

Trademarks

The following terms, denoted by an asterisk (*) at their first occurrences in this publication, are trademarks of IBM Corporation in the United States or other countries or both:

AIX
AIXwindows
DB2/6000
IBM
NETCENTER
NetView
POWERserver
POWERstation
RISC System/6000
Trouble Ticket
SQL
Systems Monitor

Other company, product, and service names, which may be denoted by a double asterisk[**], may be trademarks or service marks of others.

About This Book

This book describes the steps necessary for installing the IBM* NetView* for AIX* Version 4 program (hereafter referred to as NetView for AIX). The NetView for AIX program was formerly known as the AIX NetView/6000 program. The installation steps are slightly different based on which version of NetView for AIX you are migrating to or reinstalling. This book describes those installation steps and the migration process. This book also describes steps for installing the trapgend daemon on remote nodes and for installing NetView for AIX clients. Other information in this book includes starting, stopping, configuring, and maintaining the NetView for AIX program and obtaining service for the NetView for AIX program,

When referring to the host connection, this book assumes you are connecting to the host NetView program.

Who Should Use This Book

This book is designed for system administrators and network operators who are familiar with the operation of networks. Anyone involved in installing, configuring, and maintaining the NetView for AIX program should read this book.

This book assumes that the user has a general understanding of network management and of how the NetView for AIX program fits into that environment. An understanding of the AIX operating system is required to configure the NetView for AIX program.

How to Use This Book

This book is organized by task. Each chapter contains a task, or tasks, and the steps required to complete that task or tasks:

- Chapter 1, “Before Installing NetView for AIX” on page 1 contains information you need to know and describes what you should do before installing the NetView for AIX program. This includes software and hardware requirements and a prerequisite installation checklist.

  After checking that you have the necessary software and hardware to install and run the NetView for AIX program, and you have completed the prerequisite installation tasks, you are ready to start your installation.

- Chapter 2, “Installing and Deinstalling the NetView for AIX Server” on page 15 describes how to backup your current data, if applicable, remove your current NetView for AIX installation, and install the latest NetView for AIX installation.
- Chapter 3, “Installing and Deinstalling NetView for AIX Clients” on page 31 describes how to install NetView for AIX clients and how to configure them to talk to the correct server. It also describes how to deinstall a client.
- Chapter 4, “Installing DynaText on a Remote Machine” on page 45 describes how to install DynaText** information browser and books and the NetView for AIX online books on a remote server.

- Chapter 5, “Preparing to Use NetView for AIX” on page 51 describes how to check your installation.
- Chapter 6, “Installing and Using the trapgend Daemon” on page 53 describes the steps for installing the trapgend daemon on remote RISC System/6000 nodes and other operations available after installing the trapgend daemon, such as adding and deleting trap destinations on remote nodes.
- Chapter 7, “Starting and Stopping NetView for AIX Servers and Clients” on page 59 describes the startup process and the steps for starting the NetView for AIX program. Once the program is installed and you check the installation, you can start it with the defaults provided. This chapter also provides the steps for starting and stopping the daemons, and restarting map generation.
- Chapter 8, “Optional Configuration Tasks” on page 75 describes additional configuration options you can apply to the NetView for AIX program. You can change the defaults for the daemons, or perform other optional configuration tasks. For example, you can add entries to the object identification files (oid_to_type, oid_to_sym, or oid_to_command) anytime after installation.
- Chapter 9, “Maintaining NetView for AIX” on page 103 describes on-going maintenance tasks you can do to optimize the performance of the NetView for AIX program.

Highlighting and Operation Naming Conventions

The following highlighting conventions are used in this book, with the noted exceptions:

Bold Identifies commands and shell script paths (except in reference information), default values, user selections, daemon paths (on first occurrence), and flags (in parameter lists).

Italics Identifies parameters whose actual names or values are to be supplied by the user, and terms that are defined in the following text.

`Monospace` Identifies subjects of examples, messages in text, examples of portions of program code, examples of text you might see displayed, information you should actually type, and examples used as teaching aids.

The NetView for AIX operation naming convention used in this book shows the location of the operation in relation to the menu bar or context menu. The naming convention follows the format shown in this example:

```
Monitor..Network Configuration..Addresses
```

In this example, `Monitor` is a menu bar or context menu option, `Network Configuration` is an operation available from the Monitor submenu, and `Addresses` is an option that is available when you select Network Configuration.

Some operations require you to make selections from several layers of submenus before you reach the submenu containing the operation.

Where to Find More Information

The “Bibliography” on page 133 describes publications that can be helpful when using the NetView for AIX program. The Internet Request for Comments (RFC) documents listed are shipped on the NetView for AIX program installation media and are installed in the /usr/OV/doc directory.

Related Sources of Information

The following sources provide specific information that is not documented in the NetView for AIX Version 4 library:

- The /usr/lpp/nv6000/README file provides additional information about the NetView for AIX program.
- The online help facility provides task, dialog box, and graphical interface information to help you use this program.
- For more information about Simple Network Management Protocol (SNMP), Transmission Control Protocol/Internet Protocol (TCP/IP), and general network basics, the following list is recommended reading:

  Rose, Marshall T. *The Simple Book: An Introduction to Management of TCP/IP-based Internets*. Englewood Cliffs, NJ: Prentice-Hall, 1994 (ISBN 0-13-177254-6)

  Comer, Douglas. *Internetworking with TCP/IP: Principles, Protocols, and Architecture, Volume 1*. New York, NY: Prentice-Hall, 1991. (ISBN 0-13-468505-9)

  Black, Uyless. *Network Management Standards. The OSI, SNMP, and CMOL Protocols*. New York, NY: McGraw-Hill, 1992. (ISBN 0-07-005554-8)

Chapter 1. Before Installing NetView for AIX

This chapter describes the hardware and software required for both the NetView for AIX program and the host connection, and it describes the NetView for AIX software options. This chapter also describes some planning questions you need to answer and the tasks you need to perform before you can install the NetView for AIX program. The following topics are described in this chapter:

- "Hardware Requirements for Installing on the Server"
- "Software Requirements for Installing the NetView for AIX Program" on page 4
- "Software Components" on page 5
- "Planning your Installation" on page 6
- "Setting the LANG Variable" on page 10
- "Prerequisite Installation Tasks" on page 10

Hardware Requirements for Installing on the Server

This section includes hardware requirements for running the NetView for AIX program on the server and, optionally, for connecting to the host.

NetView for AIX Requirements

The following hardware components are required:

- A RISC System/6000* POWERstation* or POWERserver* system or a POWERpc Model 40P or C10.
- A minimum of 64MB of memory (server)

  The amount of memory needed is based on the size of your network and the number of concurrent operators. The larger your IP network, the more memory you will need. Estimate the amount of memory you will need using this procedure:

  Step 1. Determine the number of objects in the object database using one of these methods:

  - – If you do not have NetView for AIX installed, the number of objects in the database will be approximately 2 to 3 times the number of addressable devices in your network.
  - – If you have NetView for AIX installed, determine how many objects are in the object database. An object is a database entry that relates to all or part of a network device. To determine how many objects are in the object database, type **/usr/OV/bin/ovobjprint -S**.

Step 2. Use the following guidelines to estimate the amount of memory required for the size of your network:

No. of Objects	Recommended Memory
0 to 4999	64MB
5000 to 9999	80MB
10000 to 14999	96MB
15000 to 20000	112MB
>20000	>112MB

Step 3. Add 32MB for each additional X-station operator and additional memory for other applications that you are running, such as Trouble Ticket for AIX*. For example, a management station for a network with 1000 addressable devices (approximately 3000 objects), one additional user on an X-station, and no other applications requires 96MB (64MB + 32MB) of memory.

Refer to the appropriate documentation for additional memory requirements for other applications.

- A minimum of 100MB of disk space in the /usr/OV directory to install the NetView for AIX file sets.

  Note: Do not install the NetView for AIX program in an NFS-mounted /usr/OV file system, because unpredictable results will occur.

- Every 200 nodes requires 1MB of disk space. This assumes you have one read-write map. Each additional read-write map requires 1MB of disk space.
- Additional disk space is required for the following optional software components:
  - The relational database component requires 15MB of disk space. Additional disk space is required for the relational database that you plan to use. See the appropriate relational database documentation for additional disk space requirements.
  - The DynaText information viewer executable code requires 8MB of disk space.
  - The online books require 15MB of disk space.
- A minimum of 192MB of paging space.

  Use the following guidelines to determine recommended paging space based on your network's memory requirements:

Memory	Paging Space
64MB	192MB
80MB	240MB
96MB	288MB
128MB	320MB
160MB	400MB
192MB	480MB
>256MB	multiply memory by 2

- A color display supporting X Window System** Version 11 Release 5 and OSF/Motif** Version 1 Release 2 and meeting the following requirements:

Features	**Requirements**
Minimum number of colors	256
Depth	8 planes
Bits in color	8 bits
Dimensions	1280x1024 pixels
Resolution	91x92 dots per inch
Video memory on adapter	1MB minimum

- An IBM mouse or a compatible mouse.
- Tape drive, CD-ROM, or an installable file image on the server to install the NetView for AIX program.

Hardware Requirements for Installing the Client

The following hardware components are required for the client:

- A RISC System/6000 POWERstation or POWERserver system or a POWERpc Model 40P or C10.
- A minimum of 32MB of memory (48MB is recommended)
- A minimum of 55MB of disk space per client
- Every 200 nodes requires 1MB of disk space. This assumes you have one read-write map. Each additional read-write map requires 1MB of disk space.
- A minimum of 100MB of paging space (150MB is recommended)

  Note: The amount of memory, disk space, and paging space that you need are dependent on the following:

  - The size of your network
  - The speed of the connection between the client and server
  - The client/server configuration
  - The memory considerations for management applications installed on the client

- A color display supporting X Window System Version 11 Release 5 and OSF/Motif Version 1 Release 2 and meeting the following requirements:

Features	**Requirements**
Minimum number of colors	256
Depth	8 planes
Bits in color	8 bits
Dimensions	1280x1024 pixels
Resolution	91x92 dots per inch
Video memory on adapter	1MB minimum

- An IBM mouse or a compatible mouse.

Host Connection Requirements

For a host connection, the AIX NetView Service Point Version 1 Release 2 program and one of the following is required:

- IBM Token Ring High-Performance Network Adapter (#2970)
- IBM X.25 Interface Co-processor/2 (#2960)
- IBM 4-Port Multiprotocol Communication Controller (#2700)
- Ethernet High Performance Network Adapter

Software Requirements for Installing the NetView for AIX Program

This section includes software requirements for installing the NetView for AIX program and, optionally, for connecting to the host.

NetView for AIX Requirements

The following software components must be installed, configured, and operational:

- AIX Version 3 Release 2.5.

  Additional PTFs are required for installation and correct operation. Check the Memo to Users or the README file for information about PTF requirements.

  If you did not receive the PTFs or if you want more information about the latest PTF requirements and you have a support contract with IBM, call 1-800-CALLAIX.

- AIXwindows* Environment/6000

- X Window System Version 11 Release 5

- X11 fonts

  - X11fnt.ibm850.pc.fnt
  - X11fnt.coreX.fnt
  - X11fnt.kanji.aixfnt (Japanese language only)

- OSF/Motif Version 1 Release 2 with the latest PTFs

- SNMP agent

- TCP/IP

- NFS

- AIX base system locale of bs1.en_US.pc.loc

- Optionally, DynaText browser for AIX 2.3.0 or greater. The DynaText browser (dtext.brwsr.obj) is required to view the DynaText books and is included on the installation media. You do not need to install the DynaText Browser to access help for the graphical interface.

- Optionally, IBM DATABASE 2 AIX/6000 (DB2/6000**) Version 1.1, 1.2, or 2.

  For a client/server configuration, you also need IBM AIX DATABASE 2 Client Support/6000 Version 1.1, 1.2, or 2 on the server and IBM AIX DATABASE 2 Client Application Enabler/6000 Version 1.1, 1.2, or 2 on the client.

- Optionally, INFORMIX-OnLine** Version 5.0 or 6.0.

For a client/server configuration, you also need INFORMIX-NET** Version 5.0 or 6.0 for the client and possibly INFORMIX-STAR** Version 5.0 for the server.

- Optionally, INGRES** Server Release 6.4.

  For a client/server configuration, you also need INGRES/Net** Release 6.4 for remote client access.

- Optionally, ORACLE7** Server (RDBMS) 7.0.x (for AIX Version 3.2.5) or 7.1.4 (for AIX Version 3.2.5 or later).

  For a client/server configuration, you also need SQL*Net** TCP/IP (V1) for remote client access.

- Optionally, SYBASE** SQL Server Version 4.9.2 or 10.0.x, Open Client Libraries Release 4.6.2 or 10.0.x, and Embedded SQL for C Version 4.0.4 (for Version 4.9.2 only).

Other NetView for AIX Requirements for Installing on AIX 4.1

The following are requirements for AIX 4.1 if they differ from the AIX 3.2.5 requirements. If you do not see the requirement here, see "NetView for AIX Requirements" on page 4.

- AIX Version 4 Release 1
- AIX Base System Compatibility/Service Aids Requirements, such as links and log/dump
  - AIX 3.2 to 4.1 compatibility links
- Software Error Logging and Dump service aids
- AIX base system locale of bos.loc.pc_compat.En_US

Host Connection Requirements

For a host connection, you must have the following:

- Host NetView Version 2 Release 3 or later (Version 1 Release 2 or later for VSE)

- AIX NetView Service Point Version 1 Release 2 Modification 0 to use with SNA Services/6000 or AIX NetView Service Point Version 1 Release 2 Modification 1 or later to use with SNA Server/6000

- AIX SNA Services/6000 Version 1 Release 2 or AIX SNA Server/6000 Version 2 Release 1 or later

- Optionally, NETCENTER Version 1 (See *NETCENTER Service Point Interface Operation, Installation and Reference* for a list of the NETCENTER hardware and software requirements.)

Software Components

The NetView for AIX program consists of required and optional software components. The nv6000.base.obj and nv6000.features.obj components (and the nv6000.mJa_JP.msg component if you received the Japanese language feature) are required for NetView for AIX operation. The online help for the graphical interface is included in the the nv6000.features.obj component.

The following software components are optional:

Option **Description**

nv6000.database.obj

Provides relational database support. If you have a relational database installed, installing the relational database component enables you to store IP topology, trap log, and snmpCollect data in a relational database. The NetView for AIX program works with the DB2/6000, INFORMIX, INGRES, ORACLE, or SYBASE relational database management systems.

Refer to the *NetView for AIX Database Guide* for information about configuring the NetView for AIX program to use a relational database.

nv6000.nvbooks

Provides the NetView for AIX online books. You must have the DynaText online information viewer installed to see the online books.

To save file system space, you can install the DynaText executable code (dtext.brwsr.obj) and the NetView for AIX books (nv6000.books) on a remote server (a different machine than the one on which the NetView for AIX program is running).

Chapter 4, “Installing DynaText on a Remote Machine” on page 45 provides information about installing DynaText and the NetView for AIX online books on a remote server.

nv6000.client.obj

Provides the NetView for AIX client. This component is on a separate tape from the server code and related components. You can install this component on your server and push it out to all your clients. You can also install this component directly on your client machine.

See “Deciding Whether to Install Clients Remotely or Locally” on page 9 to determine how to install your clients. See Chapter 3, “Installing and Deinstalling NetView for AIX Clients” on page 31 for instructions about how to install your clients.

Planning your Installation

Before you begin installing NetView for AIX, it is wise to make some decisions about how you want to manage your network.

- Where should you install NetView for AIX?
- How many operators will you need?
- Do you want clients?
- How do you want to install those clients?
- Where do you want your maps to reside?

This section will help you make some of those decisions.

Determining Where to Install NetView for AIX

Consider the following when you select a machine on which to install NetView for AIX server:

- Disk space available
- Memory available
- Paging space available
- Location
  - In relation to your network administrators
  - In relation to the rest of your network

You will need a minimum of 100MB of disk space to install a NetView for AIX server.

The amount of memory you need depends on the size of your network and the number of local operators. See “Hardware Requirements for Installing on the Server” on page 1 to determine how much memory you need.

The amount of paging space you need depends on the amount of memory you install. See “Hardware Requirements for Installing on the Server” on page 1 to determine how much paging space you need.

The location of the machine you install the NetView for AIX program on is very important. You probably want your network administrators to be able to physically access it fairly easily. Also keep in mind that wherever you install NetView for AIX, the network maps will be drawn based on the location of that machine. The NetView for AIX server receives traps from the other machines, so it displays the network as if it were the center of the network. The discovery processes go out radially from the center machine.

This network-centric view also influences where you install NetView for AIX for performance reasons. The machine is constantly collecting data about the network. That data collection means network traffic—possibly heavy network traffic. You probably want to avoid traffic moving across several routers if you can.

For example, if your network stretches across the United States and the majority of your network is based on the East Coast, you may not want to install NetView for AIX on a machine in California. The constant traffic going between the East Coast and California could become very expensive in system time and equipment. In this case, install NetView for AIX somewhere on the East Coast, or consider multiple managers (or Mid-Level Managers) with some of them acting as backups or servers for each other.

Determining Whether to Install Clients

Consider the following when you decide whether to install client machines:

- Understanding the client/server setup
- Advantages of installing clients
- Considerations for installing clients

- Number of operators
- Location of operators
- Planning to install the trapgend subagent.

Understanding the Client/Server Setup

In a client/server configuration, the NetView for AIX daemons are separated from the end user interface (EUI) for better performance. The client runs the EUI applications.

A server includes the equivalent of a built-in local client. You cannot install both the client code and the server code on the same machine. Even though a server can perform the same functions as a client, a server cannot also be a client to another server.

Advantages of Installing Clients

The primary advantage of installing clients is performance because, in a client/server setup, you distribute the CPU and memory requirements to the client machines.

Another advantage is that you can use your hardware more efficiently. Drawing the maps on the EUI uses a fair amount of a machine's memory. In a client/server setup, you can offload that memory use onto several other machines (clients), which will enable the server machine to spend its memory on network management tasks.

Because you can use several client machines, you can also divide the management tasks among more operators at one time.

Considerations for Installing Clients

The client code is on a separate medium than the server code. So, installing clients requires a few more steps than if you were not installing clients. Configuring clients can also be more complex. See Chapter 3, “Installing and Deinstalling NetView for AIX Clients” on page 31 for details.

Another issue is map administration. Each client machine can have its own set of maps (remember: clients each run their own EUI code). If you want to make a change to all the maps without a client/server setup, you can make the changes on the machine where you installed NetView for AIX, and they will be reflected in the maps of the operators that access this machine. If you want to make a change to all the maps in a client/server setup, it is more challenging because the maps may be physically on different machines. For example, if you want to delete a router from every map, you have to delete the router from each of the client maps.

Another consideration is application installation. You will have to install applications separately on each client machine because you must install EUI applications where the EUI is installed (on the client machines).

Planning to Install the trapgend Subagent

Whether you decide to install clients or not, you should plan to install the trapgend subagent on all your remote RISC System/6000 nodes. The trapgend subagent enables all your RISC System/6000 nodes to collect the needed data and send it in a more efficient manner to the machine where NetView for AIX is installed (where the trapd daemon resides). To install trapgend on your remote nodes, you can push the code to each node using SMIT from the machine on which you installed NetView for AIX.

If you have already installed trapgend on all your nodes, consider reinstalling trapgend anyway. Having the latest version of the code is important.

Deciding Whether to Install Clients Remotely or Locally

You can install a client either remotely from the server to the client (also known as "pushing a client") or locally at the client.

If you install a client remotely, NetView for AIX does the following:

- Checks that the client machine has enough space to install the client code.
- Uses FTP to transfer the client code to the client machine.
- Installs the client code on the client machine using installp.
- Configures the server to give the client access.
- Configures the client to access the server.
- Installs the trapgend subagent on the client machine.

If you install a client locally on the client, *you* have to do the following:

- Install directly from the media you are using.
- Configure the server to give the client access.
- Configure the client to access the server.
- Optionally, install the trapgend subagent from the server using the SMIT commands on the server to push the subagent to the client machine.

If you push the client code to the client from the server, the NetView for AIX program completes more of the configuration for you. However, if you are physically at the client machine, installing the client locally is probably best. If the client code is on the server machine, you can also telnet into the server to get the client code. This could be useful if you plan to have many clients and you want each operator to install his or her client code locally.

Whether you install a client remotely or locally, you will need the root password for both the client and server machines.

Determining Whether to NFS Mount Your Map Database or Keep It on the Clients

You can network file server (NFS) mount your map database if you want all your maps to reside on the server machine. In this case, making changes to all the maps is easier because they are all in one place physically. Everyone can use the same set of maps. However, if the map database is on the server, you aren't offloading that memory utilization onto the clients.

You can keep your maps locally on the client machines if you want each client to have its own set of maps. In this case, the memory utilization is distributed onto the client machines. However, making changes to all the maps is complex because all the maps physically reside on different machines. Users cannot share the same maps.

Setting the LANG Variable

The NetView for AIX program is available in U.S. English, Japanese Kanji, and Simplified Chinese. The default setting for the LANG variable is **C**. To get full message function, set the LANG environment variable to the LANG value appropriate for your system. The LANG values (locales) for full message function are:

En_US	U.S. English locale
Ja_JP	Japanese Kanji locale
zh_CN	Simplified Chinese locale

For example, for English language users to access SMIT help, set the LANG variable to **En_US**. To set the LANG variable, enter the following:

```
LANG=En_US

export LANG
```

Warning: If the LANG variable is set to C or is not set, messages are not displayed correctly, and NetView for AIX SMIT help is not available.

If you are using the Japanese Kanji or Simplified Chinese version of NetView for AIX and a dialog box on the client is not displayed in the correct language, edit the /etc/environment AIX configuration file on the server to set the environment variables to the value appropriate for your system. Change both the LANG and LC_ALL environment variables in the /etc/environment file on the server to Ja_JP (for Japanese Kanji) or zh_CN (for Simplified Chinese). Then do one of the following:

- Stop all NetView for AIX processes and reboot the server machine.
- Run the following commands on the server machine:

  ```
  /bin/stopsrc -s inetd

  /bin/startsrc -s inetd
  ```

The NetView for AIX program has algorithms for finding language sensitive files. An attempt is made to locate the files based on the value of the LANG environment variable. However, the NetView for AIX program defaults to operating as though the LANG environment variable is set to C if one of the following happens:

- The LANG variable is not set.
- The value of the LANG variable is not a recognized locale.
- A required file is not found in the path referenced by the LANG variable.

Prerequisite Installation Tasks

For a successful installation, perform the tasks in the following checklist before you install the NetView for AIX program on your network:

__ 1. **Plan your installation**.

Make sure you have the answers to the planning issues raised in “Planning your Installation” on page 6.

__ 2. **Set the LANG variable**.

See “Setting the LANG Variable” on page 10 for information about how to set the LANG environment variable.

__ 3. **Install the prerequisite hardware and software**.

Check that the required hardware and software are installed. See “Hardware Requirements for Installing on the Server” on page 1 and “Software Requirements for Installing the NetView for AIX Program” on page 4 for hardware and software requirements.

__ 4. **Designate the management node**.

Designate a node as the management station. A management station is the node from which management applications will be run. Make sure you select a management node that is in the optimal place in your network. See “Determining Where to Install NetView for AIX” on page 7 if you need more information.

Once you designate a node, the NetView for AIX program uses the IP address and subnet mask for configuration. If you move the NetView for AIX program to a different management station, reconfigure the NetView for AIX program using the **/usr/OV/service/reset_ci** command.

__ 5. **Reserve memory**.

Check that you have enough memory. To determine how much memory your current system has, type:

```
lsdev -C -c memory
```

See memory requirements on page 1 for more information.

__ 6. **Reserve disk space**.

Check that you have enough disk space. Use the **df** command to check available disk space. See the appropriate AIX operating system documentation for information about the **df** command.

See disk space requirements on page 2 for more information.

__ 7. **Run Motif 1.2**.

Check that you are running Motif 1.2 in the shell in which you are installing the NetView for AIX program. To check the level of Motif you are running, type:

```
ls -al /usr/lib/libXm.a
```

One of the following messages is displayed:

```
/usr/lib/libXm.a —> /usr/lpp/X11/lib/libXm.a

/usr/lib/libXm.a → /usr/lpp/X11/Motif 1.2/lib/libXm.a
```

The first message indicates that you are running Motif 1.1; the second message indicates that you are running Motif 1.2.

Refer to the /usr/lpp/X11/README.MOTIF for information about how to change from Motif 1.1 to Motif 1.2.

__ 8. **Check the TCP/IP connection**.

Check the connection to your TCP/IP network. As a network manager, NetView for AIX depends on access to the network, even during installation.

Note: The following commands assume that your system is configured to use a domain name server (DNS). If your system is not configured to use a domain name server, the host names should be resolved in the /etc/hosts file.

- Make sure that you receive the appropriate response to each of the following commands:
  host 127.0.0.1

  You should receive a response similar to the following:

  ```
  localhost.raleigh.ibm.com is 127.0.0.1
  ```

  host loopback

  You should receive a response similar to the following:

  ```
  localhost.raleigh.ibm.com is 127.0.0.1, Aliases: loopback.raleigh.ibm.com
  ```

  host localhost

  You should receive a response similar to the following:

  ```
  localhost.raleigh.ibm.com is 127.0.0.1
  ```

  host *ipaddress*

  Where *ipaddress* is the IP address of your system. You should receive a response with the correct host name for your machine that is similar to the following:

  ```
  aixidw02.raleigh.ibm.com is 9.67.166.6
  ```

  host *hostname*

  Where *hostname* is the host name of your system. You should receive a response with the correct host name for your machine that is similar to the following:

  ```
  aixidw02.raleigh.ibm.com is 9.67.166.6
  ```

  host *other hostname*

  Where *other hostname* is the host name of another device on your network. Assuming the host name is iddaix01, you should receive a response similar to the following:

  ```
  iddaix01.raleigh.ibm.com is 9.67.162.190
  ```

  hostname

  You should receive a response with the correct host name of your system that is similar to the following:

  ```
  aixidw02
  ```

- Ping your system by host name and IP address and ping another device on your network to test the connection. Assuming `aixidw02` and `9.67.162.190` is the host name and IP address of your system and `aixidw01` is the host name of another device on the network, use commands similar to the following:

  ping -c 10 -q aixidw02

  ping -c 10 -q 9.67.162.190

  ping -c 10 -q aixidw01

  You should receive responses for each command similar to the following:

  ```
  10 packets transmitted, 10 packets received, 0% packet loss
  ```

Note: All the host names used when testing your TCP/IP connection must be resolved by your name server or the /etc/hosts file.

See the appropriate AIX operating system documentation for information about the **host** command, the Ping protocol, and TCP/IP.

Now that you have successfully completed the prerequisite installation tasks, you are ready to install the NetView for AIX program.

Note: You cannot install more than one version of the program on the same system.

If you want information about installing the NetView for AIX online books, see Chapter 4, "Installing DynaText on a Remote Machine" on page 45.

Chapter 2. Installing and Deinstalling the NetView for AIX Server

This chapter describes the installation process and provides the steps for installing the NetView for AIX program, including migration requirements. See Chapter 3, “Installing and Deinstalling NetView for AIX Clients” on page 31 for instructions specific to client machines.

This chapter describes the following topics:

- “Understanding what the Installation Process Does”
- “Migrating from a Previous Version of NetView for AIX” on page 16
- “Removing Downlevel NetView for AIX Software” on page 23
- “Using SMIT to Install the NetView for AIX Server” on page 25

Understanding what the Installation Process Does

The installation process does the following:

1. Checks that all the required software is installed.

   The installation process indicates if NetView for AIX cannot be installed because one or more required programs have not been applied. Because each program required for NetView for AIX has its own list of prerequisites, the program or PTF indicated might be a prerequisite of a NetView for AIX prerequisite.

2. Checks that there is adequate disk space to install the program.

3. Uses the **installp** command to install the program.

4. Checks for saved files from previous versions.

   The installation process performs a check to determine whether the saved Version 1, 2, 3, or 4 files exist. See “Migrating from a Previous Version of NetView for AIX” on page 16 for the steps to save the files. If the saved files exist, they are used during the installation process.

5. Checks that there is adequate disk space to install the additional files in the /usr/OV file system and, if necessary, increases the size of the file system.

6. Performs initial configuration, such as adding daemons to the startup configuration so the ovspmd daemon knows what to start when you execute the **nv6000** shell script. The migration and conversion of the previous version’s data are also performed as part of the initial configuration. See “Migrating from a Previous Version of NetView for AIX” on page 16 for a list of files that are migrated.

7. Starts the daemons.

Installing NetView for AIX for the First Time

Skip to “Using SMIT to Install the NetView for AIX Server” on page 25 if you are installing NetView for AIX for the first time. Otherwise, continue to the next section to save your customization information.

Migrating from a Previous Version of NetView for AIX

This section describes how to migrate from previous versions. Migration from a non-Entry version to Version 4 Entry is not supported.

The following sections explain that when you migrate from a previous version, you obtain the migration scripts, save the files you want to migrate, and run the migration script.

Note: It is *very* important that, after you run your migration scripts or backup your data files, you remove your downlevel NetView for AIX program before installing the latest NetView for AIX program.

Obtaining the Migration Scripts

There are two ways to obtain the migration scripts: over the internet or from the NetView for AIX program media.

You can use anonymous FTP to get to the netview.raleigh.ibm.com (192.35.236.7) internet server. The directory is /u/ftp/pub/uploads/NVMIGRATE. If you have World-Wide Web access, point your browser to the URL ftp://netview.raleigh.ibm.com/pub/uploads/NVMIGRATE. Look at the README file to get instructions for how to obtain and use the latest backup utilities.

If you want to get the migration scripts from the NetView for AIX program media, complete the following steps:

Step 1. Go to the /tmp directory by entering **cd /tmp**

Step 2. Get the migration scripts by entering the following:

```
restore -xvf /dev/rmt0.1 ./usr/OV/install/tools/nvp.v1r1 \
./usr/OV/install/tools/nvp.v2r1 ./usr/OV/install/tools/nvp.v3r1 \
./usr/OV/install/tools/nvp.v4r1 ./usr/OV/bin/nv6000_cmd
```

Where */dev/rmt0.1* is the device name or the name of the Version 4 image file.

Step 3. If you received a tape with multiple products on it, NetView for AIX may not be the first product on the tape. If it's not, repeat the **restore...** command to search the subsequent product files until you get to the NetView for AIX product, and the files are found.

Go to "Running the Migration Script for Version 1" if you currently have Version 1 installed. Go to "Running the Migration Scripts for Versions 2, 3, and 4" on page 18 if you currently have Version 2, 3, or 4 installed.

Running the Migration Script for Version 1

There are two ways you can migrate your files from Version 1. Either method will make your Version 1 program unusable.

The first method is to run, from the command line, the nvp.v1r1 script you obtained by using the instructions under "Obtaining the Migration Scripts." To run the script from the command line, exit the graphical interface if it is running, stop all the daemons, and enter the following command:

```
/tmp/usr/OV/install/tools/nvp.v1r1
```

Save the backup files to tape or some other external media in case you experience problems with the migration and need to try the migration again.

Note: Migration may delete some of the data you would need to retry the migration procedure.

For example, use the following command to copy the files to a tape drive:

```
tar -cvf /dev/rmt0 /etc/community.back /usr/etc/nv6000_options \
/usr/etc/nm.back /usr/adm/snmpCollect.back /usr/nvpbkup.netmon.seed
```

Once you install the Version 4 software, you will no longer be able to use the Version 1 files.

Go to “Removing Downlevel NetView for AIX Software” on page 23 for instructions on how to remove the Version 1 program before you install the Version 4 program. The second method is to copy the files manually. Complete the following steps to prepare for migration manually:

Step 1. Exit the graphical interface if it is running.

Step 2. Using SMIT, stop all the daemons.

Step 3. Save the /etc/community file by typing:

```
mv /etc/community /etc/community.back
```

Step 4. Save the /usr/etc/nm directory by typing:

```
mv /usr/etc/nm /usr/etc/nm.back
```

Step 5. Save the /usr/adm/snmpCollect directory by typing:

```
mv /usr/adm/snmpCollect /usr/adm/snmpCollect.back
```

Step 6. Save your netmon seed file, if you have one, by typing:

```
mv /usr/seedfile /usr/nvpbkup.netmon.seed
```

Where *seedfile* is the name of your netmon seed file. After migration, the seed file will be named /usr/OV/conf/V1netmon.seed.

Step 7. Save your daemon configuration options by running the following command:

```
/usr/bin/odmget nv6000_options >/usr/etc/nv6000_options
```

Step 8. Save the backup files to tape or some other external media in case you experience problems with the migration and need to try the migration again.

Note: Migration may delete some of the data you would need to retry the migration procedure.

For example, use the following command to copy the files to a tape drive:

```
tar -cvf /dev/rmt0 /etc/community.back /usr/etc/nv6000_options \
/usr/etc/nm.back /usr/adm/snmpCollect.back /usr/nvpbkup.netmon.seed
```

Once you install the Version 4 software, you will no longer be able to use the Version 1 files.

Step 9. Go to “Removing Downlevel NetView for AIX Software” on page 23 for instructions on how to remove the Version 1 program before you install the Version 4 program.

Running the Migration Scripts for Versions 2, 3, and 4

There are two ways you can run the migration scripts: either from the command line or through SMIT (Version 3 or 4 migration only).

To run the scripts from the command line, exit the graphical interface if it is running, stop all the daemons, and enter the following command:

```
/tmp/usr/OV/install/tools/nvp.v2r1 save
```

Where *nvp.v2r1* is the script that corresponds to the version that you currently have installed. You will be prompted for which categories of files you want to backup. See “Files that Migrate from Version 2, 3, or 4” on page 20 for descriptions of the categories.

Go to “Removing Downlevel NetView for AIX Software” on page 23.

To run the scripts through SMIT, which you can only do if you are migrating from Version 3 or 4, complete the following steps:

Step 1. Copy the appropriate script to the /usr/OV/install/tools directory by entering the following:

```
cp /tmp/usr/OV/install/tools/nvp.v3r1 /usr/OV/install/tools
```

Where *nvp.v3r1* should be *nvp.v4r1* if you are migrating from an earlier Version 4 installation to a later Version 4 installation.

Step 2. Save the original nv6000_cmd script by entering the following:

```
mv /usr/OV/bin/nv6000_cmd /usr/OV/bin/nv6000_cmd.orig
```

The new nv6000_cmd file should only be used in support of the final backup and deinstallation process.

Step 3. Copy the nv6000_cmd script to the /usr/OV/bin directory by entering the following:

```
cp /tmp/usr/OV/bin/nv6000_cmd /usr/OV/bin
```

Step 4. Go to “Removing Downlevel NetView for AIX Software” on page 23 to remove the Version 3 or 4 program before you install the latest Version 4 program.

Version 1 Files that Migrate

Table 1 on page 19 lists files that migrate and what happens to them during the migration process.

Table 1. Version 1 Files that Migrate

Files	What Happens During Migration
Topology map database	The topology database is converted to the format used by the ovtopmd daemon.
MIB applications	All MIB applications are converted and added to the new directory, /usr/OV/registration/C/ovmib. This includes MIB applications built by the MIB application builder.
Registration	All user-created Type III registration files are converted and placed in the /usr/OV/registration/C directory.
MIB files	All MIBs in Version 1, including MIBs you have added, are copied into the new MIB directory, /usr/OV/snmp_mibs, except the MIBs you added that have the same as the names of the MIBs available in Version 4.
Loaded MIBs	The compiled and loaded MIB files for Version 1 are copied into snmpmib.bin and snmpmib files in the MIB database in /usr/OV/conf directory for Version 4. You do not have to reload these files unless there is an error during the migration process.
trapd.conf	User-defined traps added to Version 1 are converted and placed in the Version 4 directory, /usr/OV/conf/C.
community	All the information in the /etc/community file is converted and the file is renamed to ovsnmp.conf. The ovsnmp.conf file is placed in the /usr/OV/conf directory.
snmpCol.conf	This file, which describes configuration data for the snmpCollect daemon, is migrated into the /usr/OV/conf directory.
SNMP collected data	All SNMP collected data is migrated from the Version 1 directory to the Version 4 /usr/OV/databases/snmpCollect directory.
Background maps	User-added background maps (GIF files) are migrated into the Version 4 directory, /usr/OV/backgrounds.
Modified polling intervals	All polling intervals that were modified in Version 1 are migrated into the Version 4 directory, /usr/OV/databases/openview/topo/polling.

Version 1 Files that Do Not Migrate

Migration is not provided for the following files:

Table 2. Version 1 Files that Do Not Migrate

Files	What Happens During Migration
X defaults	The X defaults file is not copied into the new directory. Changes previously made in this file for Version 1 are lost. The following Version 4 files replace the /usr/lib/X11/app-defaults/XNm X defaults file in Version 1: • /usr/OV/app-defaults/XNm • /usr/OV/app-defaults/OVw
oid_to_type	The oid_to_type file is not copied into the Version 4 directory. Any changes previously made to this file for Version 1 are lost.

Files that Migrate from Version 2, 3, or 4

If you are migrating from NetView for AIX Version 2 or 3, or if you are reinstalling Version 4, you can migrate any of the following categories of files:

NetView for AIX directory File category

/usr/OV/ALL
All categories

This includes all the categories listed in this section.

/usr/OV/ALL.USER
All user-defined categories

This includes all the categories listed in this section except, for the categories that have the .USER extension, only the user-defined categories are migrated. For example, there are two categories for MIBs: /usr/OV/snmp_mibs and /usr/OV/snmp_mibs.USER. The .USER file contains the user-defined MIBs. If you select **/usr/OV/ALL.USER**, the /usr/OV/snmp_mibs.USER category is migrated, but the /usr/OV/snmp_mibs category is not.

/usr/OV/databases/openview
Topology map database

This includes the ovwdb, mapdb, and topology databases.

/usr/OV/databases/snmpCollect
SNMP collection data

This includes all the data the snmpCollect daemon gathers. The snmpCollect task definitions are stored in the /usr/OV/conf/snmpCol.conf file, which is only migrated if you select the /usr/OV/conf file category.

/usr/OV/registration
Application registration files

This includes all product-defined, MIB, and user-added application registration files (ARFs) and all ARFs added by other integrated applications.

/usr/OV/fields
Field registration files

This includes all product-defined and user-added field registration files (FRFs) and FRFs added by other integrated applications.

/usr/OV/symbols
Symbol type registration files

This includes all product-defined and user-added symbol type registration files (STRFs) and STRFs added by other integrated applications.

/usr/OV/lrf
Local registration files

This includes all product-defined and user-added local registration files (LRFs) and LRFs added by other integrated applications.

Configuration files

/usr/OV/conf

This includes the following files:

- HPoid2type
- emstest.src
- xmpcfg.dat
- ovsuf
- ovors
- ovsnmp.conf
- trapd.conf
- oid_to_type
- oid_to_protocol
- oid_to_command
- oid_to_label
- mibExpr.conf
- mib.coerce
- mib.odi
- mib2.def
- snmpCol.conf
- dbconf.dat
- rdb_tracemask
- ovevent.db
- ovevent.dest
- snmpColFiles
- snmpmib
- snmpmib.bin
- nc.seed
- “netmon seed file”
- “backup manager seed file”
- “server clients list”
- “user-defined .modem files”
- tralertd.conf
- tralertd.default
- tralertd.filter
- tralertd_default.filter
- mnpcodes.desc
- mnpcodes.desc.undo
- ESE.automation
- nv.carriers
- nvpager.config
- nvpager.warm
- rulesets/Default.rs
- rulesets/forwardall.rs
- rulesets/* (user-added)
- C/oid_to_sym
- C/nnm_to_ovw
- C/trapd.conf

/usr/OV/app-defaults Application default files

This includes all product-defined X-Default files.

/usr/OV/security Security files

This includes all security configuration files, product-defined and user-added security registration files (SRFs), and SRFs added by other integrated applications.

/usr/OV/snmp_mibs All loadable MIB files

This includes all product-defined and user-added MIB files and MIBs added by other integrated applications.

/usr/OV/snmp_mibs.USER
User loadable MIB files

This includes all the MIB files that were not originally installed with NetView for AIX. This category is a subset of the /usr/OV/snmp_mibs category.

/usr/OV/reports Report files

This includes all product-defined and user-added reports and reports added by other integrated applications.

/usr/OV/filters Filter files

This includes all product-defined and user-added filters and filters added by other integrated applications.

/usr/OV/bitmaps All bitmap files

This includes all product-defined and user-added bitmaps and bitmaps added by other integrated applications.

/usr/OV/bitmaps.USER User bitmap files

This includes all the bitmap files that were not originally installed with NetView for AIX. This category is a subset of the /usr/OV/bitmaps category.

/usr/OV/backgrounds All background files

This includes all product-defined and user-added backgrounds and backgrounds added by other integrated applications.

/usr/OV/backgrounds.USER
User background files

This includes all the background files that were not originally installed with NetView for AIX. This category is a subset of the /usr/OV/background category.

/usr/OV/icons All icon files

This includes all product-defined and user-added icon definition files and icon definition files added by other integrated applications.

/usr/OV/icons.USER

User icon files

This includes all the icon definition files that were not originally installed with NetView for AIX. This category is a subset of the /usr/OV/icons category.

/usr/OV/help

Help files

This includes product-defined, MIB application, and user-added help files and help files added by other integrated applications.

/usr/OV/cron

Cron files

This includes all cron job scripts or cron job information. The active list of /usr/OV/crontab entries is saved in this directory.

/usr/OV/bin.USER

User bin files

This includes all the scripts or executable files that were not originally installed with NetView for AIX.

Version 2, 3, and 4 Files that Do Not Migrate

Files that are not saved in the NetView for AIX directories (/usr/OV) will not be updated.

Removing Downlevel NetView for AIX Software

After you save your customization files, remove the downlevel software before you install the latest software. See “Migrating from a Previous Version of NetView for AIX” on page 16 for instructions about how to save your customization files if you have not already done so. In order to use SMIT to remove downlevel software, you must have the appropriate migration script file in the /usr/OV/install/tools directory and the latest nv6000_cmd file in the /usr/OV/bin directory. For instructions on how to obtain the appropriate script files, see “Obtaining the Migration Scripts” on page 16.

Complete the following steps to remove any software from previous versions of NetView for AIX or if you are reinstalling the current version of NetView for AIX:

Step 1. If you have not already done so, exit the graphical user interfaces on this server and any clients and applications that reference this server.

Step 2. Enter **smit nv6000** on the server command line.

Step 3. Select **Maintain** on the NetView for AIX SMIT menu.

Step 4. Select **Remove NetView for AIX** on the Maintain menu.

Step 5. Do one of the following:

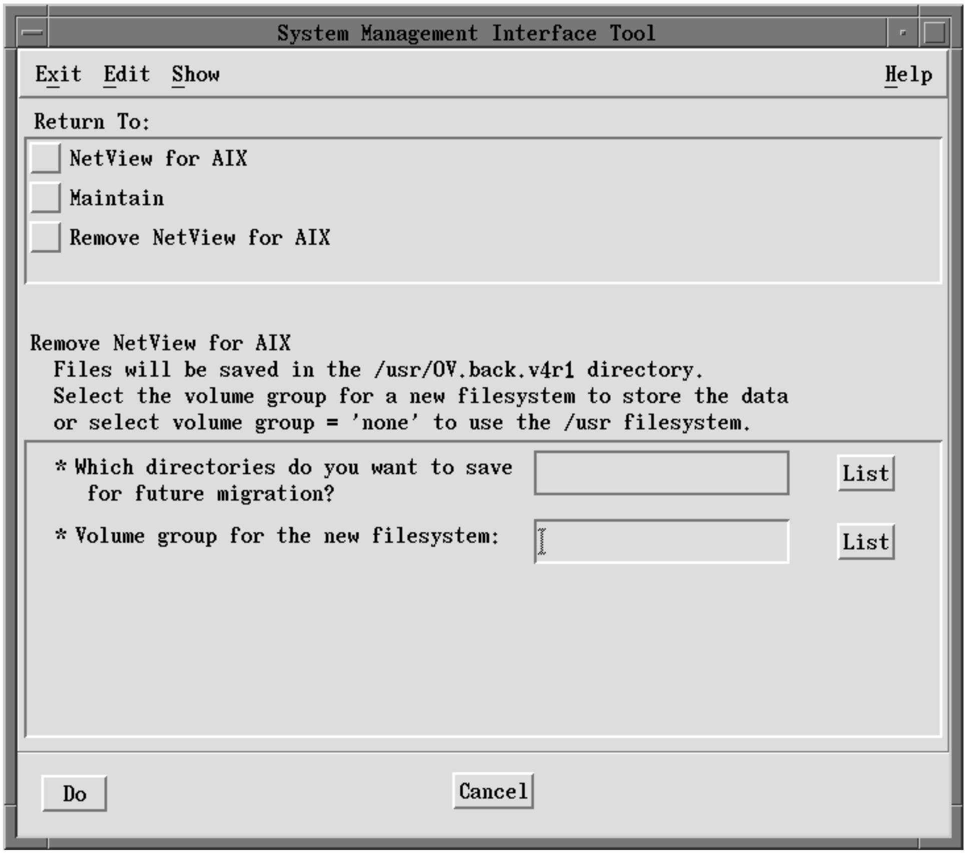
- If you want to remove any level of NetView for AIX software without saving the files, or if you already saved the files, select **Remove NetView for AIX** or **Remove AIX NetView/6000** from the Remove NetView for AIX menu.

  Go to Step 9 on page 25.

- If you want to backup a current Version 4 installation for migration, select **Save files for migration and remove NetView for AIX** from the Remove NetView for AIX menu.

  Note: Run the nvp.v3r1 or other migration scripts as described in “Running the Migration Scripts for Versions 2, 3, and 4” on page 18 for an earlier migration.

  The Remove NetView for AIX dialog box is displayed.



Return To:

□ NetView for AIX
□ Maintain
□ Remove NetView for AIX

Remove NetView for AIX
  Files will be saved in the /usr/OV.back.v4r1 directory.
  Select the volume group for a new filesystem to store the data
  or select volume group = 'none' to use the /usr filesystem.

* Which directories do you want to save for future migration?

* Volume group for the new filesystem:

Figure 1. Remove NetView for AIX Dialog Box

Continue with Step 6.

Step 6. Use the **List** button beside the Which directories do you want to save for future migration? field to select the appropriate directories. See “Files that Migrate from Version 2, 3, or 4” on page 20 for more explanation of the categories.

Step 7. Use the **List** button beside the Volume group for the new filesystem field to select which filesystem to store the data in.

Step 8. Select **Do**.

Step 9. Select **OK** on the verification message box to continue.

Step 10. Select **AIX NetView/6000** or **NetView for AIX** from the Return To menu.

The backlevel software is removed, and the NetView for AIX SMIT menu is displayed. The NetView for AIX books are removed, but the DynaText books and browser are not removed.

You should upgrade your workstation with the latest prerequisite software, such as AIX PTFs, before you install the latest level of NetView for AIX. See “Software Requirements for Installing the NetView for AIX Program” on page 4 for information about these requirements.

Using SMIT to Install the NetView for AIX Server

This section describes the procedure for installing NetView for AIX using SMIT.

Note: After you save your customization files, you *must* remove the downlevel software before you install the latest level of NetView for AIX.

You should also upgrade your workstation with the latest prerequisite software, such as AIX PTFs.

Installing NetView for AIX (nv6000.base.obj and nv6000.features.obj) using SMIT should take approximately one hour. Installing other components such as the relational database component or online books will take additional time. If you are migrating from a previous version, the installation may take significant additional time.

You can install all the NetView for AIX software components at once, or you can select the software components you want to install. The nv6000.base.obj and nv6000.features.obj components (and nv6000.mJa_JP.msg if you received the Japanese language feature) are the only components required for NetView for AIX operation. If you are migrating the relational database component, you must install the nv6000.database.obj component at the same time as the nv6000.base.obj and nv6000.features.obj components.

In addition, you can install the DynaText online information viewer code and the NetView for AIX online books on a remote server (a different machine than the one on which the NetView for AIX program is running).

SMIT has facilities that provide menus and online help to guide you through installing NetView for AIX. If you are not familiar with SMIT, refer to *AIX General Concepts and Procedures for IBM RISC System/6000* for more information.

Complete each step in order unless you are instructed to go to a different step. If you are unsure of which step to go to next, go to the step immediately following the step you just completed.

Navigating Through SMIT

These steps explain how to get to the appropriate SMIT screens to specify installation options.

Step 1. Do one of the following:

- If you are installing from a device, such as tape, insert the NetView for AIX media into the device drive.
- If you are installing from an image, start with the next step.

Step 2. Access the installation program by entering **smit**.

The SMIT System Management menu is displayed (SMIT main menu).

Step 3. Do one of the following:

- If you are using AIX 3.2.5, do the following:

  a. Select **Software Installation & Maintenance**.

  The Software Installation & Maintenance menu is displayed.

  b. Select **Install / Update Software**.

  The Install / Update Software menu is displayed.

  c. Select **Install / Update Selectable Software (Custom Install)**.

  The Install / Update Selectable Software (Custom Install) menu is displayed.

  d. Select **Install Software Products at Latest Available Level**.

  The Install Software Products at Latest Available Level dialog box is displayed. This is the first dialog box into which you enter information.

- If you are using AIX 4.1, do the following:

  a. Select **Software Installation and Maintenance**.

  The Software Installation and Maintenance menu is displayed.

  b. Select **Install and Update Software**.

  The Install and Update Software menu is displayed.

  c. Select **Install / Update Selectable Software (Custom Install)**.

  The Install / Update Selectable Software (Custom Install) menu is displayed.

  d. Select **Install Software Products at Latest Level**.

  The Install Software Products at Latest Level dialog box is displayed. This is the first dialog box into which you enter information.

Completing SMIT Dialog Boxes

These steps explain what to enter into the SMIT dialog boxes to get the appropriate installation options and how to begin the actual installation.

Step 1. Do one of the following:

- If you are installing from a mounted installation image, type the full path name for the image file in the INPUT device / directory for software field, such as:

  ```
  /pathname/nv6000.v4r1
  ```

  Where *pathname* is the mounted directory with the installation image.

  Go to Step 3.

- If you are installing from an input device, such as tape, select the **List** button next to the INPUT device / directory for software field.

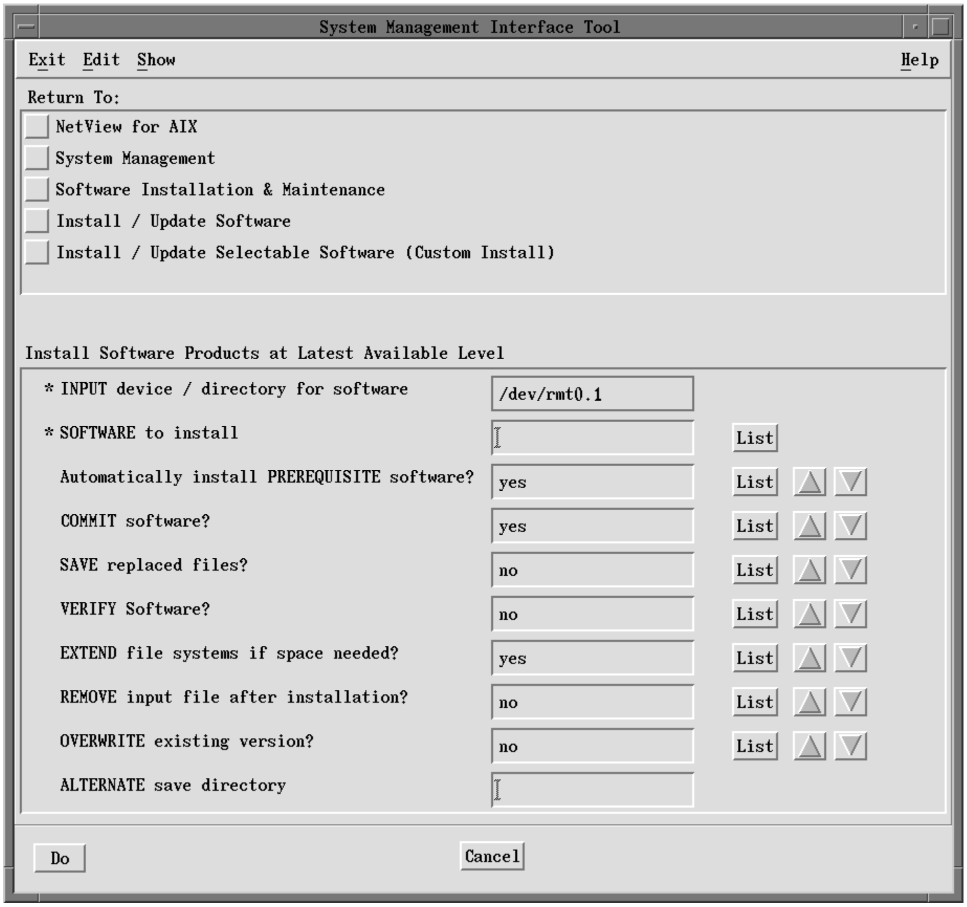
  A list of input devices is displayed. Go to the next step.

Step 2. Select an option from the list.

The input device you selected is displayed in the INPUT device / directory for software entry field. For example, `/dev/rmt0.1` may be displayed if you are installing from an 8mm tape drive.

Step 3. Select **Do**.

The installation options for AIX 3.2.5 are displayed in Figure 2 on page 28. The installation options for AIX 4.1 are displayed in Figure 3 on page 29.



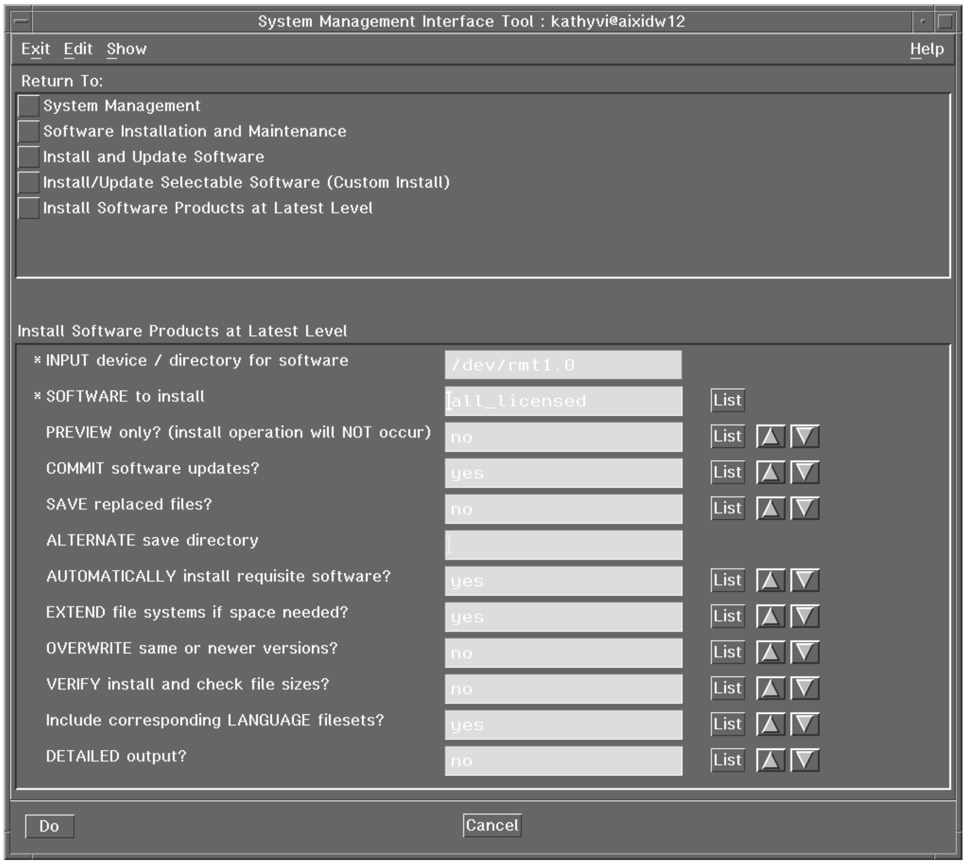
Return To:

- □ NetView for AIX
- □ System Management
- □ Software Installation & Maintenance
- □ Install / Update Software
- □ Install / Update Selectable Software (Custom Install)

Install Software Products at Latest Available Level

* INPUT device / directory for software	/dev/rmt0.1
* SOFTWARE to install	
Automatically install PREREQUISITE software?	yes
COMMIT software?	yes
SAVE replaced files?	no
VERIFY Software?	no
EXTEND file systems if space needed?	yes
REMOVE input file after installation?	no
OVERWRITE existing version?	no
ALTERNATE save directory	

Figure 2. Installation Options for Installing a Server on AIX 3.2.5



Return To:

□ System Management
□ Software Installation and Maintenance
□ Install and Update Software
□ Install/Update Selectable Software (Custom Install)
□ Install Software Products at Latest Level

Install Software Products at Latest Level

* INPUT device / directory for software	/dev/rmt1.0
* SOFTWARE to install	all_licensed
PREVIEW only? (install operation will NOT occur)	no
COMMIT software updates?	yes
SAVE replaced files?	no
ALTERNATE save directory	
AUTOMATICALLY install requisite software?	yes
EXTEND file systems if space needed?	yes
OVERWRITE same or newer versions?	no
VERIFY install and check file sizes?	no
Include corresponding LANGUAGE filesets?	yes
DETAILED output?	no

Figure 3. Installation Options for Installing a Server on AIX 4.1

Step 4. Select the **List** button next to the SOFTWARE to install field.

Step 5. Do one of the following:

- If you want to install all of the NetView for AIX software components and the DynaText online information viewer, select **ALL** from the list. The available software components are:

nv6000.base.obj	NetView for AIX program
nv6000.features.obj	NetView for AIX features
nv6000.database.obj	Relational database
dtext.brwsr.obj	DynaText online information viewer
nv6000.nvbooks	NetView for AIX online books

Note: If you received the Japanese language feature, nv6000.mJa_JP.msg is also included.

- If you want to install some of the NetView for AIX software components, select the components that you want. For example:
  - Select **nv6000.base.obj** and **nv6000.features.obj** if you want to install the NetView for AIX program without the relational database component, or the NetView for AIX online books.

    Note: The nv6000.base.obj and nv6000.features.obj components must be installed together.
  - Select **nv6000.base.obj**, **nv6000.features.obj**, and **nv6000.database.obj** if you want to install the NetView for AIX program with the relational database component.
  - Select **dtext.brwsr.obj** and **nv6000.nvbooks** DynaText online information viewer code and the NetView for AIX online books on a remote server. You may want to do this after you finish installing the NetView for AIX program. See Chapter 4, "Installing DynaText on a Remote Machine" on page 45 to install the online books separately.

Step 6. Select the **List** buttons to make any necessary changes in the other entry fields. Asterisks (*) indicate required entry fields.

Note: Selecting **yes** for the COMMIT software field or the COMMIT software updates field is not required but recommended.

The options are displayed in the entry fields.

Step 7. Select **Do**.

The appropriate NetView for AIX files are loaded into the system.

Step 8. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window is closed.

If you are migrating from Version 1, delete the migration files in the /usr/etc/nm directory to avoid migration if you reinstall the NetView for AIX program. Deleting the files also saves file system space.

Chapter 3. Installing and Deinstalling NetView for AIX Clients

This chapter describes the client installation process and provides steps for installing clients. It also describes how to deinstall a client once it has been installed.

This chapter includes the following topics:

- "Using SMIT to Install Clients from the Server"
- "Using SMIT to Install a Client Locally" on page 34
- "Configuring a Client to Access a Server" on page 39
- "Configuring a Server to Allow a Client Access" on page 38
- "Installing trapgend on the Client Machine" on page 41
- "Using SMIT to Remotely Deinstall Clients from the Server" on page 42

Using SMIT to Install Clients from the Server

You can install a client either remotely from the server to the client (also known as "pushing a client") or locally at the client. This section describes how to install a client remotely. If you are installing locally at the client, go to "Using SMIT to Install a Client Locally" on page 34.

When you install a client remotely, NetView for AIX does the following:

- Checks that the client machine has enough space to install the client code.
- Uses FTP to transfer the client code to the client machine.
- Installs the client code on the client machine.
- Configures the server to give the client access.
- Configures the client to access the server.
- Installs the trapgend subagent on the client machine.

Note: Before you install the client code, make sure the date and time on the server machine is the same as the client machine.

Copying the Client Code to the Server

Before you can install a client, copy the client code from the installation medium into a directory on your server. If you are installing from a disk file, go to "Pushing the Client Code from the Server" on page 32.

Complete the following steps:

Step 1. Insert the NetView for AIX media into the device drive.

Step 2. Access the installation program by entering **smit**.

The SMIT System Management menu is displayed (SMIT main menu).

Step 3. Select **Software Installation & Maintenance.**

The Software Installation & Maintenance menu is displayed.

Step 4. Select **Install / Update Software**.

The Install / Update Software menu is displayed.

Step 5. Select **Copy Software to Hard Disk for Future Installation**.

The Copy software to hard disk for future installation dialog box is displayed.

Step 6. Select the **List** button next to the INPUT device / directory for software field and select the device you are using.

Step 7. Select **Do**.

Step 8. Complete the second Copy software to hard disk for future installation dialog box.

Step 9. Select **Do**.

The client code is copied to the directory you specified. Go to “Pushing the Client Code from the Server” for further instructions.

Pushing the Client Code from the Server

You must have root permissions on the client and server to install clients. Make sure the server code is already installed on the server. Complete the following steps:

Step 1. Access SMIT using one of the following methods:

- Enter **smit nv6000** at the command line.
- Select **NetView SMIT** from the Administer pull-down menu.

Step 2. Select **Configure**.

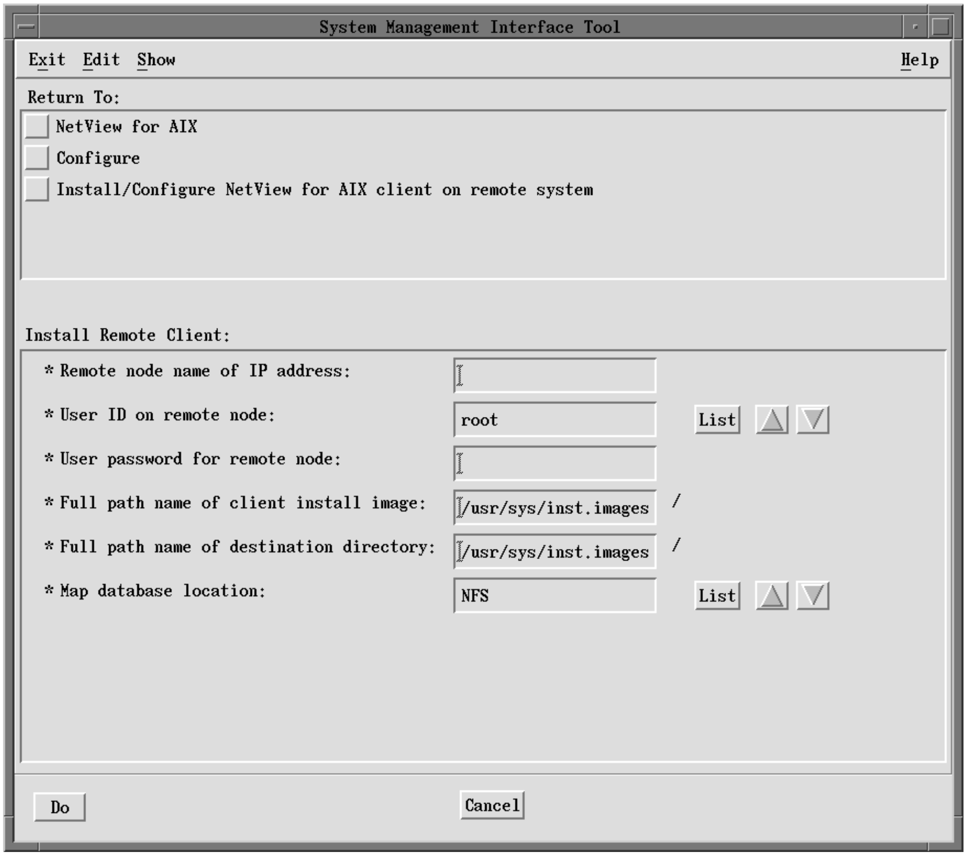
The Configure menu is displayed.

Step 3. Select **Install/Configure NetView for AIX client on remote system**.

The Install/Configure NetView for AIX client on remote system menu is displayed.

Step 4. Select **Install Remote Client**.

The Install remote client dialog box is displayed.



Return To:

- NetView for AIX
- Configure
- Install/Configure NetView for AIX client on remote system

Install Remote Client:

* Remote node name of IP address:	
* User ID on remote node:	root
* User password for remote node:	
* Full path name of client install image:	/usr/sys/inst.images /
* Full path name of destination directory:	/usr/sys/inst.images /
* Map database location:	NFS

Figure 4. Install Remote Client Dialog Box

Step 5. Make the necessary changes to the defaults in the fields.

At the time of the remote install, NFS mounts are performed from the client to the server for the following filesystems:

- /usr/OV/conf
- /usr/OV/databases/snmpCollect

In addition, if the map database location is set to NFS, NFS mounts to the server are also performed for the following:

- /usr/OV/databases/openview/mapdb
- /usr/OV/databases/openview/defmap

See “Determining Whether to NFS Mount Your Map Database or Keep It on the Clients” on page 9 for more information.

Step 6. Select **Do**.

The information is processed and the client is installed on the remote node that you specified.

Step 7. Make sure the date and time on the client machine are the same as the date and time on the server machine. Use the **date** command to check. The date and time must be synchronized for security and map administration to work correctly.

Using SMIT to Install a Client Locally

You can install the client code directly on the client machine. However, you will also have to do the following:

- Configure the server to give the client access
- Configure the client to access the server
- Install the trapgend subagent from the server by using SMIT on the server to push trapgend to the client (optional)

You must be root to install clients.

Navigating Through SMIT

To install the client image locally, complete the following steps:

Step 1. Insert the NetView for AIX media into the device drive.

Step 2. Access the installation program by entering **smit**.

The SMIT System Management menu is displayed (SMIT main menu).

Step 3. Do one of the following:

- If you are using AIX 3.2.5, do the following:

  a. Select **Software Installation & Maintenance**.

  The Software Installation & Maintenance menu is displayed.

  b. Select **Install / Update Software**.

  The Install / Update Software menu is displayed.

  c. Select **Install / Update Selectable Software (Custom Install)**.

  The Install / Update Selectable Software (Custom Install) menu is displayed.

  d. Select **Install Software Products at Latest Available Level**.

  The Install Software Products at Latest Available Level dialog box is displayed. This is the first dialog box into which you enter information.

- If you are using AIX 4.1, do the following:

  a. Select **Software Installation and Maintenance**.

     The Software Installation and Maintenance menu is displayed.

  b. Select **Install and Update Software**.

     The Install and Update Software menu is displayed.

  c. Select **Install / Update Selectable Software (Custom Install)**.

     The Install / Update Selectable Software (Custom Install) menu is displayed.

  d. Select **Install Software Products at Latest Level**.

     The Install Software Products at Latest Level dialog box is displayed. This is the first dialog box into which you enter information.

Completing SMIT Dialog Boxes

These steps explain what to enter into the SMIT dialog boxes to get the appropriate client installation options and how to begin the actual installation.

Step 1. Do one of the following:

- If you are installing from a mounted installation image, type the full path name for the image file in the INPUT device/directory for software field, such as:

  ```
  /pathname/nv6000.usr.4.1.0.0
  ```

  Where *pathname* is the mounted directory with the installation image.

  Go to Step 3.

- If you are installing from an input device, such as tape, select the **List** button next to the INPUT device / directory for software field.

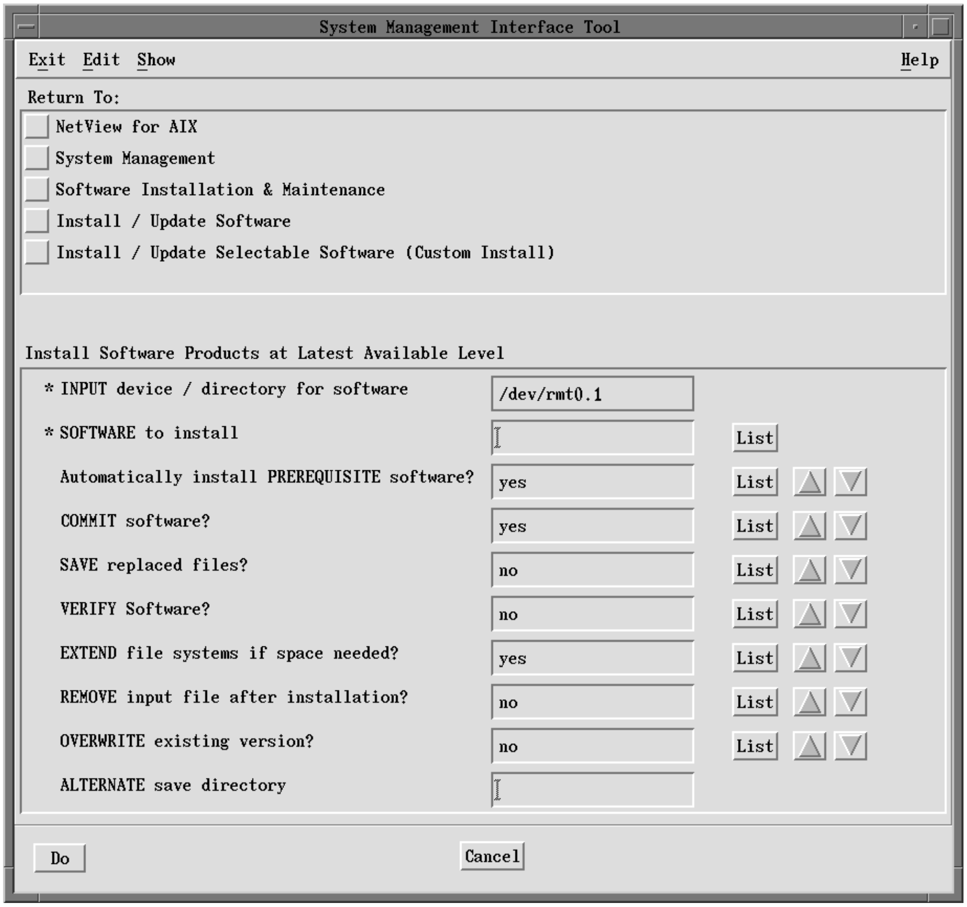
  A list of input devices is displayed. Go to the next step.

Step 2. Select an option from the list.

The input device you selected is displayed in the INPUT device / directory for software field. For example, `/dev/rmt0.1` is displayed if you are installing from an 8mm tape drive.

Step 3. Select **Do**.

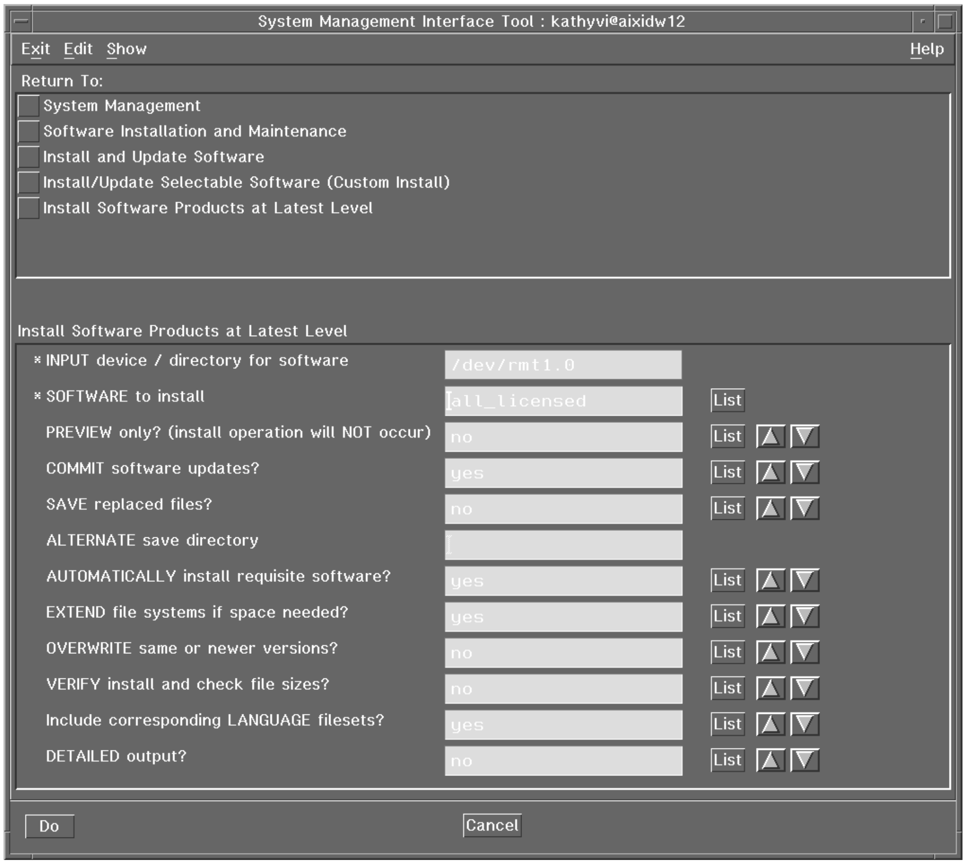
The installation options for AIX 3.2.5 are displayed in Figure 5 on page 36. The installation options for AIX 4.1 are displayed in Figure 6 on page 37.


System Management Interface Tool
Exit
Edit
Show
Help
Return To:
□ NetView for AIX
□ System Management
□ Software Installation & Maintenance
□ Install / Update Software
□ Install / Update Selectable Software (Custom Install)
List
Do
Cancel

Install Software Products at Latest Available Level

```
* INPUT device / directory for software          /dev/rmt0.1
* SOFTWARE to install
  Automatically install PREREQUISITE software?   yes
  COMMIT software?                               yes
  SAVE replaced files?                           no
  VERIFY Software?                               no
  EXTEND file systems if space needed?           yes
  REMOVE input file after installation?          no
  OVERWRITE existing version?                    no
  ALTERNATE save directory
```

Figure 5. Installation Options for Installing a Local Client on AIX 3.2.5



Return To:

- System Management
- Software Installation and Maintenance
- Install and Update Software
- Install/Update Selectable Software (Custom Install)
- Install Software Products at Latest Level

Install Software Products at Latest Level

```
* INPUT device / directory for software           /dev/rmt1.0
* SOFTWARE to install                             all_licensed
  PREVIEW only? (install operation will NOT occur) no
  COMMIT software updates?                         yes
  SAVE replaced files?                             no
  ALTERNATE save directory
  AUTOMATICALLY install requisite software?        yes
  EXTEND file systems if space needed?             yes
  OVERWRITE same or newer versions?                no
  VERIFY install and check file sizes?             no
  Include corresponding LANGUAGE filesets?         yes
  DETAILED output?                                 no
```

Figure 6. Installation Options for Installing a Local Client on AIX 4.1

Step 4. Make any necessary changes in the entry fields.

Step 5. Select **Do**.

Step 6. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window is closed.

Step 7. Make sure the date and time on the client machine are the same as the date and time on the server machine. Use the **date** command to check. The date and time must be synchronized for security and map administration to work correctly.

After you install the client image locally, configure the server to allow a client access.

Configuring a Server to Allow a Client Access

When a server pushes a client, the server is automatically configured to allow access to the client it pushed. There are three situations in which you would have to manually configure the server to give a client access:

- If you installed the client locally at the client machine and you want it to have access to this server
- If you pushed the code to the client from another server and now you want it to have access to this server
- If you pushed the code from this server, removed client access, and now want to grant client access again

A client can access more than one server, but never more than one at a time. If you want your client to temporarily access another server, you do not have to remove the client access at the server.

To add client access, complete the following steps:

Step 1. Go to the server machine.

Step 2. Access SMIT using one of the following methods:

- Enter **smit nv6000** at the command line.
- Select **NetView SMIT** from the Administer pull-down menu.

Step 3. Select **Configure**.

The Configure menu is displayed.

Step 4. Select **Install/Configure NetView for AIX client on remote system**.

The Install/Configure NetView for AIX client on remote system menu is displayed.

Step 5. Select **Add Client Access**.

The Add client access dialog box is displayed.

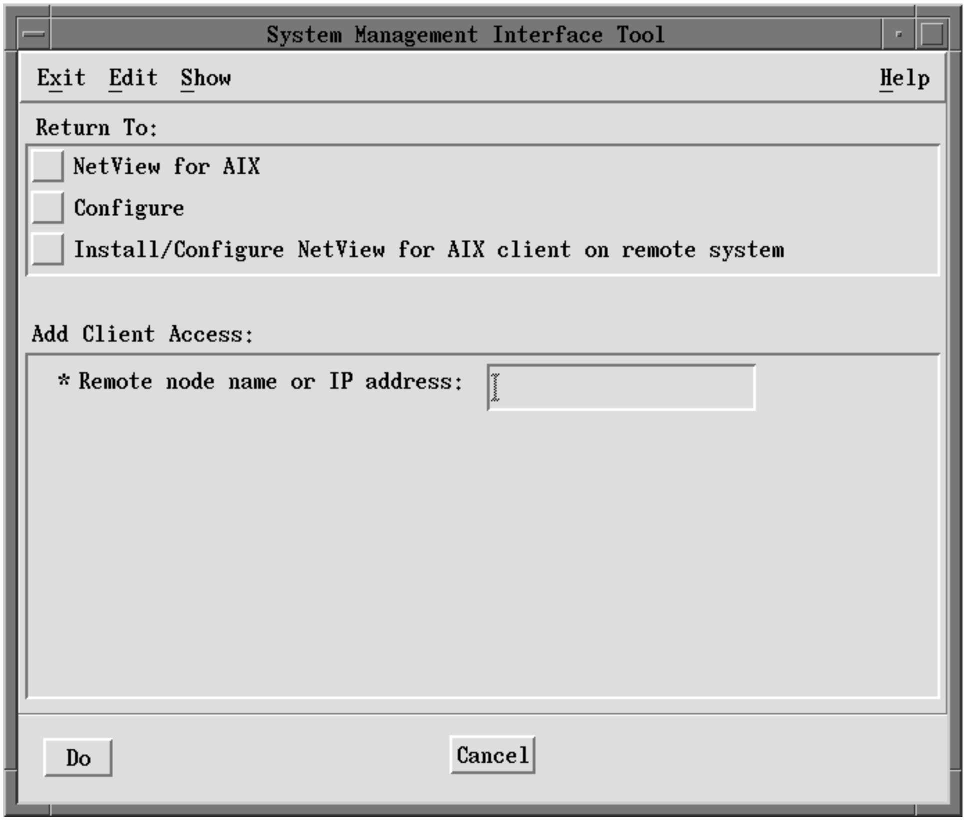

System Management Interface Tool
Exit
Edit
Show
Help
Return To:
NetView for AIX
Configure
Install/Configure NetView for AIX client on remote system
Add Client Access:
* Remote node name or IP address:
Do
Cancel

Figure 7. Add Client Access Dialog Box

Step 6. Make the necessary changes to the defaults in the fields.

Step 7. Select **Do**. The information is processed and the server gives access to the remote node that you specified.

If you installed the client code locally, configure the client to access the appropriate server.

Configuring a Client to Access a Server

When a server pushes a client, the client is automatically configured to access the server that pushed it. There are three situations in which you would have to manually configure a client to access a server:

- If you installed the client locally at the client machine and you want to tell it which server to access
- If you pushed the code to the client from another server and now you want to give the client access to a different server

- If you pushed the code from a server, removed access to that server, and now want to access that server again

A client can talk to different servers, but never more than one at a time.

Make sure you have granted the client access to the server already. If you have not, complete the steps in “Configuring a Server to Allow a Client Access” on page 38.

To configure a client to talk to a server, complete the following steps on the client machine:

Step 1. Access SMIT using one of the following methods:

- Enter **smit nv6000** at the command line.
- Select **NetView SMIT** from the Administer pull-down menu.

Step 2. Select **Configure**.

The Configure menu is displayed.

Step 3. Select **Add/Change Server**.

The Add/Change Server dialog box is displayed.

Step 4. Make the necessary changes to the defaults in the fields.

The Map database location field asks you to select either **local** or **NFS**. If you select **local**, the map database will reside on the client. If you select **NFS**, NFS mounts are performed to the server, and the map database will reside on the server.

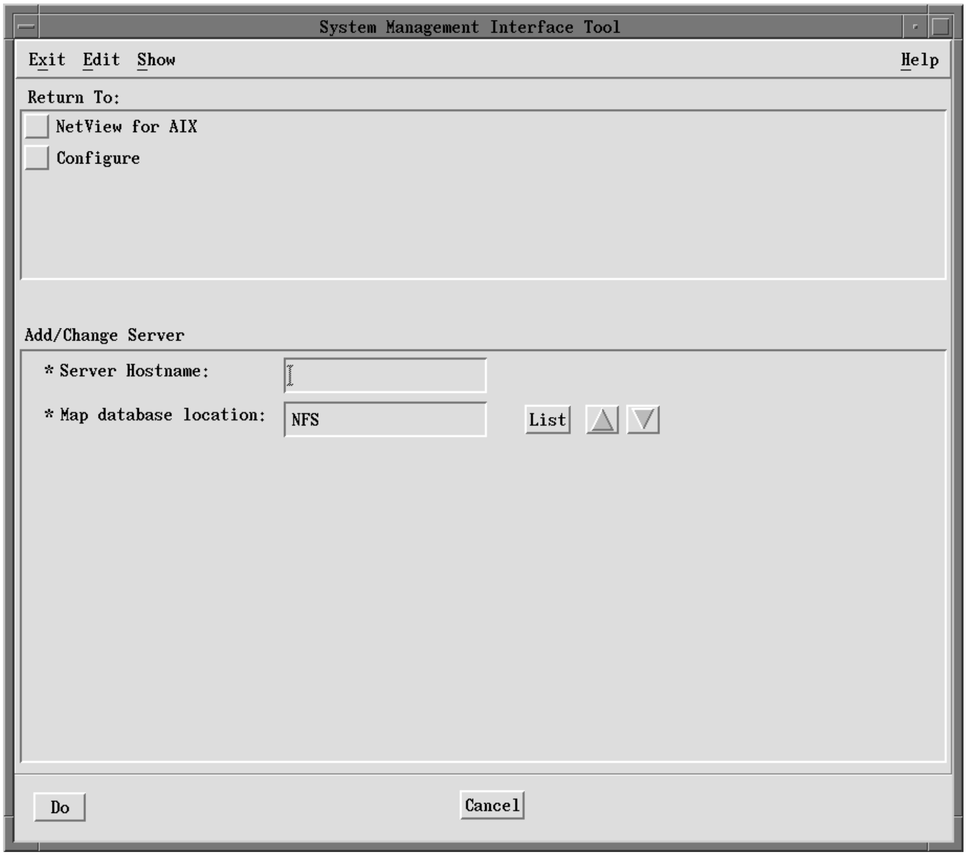
At the time of configuring a client to access a server, NFS mounts from the client to the server are performed for the following:

- /usr/OV/conf
- /usr/OV/databases/snmpCollect

In addition, if the map database is set to NFS, NFS mounts to the server are also performed for the following:

- /usr/OV/databases/openview/mapdb
- /usr/OV/databases/openview/defmap

See “Determining Whether to NFS Mount Your Map Database or Keep It on the Clients” on page 9 for more information.



* Server Hostname:

* Map database location: NFS

Figure 8. Add/Change Server Dialog Box

If you installed the client code locally, install the trapgend daemon from the server image onto the client machine, if you want to.

Installing trapgend on the Client Machine

The trapgend agent is not part of the client code. If you push the client code from the server, the server also pushes a copy of the trapgend code to the client automatically. If you install the client locally at the client machine, however, you will have to install the trapgend subagent on the client from the server. Installing trapgend on the client is optional, but recommended.

For information about installing trapgend, including instructions, see Chapter 6, “Installing and Using the trapgend Daemon” on page 53.

Using SMIT to Remotely Deinstall Clients from the Server

You can deinstall a client either remotely from the server or locally. This section describes how to deinstall a client remotely.

When you deinstall a client remotely, NetView for AIX does the following:

- Removes the client code from the client machine.
- Removes NFS mount connections.
- Removes the client's name from the server's list of clients that have access to it.

Note: When you deinstall a client, the trapgend subagent is not removed. If you want to remove the trapgend subagent, you will have to do this separately.

You must be have root permissions on the server and the client to deinstall a client.

Note: If the client you are removing has local maps, delete those maps using the graphical user interface on the client before you remove the client code. See the *NetView for AIX Administrator's Guide* for instructions. If you do not remove the client's local maps, the server's object database will contain incorrect information about the number of maps that exist and where the maps reside.

From the server, complete the following steps:

Step 1. Access SMIT using one of the following methods:

- Enter **smit nv6000** at the command line.
- Select **NetView SMIT** from the Administer pull-down menu.

Step 2. Select **Configure**.

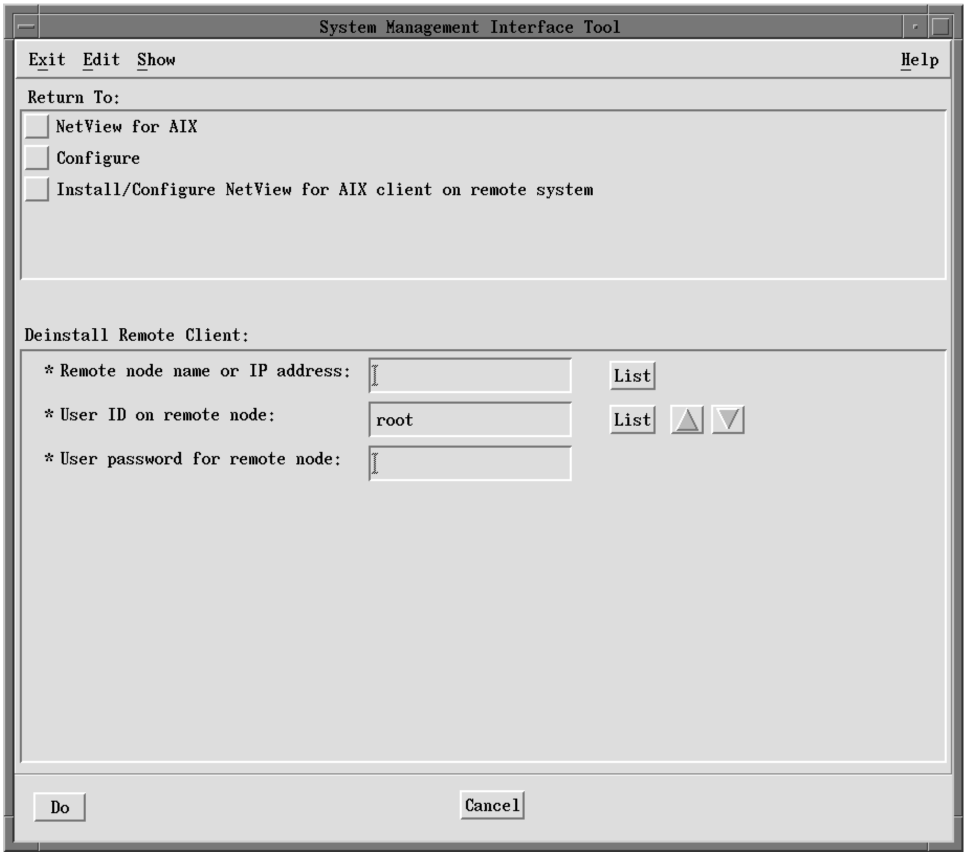
The Configure menu is displayed.

Step 3. Select **Install/configure NetView for AIX client on remote system**.

The Install/configure NetView for AIX client on remote system menu is displayed.

Step 4. Select **Deinstall Remote Client**.

The Deinstall remote client dialog box is displayed.


System Management Interface Tool
Exit
Edit
Show
Help
Return To:
NetView for AIX
Configure
Install/Configure NetView for AIX client on remote system
List
List
Do
Cancel

Deinstall Remote Client:

* Remote node name or IP address:

* User ID on remote node: root

* User password for remote node:

Figure 9. Deinstall Remote Client Dialog Box

Step 5. Make the necessary changes to the defaults in the fields.

Step 6. Select **Do**.

The information is processed and the client is installed on the remote node that you specified.

Using SMIT to Locally Deinstall Clients

You can deinstall a client either remotely from the server or locally. This section describes how to deinstall a client locally.

When you deinstall a client locally, you use SMIT to remove the client code from the client machine. This processes also removes NFS mount connections. The trapgend subagent is not removed from the client machine.

You must be have root permissions on the client to deinstall a client. From the client, complete the following steps:

Step 1. If the client you are removing has local maps, delete those maps using the graphical user interface on the client before you remove the client code. See the *NetView for AIX Administrator's Guide* for instructions. If you do not remove the client's local maps, the server's object database will contain incorrect information about the number of maps that exist and where the maps reside.

Step 2. Enter **smit nv6000** at the command line.

Step 3. Select **Maintain**.

The Maintain menu is displayed.

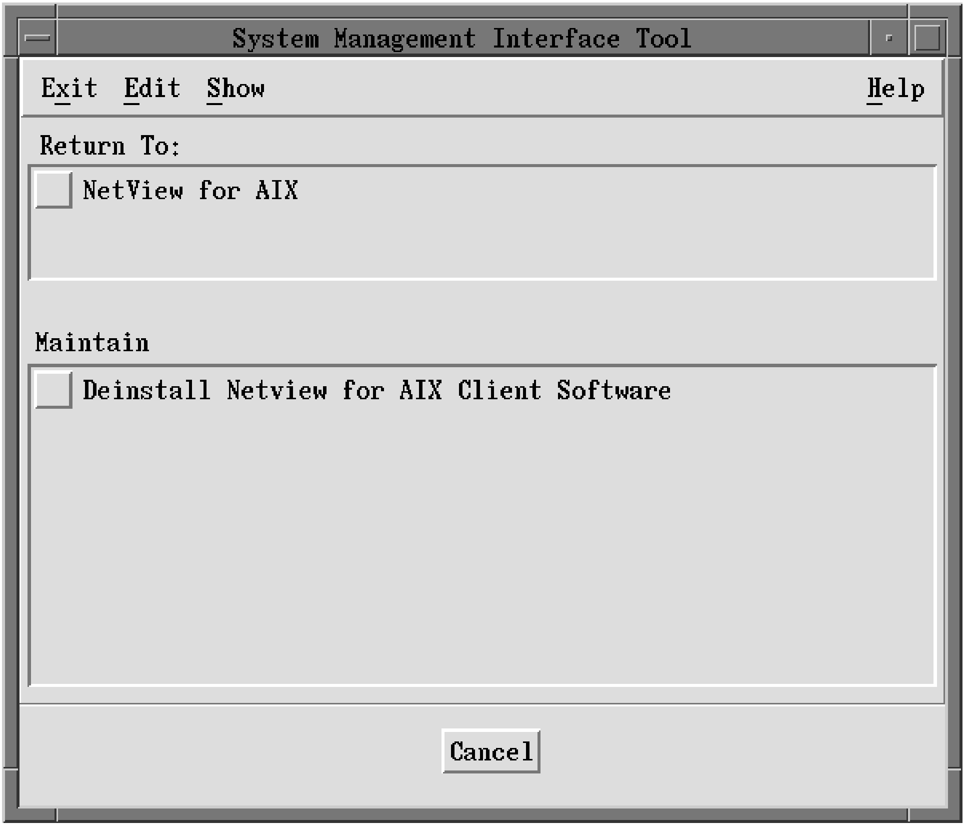

System Management Interface Tool
Exit
Edit
Show
Help
Return To:
NetView for AIX
Maintain
Deinstall Netview for AIX Client Software
Cancel

Figure 10. Deinstall NetView for AIX Client Software Option

Step 4. Click on **Deinstall NetView for AIX Client Software**.

Step 5. Select **OK** on the verification message box to continue.

The NetView for AIX client code is removed from the client machine.

Chapter 4. Installing DynaText on a Remote Machine

This chapter describes how to install the the DynaText information viewer executable code (dtext.brwsr.obj) and the NetView for AIX online books (nv6000.nvbooks) on a remote machine using SMIT. A remote machine is a different machine than the one on which the NetView for AIX program is running. The remote machine can be a client or another server. You can install DynaText on any number of machines.

There are two ways to install the DynaText code: locally on a machine or using NFS mounts. To install DynaText locally, see "Installing the Online Books." To NFS mount DynaText, see "Mounting the DynaText Directory" on page 49.

Installing the Online Books

This section describes how to install the online books locally on a client machine or on another server machine.

Navigating Through SMIT

You must have root permissions. To install DynaText on a remote machine, complete the following steps:

Step 1. Do one of the following:

- If you are installing from a device, such as tape, insert the NetView for AIX media into the device drive.
- If you are installing from an image, start with the next step.

Step 2. Access the installation program by entering **smit**.

The SMIT System Management menu is displayed (SMIT main menu).

Step 3. Do one of the following:

- If you are using AIX 3.2.5, do the following:

  a. Select **Software Installation & Maintenance**.

     The Software Installation & Maintenance menu is displayed.

  b. Select **Install / Update Software**.

     The Install / Update Software menu is displayed.

  c. Select **Install / Update Selectable Software (Custom Install)**.

     The Install / Update Selectable Software (Custom Install) menu is displayed.

  d. Select **Install Software Products at Latest Available Level**.

     The Install Software Products at Latest Available Level dialog box is displayed. This is the first dialog box into which you enter information.

- If you are using AIX 4.1, do the following:

  a. Select **Software Installation and Maintenance**.

     The Software Installation and Maintenance menu is displayed.

  b. Select **Install and Update Software**.

     The Install and Update Software menu is displayed.

  c. Select **Install / Update Selectable Software (Custom Install)**.

     The Install / Update Selectable Software (Custom Install) menu is displayed.

  d. Select **Install Software Products at Latest Level**.

     The Install Software Products at Latest Level dialog box is displayed. This is the first dialog box into which you enter information.

Completing SMIT Dialog Boxes

These steps explain what to enter into the SMIT dialog boxes to get the appropriate DynaText installation options and how to begin the actual installation.

Step 1. Do one of the following:

- If you are installing from a mounted installation image, type the full path name for the image file in the INPUT device/directory for software field, such as:

  /*pathname*/nv6000.v4r1

  Where *pathname* is the mounted directory with the installation image.

  Go to Step 3.

- If you are installing from an input device, such as tape, select the **List** button next to the INPUT device / directory for software field.

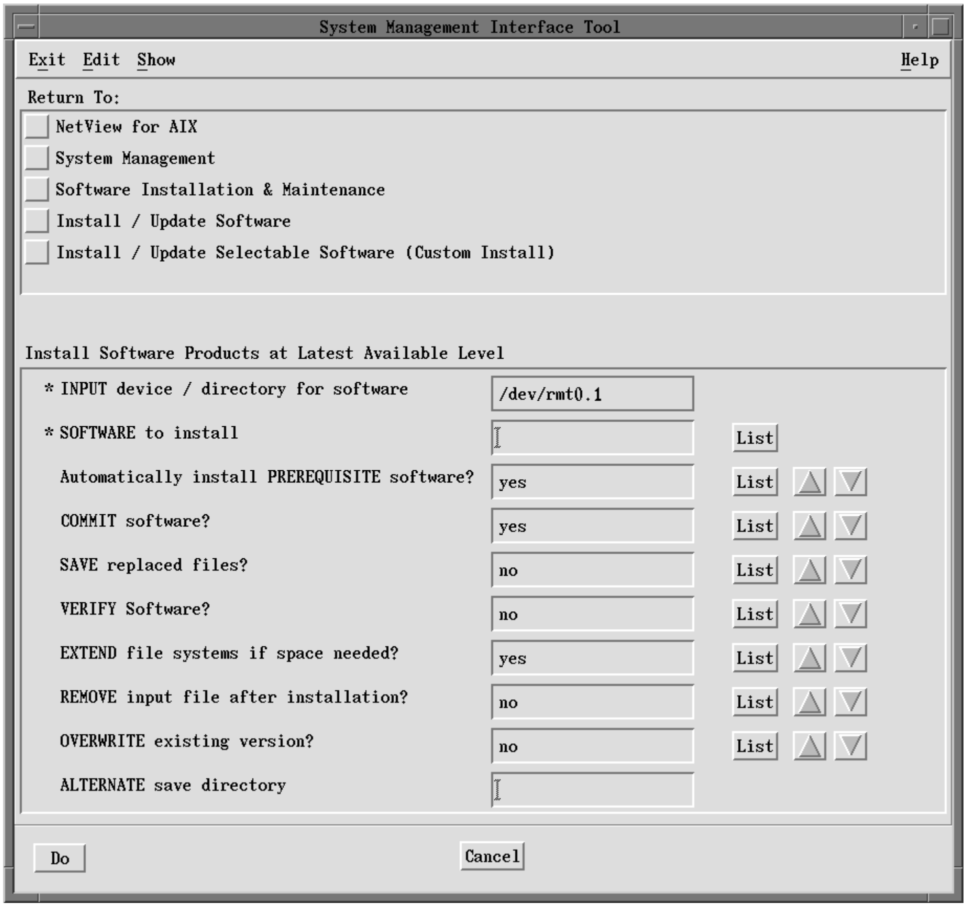
  A list of input devices is displayed. Go to the next step.

Step 2. Select an option from the list.

The input device you selected is displayed in the INPUT Device entry field. For example, `/dev/rmt0.1` may be displayed if you are installing from an 8mm tape drive.

Step 3. Select **Do**.

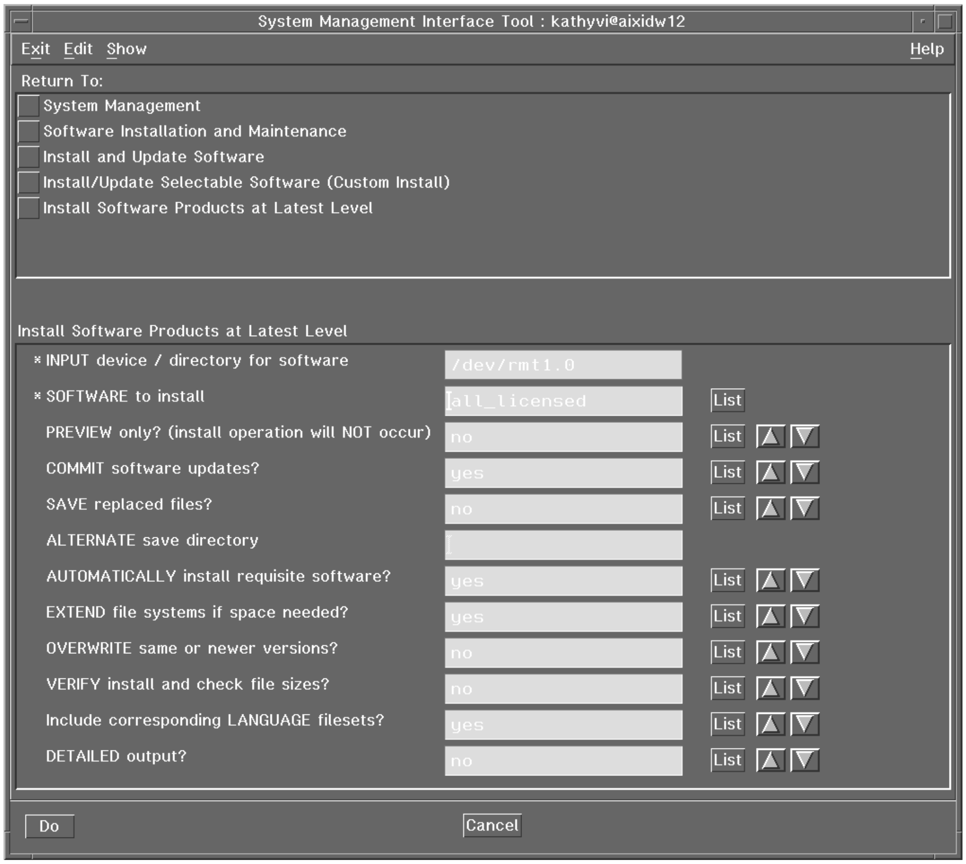
The installation options for AIX 3.2.5 are displayed in Figure 11 on page 47. The installation options for AIX 4.1 are displayed in Figure 12 on page 48.


System Management Interface Tool
Exit
Edit
Show
Help
Return To:
NetView for AIX
System Management
Software Installation & Maintenance
Install / Update Software
Install / Update Selectable Software (Custom Install)
List
Do
Cancel

Install Software Products at Latest Available Level

* INPUT device / directory for software	/dev/rmt0.1	
* SOFTWARE to install		List
Automatically install PREREQUISITE software?	yes	List
COMMIT software?	yes	List
SAVE replaced files?	no	List
VERIFY Software?	no	List
EXTEND file systems if space needed?	yes	List
REMOVE input file after installation?	no	List
OVERWRITE existing version?	no	List
ALTERNATE save directory		

Figure 11. Installation Options for Installing DynaText on AIX 3.2.5



Return To:

□ System Management
□ Software Installation and Maintenance
□ Install and Update Software
□ Install/Update Selectable Software (Custom Install)
□ Install Software Products at Latest Level

Install Software Products at Latest Level

* INPUT device / directory for software	/dev/rmt1.0
* SOFTWARE to install	all_licensed
PREVIEW only? (install operation will NOT occur)	no
COMMIT software updates?	yes
SAVE replaced files?	no
ALTERNATE save directory	
AUTOMATICALLY install requisite software?	yes
EXTEND file systems if space needed?	yes
OVERWRITE same or newer versions?	no
VERIFY install and check file sizes?	no
Include corresponding LANGUAGE filesets?	yes
DETAILED output?	no

Figure 12. Installation Options for Installing DynaText on AIX 4.1

Step 4. Select the following options using the List option in the Software to install entry field:

dtext.brwsr.obj	DynaText online information viewer
nv6000.nvbooks	NetView for AIX online books

Step 5. Select the **List** buttons to make any necessary changes in the other entry fields. Asterisks (*) indicate required entry fields. See Figure 11 on page 47 for the installation options and values.

The options are displayed in the entry fields.

Step 6. Select **Do**.

The NetView for AIX online books are loaded into the system. The *Shuttle Press Kit* that DynaText refers to in some of its documentation is not provided with the NetView for AIX software.

The DynaText browser and books are not removed when you remove the NetView for AIX product as described in “Removing Downlevel NetView for AIX Software” on page 23. The NetView for AIX books are removed.

Mounting the DynaText Directory

You must have root permissions. To mount the DynaText directory, complete the following steps:

Step 1. Export the /usr/ebt directory on the remote server using the **Add A Directory to Exports List** from SMIT NFS.

The hosts you specify have mount access.

Step 2. Create the directory for the mounted file system on the remote workstation by entering:

```
mkdir /usr/ebt
```

The /usr/ebt directory is created on the remote workstation.

Step 3. Mount the /usr/ebt file system on the remote workstation using the **Add A File System for Mounting** option from SMIT NFS.

The /usr/ebt file system is mounted on the remote workstation. The Shuttle Press Kit** is not provided with the NetView for AIX software.

Step 4. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window is closed.

The DynaText browser and books are not removed when you remove the NetView for AIX product as described in “Removing Downlevel NetView for AIX Software” on page 23. The NetView for AIX books are removed.

Chapter 5. Preparing to Use NetView for AIX

This chapter describes how to verify the NetView for AIX installation and what to do after verifying the installation.

To verify the installation of the NetView for AIX program, use the following procedure:

Step 1. Read the installp output displayed on the screen or logged in the $HOME/smit.log file to check for installation errors.

A list of installed software for the NetView for AIX program is displayed at the bottom of the smit.log file. The word COMPLETE should appear in the Status column. If not, the installation was not successful.

Step 2. Read the /tmp/update.log to review the results of the installation. Notes, error messages, and warnings about conditionally installed files and configuration options are logged to the /tmp/update.log. If you are migrating from a previous version, read this file for error information. Follow the steps listed in the /tmp/update.log to correct any errors.

Step 3. You can monitor disk space using the Systems Performance Monitoring application (shpmon). Refer to the *NetView for AIX Administrator's Guide* for more information.

The installation procedure adds entries for NetView for AIX's processes to the appropriate files. The entries should not be changed. See Table 7 on page 81 for a description of the installation entries.

If you plan to use a relational database, see *NetView for AIX Database Guide* to configure your database before you invoke NetView for AIX.

If you have not already done so, rename or delete any existing files from a previous installation, such as Version 1 migration files (/usr/etc/nm), Version 2 migration files (/usr/OV.back.v2r1), Version 3 migration files (/usr/OV.back.v3r1), or Version 4 migration files (/usr/OV.back.v4r1). Deleting or renaming these files prevents data from being migrated if you decide to reinstall Version 4. Deleting the files saves file system space.

Online help is available for all SMIT menus related to the NetView for AIX program and for the graphical interface. Read the /usr/lpp/nv6000/README file provided with the NetView for AIX program. The README file contains additional product information.

Configuring the NetView for AIX program is *not* necessary; you can start the NetView for AIX program using the defaults provided. However, you can modify the defaults if you choose. See Chapter 8, “Optional Configuration Tasks” on page 75 for information about NetView for AIX configuration options, including daemon options.

If you want the initial map to include all the networks in your administrative domain, or if you have a large network, you might want to pre-configure your system. For example, you might want to start netmon with a seed file. See “Configuring netmon to Use a Seed File” on page 88 for information about starting the netmon daemon with a seed file.

You might also want to reduce or increase the amount of memory used by the ovwdb daemon. See “Topology Discovery and Database Daemons” on page 77 for information about reducing or increasing the amount of memory used by the ovwdb daemon.

Chapter 6. Installing and Using the trapgend Daemon

Install the latest level of the trapgend daemon on all remote RISC System/6000 nodes. Installing the trapgend daemon on all remote RISC System/6000 nodes provides additional management capabilities by:

- Enabling remote ping
- Enabling CPU utilization and disk space monitoring
- Converting AIX alertable errors to SNMP traps

If you are migrating from Version 1 and you do not install the trapgend daemon on all remote RISC System/6000 nodes, traps can still be sent from the Version 1 trapgend daemon to the NetView for AIX Version 4 program, but you cannot perform trapgend operations.

You can find more information on the trapgend daemon than this section provides by referring to the Systems Monitor* documentation.

Understanding the trapgend Daemon

The trapgend daemon is a subagent provided with the NetView for AIX program.

The trapgend daemon converts alertable errors generated by a remote RISC System/6000 node to SNMP traps and sends them to the NetView for AIX management system. The traps can be found in two places. On the agent, the trap can be found in system error log (errpt -c). On the management system the trap can be found in the trapd.log.

Note: To include failing hardware information in the alerts, you must install the Product Topology Data diskette on the remote RISC System/6000 node. This diskette contains vital product data for your system unit. For information about installing the Product Topology Data diskette, refer to the documentation shipped with your system unit.

For best results, install trapgend on every IBM RISC System/6000 system running AIX Version 3 Release 2 or later.

The installation process adds an error notification object for the trapgend daemon to the Object Data Management (ODM) database and automatically starts the trapgend daemon and the AIX SNMP agent, snmpd, on the remote node.

You can install the trapgend daemon and access trapgend operations using the following methods:

- Using SMIT

  Using SMIT for trapgend daemon operations enables you to perform one trapgend operation on one remote node at a time. See “Installing and Configuring trapgend Using SMIT” on page 54 for information about using SMIT to access trapgend operations.

- Using the **nv6000_smit** shell script

  Using the **nv6000_smit** shell script enables you to perform multiple trapgend operations on a remote node. See "Installing and Configuring trapgend Using a Shell Script" on page 57 for information about using the **nv6000_smit** shell script to access trapgend operations.

Warning: When you perform trapgend operations using either method, a root password is required. This password is written in the smit.log and smit.script files, which anyone can read.

With either method, you can perform the following trapgend operations:

- Install the trapgend daemon.
- Add and delete trap destinations.
- Start and stop the trapgend daemon.
- Check the status and test the trapgend daemon.
- Remove the trapgend daemon.

  Note: You can remove the trapgend daemon from a remote node only if the NetView for AIX program is not installed on the remote node.

Installing and Configuring trapgend Using SMIT

You must have root permissions to perform any of the trapgend operations. To access trapgend operations using SMIT, follow this procedure:

Step 1. Access SMIT using one of the following methods:

- Enter **smit nv6000** on the command line
- Select **NetView SMIT** from Administer pull-down menu.

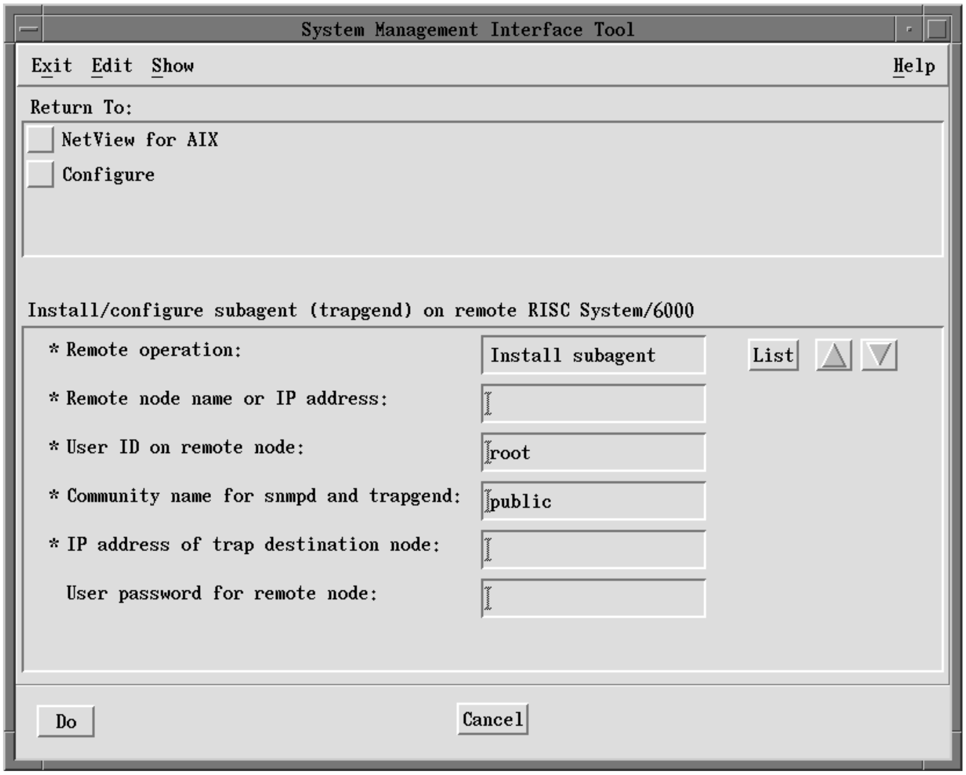
The NetView for AIX SMIT menu is displayed.

Step 2. Select **Configure**.

The Configure menu is displayed.

Step 3. Select **Install/configure subagent (trapgend) on system**.

The Install/configure subagent (trapgend) on system dialog box is displayed.



Install/configure subagent (trapgend) on remote RISC System/6000

* Remote operation: Install subagent

* Remote node name or IP address:

* User ID on remote node: root

* Community name for snmpd and trapgend: public

* IP address of trap destination node:

User password for remote node:

Figure 13. Dialog Box to Install trapgend

Step 4. Make any necessary changes in the required entry fields. Use Table 3 on page 56 to make any changes.

Table 3. trapgend SMIT Options

Option	Action	
Remote operation	Select the operation you want to perform on the remote node.	
	Select...	**To...**
	Install subagent	Install the trapgend daemon on a remote node.
	Status of subagent	View status of the trapgend daemon and trap destinations.
	Start subagent	Start the trapgend daemon without any other options.
	Test subagent	Test the operation of the trapgend daemon.
	Stop subagent	Stop the trapgend daemon.
	Add trap destination only	Add a trap destination on a remote node.
	Delete trap destination only	Delete a trap destination on a remote node.
	Remove subagent	Remove the trapgend daemon from a remote node. The NetView for AIX program cannot be installed on the remote node.
Remote node name or IP address	Type the node name or IP address of the remote node.	
User ID on the remote node	Type the user ID on the remote node. The default is **root**, but you can specify a user ID that has the appropriate permissions (a member of the system group, group 0).	
Community name for snmpd and trapgend	Type the community name of the remote node. The default is **public**.	
IP address of trap destination node	Type the IP address of the manager node set to receive traps from the remote node (if different than the default provided).	
User password for remote node	Optional. Type the password for the user ID on the remote node. If you type the password here, it will be displayed as you type it. If you leave this field blank, the program will prompt you for a password, and it will not be displayed as you type it.	

Step 5. Select **Do**.

Step 6. Do one of the following:

- If you entered a password in the Password for the remote node field of the Install/configure subagent on remote RISC System/6000 SMIT menu, go to Step 7. The entries will be processed and the latest trapgend will be installed on the remote node.
- If you did not enter a password, enter a password when the program prompts you for it. The password will not be displayed as you type it, and the cursor will not move as you type. The entries will be processed and the latest trapgend will be installed on the remote node.

Step 7. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window is closed.

Installing and Configuring trapgend Using a Shell Script

You can create a shell script to call the /usr/OV/bin/nv6000_smit shell script to perform multiple trapgend operations on remote nodes. You must have root permissions to use the /usr/OV/bin/nv6000_smit shell script.

Note: The /usr/OV/bin/nv6000_smit shell script requires a password for the user ID you specify in your shell script. If you do not wish to include the password in your shell script, run the shell script in the foreground, and you will be prompted to enter the password. If you want your shell script to be able to run unattended, you must include the password in your shell script.

To use the /usr/OV/bin/nv6000_smit shell script for multiple operations, follow this procedure:

Step 1. Create a shell script.

Step 2. Add a new line for each operation you want the shell script to perform. See "Example of a Shell Script" on page 58 for an example of lines in the **nv6000** shell script. Each line in the shell script must call the **/usr/OV/bin/nv6000_smit** shell script and include the following parameters:

- Keyword (subagentR)
- Operation to perform (install, status, start, test, stop, addtrap, deletetrap, or remove)
- Remote Node name or IP address
- User ID on the remote node (root or a user ID with the appropriate permissions, a member of the system group, group 0)
- Community name
- Trap destination
- Password for the user ID on the remote node (optional). If you do not specify a password, you will be prompted to enter one when your shell script is run.

Step 3. Save and execute the shell script file.

Example of a Shell Script

The following example shows lines in a shell script created for multiple trapgend daemon operations. The first line adds a trap destination for a remote node. The second line installs the trapgend daemon on a remote node.

```
/usr/OV/bin/nv6000_smit subagentR addtrap mlsnm003 userID \
  public 9.67.5.189

/usr/OV/bin/nv6000_smit subagentR install mdcnm008 userID \
  public 9.67.163.41 password
```

The variables indicate the following:

`subagentR`	Keyword
`addtrap`	Remote operation
`mlsnm003`	Remote node name
`user ID`	User ID on the remote node (root or the user ID with the appropriate permissions, a member of the system group, group 0)
`public`	Community name
`9.67.5.189`	IP address of the manager node to receive traps
`password`	Password for the user ID on the remote node

Chapter 7. Starting and Stopping NetView for AIX Servers and Clients

This chapter provides the necessary steps for starting and stopping the NetView for AIX program and its daemons.

The following topics are described:

Startup Behavior of the nv6000 Shell Script

This section defines the behavior of the nv6000 shell script, which starts the NetView for AIX program.

If you are on the server and have root permissions, the nv6000 shell script first executes the netnmrc shell script, which starts the snmpd daemon, the nettl facility (the network logging and tracing facility), if they are not running, and the daemons registered in the ovsuf startup file. The daemons are started using the ovstart command.

Then, the nv6000 shell script executes the ovw command, which starts the graphical interface. If you are on the client and have root permissions, the nv6000 shell script starts the graphical user interface on the client machine.

Customizing Startup

To customize the startup process, you should modify the /usr/OV/bin/applsetup and /usr/OV/bin/netnmrc.aux shell scripts rather than the nv6000 and netnmrc shell scripts, respectively. Doing so, prevents the possible loss of startup configuration because the nv6000 and netnmrc shell scripts are subject to modification with any service update or new version of the NetView for AIX program. The applsetup and netnmrc.aux shell scripts, however, reside in the /usr/OV/bin directory, which is backed up and migrated when you select the /usr/OV/bin.USER category during migration. See "Files that Migrate from Version 2, 3, or 4" on page 20 for more information.

The nv6000 shell script runs the /usr/OV/bin/applsetup script (if it exists), just prior to starting the graphical user interface. The applsetup script is run in the same process as the nv6000 command and thus allows the setting or changing of environment variables and other customized actions to be performed just as though the code had been edited into the nv6000 shell script itself. Users or application vendors who want to set environment variables or execute scripts when the nv6000 command is executed should make these modifications in the applsetup script.

See the nv6000 man page for more information about editing the applsetup script.

The netnmrc shell scripts runs the /usr/OV/bin/netnmrc.aux shell script, if it exists. If you want to start processes that run independently of the graphical user interface and that require root access, make these modifications in the netnmrc.aux shell script. Entries in the netnmrc.aux shell script do not have to run in the current process.

Preparing to Start NetView for AIX

The installation process starts all the daemons registered in the ovsuf file and checks the status of the daemons. If you have root permissions, the SNMP agent and all registered daemons are started when you start the graphical interface using the **nv6000** command or SMIT.

To check the status of the daemons from the server, use the **ovstatus** command or use SMIT. To use SMIT, see “Checking Daemon Status Using SMIT” on page 61. To check the status of the daemons from the client, use the **nvstatus** command.

Start any daemons that are not running. If the trapd, pmd, and ovwdb daemons are not running, the graphical interface will not execute. Have the system administrator start the daemons for you if you do not have root authority.

For information about restarting the NetView for AIX daemons, see “Restarting the Daemons” on page 69.

Checking Daemon Status Using SMIT

The installation process starts all the daemons registered in the ovsuf file. However, before you start NetView for AIX, you might want to check the status of the daemons and start them if necessary. You do not need root permissions to check the status of the daemons but you must have root permissions to start them. If the trapd, pmd, and ovwdb daemons are not running, the end user interface (EUI) will not run.

To check the status of the NetView for AIX daemons, follow these steps:

Step 1. Access SMIT using one of the following methods:

- Enter **smit nv6000**
- Select **NetView SMIT** from the Administer pull-down menu.

The NetView for AIX SMIT menu is displayed.

Step 2. Select **Control.**

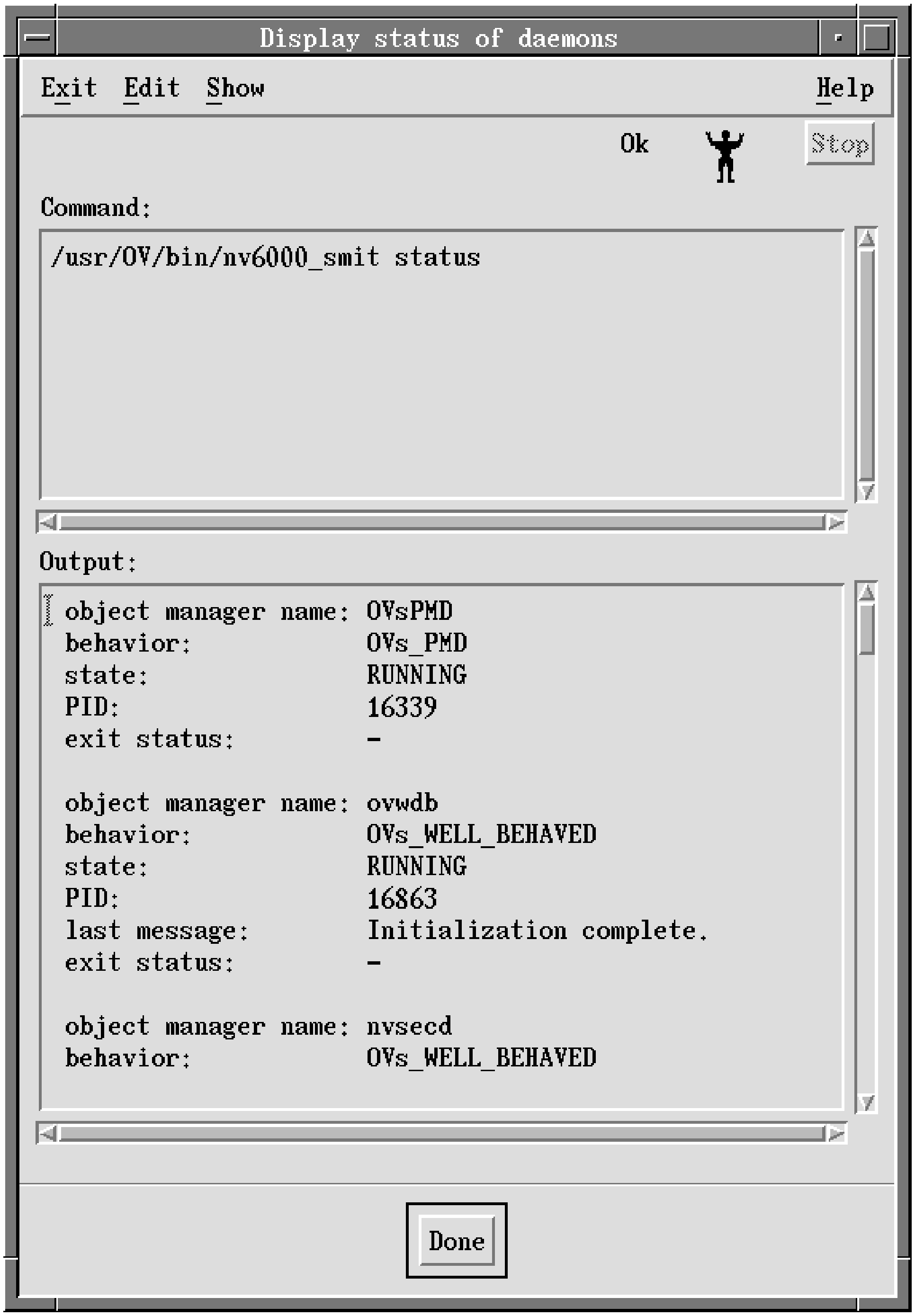
The Control menu is displayed.

Step 3. Select **Display NetView for AIX status**.

The Display NetView for AIX status menu is displayed.

Step 4. Select **Display status of daemons**.

All the NetView for AIX daemons and their status is displayed.



```
/usr/OV/bin/nv6000_smit status
```

```
object manager name: OVsPMD
behavior:            OVs_PMD
state:               RUNNING
PID:                 16339
exit status:         -

object manager name: ovwdb
behavior:            OVs_WELL_BEHAVED
state:               RUNNING
PID:                 16863
last message:        Initialization complete.
exit status:         -

object manager name: nvsecd
behavior:            OVs_WELL_BEHAVED
```

Figure 14. Display Status of Daemons Example

Starting NetView for AIX

Start the NetView for AIX program using SMIT or the **nv6000** shell script. SMIT uses the **nv6000** shell script to start the NetView for AIX program.

Using the nv6000 Shell Script

Use the **nv6000** shell script, which is executable whether you have root permissions or not, to start the NetView for AIX program. See the **nv6000** man page for information about the command options. If the /usr/OV/bin directory is not in your PATH, the /usr/OV/bin/nv6000 command path should be executed or add the directory /usr/OV/bin to your PATH.

Starting NetView for AIX Using SMIT

To start NetView for AIX using SMIT, follow these steps:

Step 1. Access SMIT by entering **smit nv6000**.

The NetView for AIX SMIT menu is displayed.

Step 2. Select **Control**.

The Control menu is displayed.

Step 3. Select **Start user interface**.

The Start daemons and user interface menu is displayed.

Step 4. Using the List option, make necessary changes to required entry fields.

Step 5. Select **Do**.

The NetView for AIX program is started and the selected map is displayed.

Step 6. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window is closed.

If the topology map does not appear, see Chapter 5, “Preparing to Use NetView for AIX” on page 51 to make sure all your files were loaded.

Logging Output

In some cases, NetView for AIX displays messages on the screen. Whether the NetView for AIX program is started from the command line or through SMIT, these messages and output from integrated applications are also logged in the $HOME/nv6000.log file. The **-nl** option is also useful if you have an application that writes realtime information to the stdout or stderr files, but you want to see the errors as they occur. For more explanation about some of the log file errors, refer to *NetView for AIX Diagnosis Guide*.

You can change the option to log output through the NetView for AIX SMIT Configure..Start user interface option or by starting the NetView for AIX program using the **nv6000 -nl** command. You might find this useful if you are running applications that produce a large amount of data. This prevents the log file from increasing and consuming system resources.

Generating the Map

When the daemons are first started, you can expect intense polling traffic, because the netmon daemon is working to discover objects on your network. The first time NetView for AIX creates a map on a client, especially if the database is NFS mounted, the synchronization may take several minutes.

Generally, a client machine is smaller than a server machine, but the client has to "learn" all the map information that the server already knows. When the client brings up the EUI, it synchronizes the information that it displays with the database information. The amount of time this takes varies according to the size of your network.

The graphical interface creates and displays an interactive, graphical map, which represents the logical topology of your network. For each map, an environment of interactive windows called submaps is created. A submap is a particular view of some part of the network that displays symbols that represent objects.

Defining the Network Management Region

The set of networks and nodes that the netmon daemon is monitoring define a management region. When the daemons are started for the first time, the default management region is the management system (the node on which the NetView for AIX program is executing) and the networks to which it is directly attached. The map's initial management region displays networks or subnets, segments, and gateways. Unmanaged nodes are displayed in beige.

Customizing Your Map

To expand and customize your submap, use the submap menu's `Options..Manage Objects` operation and the Edit menu's options if you have a map with read-write authorization. After an unmanaged network is managed, the netmon daemon starts discovering nodes for that network. Once again any new networks that are discovered are discovered as unmanaged. The management region is preserved between invocations of the graphical interface.

Using a Seed File

The initial management region can also be defined using a seed file. A seed file contains a list of host names, IP addresses, or a range of IP addresses. A seed file can be used to restrict network discovery or prioritize discovery so that the most important nodes are found first.

For information about creating a seed file, see "Using a Seed File to Customize Discovery" on page 82.

Discovering IP Objects

Only IP objects are discoverable by netmon. Initially, the topology map will contain the following objects:

- IP networks, gateways, and routers on the Internet submap
- Segments, gateways, routers, hubs, and bridges on the Network submaps
- Hosts, gateways, routers, hubs, and bridges on the Segment submaps

Instead of computers, some IP nodes that are connectors, such as bridges and repeaters, or devices, appear on the map as hosts. However, connectors that support IP and SNMP appear on the map as the appropriate connector. Whether or not the nodes are appropriately represented on the map is dependent on the ability of the management system to map a sysObjectID to an OVW symbol type. For information about mapping symbols to nodes, see “Mapping Symbols to Nodes” on page 91.

If an IP node supports SNMP, automatic topology map generation detects its existence, physical address, IP address, type of device, system Object ID, MIB data, and other information. If an IP node does not support SNMP, automatic topology map generation can detect only its existence, physical address, and IP address.

Discovering Non-IP Objects

When the netmon daemon discovers an IP node, it forwards the SNMP traps to the trapd daemon. The noniptopod daemon registers with the trapd daemon for notification of events that indicate an IP address has been discovered.

The noniptopod daemon then issues an snmpget request for all of the object IDs (OIDs) listed in the oid_to_command file. If an agent responds to the snmpget request, the start command associated with the OID is executed using the IP address as a parameter. The application started by the start command is now responsible for discovering objects supported by the applications protocol and forwarding its topology data to the gtmd daemon. You must register the noniptopod and gtmd daemons before you can start them.

See “Registering and Unregistering the Daemons” on page 70 for information on how to register these daemons.

For information about creating the non-IP protocol proprietary daemon, refer to the *NetView for AIX Programmer's Guide*.

Displaying Nodes

When putting symbols on a map, the management system matches the sysObjectID to a symbol type to be used in the map. If the system can match a sysObjectID to a symbol type, the node will be shown with the appropriate symbol in the map; if not, the node will be represented as a generic symbol. For more information about sysObjectID, see “Editing the oid_to_sym Registration File” on page 91.

A node appears as a gateway if its MIB value for IP forwarding is not zero, and the node has at least two interfaces. IP nodes with multiple interfaces on the same network may appear multiple times on segments. A node might also appear as a gateway if the gateway flag is set in the oid_to_type file. For more information about the oid_to_type file, see “Editing the oid_to_type Registration File” on page 93.

If a device within your domain is not specified on your name server, or in the /etc/hosts file, its IP address will be displayed and not its device name.

Map Layout Dependencies

The map layout and usefulness is dependent on four things:

- Correct subnet masks
- Correct IP addressing
- Network design principles that aid isolation of network faults and traffic
- SNMP-based, MIB-I (RFC 1156), or MIB-II (RFC 1158) compliant agents throughout the network

The automatically generated topology map showing your networks or subnets and the gateways that connect them is based on your internetwork’s IP addressing scheme. It is crucial that IP network (subnet) masks are correct at least on the management system, all SNMP gateways, all SNMP routers, and all nodes listed in the seed file. Otherwise, the automatically generated topology map could contain incorrect networks with nodes from outside your administrative domain.

Network Design Principles

The following design principles can result in a more useful topology map layout:

- The logical breakdown of an internet topology into manageable networks or subnetworks through gateways and IP addressing. For example, you can subdivide a large network into several subnetworks, through IP subnetting, with gateways to route among the subnetworks.
- The physical breakdown of networks or subnetworks into manageable segments through repeaters, bridges, multiport repeaters, and gateways. For example, you can subdivide a large segment into several smaller segments connected through a multiport repeater.

If the automatically-generated topology map layout is not as useful as you would like, you can use the graphical network map's editing operations to subdivide segments.

Accessing Online Help for the Graphical Interface

When the graphical network map is displayed, you can use the online Help facility to find task-specific information.

To access help for the graphical interface, select **NetView for AIX Help** from the Help pull-down menu.

Accessing NetView for AIX Online Books

To access the NetView for AIX online books, the DynaText documentation viewer code and the online information option must be installed. You can access the NetView for AIX online books by either of the following methods:

- If you have started the NetView for AIX program, select **Help** from the menu bar. From the Help menu, select **NetView for AIX Library**.
- If you have not started the NetView for AIX program, enter **/usr/ebt/bin/dtext** on the command line. This command starts the DynaText documentation viewer.

Restarting Automatic Map Generation

If a particular network on the map does not appear as it should, use the graphical interface to edit the map. However, if the entire map does not accurately represent your network, you might want to restart automatic map generation. You must have root permissions to perform this task.

The following list describes examples of when you might want to restart automatic map generation:

- IP topology of your entire management domain has changed dramatically.
- Map or topology databases are corrupted.
- Manager station has moved to another network.

Steps for Restarting Map Generation

Because all topology databases are removed when you restart map generation, you might want to back up your existing databases before you restart automatic map generation. You must have root permissions.

To back up the databases, stop all the daemons and enter the following command:

```
tar -cvf /tmp/filename /usr/OV/databases
```

Where *filename* is the name of the file in which the data will be saved.

If you need to restore the data, enter the following command:

```
tar -xvf /tmp/filename
```

Where *filename* is the name of the file in which you saved the data you want to restore.

To restart automatic map generation, follow these steps:

Step 1. Select **Exit** from the File pull-down menu.

This exits the graphical interface.

Step 2. Enter **smit nv6000** on the command line.

The NetView for AIX SMIT menu is displayed.

Step 3. Select **Control**.

The Control menu is displayed.

Step 4. Select **Restart automatic map generation**.

All the daemons are stopped. All existing databases, except Agent Policy Manager definitions, collection definitions, and master polling and discovery settings are deleted.

The /usr/OV/log/trapd.log, /usr/OV/log/ovevents.log, and /usr/OV/log/ovevents.log.BAK files are removed.

All the daemons are restarted.

Step 5. Run the **nv6000** shell script.

The NetView for AIX program is restarted and a new map is generated. However, if automatic discovery was turned off before you restarted the daemons, you will have to restart automatic discovery separately.

Note: When you use SMIT to restart map generation, all the daemons are stopped and restarted. When you use SMIT to clear map databases, all the daemons are stopped, but not restarted.

Restarting the Daemons

If the daemons stop running while the manager system is running, restart them using the **ovstart** command or SMIT. You must have root permissions to restart the daemons. You can restart all the NetView for AIX daemons or select individual daemons to restart. You can also use the **/etc/netnmrc** shell script, which starts all the daemons including the snmpd daemon. If you are starting daemons individually, all prerequisite daemons are automatically started.

Restarting the Daemons from the Command Line

Restart the daemons using the **ovstart** command. To restart all the daemons, enter:

```
/usr/OV/bin/ovstart
```

The **ovstart** command starts the process management daemon, ovspmd, and all of the background daemons.

Note: The **ovstart** command does not start the SNMP agent, snmpd, if it is not running. If the snmpd daemon is not running, use the command **startsrc -s snmpd** to start it before starting the other daemons, or invoke the **/etc/netnmrc** shell script.

By using the process name parameter, you can start one or more particular processes. To restart one daemon, for example the netmon daemon, enter:

```
/usr/OV/bin/ovstart netmon
```

In general, the names that you use to start the processes are obvious, but there are a few exceptions:

If this is the common name...	Use this name with ovstart
orsd	OVORS_M
ovelmd	ems_log_agent
ovesmd	ems_sieve_agent

Normally **ovstart** reports only if a process fails to start. The **-v** option requests “verbose” mode of operation, which produces information about what is occurring during the startup process. This option is useful for diagnosing problems. For example, to restart the netmon daemon with verbose mode, enter:

```
/usr/OV/bin/ovstart -v netmon
```

If a daemon requires other daemons to be running, the prerequisite daemons are started automatically.

Restarting NetView for AIX Daemons Using SMIT

To restart NetView for AIX daemons with SMIT, follow these steps:

Step 1. Access SMIT using one of the following methods:

- Enter **smit nv6000** on the command line.
- Select **NetView SMIT** from the Administer pull-down menu.

The NetView for AIX SMIT menu is displayed.

Step 2. Select **Control.**

The Control menu is displayed.

Step 3. Do one of the following:

- Select **Restart all stopped daemons** to restart all the daemons.

  All the daemons are restarted. Go to Step 9.

- Click on **Select daemons to stop or restart** to select individual daemons to restart.

  Go to Step 4.

Step 4. Select one of the following:

- **Set options for topology, discovery, and database daemons**
- **Set options for event and trap processing daemons**
- **Set options for host connection daemons**
- **Set options for Agent Policy Manager daemons**

Step 5. Select the **List** button next to the daemon you want to restart.

Step 6. Select **restart**.

Step 7. Repeat Steps 4 through 6 for each category of daemons you want to restart.

Step 8. Select **Do**.

All selected daemons are restarted.

Step 9. Select **Exit SMIT** from the Exit pull-down menu.

SMIT window is closed.

Registering and Unregistering the Daemons

The gtmd, noniptopod, C5d, tralertd, and spappld daemons are not automatically registered in the startup file. Therefore, these daemons do not get started as part of the default startup process. These daemons must be registered before they can be started. Once they are registered, they are started every time you execute the **nv6000** command as root and the **ovstart** command or you start the system, until you unregister the daemons. You can use SMIT or the **ovaddobj** command to register the daemons. SMIT executes the **ovaddobj** command.

Registering and Starting Daemons from the Command Line

Use the following commands to register and start a daemon:

```
/usr/OV/bin/ovaddobj /usr/OV/lrf/daemon.lrf

/usr/OV/bin/ovstart daemon
```

Where *daemon* is the name of the daemon you are registering as shown in the following example:

```
/usr/OV/bin/ovaddobj /usr/OV/lrf/noniptopod.lrf

/usr/OV/bin/ovstart noniptopod
```

Registering and Starting Daemons Using SMIT

To use SMIT to register the daemons, follow these steps:

Step 1. Access SMIT using one of the following methods:

- Enter **smit nv6000** on the command line.
- Select **NetView SMIT** from the Administer pull-down menu.

The NetView for AIX SMIT menu is displayed.

Step 2. Select **Configure**.

The Configure menu is displayed.

Step 3. Select **Set options for daemons**.

The Set options for NetView for AIX daemons menu is displayed.

Step 4. Select one of the following:

- **Set options for topology, discovery, and database daemons**
- **Set options for event and trap processing daemons**
- **Set options for host connection daemons**
- **Set options for Agent Policy Manager daemons**

Step 5. Select the daemon you want to register.

The dialog box for the selected daemon is displayed.

Step 6. Select the **Do** button. You do not need to change the defaults in the entry fields.

The daemon is registered and added to the startup file.

Step 7. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window is closed.

If you decide not to use these daemons and do not want them started, you must unregister the daemons. See “Unregistering Daemons” on page 72 for those instructions.

Unregistering Daemons

Using SMIT, you can delete daemons from the startup file to prevent them from being started. You must have root permissions to perform this task.

Deleting unused daemons from the ovsuf file improves utilization of system resources. You can delete the following daemons from the ovsuf file:

- spappld
- tralertd
- gtmd
- noniptopod
- trapgend

Using SMIT to Unregister Daemons

To delete daemons from the ovsuf file, follow these steps:

Step 1. Access SMIT using one of the following methods:

- Enter **smit nv6000** at the command line.
- Select **NetView SMIT** from the Administer pull-down menu.

The NetView for AIX SMIT menu is displayed.

Step 2. Select **Configure**.

The Configure menu is displayed.

Step 3. Select **Delete daemon from ovsuf startup file**.

The Delete daemon from ovsuf startup file dialog box is displayed.

Step 4. Using the **List** button, select the daemon you are deleting.

The selected daemon is displayed in the Daemon to delete field.

Step 5. Select **Do**.

The information is processed and the daemon is deleted.

Step 6. Repeat Steps 4 and 5 for each daemon you are deleting.

The selected daemons are deleted from the startup file, but the daemons are not stopped if they are running.

Step 7. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window is closed.

If you decide to use the daemon you deleted, you must register the daemon in the ovsuf file before you start it. For more information, see “Registering and Unregistering the Daemons” on page 70.

Stopping NetView for AIX

To stop the EUI, select **Exit** from the File pull-down menu. Selecting Exit does not stop the daemons, only the EUI.

If you want the NetView for AIX program to continuously monitor and track changes to your network and the management system, always keep netmon, trapd, ovwdb, ovtopmd, snmpCollect, trapgend, and snmpd, running, even if the graphical network topology map (EUI) is not operational. If you are performing multiprotocol management, the gtmd and noniptopod daemons should be running also. If you are using the Agent Policy Manager application, the C5d daemon should be running. If you have a host connection, keep tralertd and spappld running.

Stopping the Daemons

Use the command line or SMIT to stop the daemons. You must have root permissions to perform this task.

Stopping the Daemons Using the Command Line

To stop all the daemons using the command line, exit the EUI and any other applications that use the daemons. Enter:

```
/usr/OV/bin/ovstop
```

All the daemons are stopped, except the nvsecd and ovspmd. The nvsecd daemon must be running for the NetView for AIX program to run, and ovspmd must be running if any of the other daemons are running (like nvsecd). If you stop nvsecd, all users are logged out, so limit stopping nvsecd to workstation shutdown or problem resolution situations. You can stop the nvsecd and the ovspmd daemons individually.

To stop an individual daemon, such as the nvsecd daemon, enter:

```
/usr/OV/bin/ovstop nvsecd
```

Warning: Do not stop daemons that are dependent on other daemons. This can corrupt your database.

To stop several daemons at the same time, list each daemon that you want to stop. For example, to stop the ovwdb, ovtopmd, and netmon daemons, enter:

```
/usr/OV/bin/ovstop ovwdb ovtopmd netmon
```

Note: The **ovstop** command does not stop the nettl facility. To stop the nettl facility, enter:

```
/usr/OV/bin/nettl -stop
```

Stopping the Daemons Using SMIT

To stop NetView for AIX daemons using SMIT, follow these steps:

Step 1. Access SMIT using one of the following methods:

- Enter **smit nv6000** on the command line.
- Select **NetView SMIT** from the Administer pull-down menu.

The NetView for AIX SMIT menu is displayed.

Step 2. Select **Control.**

The Control menu is displayed.

Step 3. Do one of the following:

- To stop all the daemons, select **Stop all running daemons**.

  All daemons are stopped. Go to Step 9.

- To stop individual daemons, click on **Select daemons to stop or restart**.

  Go to Step 4.

Step 4. Select one of the following:

- **Set options for topology, discovery, and database daemons**
- **Set options for event and trap processing daemons**
- **Set options for host connection daemons**
- **Set options for Agent Policy Manager daemons**

Step 5. Select the **List** button next to the daemon you want to stop.

Step 6. Select **stop**.

Step 7. Repeat Steps 4 through 6 for each category of daemons you want to stop.

Step 8. Select **Do**.

All selected daemons are stopped.

Step 9. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window closes.

Chapter 8. Optional Configuration Tasks

This chapter describes additional ways you can configure the NetView for AIX program. The following configuration options are described:

- “Changing Daemon Defaults”
- “Installation Entries” on page 81
- “Using a Seed File to Customize Discovery” on page 82
- “Unregistering Daemons” on page 72
- “Changing File Owner, Group, or Mode” on page 90
- “Mapping Symbols to Nodes” on page 91
- “Editing the oid_to_command Registration File” on page 97
- “Editing the oid_to_protocol Registration File” on page 98
- “Redirecting AIXwindows Display” on page 99
- “Using a Relational Database for Data Storage” on page 100
- “Configuring for Backup Manager” on page 100
- “Configuring SNMP Values” on page 100

Changing Daemon Defaults

Changing the defaults for the daemons is not necessary. However, you might want to configure the daemons to use values different from the defaults provided. For example, if you want netmon to start discovery using a seed file or if you have a device that supports secondary addressing, go to the netmon daemon dialog box and change the defaults for those options. Or, if you want the ovtopmd daemon to use an SQL relational database, go to the ovtopmd daemon dialog box and change the default for that option.

You can change the defaults using the command line or SMIT. This section describes the steps for using SMIT. Refer to the *NetView for AIX Administrator's Reference* for information about using the command line to set daemon options. Using SMIT prevents the possibility of creating errors in the LRF files. You must have root permissions to set options for the NetView for AIX daemons.

When you change the daemon options using SMIT, SMIT does the following:

- Updates the LRF files
- Updates the ovsuf startup files
- Stops and starts the daemons using the new values

From then on, when you start the system or execute the **nv6000** and **ovstart** commands, the new values are used.

You can change the defaults for the following daemons:

- Topology discovery and database daemons

  netmon
  ovtopmd
  ovwdb
  noniptopod
  gtmd

- Event and trap processing daemons

  pmd
  orsd
  trapd
  trapgend
  snmpCollect
  ovelmd
  ovactiond

- Host connection daemons

  tralertd
  spappld

- Collection and Agent Policy Manager daemons

  Agent Policy Manager

Refer to the *NetView for AIX and the Host Connection* for information about configuring host connection daemons.

Using SMIT to Change Daemon Defaults

To use SMIT to change the defaults of the daemons, follow these steps:

Step 1. Access SMIT using one of the following methods:

- Enter **smit nv6000** on the command line.
- Select **NetView SMIT** from the Administer pull-down menu.

The NetView for AIX SMIT menu is displayed.

Step 2. Select **Configure**.

The Configure menu is displayed.

Step 3. Select **Set options for daemons**.

The Set options for daemons menu is displayed.

Step 4. Select one of the following:

- **Set options for topology discovery and database daemons**
- **Set options for event and trap processing daemons**
- **Set options for host connection daemons**
- **Set options for Agent Policy Manager daemons**

The selected choice menu is displayed.

Step 5. Select a daemon.

The daemon dialog box is displayed.

Step 6. Make the necessary changes to the defaults in the entry fields.

Step 7. Select **Do**.

The information is processed and the options are set.

Step 8. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window is closed.

Understanding the Daemons, Options, and Defaults

This section lists the daemons, their options, and their defaults as they appear in SMIT. Refer to the *NetView for AIX Administrator's Reference* or use the SMIT online help facility for more information about the options.

Note: The LANG variable must be set to a valid language setting other than C to access SMIT help. For example, for English language users, use the following command to set this variable: **export LANG=En_US**.

Topology Discovery and Database Daemons

Table 4 on page 78 lists all the topology discovery and database daemon options and defaults.

Table 4. Discovery and Database Daemon Options

Daemon	Option	Default
netmon	Full path name of SysObjectID file	/usr/OV/conf/oid_to_type
	Tracing mask	0
	Full path name of trace file	/usr/OV/log/netmon.trace
	Ring bit-swapping storage flag	none
	Secondary addressing support?	no
	Load seed file from	
	Speed node discovery?	no
	Unnumbered IP address support?	no
	Ignore source route bit in physical address?	no
	Use Systems Monitor MLM feature?	no
	Full path of Systems Monitor MLM seed file	
	Use Systems Monitor MLM feature for discovery?	no
	Systems Monitor MLM domain collection prefix	mlmDomain_
ovtopmd	Do you want to use an SQL relational database?	no
	Port used to receive request over tcp	yes
ovwdb	Number of objects to hold in cache	5000
	Port used to receive request over tcp	yes
noniptopod	Full path name of configuration file	/usr/OV/conf/oid_to_command
gtmd	Full path name of log file	/usr/OV/log/gtmd.log
	Full path name of trace file	/usr/OV/log/gtmd.trace
	Seconds between storing data to database	900
	Buffers allocated for trap data before sending to xxmap	1000

Event and Trap Processing Daemons

Table 5 lists all the event and trap processing daemons, options, and defaults.

Table 5 (Page 1 of 2). Event and Trap Processing Daemon Options

Daemon	Option	Default
pmd	Allow the pmd to receive SNMP	traps
	Allow the pmd to receive CMOT request over	both (tcp and udp)
	Allow the pmd to receive CMOT events over	both (tcp and udp)
	Number of users to bind above the pmd	40
	Maximum time (minutes) to keep an association open without traffic	15
	Maximum time (minutes) to wait for association open without traffic	2
	Maximum number of network connections that pmd can support	1024
	Maximum time to wait for response to confirmed request to a local agent	4 (minutes)
	Maximum time to wait for response to confirmed request to a remote agent	6 (minutes)
orsd	Time (minutes) to check if garbage collection needed	0
	Percent data in database before garbage collection needed	60
	Bytes of shared memory allocated to ORS cache (inbound)	100
	Bytes of shared memory allocated to ORS cache (outbound)	100
	Bytes of shared memory allocated to ORS cache (proxy)	100

Table 5 (Page 2 of 2). Event and Trap Processing Daemon Options

Daemon	Option	Default
trapd	Log events and traps?	yes
	Full path name of log file	/usr/OV/log/trapd.log
	Full path name of trace file	/usr/OV/log/trapd.trace
	Hex dump all packets received/sent by trapd?	no
	Receive buffer size for TCP/UDP socket	9216
	Create socket connection for V1R1 applications?	no
	Maximum size of trapd.log file: (Kbytes)	4096
	Full path name of trapd log maintenance script	N/A
	Destination hostname for forwarded traps	N/A
	Port used to receive snmp traps over udp	162
	Port used to receive snmp traps over tcp	162
trapgend	Maximum size log file in kilobytes	100
	Maximum number of log files	5
	Full path name of log and trace file	/usr/OV/log/trapgend.log
	Throttle time (seconds) for trap generation	60
	Trace events	none
snmpCollect	Defer time when node down, minutes	1440
	Full path name of trace file	/usr/OV/log/snmpCol.trace
ovelmd	Maximum size of ovevent.log file (Kbytes)	128
ovactiond	Full path name of log file	/usr/OV/log/ovactiond.log
	Traces the execution of ovactiond?	no
	Make command output verbose?	no
	Max wait time for command to execute?	300

Agent Policy Manager Daemons

Table 6 lists all the Agent Policy Manager daemons, options, and defaults.

Table 6. Collection and Agent Policy Manager Daemon Options

Daemon	Option	Default
collection	Do you want to start the Collection Facility	no
Agent Policy Manager	Full path name of log file	/usr/OV/log/C5dlog
	Traces the execution of ovactiond?	no
	Full path name of trace file	/usr/OV/log/C5dtrace
	Number of minutes between daemon attempts	60
	Number of threshold events stored in history file	200

Installation Entries

The installation procedure adds the following entries for NetView for AIX's processes to the following files. These entries should not be changed.

Table 7 (Page 1 of 2). Installation Entries

Entry	Process	File
`/etc/netnmrc`	Background daemons	/etc/rc.tcpip
`snmp 161/udp`	TCP/IP Agent (snmpd process)	/etc/services
`cmot_manager 163/tcp`	pmd	/etc/services
`cmot_manager 163/udp`	pmd	/etc/services
`cmot_agent 164/tcp`	pmd	/etc/services
`cmot_agent 164/udp`	pmd	/etc/services
`ovwdb 9999/tcp`	ovwdb	/etc/services
`ovtopmd 8888/tcp`	ovtopmd	/etc/services
`gtmd 2112/tcp`	gtmd	/etc/services
`xxmd 3313/tcp`	gtmd	/etc/services
`snmp-trap 162/udp`	pmd	/etc/services
`snmp-trap 162/tcp`	pmd	/etc/services
`nvtrapd-trap 162/tcp`	trapd	/etc/services
`nvtrapd-trap 162/udp`	trapd	/etc/services
`nvtrapd-client 2213/tcp`	trapd	/etc/services
`smux 1.3.6.1.4.1.2.6.4.1 nv6000`	trapgend	/etc/snmpd.conf

Table 7 (Page 2 of 2). Installation Entries

Entry	Process	File
`trapgend 1.3.6.1.4.1.2.6.4.1 nv6000`	trapgend	/etc/snmpd.peers

Using a Seed File to Customize Discovery

A seed file is an ASCII file that helps you tell the netmon discovery daemon which nodes in your network should and should not be discovered. A seed file can contain IP addresses, host names, IP address ranges, and optional comments. The devices listed in the seed file should support SNMP.

Listing non-SNMP devices (or SNMP devices whose community names you do not know) in the seed file can negatively affect the discovery process. In general, netmon determines a device's subnet based on the IP address and subnet mask of the last router in the path to the device. If netmon does not know the path to the device (for example, if the device is listed at the top of the seed file), netmon tries to get SNMP information from the device to determine the subnet mask. If the device is non-SNMP and netmon does not know the path, netmon looks at the class of the IP address and takes the corresponding subnet mask.

You have a non-SNMP device in your seed file whose subnet mask does not match the class of the IP address, and netmon does not know the path to the device. Therefore, you should not put non-SNMP devices in your seed file.

Format of a Seed File

The format of the seed file is a list of host names, IP addresses, or IP address ranges of SNMP nodes within your administrative domain. Each host name, IP address, or IP address range must be listed on separate lines. Comments, preceded by the # symbol, are permitted after the host name, IP address, or IP address range on a line.

Note: You choose the name and location of the seed file. The seed file name you choose cannot contain a colon. Seed file names are saved in the LRF file for netmon. Because the LRF file uses a colon as a separator, do not use a colon in the seed file name.

Seed File Format Examples

The following example shows the format of a seed file that expands the initial discovery process:

```
node1.division.company.com
router4.division.company.com      #Gateways make the best seeds
9.67.1.5
```

The following example shows the format of a seed file that limits the discovery process:

```
router2.division.company.com
router3.division.company.com
9.67.179.70-79
9.67.179.200
9.*.160.*
```

Routers are included in this example to provide a path to the nodes within the IP address range 9.67.179.70-79 that are more than one router away from the management station.

Note: You can use an asterisk (*) to match any number.

How netmon Uses a Seed File

The following factors affect how netmon uses a seed file:

- Whether New Node Discovery is turned on or off.
- Whether there are specific IP addresses or host names specified in the seed file. Listing specific IP addresses or host names in the seed file tells netmon which nodes to discover.
- Whether there are IP address ranges specified in the seed file. Listing IP address ranges in the seed file tells netmon which nodes *not* to discover.

A seed file can contain both specific IP addresses, host names, and IP address ranges. A single seed file, therefore, can tell netmon which nodes to discover and which nodes *not* to discover. Table 8 summarizes how discovery can be affected by the New Node Discovery setting and the contents of the seed file:

Table 8 (Page 1 of 2). The Discovery Process Using a Seed File

New Node Disc Switch	IP Address Range	Specific IP Addresses and/or Names	Minimum discovered (*)	Maximum discovered
OFF	No	No	NetView for AIX workstation	NetView for AIX workstation
OFF	No	Yes	The nodes listed in the seed file	The nodes listed in the seed file
OFF	Yes	No	NetView for AIX workstation	All nodes that reside within the range(s)
OFF	Yes	Yes	The nodes listed in the seed file	The nodes listed in the seed file, plus all nodes that reside within the range(s)
ON	No	No	NetView for AIX workstation	All nodes in your network
ON	No	Yes	The nodes listed in the seed file	All nodes in your network
ON	Yes	No	NetView for AIX workstation	All nodes that reside within the range(s)

Table 8 (Page 2 of 2). The Discovery Process Using a Seed File

New Node Disc Switch	IP Address Range	Specific IP Addresses and/or Names	Minimum discovered (*)	Maximum discovered
ON	Yes	Yes	The nodes listed in the seed file	All nodes that reside within the range

* Netmon always discovers the node on which netmon resides, regardless of seed file or New Node Discovery settings.

Telling netmon Which Nodes to Discover

By listing specific IP addresses and host names in a seed file, you can tell netmon which nodes it should discover. If you place a specific IP address in a seed file, the node that has that IP address will be discovered as long as the IP address responds to a ping.

When you are building your seed file, consider the following facts:

- If New Node Discovery is turned off, netmon still tries to discover the nodes whose IP addresses are listed in the seed file.
- If New Node Discovery is turned on, netmon tries to discover all of the nodes in the seed file first, and then it tries to discover additional nodes not listed in the seed file. In other words, if New Node Discovery is turned on, netmon will not limit itself to only the IP addresses specifically listed in the seed file.
- If you cannot ping an IP address in the seed file, netmon cannot create a node for the IP address.
- If netmon discovers an IP address in the seed file in a network that has not been discovered yet, netmon will create and manage that network.
- If netmon discovers a node, it discovers all IP addresses on that node, regardless of whether those IP addresses are listed in the seed file.
- netmon always discovers the node on which netmon resides regardless of whether New Node Discovery is on, and regardless of whether that node is listed in the seed file.

Telling netmon Which Nodes Not to Discover

By listing one or more IP address ranges in a seed file, you can tell netmon to ignore all IP addresses that are *outside* those ranges. A range is very much like a filter.

When you are building your seed file, consider the following facts and exceptions:

- Specifying ranges does not guarantee that netmon will discover nodes within those ranges; it guarantees that netmon will *not* discover nodes that are *outside* of the ranges. To make sure that netmon discovers a node within a range, see “Ensuring That netmon Discovers Nodes in a Seed File Range” on page 85.

- netmon always discovers the node on which netmon resides regardless of whether New Node Discovery is on, and regardless of whether that node is within the IP address ranges listed in the seed file.
- When netmon discovers a node, it discovers all IP addresses on that node, regardless of whether those IP addresses lie outside the ranges in the seed file.
- If New Node Discovery is turned off, netmon ignores whether you specified IP address ranges in the seed file.
- netmon discovers individual IP addresses and host names in a seed file regardless of whether they lie outside the ranges in the seed file.
- When netmon discovers a node, the node will not be deleted as a result of changing your seed file (although the node might be deleted for other reasons). You cannot redefine IP address ranges in the seed file to remove existing nodes from your map.

Ensuring That netmon Discovers Nodes in a Seed File Range

To make sure that netmon discovers a node that lies within a seed file IP address range, the following criteria must be met:

- The network in which the node resides must be managed in the IP topology database.
- netmon must be instructed to discover an IP address in the node.

There are several various ways to make sure that the network in which the node resides is managed in the IP topology database:

- Manually add the network symbol using the EUI.
- Make sure that the gateway leading to that network is discovered and manually manage the network symbol on the map.
- Put the node's address in the seed file. If a node's IP address is written in the seed file, netmon will automatically create its network.
- Put the IP address of another node that is in the same network in the seed file to tell netmon to create its network.

When the network is managed in the IP topology database, netmon needs to "learn" the existence of the IP addresses of the nodes you want netmon to discover. In most cases, once netmon discovers the network, netmon can discover the nodes inside the network by checking various tables in various MIBs of nodes that it has already discovered. In some cases, netmon might have no way of learning of the existence of that node. For example, the node might generate too little network traffic. When this happens, and you want to guarantee that netmon discovers the node, provide these specific IP addresses in the seed file. See "Understanding Examples of Seed File Setup and Usage" on page 86 for examples.

Understanding Examples of Seed File Setup and Usage

This section shows you examples of how you can use a seed file.

Telling netmon Where to Start Looking for Nodes Without Limiting Discovery

If you want NetView for AIX to use your seed file as a starting point and then go discover the rest of the nodes, complete the following steps:

Step 1. Create a seed file that contains only a list of individual IP addresses and hostnames. See “Telling netmon Which Nodes to Discover” on page 84 for a list of considerations for this seed file.

Step 2. Enter **smit nv6000** on the command line.

The NetView for AIX SMIT menu is displayed.

Step 3. Select **Configure**.

The Configure menu is displayed.

Step 4. Select **Set options for daemons**.

The Set options for daemons menu is displayed.

Step 5. Select **Set options for topology discovery and database daemons**.

The Set options for topology discovery and database daemons menu is displayed.

Step 6. Select **Set options for netmon daemon**.

The Set options for netmon daemon dialog box is displayed.

Step 7. Enter the name of the seed file in the Load seed file from field.

Step 8. Select **Do**.

Step 9. Exit SMIT.

Step 10. Restart NetView for AIX using SMIT or the **nv6000** command.

If you do this procedure, netmon does not limit itself to discovering only the nodes in the seed file. You can use this procedure to make sure that netmon discovers certain nodes, especially nodes that are more than one hop beyond the management station.

Limiting Discovery to the Nodes Individually Listed in the Seed File

If you want NetView for AIX to discover only the nodes in the seed file, complete the following steps:

Step 1. Create your seed file. See “Telling netmon Which Nodes to Discover” on page 84 for a list of considerations for this seed file.

Step 2. Clear the topology database.

Step 3. Enter **ovstart ovtopmd** to start the topology database.

Step 4. Enter **ovstart OVORS_M**.

Step 5. Enter **ovw** to start the NetView for AIX EUI.

Step 6. Select **Options** from the menu bar.

Step 7. Select **Topology/Status Polling Intervals: IP** from the Options menu.

Step 8. Turn the New Node Discovery Switch to **off**.

Step 9. Select **OK**.

Step 10. Select **File** from the menu bar and exit the EUI.

Step 11. Enter **smit nv6000** at the command line.

The NetView for AIX SMIT menu is displayed.

Step 12. Select **Configure**.

The Configure menu is displayed.

Step 13. Select **Set options for daemons**.

The Set options for daemons menu is displayed.

Step 14. Select **Set options for topology discovery and database daemons**.

The Set options for topology discovery and database daemons menu is displayed.

Step 15. Select **Set options for netmon daemon**.

The Set options for netmon daemon dialog box is displayed.

Step 16. Enter the name of the seed file in the Load seed file from field.

Step 17. Select **Do**.

Step 18. Exit SMIT.

Step 19. Restart NetView for AIX using SMIT or the **nv6000** command.

Limiting Discovery to a Range of Nodes Using Seed File Wildcards

To limit discovery to the nodes within a certain range or ranges of IP addresses, complete the following steps:

Step 1. Create your seed file. See “Telling netmon Which Nodes Not to Discover” on page 84 for a list of considerations for this seed file. At least one of the lines in the seed file must contain a wildcard character (either * or -).

Step 2. Clear the topology database.

Step 3. Enter **ovstart OVORS_M**.

Step 4. Enter **smit nv6000**.

The NetView for AIX SMIT menu is displayed.

Step 5. Select **Configure**.

The Configure menu is displayed.

Step 6. Select **Set options for daemons**.

The Set options for daemons menu is displayed.

Step 7. Select **Set options for topology discovery and database daemons**.

The Set options for topology discovery and database daemons menu is displayed.

Step 8. Select **Set options for netmon daemon**.

The Set options for netmon daemon dialog box is displayed.

Step 9. Enter the name of the seed file in the Load seed file from field.

Step 10. Select **Do**.

Step 11. Exit SMIT.

Step 12. Restart NetView for AIX using SMIT or the **nv6000** command.

Again, specifying a range in a seed file does not guarantee that netmon can discover anything within the range. When you specify a range, you are telling NetView for AIX *not* to discover anything *outside* the ranges. To make sure that nodes within the range are discovered, you should explicitly list a few specific IP addresses in the seed file that fall within the range. A range is like a filter, and specifying a range by itself does not help the netmon daemon discover nodes.

You can use an IP address range in a seed file to limit discovery to a list of specific IP addresses without turning New Node Discovery off. To do this, create a seed file that contains a list of IP addresses and an IP address range that you know would have no IP addresses in it. For example, if you only want to discover IP addresses 1.1.1.1 and 1.1.1.2, and you know that you do not have any IP addresses in the range 3.*.*.*, you would create a seed file that look like this:

```
1.1.1.1
1.1.1.2
3.*.*.*
```

This seed file would limit the discovery to the two IP address, and it would not require that you turn off New Node Discovery.

Configuring netmon to Use a Seed File

You can configure the netmon daemon to use a Mid-Level Manager (MLM) seed file or any other kind of seed file. When you configure netmon to use a seed file that contains a list of Mid-Level Manager nodes, the Mid-Level Manager polls nodes in its own domain and reports status changes to the NetView for AIX program. The MLM seed file makes sure that your Mid-Level Manager nodes are discovered quickly. Refer to the Systems Monitor documentation for more information about the Mid-Level Manager.

To configure the netmon daemon to use any seed file, you must have root permissions. Complete the following steps:

Step 1. Access SMIT using one of the following methods:

- Enter **smit nv6000** at the command line.
- Select **NetView SMIT** from the Administer pull-down menu.

The NetView for AIX SMIT menu is displayed.

Step 2. Select **Configure**.

The Configure menu is displayed.

Step 3. Select **Set options for daemons**.

The Set options for daemons menu is displayed.

Step 4. Select **Set options for topology, discovery, and database daemons**.

The Set options for topology, discovery, and database daemons menu is displayed.

Step 5. Select **Set options for netmon daemon**.

The Set options for netmon daemon dialog box is displayed.

Step 6. Do one of the following:

- To use a Mid-Level Manager seed file, use the **List** button to select **yes** in the Use Systems Monitor MLM entry field.

  Go to Step 7.
- To use a seed file other than a Mid-Level Manager seed file, type the full path name of the seed file you want to load in the Load seed file from field.

  Go to Step 8.

Step 7. Type the full path name of the Mid-Level Manager seed file in the Full path name of Systems Monitor MLM seed file field.

Step 8. Select **Do**.

The information is processed. The netmon daemon will use the specified seed file the next time the netmon daemon is started.

Step 9. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window is closed.

If you are using a seed file to limit the discovery process, restart map generation to remove nodes from the database and put only those nodes listed in the seed file into the database. When you restart map generation, all existing databases are removed. When you restart the NetView for AIX program, the seed file is used to generate a new map. See "Restarting Automatic Map Generation" on page 68 for information about how to restart map generation.

After initial map generation using a seed file, any expansion of the topology map takes precedence over the contents of the seed file. However, if the seed file contains nodes not already on the topology map, these nodes and their corresponding networks are added to the topology map when the netmon daemon is started. The seed file is used every time the netmon daemon is started.

Changing File Owner, Group, or Mode

You can use SMIT to change file owners, file groups, and file modes for all NetView for AIX topology database files. You must have root permissions to perform this task. These changes do not affect the owner, group, or mode for directories.

To change an owner, group, or mode, follow these steps:

Step 1. Exit the graphical map and all NetView for AIX windows.

The graphical interface windows close.

Step 2. Access SMIT using one of the following methods:

- Enter **smit nv6000** from the command line.
- Select **NetView SMIT** from the Administer pull-down menu.

The NetView for AIX SMIT menu is displayed.

Step 3. Select **Configure**.

The Configure menu is displayed.

Step 4. Select **Change Map(s) owner/group/mode**.

The Change Map(s) owner/group/mode dialog box is displayed.

Step 5. Type or select from the List option:

- User ID of new owner
- Group ID of new group
- Permission codes for new mode read (4), write (2), or execute (1). To specify a group of permissions, add together the appropriate octal numbers:

  3 = -wx (2 + 1)
  6 = rw- (4 + 2)
  7 = rwx (4 + 2 + 1)
  0 = --- (no permissions)

- Change global map permissions owner/group/mode only
- Map name to change
- List current permissions, owner, and group

The information is displayed in the entry fields.

Step 6. Select **Do**.

The information is processed.

Step 7. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window is closed.

Mapping Symbols to Nodes

The nodes in your network are represented in the graphical interface as symbols. The NetView for AIX program displays these symbols based on mappings from the sysObjectID to symbol types, vendors, SNMP agents, and IP topology attributes. This mapping is done using the following configuration files:

- oid_to_sym

  The IPMap and xxmap applications use the oid_to_sym configuration file. The /usr/OV/conf/C/oid_to_sym registration file specifies a mapping from the sysObjectID of an agent to a default symbol class and subclass. The NetView for AIX program chooses an appropriate symbol type to represent nodes in the IP topology maps in the graphical interface based on the value of sysObjectID.

- oid_to_type

  The netmon daemon uses the oid_to_type configuration file to map the sysObjectID of a node into the correct IP topology behavior and to the correct vendor and SNMP agent values. The /usr/OV/conf/oid_to_type registration file specifies a mapping from the sysObjectID of an agent to the correct IP topology behavior and to the correct vendor and SNMP agent values. The oid_to_type file shipped with the NetView for AIX product contains entries for specific network devices.

This section describes how you can edit these files so that the nodes in your network will be represented with an appropriate symbol in the graphical interface.

Editing the oid_to_sym Registration File

The oid_to_sym file shipped with the NetView for AIX program contains entries for various agents. You can edit these entries or add new ones.

Steps for Adding an Entry to the oid_to_sym File

Use SMIT to add or change entries in the oid_to_sym file. Edit the oid_to_sym file using your text editor to delete entries from the file. You must have root permissions to perform this task.

To add an entry to the oid_to_sym file, follow these steps:

Step 1. Access SMIT using one of the following methods:

- Enter **smit nv6000** from the command line.
- Select **NetView SMIT** from the Administer pull-down menu.

The NetView for AIX SMIT menu is displayed.

Step 2. Select **Configure**.

The Configure menu is displayed.

Step 3. Select **Configure object identification registration files**.

The Configure object identification registration files menu is displayed.

Step 4. Select **Update oid_to_sym registration files**.

The Update oid_to_sym registration file dialog box is displayed.

Step 5. Type, or select from the List option, required information in the entry fields.

See “Field Definitions” for information about the fields.

Step 6. Select **Do**.

The information is processed and the entry is added or changed.

Step 7. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window is closed.

Note: Existing symbols will not be changed. You can change these with the `Edit..Change symbol type` operation.

Example of an oid_to_sym File

Each entry in the oid_to_sym file consists of three fields separated by a colon (:). The following example is from the default oid_to_sym file:

```
# IBM Network Enterprises
1.3.6.1.4.1.2.3.1.2.1.1.2:Computer:Workstation   # IBM AIX workstation
1.3.6.1.4.1.2.2.1.2.2:Computer:PC                # IBM TCP/IP Agent on OS2
1.3.6.1.4.1.2.6.1:Connector:Bridge               # IBM 3172 LAN attachment
1.3.6.1.4.1.2.2.1.2.3:Computer:Main Frame        # IBM 3090 TCP/IP Agent
```

Field Definitions

The following list describes the fields used in an entry of the oid_to_sym file (as shown in the example).

- The first field is the value of the Internet-standard MIB-II system.sysObjectID reported by the device’s SNMP agent. For example:

  `1.3.6.1.4.1.11.2.3.2.2.`

- The second field is the default symbol class. Valid symbol class entries are connector, computer, or device. The default value is **computer**.

- The third field is the default symbol subclass. Some valid symbol subclass entries for the computer class are workstation, mini, and PC.

The class and subclass fields together make up the OVW symbol type. The number symbol (#) indicates the beginning of a comment. Blank lines are ignored.

The values for symbol class and subclass must match one of the registered symbol types with the graphical interface, or you can create new ones. To see the currently defined symbols, see the /usr/OV/symbols/C registration files or `Help..Legend`. To learn how to create new symbols, refer to the *NetView for AIX Programmer's Guide*.

Example of Changing a Symbol: If you want to change the symbol for a RISC System/6000 320 agent from the default symbol subclass Workstation to a minicomputer, edit the following line:

```
1.3.6.1.4.1.11.2.3.2.2:Computer:Workstation   # 320
```

to look like this:

```
1.3.6.1.4.1.11.2.3.2.2:Computer:Mini          # 320
```

When you add new symbol types you can add or change entries in the oid_to_sym file to take advantage of the new symbols. However, the symbol class and subclass must always match the list of symbols supported by the graphical interface. If they do not match, ipmap may not be able to add the symbol to the IP topology map.

Editing the oid_to_type Registration File

You can edit the existing file and add or change lines as needed.

Making Changes to the oid_to_type File

Use SMIT to add or change entries in the oid_to_type file. Edit the oid_to_type file using your text editor to delete entries from the file. You must have root permissions to perform this task.

To add or change an entry, follow these steps:

Step 1. Access SMIT using one of the following methods:

- Enter **smit nv6000** at the command line.
- Select **NetView SMIT** from the Administer pull-down menu.

The NetView for AIX SMIT menu is displayed.

Step 2. Select **Configure**.

The Configure menu is displayed.

Step 3. Select **Configure object identification registration files**.

The Configure object identification registration files menu is displayed.

Step 4. Select **Update oid_to_type registration file**.

The Update oid_to_type registration file dialog box is displayed.

Step 5. Type, or select from the List option, required information in the entry fields.

See “Field Definitions” for a description of these fields.

Step 6. Select **Do**.

The information is processed, and the entry is added or changed.

Step 7. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window is closed.

Example of an oid_to_type File

Each entry in the oid_to_type file consists of four fields separated by a colon (:). The following example shows sample entries in the oid_to_type file:

```
1.3.6.1.4.1.2.3.1.2.1.1.2:IBM:IBM RS/6000:H # SNMP agent for AIX 3.2
1.3.6.1.4.1.23.1.1.1:Novell:Novell Lantern
1.3.6.1.4.1.42.2.1.1:Sun:Sun Microsystems SunOS
1.3.6.1.4.1.36.1:DEC:DECstation
```

Field Definitions

The following list describes the fields used in an entry of the oid_to_type file. See “Example of an oid_to_type File” for an example of the oid_to_type file. These fields also apply to the entry fields used in SMIT.

- The first field is the value of the Internet-standard MIB-II system.sysObjectID reported by the device’s SNMP agent. For example: `1.3.6.1.4.1.23.1.1.1`.
- The second field is the vendor that manufactures the given device or node. The vendor name must match one of the enumerated values in the field registration file, /usr/OV/fields/C/ovw_fields, for the vendor field, such as IBM, Hewlett-Packard, Sun, or DEC.

If the vendor name does not match, it is not set. To add new values for the vendor field, see “Adding Values for Vendor and SNMP Agent Fields” on page 96.

- The third field is the agent type currently running on the given device or node. The agent name must match one of the enumerated values in the field registration file, /usr/OV/fields/C/snmp_fields, for the SNMPAgent field. The typical agent name includes the manufacturer of the agent software and the type of device on which the agent software runs, such as IBM RISC System/6000 and AIX Version 3 Release 2 SNMP Agent.
- The fourth field is a set of flags controlling what topology attributes should be applied to an object with this sysObjectID. The topology attributes field controls how the device will be treated by the IP-specific components of the system. These are only default attributes; if it can be determined that a device is or is not performing any of these roles, the attributes for that particular device will be set correctly. Specifically, any combination of flags may be applied to a sysObjectID.

Topology Attribute Flags: Table 9 describes the flags that can be used in the fourth field of the oid_to_type file:

Table 9. SNMP Topology Attributes

Flag	Meaning
G	Treat the device topologically as a gateway (router). A symbol for this object will appear in the Segment, Network, and Internet submaps, and the symbol can be used to connect networks.
B	Treat the object as a bridge or simple repeater. A symbol for objects with this sysObjectID will appear in the Segment and Network submaps, and the symbol can be used to connect segments.
H	Treat the object as a multiport repeater or hub. A symbol for objects with this sysObjectID will appear in the Segment and Network submaps, and the symbol can be used to connect segments. Also, this symbol can appear at the center (hub) of Star segments.
I	Ignore the node’s ability to support SNMP.
S	Treat the device as if it supports secondary addresses but does not report them via SNMP in its ip.ipAddrTable. These devices have interfaces that are added, deleted, and then re-added by the netmon daemon in a regular pattern. The S option prevents the deletion of the secondary interfaces.
T	Report the node’s address as if it were a terminal server.
U	Treat the device as if it were unmanaged.

Adding Values for Vendor and SNMP Agent Fields

To define additional values for the vendor and SNMP agent fields, follow these steps:

Step 1. Create a file with definition extensions.

For example, if you work for the Cary Company and you want to add four entries to the SNMPAgent field, create a new file with the following information:

```
Field "SNMPAgent" {
        Type Enumeration;
        Flags    capability, general, locate;
        Enumeration "Unset",
            "Lou Router",
            "Calvin Hub",
            "Greg Bridge",
            "Ken Repeater";
}

Field "vendor" {
        Type Enumeration;
        Flags    capability, general, locate;
        Enumeration "Unset",
            "Cary Company";
}
```

Step 2. Save your new file in the /usr/OV/fields/C directory.

Step 3. Enter **ovw -fields** to add the new definitions to the object database.

The first four lines of the SNMPAgent field are identical to the definition lines in the snmp_fields file, and the first four lines of the vendor field are identical to the definition lines in the ovw_fields file. The values, except for "Unset," must be unique from those defined in the standard NetView for AIX program.

For more details about the syntax, refer to the *NetView for AIX Programmer's Guide.*

The new definitions appear in the general attributes selection of the `Edit..Modify/Describe` operation and can be referenced in oid_to_type mappings described in “Editing the oid_to_type Registration File” on page 93.

Editing the oid_to_command Registration File

The /usr/OV/conf/oid_to_command registration file contains a list of object identifiers (OIDs) and the associated commands provided by the proprietary protocol owners, for example, FDDI and APPN. Each entry in the oid_to_command registration file includes the following information:

- Object ID (required)
- Host name (required only if the host is remote)
- Start command (required)
- Stop command
- Comment

Use SMIT to add an entry to the oid_to_command registration file. To make changes or delete entries, use your text editor to edit the file. You must have root permissions to perform this task.

Each entry in the oid_to_command registration file must conform to the following syntax:

```
OID [host name:]start command [options] |  [stop command] [options]
```

Adding Entries to the oid_to_command File

To add an entry to the oid_to_command registration file, follow these steps:

Step 1. Access SMIT using one of the following methods:

- Enter **smit nv6000** at the command line.
- Select **NetView SMIT** from the Administer pull-down menu.

The NetView for AIX SMIT menu is displayed.

Step 2. Select **Configure**.

The Configure menu is displayed.

Step 3. Select **Configure object identification registration files**.

The Configure object identification registration files menu is displayed.

Step 4. Select **Update oid_to_command registration file**.

The Update oid_to_command registration dialog box is displayed.

Step 5. Type the required information in the entry fields.

See “Field Definitions” on page 98 for information on fields.

Step 6. Select **Do**.

The information is processed, and the new entry is added.

Step 7. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window is closed.

Example of oid_to_command File

Following are examples of entries in the oid_to_command registration file:

```
1.0.8571.5.1 aixnmj01:/home/sam/my_daemon | /home/sam/3xtree/stop_daemon

1.0.56.78 /my_sub/bin/start_daemon | /my_other_sub/bin/stop_daemon
```

Note: The host name should be provided *only* if the host is remote. Do **not** add the host name if the host is local.

Field Definitions

The following list describes the fields used in an entry of the oid_to_command registration file. These fields also apply to the entry fields used in SMIT.

- The first field is the object identifier (OID). This must be in dot notation format for example, 1.2.3.4.5.
- The second field is the host name. A host name is necessary only when the host is remote. This is the name of the host where the proprietary protocol daemon resides. You must have authorization to execute processes on this remote host. The proprietary protocol daemon is expected to forward topology information to the gtmd daemon. For information about creating the protocol proprietary daemon, refer to the *NetView for AIX Programmer's Guide*.
- The third field is the full path name of the start command and options (if any). The start command is the command used to start the proprietary protocol daemon on the host.
- The fourth field is the full path name of the stop command and options (if any). The stop command is the command used to stop the proprietary protocol daemon if the NetView for AIX program should stop or shut down. This command will be used only if the proprietary protocol daemon was started using the start command as described above.
- The fifth field is a comment field.

Editing the oid_to_protocol Registration File

The /usr/OV/conf/oid_to_protocol registration file is a configuration file for open topology. The file contains a list of OIDs with text strings identifying the protocols used with those objects. You can add OIDs and their associated protocols for private use by editing the oid_to_protocol registration file. If you add entries to the oid_to_protocol file, you should add corresponding entries to the snmp_fields file. See *NetView for AIX Programmer's Guide* for more information. To add OIDs for public applications, contact the NetView Association to request OIDs for new protocols. Otherwise, conflicts can result among vendors.

Example of an oid_to_protocol File

Each entry in the oid_to_protocol file consists of the OID and the text string that represents the protocol name. Following are examples of entries in the oid_to_protocol file:

```
# comment
“SNMP ifType”=1.3.6.1.2.1.2.2.1.3

${SNMP ifType}.1=“Other”
${SNMP ifType}.2=“Regular 1822”
${SNMP ifType}.3=“HDH 1822”
${SNMP ifType}.4=“DDN X.25”
${SNMP ifType}.5=“RFC 877 X.25”
${SNMP ifType}.6=“Ethernet CMSACD”
```

This could also be represented as:

```
# comment

1.2.6.1.2.1.2.2.1.3.1=“Other”
1.2.6.1.2.1.2.2.1.3.2=“Regular 1822”
1.2.6.1.2.1.2.2.1.3.3=“HDH 1822”
1.2.6.1.2.1.2.2.1.3.4=“DDN X.25”
1.2.6.1.2.1.2.2.1.3.5=“RFC 877 X.25”
1.2.6.1.2.1.2.2.1.3.6=“Ethernet CMSACD”
```

Redirecting AIXwindows Display

You can choose the host system where you want AIXwindows to be displayed. To redirect your AIXwindows display, follow these steps:

Step 1. Make sure the management system has permission to display windows on the host you specified. If the management system does not have permission, use the **xhost** command on the host system. To do so, on the host system, enter:

```
xhost + manager hostname
```

Where *manager hostname* is the host name for the management system. Refer to the appropriate AIX operating system documentation for more information about the **xhost** command.

Step 2. On the management system, set the AIXwindows DISPLAY variable by entering the two following commands:

```
DISPLAY=hostname:0.0

export DISPLAY
```

Where *hostname* is the host name of the system and display number to which you are redirecting the AIXwindows display. The default display number is **0.0** (zero is the first display identified to the X-server).

Refer to *NetView for AIX Diagnosis Guide* if you have problems with AIXwindows.

Using a Relational Database for Data Storage

If the relational database component is installed, you can configure NetView for AIX to use a relational database management system to store NetView for AIX data. For example, you can configure NetView for AIX to store IP topology data, trap log data, and snmpCollect data in a relational database. The NetView for AIX program can work with the DB2/6000, INGRES, INFORMIX, ORACLE, or SYBASE relational database management systems.

Refer to the *NetView for AIX Database Guide* for information about how to configure NetView for AIX to store data in a relational database.

Configuring for Backup Manager

You can segment a large network by configuring a backup manager, which creates individualized spheres of control for each management station. Multiple NetView for AIX programs can be used; each can be configured to cause minimal duplication of network management traffic.

Refer to the *NetView for AIX Administrator's Guide* for information about configuring a backup manager.

Configuring SNMP Values

Use the `Options..SNMP Configuration` menu item to configure SNMP values for SNMP communication. The SNMP Configuration menu item enables you to change the default values for the following items:

- Agent community names
- Proxies
- Time-out intervals and number of attempts
- netmon status polling intervals

You can also configure different default values for a specific node or a group of nodes. Configure a group of nodes by specifying an IP address global character (for example, 15.122.*.*). The IP address global character is useful when you want to configure different time-out values and number of retries for wide area networks (WANs).

For information about using the SNMP Configuration operation, see the online help or the *NetView for AIX Administrator's Guide*. For technical information, refer to the ovsnmp.conf file in the *NetView for AIX Administrator's Reference*.

Configuring Agent Community Names

A community name is a password that enables SNMP access to MIB values on an agent. The NetView for AIX program works with agent community names in the following ways:

- By default, the manager's SNMP-based network management operations send the community name `public` in SNMP requests to agents.

- The manager's SNMP-based network management operations look up agent community names in the list shown in the Options..SNMP Configuration dialog box. The SNMP Configuration operation allows network management operations to request MIB values from agents without requiring entry of a community name. By default, the only community name entered is `public`.

The /usr/OV/conf/ovsnmp.conf file contains node names or IP addresses with SNMP community names, time-out and retry intervals, and proxies. Any changes you make using the `Options..SNMP Configuration` operation are saved in the ovsnmp.conf file. If you are changing the community name on the manager workstation, you must change it in both of the following files:

- /usr/OV/conf/ovsnmp.conf (the NetView for AIX program must communicate with the SNMP agent.)
- /etc/snmpd.conf (the SNMP agent must use the new community name)

When to Configure Agent Community Names

You need to configure agent community names under the following conditions:

- If your SNMP agents have a community name other than public, use the `Options..SNMP Configuration` operation to configure the management system to use the proper community name for the agents.
- If you want to set MIB values on an agent, you may also need to configure the SNMP agent to respond to SNMP SetRequests. Many SNMP agents do not support SetRequests, but the ones that do generally require you to enter a community name. How the community name is implemented and used depends on the agent. For information about an agent's community name, see the documentation provided by the vendor of the agent.

  For information about the AIX SNMP agent, see the appropriate AIX operating system documentation.

Authentication Failure

An authentication failure results when the community name, sent by a manager system to an agent, is not valid. When an agent receives a community name that is not valid, it can send an authentication failure trap to the NetView for AIX program, which logs authentication failure traps in its event log, /usr/OV/log/ovevent.log.

Configuring a Proxy Agent

You can use a proxy agent to allow SNMP access to nodes that do not support SNMP. When you configure a proxy, the proxy agent receives the SNMP request and forwards it to the requested node using a non-SNMP protocol. How the proxy gets information from the target node depends on the target.

See the *NetView for AIX Programmer's Guide* for information about configuring a proxy agent.

Example of Using a Proxy

If you want to get information about a LAN Manager/X client, which is a PC node, the information does not come directly from the PC node, because the PC does not support SNMP. However, the LAN Manager/X server supports SNMP and the server can communicate with the PC node. In this example, you can configure the LAN Manager/X server to act as a proxy for the target PC node. All requests to the target PC node are really sent to the server.

Configuring Time-Out and Retry Values

To do effective polling, you may want to change the time-out and retry values. For example, latency times are greater over WANs than LANs. Increasing the time-out and retry values prevents the management station from prematurely timing out when making requests across a WAN.

Configuring netmon Polling Intervals

Use the `Options..SNMP Configuration` menu item to change netmon status polling intervals. The community name is also used by netmon, and the time-out interval is used as an initial estimate. To configure other netmon configuration parameters, such as frequency of discovery, poll operations, address table poll operations, and configuration check operations, use the `Options..Topology/Status Polling Intervals: IP` menu item.

Chapter 9. Maintaining NetView for AIX

To optimize the performance of the NetView for AIX program, you might need to perform various maintenance tasks. This chapter describes the following tasks:

Maintaining Daemon and Process Logs

Maintain the daemon and process logs to make sure they do not grow too large and use up available file system space. A large log file can also adversely affect the performance of the Events menu. To prevent these problems, use one of the following methods:

- Periodically check the size of the log files and clear the contents as necessary. See “Clearing Log and Trace Files Using SMIT” for steps on using SMIT to clear log and trace files.
- Create crontab entries to automatically clear log and trace files. See “Running Commands at Preset Times” on page 105 for steps on using SMIT to set a crontab entry.
- Configure the trapd daemon to automatically archive trapd log data.

  See “Maintaining the trapd Log File” on page 104 for steps on configuring the trapd daemon.
- Check disk space using the Systems Performance Monitor (shpmon) application.

  Refer to the *NetView for AIX Administrator's Guide* for instructions.

Clearing Log and Trace Files Using SMIT

To clear the contents of the log and trace files using SMIT, follow these steps:

Step 1. Access SMIT using one of the following methods:

- Enter **smit nv6000** at the command line.
- Select **NetView SMIT** from the Administer pull-down menu.

The NetView for AIX SMIT menu is displayed.

Step 2. Select **Maintain**.

The Maintain menu is displayed.

Step 3. Select **Clear log, trace, or collector files**.

The Clear log, trace, or collector files dialog box is displayed.

Step 4. Select the log or trace file you want to clear using the **List** button.

The selected file is displayed in the Log, trace, or collector file name field.

Step 5. Select **Do**.

The information is processed, and the selected file is cleared.

Step 6. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window is closed.

Maintaining the trapd Log File

By default, the trapd daemon automatically clears the trapd.log file and moves the data to the trapd.log.old file when the trapd.log file reaches a specified size, 4096KB by default. You can gain additional control over the trapd log data by configuring the trapd daemon to run your own script or the trapd.log_Maint script when the trapd.log file reaches the specified size. You must have root permissions to perform this task.

The trapd.log_Maint script does the following processing of the data in the trapd.log.old file, depending on the parameters you set for the trapd.log_Maint script:

- Transfers the data to a relational database.

  Refer to the *NetView for AIX Database Guide* for information about transferring data to a relational database.

- Archives the data in the specified directory.

  The data is archived in a file that includes a julian date and time stamp in the file name to indicate when the data was archived. For example, the file name trapd.log.94215153001 indicates that this file was archived on August 3, 1994 at 3:30:01 p.m.

- Discards archived data that is older than the specified maximum age.

- Verifies that the maximum amount of disk space used to store archived trapd.log data has not been exceeded. When the specified limit is reached, the oldest trapd.log data is discarded.

  Note: The archive maintenance actions do not affect trapd.log data stored in a relational database.

To maintain the trapd.log file by configuring the trapd daemon, follow these steps:

Step 1. Access SMIT using one of the following methods:

- Enter **smit nv6000** at the command line.
- Select **NetView SMIT** from the Administer pull-down menu.

The NetView for AIX SMIT menu is displayed.

Step 2. Select **Configure**.

The Configure menu is displayed.

Step 3. Select **Set options for daemons**.

The Set options for daemons menu is displayed.

Step 4. Select **Set options for event and trap processing daemons**.

The Set options for event and trap processing daemons menu is displayed.

Step 5. Select **Set options for trapd daemon**.

The Set options for trapd daemon dialog box is displayed.

Step 6. Make the necessary changes to the entry fields:

- Maximum size of trapd.log file
- Full path name of trapd log maintenance script

  Enter the full path name of any script you want to use or use the List option to select the trapd.log_Maint script.

Step 7. Select **Do.**

- If you did not select the trapd.log_Maint script, the trapd daemon is configured as specified. Skip to Step 9.
- If you selected the trapd.log_Maint script, make the necessary changes to the trapd.log_Maint parameters that are displayed:
  - Directory for storage of archived trapd.log files
  - Maximum age of any archived trapd.log file
  - Maximum total size of all archived trapd.log files
  - Migrate data to SQL database

  Refer to the NetView for AIX SMIT online help for additional information about the entry fields.

Step 8. Select **Do**.

Step 9. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window is closed.

Running Commands at Preset Times

You can use NetView for AIX SMIT to add crontab entries to run shell commands at preset dates and times. Adding crontab entries can help you organize and schedule various routine tasks. You must have root permissions to use this option.

Refer to the appropriate AIX operating system documentation for information about the **crontab** command and job scheduling.

The NetView for AIX program provides several shell scripts for routine maintenance. Using NetView for AIX SMIT, you can add a crontab entry for the following shell scripts:

Script	Purpose
netmon.trace_Maint	Clears the netmon.trace file while keeping the last two versions of the file. The netmon.trace file is moved to /usr/OV/log/netmon.trace.BAK1, and the netmon.trace.BAK1 file is moved to /usr/OV/log/netmon.trace.BAK2.
snmpCol.trace_Maint	Clears the snmpCol.trace file while keeping the last two versions of the file. The snmpCol.trace file is moved to /usr/OV/log/snmpCol.trace.BAK1, and the snmpCol.trace.BAK1 file is moved to /usr/OV/log/snmpCol.trace.BAK2.
trapd.trace_Maint	Clears the trapd.trace file while keeping the last two versions of the file. The trapd.trace file is moved to /usr/OV/log/trapd.trace.BAK1, and the trapd.trace.BAK1 file is moved to /usr/OV/log/trapd.trace.BAK2.

You can add scripts or programs to those displayed when you add a crontab entry by putting them in the /usr/OV/cron directory. Any executable file in the /usr/OV/cron directory appears in the selection list of actions.

Because the /usr/OV/cron directory is part of the NetView for AIX program, if the NetView for AIX program is removed from the system, all files in the /usr/OV/cron directory may be lost. To avoid losing your executable files, either save them through SMIT before you remove NetView for AIX or create a symbolic link to the /usr/OV/cron directory. For example, the following command causes the date command to appear in the list of actions:

```
ln -s /usr/bin/date /usr/OV/cron/date
```

Creating a crontab Entry

To set a crontab entry using SMIT, follow these steps:

Step 1. Access SMIT using one of the following methods:

- Enter **smit nv6000** at the command line.
- Select **NetView SMIT** from the Administer pull-down menu.

The NetView for AIX SMIT menu is displayed.

Step 2. Select **Maintain**.

The Maintain menu is displayed.

Step 3. Select **Manage crontab entries**.

The Manage crontab entries menu is displayed.

Step 4. Select **Add crontab entry**.

The Add crontab entry dialog box is displayed.

Step 5. Make the necessary changes to the defaults in the entry fields.

Step 6. Use the List option to enter the name of the appropriate script in the Action field.

Step 7. Select **Do**.

The information is processed, and a crontab entry is added.

Step 8. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window is closed.

To see or clear a previously set crontab, select **List crontab entries** or **Remove crontab entry** on the Manage crontab entries menu.

Example of a Crontab Entry

The following is an example of a crontab entry that was set for the **netmon.trace_Maint** script:

```
59  1  *  *  1,3,5  /usr/OV/cron/netmon.trace_Maint
```

The netmon.trace_Maint script is executed at 1:59 a.m. every Monday, Wednesday, and Friday.

Maintaining Data Collection Files

Maintain the following data collection directories to make sure they do not use up all available disk space:

- /usr/OV/databases/openview
- /usr/OV/databases/tralertd
- /usr/OV/databases/snmpCollect
- /usr/OV/log

These directories continue to grow as long as you are collecting data. To prevent this problem, do any of the following:

- Create a crontab entry, using SMIT to periodically remove log, trace, and collector files.

  See “Running Commands at Preset Times” on page 105 for information about how to create a crontab entry.

- Configure the trapd daemon to automatically archive trapd log data.

  See “Maintaining the trapd Log File” on page 104 for information about how to configure the trapd daemon.

- Maintain the databases.

  See “Maintaining the Databases” on page 108 for information about how to maintain the databases.

- For the snmpCollect directory only:
  - Reduce the polling intervals.

Using the `Tools..Data Collection & Thresholds: SNMP` operation, decrease the polling interval. If you only want to check thresholds, do not store the data.

- Remove the last 100 entries of a file in the snmpCollect directory using the following commands:

  ```
  snmpColDump -tTI /usr/OV/databases/snmpCollect/file | \
     awk -F\t '{printf("%d\t%d\t%s\t%1g\n", $4, $5, $6, $3)}' | \
     tail -100 > /tmp/save
  snmpColDump -r /tmp/save /usr/OV/databases/snmpCollect/file
  ```

  Where *file* is the name of the collection file in the snmpCollect directory.

Maintaining the Databases

Databases continue to grow and consume file system space as long as you are collecting data. This can adversely affect performance. To regain file system space, use one or more of the following methods:

- Resolve inconsistencies between the IP topology database and the database maintained by the **ovwdb** command for the graphical interface. Resolving inconsistencies can result in deleting unneeded objects from the IP topology database.

  See "Resolving Database Inconsistencies" on page 109 for more information.

- Compress the IP topology database.

  Compressing the IP topology database can be effective in regaining file system space if a significant number of objects have been deleted from the IP topology database, either through normal editing or by using the ovtopofix command.

  See "Compressing the IP Topology Database" on page 109 for more information.

- Clear the databases.

  Because customization data is lost when you clear the databases, you should clear the databases only if you were unable to regain file system space after trying the preceding methods.

  You can clear the following databases:

  - tralertd
  - snmpCollect
  - topology
    - ovwdb
    - topo
    - mapdb
    - defmap
    - gtmdb

  See "Clearing Databases" on page 110 for more information.

Resolving Database Inconsistencies

To resolve inconsistencies between the IP topology database and the database maintained by the ovwdb command for the graphical interface, with root permissions, follow these steps:

Step 1. Exit all EUIs, including the EUIs on the client machines.

Step 2. Enter **smit nv6000** at the command line.

The NetView for AIX SMIT menu is displayed.

Step 3. Select **Maintain**.

The Maintain menu is displayed.

Step 4. Select **Resolve inconsistencies between ovtopmd and ovwdb databases**.

The Resolve inconsistencies between ovtopmd and ovwdb databases dialog box is displayed.

Step 5. Make the necessary changes to the entry fields.

Refer to the SMIT online help for information about the entry fields.

Step 6. Select **Do**.

A warning dialog box is displayed.

Step 7. Select **OK**.

The **ovtopofix** command is used to resolve inconsistencies.

Step 8. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window is closed.

Compressing the IP Topology Database

To compress the IP topology database using SMIT, follow these steps:

Step 1. Access SMIT using one of the following methods:

- Enter **smit nv6000** at the command line.
- Select **NetView SMIT** from the Administer pull-down menu.

The NetView for AIX SMIT menu is displayed.

Step 2. Select **Maintain**.

The Maintain menu is displayed.

Step 3. Select **Compress the IP topology database**.

The Compress the IP topology database dialog box is displayed.

Step 4. Use the List option to select **yes**.

Step 5. Select **Do**.

A warning dialog box is displayed.

Step 6. Select **OK**.

The IP topology database is compressed by reading in all data from the IP topology database, truncating the private IP topology database, and rewriting the data.

Step 7. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window is closed.

Clearing Databases

Warning: When you clear the databases, customization data is lost.

To clear the contents of the databases using SMIT, follow these steps:

Step 1. Access SMIT using one of the following methods:

- Enter **smit nv6000** at the command line.
- Select **NetView SMIT** from the Administer pull-down menu.

The NetView for AIX SMIT menu is displayed.

Step 2. Select **Maintain**.

The Maintain menu is displayed.

Step 3. Select **Clear databases**.

The Clear databases menu is displayed.

Step 4. Do one of the following:

- Select **Clear topology databases (limited)** to remove the data from the /usr/OV/databases/openview/topo directory, except the Agent Policy Manager definitions, collection definitions, and master polling and discovery settings.
- Select **Clear topology databases (completely)** to remove all the data from the /usr/OV/databases/openview/topo directory.
- Select **Clear tralertd database** to remove all the files from the /usr/OV/databases/tralertd directory.
- Select **Clear snmpCollect database** to remove all the files from the /usr/OV/databases/snmpCollect.

A warning box is displayed.

Step 5. Select **OK**.

The selected database is cleared.

Step 6. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window is closed.

Note: When you use SMIT to clear openview databases, all the daemons are stopped but not restarted. When you use SMIT to restart map generation, all the daemons are stopped and restarted.

Deleting Unused Entries in the ovsuf File

The ovsuf file contains the configuration information that prompts the startup process to start the specified daemons. Every time you set options for the NetView for AIX daemons, entries are added to the ovsuf file or marked as unused. The entries that are marked as unused begin with the number `1:` in the ovsuf file. The `1:` causes the startup process not to start this particular entry. You might want to delete these entries to prevent the file from becoming too large. Use SMIT to delete unused entries (entries beginning with the `1:`). You must have root permissions to perform this task.

See “Deleting Entries in the ovsuf File Using SMIT” for the steps to accomplish this task.

Example of ovsuf File

Following is an example of the ovsuf file:

```
1:ovwdb:/usr/OV/bin/ovwdb:OVs_YES_START::-O:OVs_WELL_BEHAVED:15:
0:trapd:/usr/OV/bin/trapd:OVs_YES_START:::OVs_WELL_BEHAVED::
0:pmd:/usr/OV/bin/pmd:OVs_YES_START::-Au:OVs_WELL_BEHAVED::
```

Deleting Entries in the ovsuf File Using SMIT

To delete unused entries in the ovsuf file, follow these steps:

Step 1. Access SMIT using one of the following methods:

- Enter **smit nv6000** at the command line.
- Select **NetView SMIT** from the Administer pull-down menu.

The NetView for AIX SMIT menu is displayed.

Step 2. Select **Maintain**.

The Maintain menu is displayed.

Step 3. Select **Reset startup files**.

The Reset startup files menu is displayed.

Step 4. Select **Remove unused records from ovsuf startup file**.

A warning box is displayed.

Step 5. Select **OK**.

Unused records are deleted.

Step 6. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window is closed.

Removing Old Snapshots

To free memory and improve system performance, the NetView for AIX graphical interface has a `File..Map Snapshot..Delete` menu item that enables you to remove snapshots you no longer need.

Alternatively, you can remove snapshots using commands or through SMIT.

Removing Snapshots Using the Command Line

To use commands to remove snapshots, follow these steps:

Step 1. List all current maps by entering:

```
/usr/OV/bin/ovmapdump -l
```

This produces a list similar to the following example:

```
MAP            PERMS  CREATION TIME             COMMENTS
default        R/W    Mon Apr 27 11:52:32 1992
Example Map 1  R/O    Wed Apr 22 12:05:48 1991  example map
Example Map 2  None   Tue Apr 28 14:37:49 1992
```

Step 2. List all available snapshots for a given map by entering:

```
/usr/OV/bin/ovmapsnap -l -m mapname
```

Where *mapname* is the name of the map.

This produces a list similar to the following example:

```
NAME      CREATION TIME                COMMENTS
Testing   Fri Apr 24 12:05:48 1992     testing ovmapsnap
```

Step 3. Enter the following to delete a snapshot:

```
/usr/OV/bin/ovmapsnap -d -n “snapshot” -m mapname
```

If you want to automatically delete the oldest entry, use the following command to set up a crontab entry:

```
/usr/OV/bin/ovmapsnap -d -f -m mapname
```

See the **ovmapsnap** command in the *NetView for AIX Administrator's Reference* for more information about the **ovmapsnap** command.

Removing Snapshots Using SMIT

To remove old snapshots using SMIT, follow these steps:

Step 1. Access SMIT using one of the following methods:

- Enter **smit nv6000** at the command line.
- Select **NetView SMIT** from the Administer pull-down menu.

The NetView for AIX SMIT menu is displayed.

Step 2. Select **Maintain**.

The Maintain menu is displayed.

Step 3. Select **Manage map snapshots**.

The Manage map snapshots menu is displayed.

Step 4. Select **Remove map snapshot**.

The Remove map snapshot dialog box is displayed.

Step 5. Type, or use the List option, to specify the map that contains the map snapshot you are deleting.

Step 6. Type or use the List option to specify the map snapshot name.

Step 7. Select **Do**.

The information is processed, and the map snapshot is deleted.

Step 8. Select **Exit SMIT** from the Exit pull-down menu.

The SMIT window is closed.

Cleaning Up the ORS Database

When the orsd daemon removes entries from its ORS database, it does not physically delete them, but marks the entries as having been deleted. The reason for this is to avoid rewriting the database each time an entry is removed, making the removal process faster.

However, keeping deleted entries in the database over a long period of time can waste file space and reduce the performance rate of database inquiries. Therefore, the orsd daemon is capable of removing the deleted entries from the database. This is known as *garbage collection*.

By default, the orsd daemon will periodically remove the deleted entries. Or, you can initiate garbage collection by using the **ovorsutil -g** command. You must have root permissions to issue this command.

You can use SMIT to set options on the orsd daemon to automatically do periodic garbage collections. You can set the following values:

- How often the orsd daemon checks to see if there are deleted entries in the database.
- The percentage of garbage that must be in the database before a garbage collection is performed.

See “Event and Trap Processing Daemons” on page 79 for information on setting these orsd daemon options.

Glossary, Bibliography, and Index

Glossary

This glossary includes terms and definitions from:

- The *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies may be purchased from the American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Definitions are identified by the symbol (A) after the definition.
- The ANSI/EIA Standard—440-A, *Fiber Optic Terminology*. Copies may be purchased from the Electronic Industries Association, 2001 Pennsylvania Avenue, N.W., Washington, DC 20006. Definitions are identified by the symbol (E) after the definition.
- The *Information Technology Vocabulary*, developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions of published parts of this vocabulary are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.
- The *IBM Dictionary of Computing*, New York: McGraw-Hill, 1994.
- Internet Request for Comments: 1208, *Glossary of Networking Terms*.
- Internet Request for Comments: 1392, *Internet Users' Glossary*.
- The *Object-Oriented Interface Design: IBM Common User Access Guidelines*, Carmel, Indiana: Que, 1992.

The following cross-references are used in this glossary:

Contrast with: This refers to a term that has an opposed or substantively different meaning.

Synonym for: This indicates that the term has the same meaning as a preferred term, which is defined in its proper place in the glossary.

Synonymous with: This is a backward reference from a defined term to all other terms that have the same meaning.

See: This refers the reader to multiple-word terms that have the same last word.

See also: This refers the reader to terms that have a related, but not synonymous, meaning.

Deprecated term for: This indicates that the term should not be used. It refers to a preferred term, which is defined in its proper place in the glossary.

A

abstract syntax. A data specification that includes all distinctions that are needed in data transmissions, but that omits (abstracts) other details such as those that depend on specific computer architectures. See also *abstract syntax notation 1 (ASN.1)* and *basic encoding rules (BER)*.

abstract syntax notation 1 (ASN.1). The Open Systems Interconnection (OSI) method for abstract syntax specified in ISO 8824. See also *basic encoding rules (BER)*.

action. (1) An operation on a managed object, the semantics of which are defined as part of the managed object class definition. (2) In the AIX operating system, a defined task that an application performs. An action modifies the properties of an object or manipulates the object in some way.

active. (1) The state of a resource when it has been activated and is operational. (2) In the AIX operating system, pertaining to the window pane in which the text cursor is currently positioned. (3) Contrast with *inactive* and *inoperative*.

adapter. A part that electrically or physically connects a device to a computer or to another device.

address mask. For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address. Synonymous with *subnet mask* and *subnetwork mask*.

Administrative Domain. A collection of hosts and routers, and the interconnecting networks, managed by a single administrative authority.

agent. (1) In systems management, a user that, for a particular interaction, has assumed an agent role.

(2) An entity that represents one or more managed objects by (a) emitting notifications regarding the objects and (b) handling requests from managers for management operations to modify or query the objects. (3) A system that assumes an agent role.

AIX. Advanced Interactive Executive.

AIX NetView Service Point. See *NetView for AIX Service Point*.

AIX NetView/6000. See *NetView for AIX*.

AIX operating system. IBM's implementation of the UNIX operating system. The RISC System/6000 system, among others, runs the AIX operating system.

AIX SystemView NetView/6000. See *NetView for AIX*.

API. Application programming interface.

application programming interface (API). The set of programming language constructs or statements that can be coded in an application program to obtain the specific functions and services provided by an underlying operating system or service program.

application registration file. A file created to integrate an application program into NetView for AIX by defining (a) the application program's position in the menu structure for NetView for AIX, (b) where help information is found, (c) the number and types of parameters allowed, (d) the command used to start the application program, and (e) other characteristics of the application program.

Apply. A push button that carries out the selected choices in a window without closing the window.

ASCII (American National Standard Code for Information Interchange). The standard code, using a coded character set consisting of 7-bit coded characters (8 bits including parity check), that is used for information interchange among data processing systems, data communication systems, and associated equipment. The ASCII set consists of control characters and graphic characters. (A)

ASN.1. Abstract syntax notation 1.

attribute. (1) A characteristic that identifies and describes a managed object. The characteristic can be determined, and possibly changed, through operations on the managed object. (2) Information within a managed object that is visible at the object boundary. An attribute has a type, which indicates the range of information given by the attribute, and a value, which is within that range. (3) Variable data that is logically a part of an object and that represents a property of the object. For example, a serial number is an attribute of an equipment object.

authentication. (1) In computer security, verification of the identity of a user or the user's eligibility to access an object. (2) In computer security, verification that a message has not been altered or corrupted. (3) In computer security, a process used to verify the user of an information system or protected resources.

authentication failure. In the Simple Network Management Protocol (SNMP), a trap that may be generated by an authentication entity when a requesting client is not a member of the SNMP community.

authorization. (1) In computer security, the right granted to a user to communicate with or make use of a computer system. (T) (2) An access right. (3) The process of granting a user either complete or restricted access to an object, resource, or function.

B

basic encoding rules (BER). The rules specified in ISO 8825 for encoding data units described in abstract syntax notation 1 (ASN.1). The rules specify the encoding technique, not the abstract syntax.

behavior. (1) Ideally, a collection of assertions that describe the allowed states that a managed object can assume. An assertion can be a precondition, a postcondition, or an invariant. In practice, the behavior is often an informal description of the semantics of attributes, operations, and notifications. (2) The way in which managed objects, name bindings, attributes, notifications, and operations interact with the actual resources that they model and with each other.

BER. Basic encoding rules.

Berkeley Internet Name Domain (BIND). The Berkeley implementation of the Domain Name System (DNS).

bind. To relate an identifier to another object in a program; for example, to relate an identifier to a value, an address or another identifier, or to associate formal parameters and actual parameters. (T)

BIND. Berkeley Internet Name Domain.

bridge. (1) A functional unit that interconnects two local area networks that use the same logical link control protocol but may use different medium access control protocols. (T) (2) A functional unit that interconnects multiple LANs (locally or remotely) that use the same logical link control protocol but that can use different medium access control protocols. A bridge forwards a frame to another bridge based on the medium access control (MAC) address. (3) In the connection of local loops, channels, or rings, the equipment and techniques used to match circuits and to facilitate accurate data transmission. (4) Contrast with *gateway* and *router*.

buffer. (1) To allocate and schedule the use of buffers. (A) (2) A portion of storage used to hold input or output data temporarily.

bus. (1) A facility for transferring data between several devices located between two end points, only one device being able to transmit at a given moment. (T) (2) A computer configuration in which processors are interconnected in series.

button. (1) A mechanism on a pointing device, such as a mouse, used to request or initiate an action or a process. (2) A graphical device that identifies a choice. (3) A graphical mechanism that, when selected, performs a visible action. For example, when a user clicks on a list button, a list of choices appears. (4) See *mouse button*, *push button*, *radio button*, and *spin button*.

C

cache. (1) A special-purpose buffer storage, smaller and faster than main storage, used to hold a copy of instructions and data obtained from main storage and likely to be needed next by the processor. (T) (2) A buffer storage that contains frequently accessed instructions and data; it is used to reduce access time. (3) An optional part of the directory database in network nodes where frequently used directory information may be stored to speed directory searches. (4) To place, hide, or store in a cache.

card. In NetView for AIX, see *event card*.

class. (1) In object-oriented design or programming, a group of objects that share a common definition and that therefore share common properties, operations, and behavior. Members of the group are called instances of the class. (2) In the AIX operating system, pertaining to the I/O characteristics of a device. System devices are classified as block or character devices.

click. To press and release a button on a pointing device without moving the pointer off of the object or choice.

client. (1) A functional unit that receives shared services from a server. (T) (2) A user. (3) In an AIX distributed file system environment, a system that is dependent on a server to provide it with programs or access to programs.

client/server. In communications, the model of interaction in distributed data processing in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client; the answering program is called a server.

Close. A choice that removes a window and all of the windows associated with it from the workplace. For example, if a user is performing a task in a window and a message appears, or the user asks for help, both the message and the help windows disappear when the user closes the original window.

CMIP. Common Management Information Protocol.

CMOT. Common Management Information Protocol over TCP/IP.

command. A request from a terminal for the performance of an operation or the execution of a particular program.

Common Management Information Protocol (CMIP). The OSI standard protocol defined in ISO/IEC 9596-1 for the interaction between managers and agents that use the Common Management Information Service Element (CMISE).

Common Management Information Protocol over TCP/IP (CMOT). An Internet Engineering Task Force (IETF) specification for the use of CMIP over a TCP/IP protocol stack.

Common Management Information Service (CMIS). The set of services provided by the Common Management Information Service Element.

communication controller. A type of communication control unit whose operations are controlled by one or more programs stored and executed in the unit. It manages the details of line control and the routing of data through a network.

community. In the Simple Network Management Protocol (SNMP), an administrative relationship between entities.

community name. In the Simple Network Management Protocol (SNMP), a string of octets identifying a community.

component. Hardware or software that is part of a functional unit.

configuration. (1) The manner in which the hardware and software of an information processing system are organized and interconnected. (T) (2) The devices and programs that make up a system, subsystem, or network.

configuration file. A file that specifies the characteristics of a system device or network.

connection. (1) In data communication, an association established between functional units for conveying information. (I) (A) (2) In Open Systems Interconnection architecture, an association established by a given layer between two or more entities of the next higher layer for the purpose of data transfer. (T) (3) In TCP/IP, the path between two protocol applications that provides reliable data stream delivery service. In the Internet, a connection extends from a TCP application on one system to a TCP application on another system. (4) In system communications, a line over which data can be passed between two systems or between a system and a device. (5) Synonym for *physical connection*.

Copy. A choice that places a copy of a selected object onto the clipboard.

D

daemon. A program that runs unattended to perform a standard service. Some daemons are triggered automatically to perform their task; others operate periodically.

data. A representation of facts or instructions in a form suitable for communication, interpretation, or processing by human or automatic means. Data include constants, variables, arrays, and character strings.

Note: Programmers make a distinction between instructions and the data they operate on; however, in the usual sense of the word, data includes programs and program instructions.

data set. Synonym for *file*.

default. Pertaining to an attribute, condition, value, or option that is assumed when none is explicitly specified. (I)

Delete. A choice that removes a selected object. The space it occupied is usually filled by the remaining object or objects in the window.

destination. Any point or location, such as a node, station, or a particular terminal, to which information is to be sent.

device. A mechanical, electrical, or electronic contrivance with a specific purpose.

dialog box. In OSF/Motif, a collection of data fields and buttons for setting controls, selecting from lists, choosing from mutually exclusive options, entering data, and presenting the user with messages.

discovery. In data communication, the automatic detection of network topology changes (for example, new and deleted nodes or new and deleted interfaces).

display. (1) A visual presentation of data. (I) (A) (2) To present data visually. (I) (A) (3) Deprecated term for *panel*.

display panel. In computer graphics, a predefined display image that defines the locations and characteristics of display fields on a display surface.

DNS. Domain Name System.

domain. (1) That part of a computer network in which the data processing resources are under common control. (T) (2) In SNA, see *end node domain*, *network node domain*, and *system services control point (SSCP) domain*. (3) In Open Systems Interconnection (OSI), a part of a distributed system or a set of managed objects to which a common policy applies. (4) In a database, all the possible values of an attribute or a data element. (5) See *Administrative Domain* and *domain name*.

domain name. In the Internet suite of protocols, a name of a host system. A domain name consists of a sequence of subnames separated by a delimiter character. For example, if the fully qualified domain name (FQDN) of a host system is `ralvm7.vnet.ibm.com`, each of the following is a domain name:

- `ralvm7.vnet.ibm.com`
- `vnet.ibm.com`
- `ibm.com`

Domain Name System (DNS). In the Internet suite of protocols, the distributed database system used to map domain names to IP addresses.

DOS. Disk Operating System. See *IBM Disk Operating System*.

dump. (1) To record, at a particular instant, the contents of all or part of one storage device in another storage device. Dumping is usually for the purpose of debugging. (T) (2) Data that has been dumped. (T) (3) To copy data in a readable format from main or auxiliary storage onto an external medium such as tape, diskette, or printer.

E

EFD. Event forwarding discriminator.

EMS. Event management services.

enable. To make functional.

end node domain. An end node control point, its attached links, and its local LUs.

end user. A person, device, program, or computer system that utilizes a computer network for the purpose of data processing and information exchange. (T)

end-user interface (EUI). In NetView for AIX, synonym for *graphical user interface (GUI)*.

error. A discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition. (I) (A)

Ethernet. A 10-Mbps baseband local area network that allows multiple stations to access the transmission medium at will without prior coordination, avoids contention by using carrier sense and deference, and resolves contention by using collision detection and delayed retransmission. Ethernet uses carrier sense multiple access with collision detection (CSMA/CD).

EUI. End-user interface.

event. (1) An occurrence of significance to a task; for example, an SNMP trap, the opening of a window or a submap, or the completion of an asynchronous operation. (2) In the NetView and NETCENTER programs, a record indicating irregularities of operation in physical elements of a network. (3) See also *event report*.

event card. In NetView for AIX, a graphical representation, resembling a card, of the information contained in an event sent by an agent to a manager reflecting a change in the status of one of the agent's managed nodes.

event filter. In NetView for AIX, a logical expression of criteria that determine which events are forwarded to the application program that registers the event filter with the event sieve agent. A filter is referred to as “simple” or “compound” depending on how it is handled by the filter editor.

event forwarding discriminator (EFD). A managed object that describes and controls the criteria used to select which event reports are sent and to whom they are sent.

event management services (EMS). In NetView for AIX, a centralized method of generating, receiving, routing, and logging network events.

event report. The unsolicited report that an event has occurred. When a managed object emits a notification, the agent uses one or more event forwarding discriminators (EFDs) to find the destinations to which the report is sent.

event sieve. In NetView for AIX, an object that is managed by the “ovesmd” daemon, which is the event sieve agent. The event sieve agent stores information about the event sieve object in a database and reads that information when the agent is started. See also *event filter* and *event forwarding discriminator (EFD)*.

exec. (1) In the AIX operating system, to overlay the current process with another executable program. (2) See also *fork*.

F

FDDI. Fiber Distributed Data Interface.

feature. A part of an IBM product that may be ordered separately by the customer.

Fiber Distributed Data Interface (FDDI). An American National Standards Institute (ANSI) standard for a 100-megabit-per-second LAN using optical fiber cables.

field. (1) An identifiable area in a window. Examples of fields are: an entry field, into which a user can type or place text, and a field of radio button choices, from which a user can select one choice. (2) In NetView for

AIX, the building block of which objects are composed. A field is characterized by a field name, a data type (integer, Boolean, character string, or enumerated value), and a set of flags that describe how the field is treated by NetView for AIX. A field can contain data only when it is associated with an object.

field registration file. In NetView for AIX, a file used to define fields for use in the object database.

file. A named set of records stored or processed as a unit. (T) Synonymous with *data set*.

File Transfer Protocol (FTP). In the Internet suite of protocols, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

filter. (1) A device or program that separates data, signals, or material in accordance with specified criteria. (A) (2) In the NetView program, a function that limits the data that is to be recorded on the database and displayed at the terminal. (3) In the AIX operating system, a command that reads standard input data, modifies the data, and sends it to the display screen. (4) See also *recording filter* and *viewing filter*.

flag. (1) To mark an information item for selection for further processing. (T) (2) A character that signals the occurrence of some condition, such as the end of a word. (A)

fork. In the AIX operating system, to create and start a child process.

FQDN. Fully qualified domain name.

FTP. File Transfer Protocol.

fully qualified domain name (FQDN). In the Internet suite of protocols, the name of a host system that includes all of the subnames of the domain name. An example of a fully qualified domain name is `ralvm7.vnet.ibm.com`. See also *host name*.

G

gateway. (1) A functional unit that interconnects two computer networks with different network architectures. A gateway connects networks or systems of different architectures. A bridge interconnects networks or systems with the same or similar architectures. (T) (2) In the AIX operating system, an entity that operates above the link layer and translates, when required, the interface and protocol used by one network into those used by another distinct network. (3) In TCP/IP, synonym for *router*.

GIF. Graphical interchange format.

global character. Synonym for *pattern-matching character*.

graphical interchange format (GIF). In NetView for AIX, the format used for the background pictures of a network topology map.

graphical user interface (GUI). (1) A type of computer interface consisting of a visual metaphor of a real-world scene, often of a desktop. Within that scene are icons, representing actual objects, that the user can access and manipulate with a pointing device. (2) In NetView for AIX, the integrating interface application program that provides the means for displaying submaps and for integrating network application programs. The graphical user interface is a single, consistent interface that enables the user to interact with multiple application programs. Synonymous with *end-user interface (EUI)*.

GUI. Graphical user interface.

H

hardcopy. (1) A permanent copy of a display image generated on an output device such as a printer or plotter, and which can be carried away. (T) (2) A printed copy of machine output in a visually readable form; for example, printed reports, listings, documents, and summaries. (3) Contrast with *softcopy*.

Help. A choice that gives a user access to helpful information about objects, choices, tasks, and products. A Help choice can appear on a menu bar or as a push button.

help panel. Information displayed by a system in response to a help request from a user.

highlighting. Emphasizing a display element or segment by modifying its visual attributes. (I) (A)

host. (1) In the Internet suite of protocols, an end system. The end system can be any workstation; it does not have to be a mainframe. (2) See *host processor*.

host name. In the Internet suite of protocols, the name given to a machine. Sometimes, “host name” is used to mean *fully qualified domain name (FQDN)*; other times, it is used to mean the most specific subname of a fully qualified domain name. For example, if `ralvm7.vnet.ibm.com` is the fully qualified domain name, either of the following may be considered the host name:

- `ralvm7.vnet.ibm.com`
- `ralvm7`

host processor. (1) A processor that controls all or part of a user application network. (T) (2) In a network, the processing unit in which the data communication access method resides.

I

IBM Disk Operating System (DOS). A disk operating system based on MS-DOS that operates with all IBM personal computers.

icon. (1) A graphic symbol, displayed on a screen, that a user can point to with a device such as a mouse in order to select a particular function or software application. (T) (2) A graphical representation of an object, consisting of an image, image background, and a label.

ID. (1) Identifier. (2) Identification.

IEEE. Institute of Electrical and Electronics Engineers.

inactive. (1) Not operational. (2) Pertaining to a node or device not connected or not available for connection to another node or device. (3) In the AIX operating system, pertaining to a window that does not have an input focus. (4) Contrast with *active*. (5) See also *inoperative*.

inoperative. (1) The condition of a resource that has been active but is not currently active. A resource may be inoperative for reasons such as the following: (a) it may have failed, (b) it may have received an INOP request, or (c) it may be suspended while a reactivate command is being processed. (2) See also *inactive*.

Institute of Electrical and Electronics Engineers (IEEE). A professional society accredited by the American National Standards Institute (ANSI) to issue standards for the electronics industry.

interface. A shared boundary between two functional units, defined by functional characteristics, signal characteristics, or other characteristics, as appropriate. The concept includes the specification of the connection of two devices having different functions. (T)

International Organization for Standardization (ISO). An organization of national standards bodies from various countries established to promote development of standards to facilitate international exchange of goods and services, and develop cooperation in intellectual, scientific, technological, and economic activity.

internet. A collection of networks interconnected by a set of routers that allow them to function as a single, large network. See also *Internet*.

Internet. The internet administered by the Internet Architecture Board (IAB), consisting of large national backbone networks and many regional and campus networks all over the world. The Internet uses the Internet suite of protocols.

Internet Protocol (IP). A connectionless protocol that routes data through a network or interconnected networks. IP acts as an intermediary between the higher protocol layers and the physical network. However, this protocol does not provide error recovery and flow control and does not guarantee the reliability of the physical network.

IP. Internet Protocol.

IP address. The 32-bit address defined by the Internet Protocol, standard 5, Request for Comment (RFC) 791. It is usually represented in dotted decimal notation.

ISO. International Organization for Standardization.

K

keyword. (1) In programming languages, a lexical unit that, in certain contexts, characterizes some language construct; for example, in some contexts, IF characterizes an if-statement. A keyword normally has the form of an identifier. (I) (2) One of the predefined words of an artificial language. (A) (3) A name or symbol that identifies a parameter. (4) The part of a command operand that consists of a specific character string (such as `DSNAME=`).

L

LAN. Local area network.

layout. See *layout algorithm*.

layout algorithm. A method of arranging displayed or printed data.

link. The combination of the link connection (the transmission medium) and two link stations, one at each end of the link connection. A link connection can be shared among multiple links in a multipoint or token-ring configuration.

list button. A button labeled with an underlined down-arrow that presents a list of valid objects or choices that can be selected for that field.

local. (1) Pertaining to a device accessed directly without use of a telecommunication line. (2) Contrast with *remote*.

local area network (LAN). (1) A computer network located on a user's premises within a limited geographical area. Communication within a local area network is not subject to external regulations; however, communication across the LAN boundary may be subject to some form of regulation. (T) (2) A network in which a set of devices are connected to one another for communication and that can be connected to a larger network. (3) See also *Ethernet* and *token ring*. (4) Contrast with *metropolitan area network (MAN)* and *wide area network (WAN)*.

local registration file (LRF). In NetView for AIX, a file that provides information about an agent or daemon, such as the name, the location of the executable code, the names of processes dependent on the agent or daemon, and details about the objects that an agent manages.

LRF. Local registration file.

M

MAN. Metropolitan area network.

managed object. (1) A component of a system that can be managed by a management application. (2) The systems management view of a resource that can be managed through the use of systems management protocols.

Management Information Base (MIB). (1) A collection of objects that can be accessed by means of a network management protocol. (2) A definition for management information that specifies the information available from a host or gateway and the operations allowed. (3) In OSI, the conceptual repository of management information within an open system.

management region. In NetView for AIX, the set of managed objects on a particular map that defines the extent of the network that is being actively managed. The management region may vary across maps.

management services (MS). (1) One of the types of network services in control points (CPs) and physical units (PUs). Management services are the services provided to assist in the management of SNA networks, such as problem management, performance and accounting management, configuration management, and change management. (2) Services that assist in the management of systems and networks in areas such as problem management, performance management, business management, operations management, configuration management, and change management.

manager. (1) In systems management, a user that, for a particular interaction, has assumed a manager role. (2) An entity that monitors or controls one or more managed objects by (a) receiving notifications regarding the objects and (b) requesting management operations to modify or query the objects. (3) A system that assumes a manager role.

map. In NetView for AIX, a database represented by a set of related submaps that provide a graphical and hierarchical presentation of a network and its systems.

medium. A physical material in or on which data may be represented.

menu. (1) A list of options displayed to the user by a data processing system, from which the user can select an action to be initiated. (T) (2) A list of choices that can be applied to an object. A menu can contain choices that are not available for selection in certain contexts. Those choices are indicated by reduced contrast.

menu bar. (1) The area near the top of a window, below the title bar and above the rest of the window, that contains choices that provide access to other menus. (2) In the AIX operating system, a rectangular area at the top of the client area of a window that contains the titles of the standard pull-down menus for that application.

message. (1) An assembly of characters and sometimes control codes that is transferred as an entity from an originator to one or more recipients. A message consists of two parts: envelope and content. (T) (2) A communication sent from a person or program to another person or program.

metropolitan area network (MAN). A network formed by the interconnection of two or more networks which may operate at higher speed than those networks, may cross administrative boundaries, and may use multiple access methods. (T) Contrast with *local area network (LAN)* and *wide area network (WAN)*.

MIB. (1) MIB module. (2) Management Information Base.

migration. The installation of a new version or release of a program to replace an earlier version or release.

modem (modulator/demodulator). (1) A functional unit that modulates and demodulates signals. One of the functions of a modem is to enable digital data to be transmitted over analog transmission facilities. (T) (A) (2) A device that converts digital data from a computer to an analog signal that can be transmitted on a telecommunication line, and converts the analog signal received to data for the computer.

monitor. (1) A device that observes and records selected activities within a data processing system for analysis. Possible uses are to indicate significant departure from the norm, or to determine levels of utilization of particular functional units. (T) (2) Software or hardware that observes, supervises, controls, or verifies operations of a system. (A)

Motif. See *OSF/Motif*.

mouse. A commonly used pointing device, containing one or more buttons, with which a user can interact with a product or the operating environment.

mouse button. A mechanism on a mouse pointing device used to select objects or choices, initiate actions, or directly manipulate objects; a user presses a mouse button to interact with a computer system. The button makes a “clicking” sound when pressed and released.

Multiple Virtual Storage (MVS). See *MVS*.

multiport repeater. A repeater that contains multiple ports, for example, ThinLAN hubs or EtherTwist hubs.

MVS. Multiple Virtual Storage. Implies MVS/370, the MVS/XA product, and the MVS/ESA product.

N

NETCENTER. A software product that assists the network operator and other technical personnel at a network control center in managing the network.

NetView for AIX. (1) Formerly known as *AIX SystemView NetView/6000* (or its abbreviated name, which is *AIX NetView/6000*). (2) An IBM licensed program for systems management in the AIX environment. NetView for AIX can use the NetView for AIX Service Point to communicate with the NetView and NETCENTER programs.

NetView for AIX Service Point. (1) Formerly known as the *AIX NetView Service Point*. (2) An IBM licensed program that operates in the AIX and UNIX environments. It functions as a gateway in an unattended environment.

NetView program. An IBM licensed program used to monitor and manage a network and to diagnose network problems.

network. (1) An arrangement of nodes and connecting branches. (T) (2) A configuration of data processing devices and software connected for information interchange. (3) A group of nodes and the links interconnecting them.

Network File System (NFS). A protocol developed by Sun Microsystems, Incorporated, that allows any host in a network to mount another host's file directories. Once mounted, the file directory appears to reside on the local host.

network manager. A program or group of programs that is used to monitor, manage, and diagnose the problems of a network.

network node domain. An APPN network-node control point, its attached links, the network resources for which it answers directory search requests (namely, its local LUs and adjacent LEN end nodes), the adjacent APPN end nodes with which it exchanges directory search requests and replies, and other resources (such as a local storage device) associated with its own node or an adjacent end node for which it provides management services.

NFS. Network File System.

node. (1) In network topology, the point at an end of a branch. (T) (2) The representation of a state or an event by means of a point on a diagram. (A) (3) In a tree structure, a point at which subordinate items of data originate. (A) (4) An endpoint of a link or a junction common to two or more links in a network. Nodes can be processors, communication controllers, cluster controllers, or terminals. Nodes can vary in routing and other functional capabilities.

notification. (1) An unscheduled, spontaneously generated report of an event that has occurred. (2) In systems management, information emitted by a managed object relating to an event that has occurred within the managed object, such as a threshold violation or a change in configuration status.

O

object. (1) In object-oriented design or programming, an abstraction consisting of data and the operations associated with that data. See also *class*. (2) An item that a user can manipulate as a single unit to perform a task. An object can appear as text, an icon, or both.

object identifier. An administratively assigned data value of the type defined in abstract syntax notation 1 (ASN.1).

object registration service (ORS). In NetView for AIX, a component that creates and maintains a global directory of object managers, their locations, and their protocols. The postmaster daemon uses this directory to route messages and provide location transparency for managers and agents.

Off. A choice that appears in the cascaded menu from the Refresh choice. It sets the refresh function to off.

OK. A push button that accepts the information in a window and closes it. If the window contains changed information, those changes are applied before the window is closed.

On. A choice that appears in a cascaded menu from the Refresh choice. It immediately refreshes the view in a window.

online. (1) Pertaining to the operation of a functional unit when under the direct control of the computer. (T) (2) Pertaining to a user's ability to interact with a computer. (A)

online information. Information stored in a computer system that can be displayed, used, and modified in an interactive manner without any need to obtain hardcopy.

Open. A choice that leads to a window in which users can select the object they want to open.

Open Software Foundation (OSF). A nonprofit research and development organization whose goals are (a) to develop specifications and software for use in an open software environment and (b) to make the specifications and software available to information technology vendors under fair and equitable licensing terms. For example, OSF developed the Distributed Computing Environment (DCE).

Open Systems Interconnection (OSI). The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information. (T) (A)

Open Systems Interconnection (OSI) architecture. Network architecture that adheres to that particular set of ISO standards that relates to Open Systems Interconnection. (T)

Open Systems Interconnection (OSI) reference model. A model that describes the general principles of the Open Systems Interconnection, as well as the purpose and the hierarchical arrangement of its seven layers. (T)

operating system (OS). Software that controls the execution of programs and that may provide services such as resource allocation, scheduling, input/output control, and data management. Although operating systems are predominantly software, partial hardware implementations are possible. (T)

operation. In object-oriented design or programming, a service that can be requested at the boundary of an object. Operations include modifying an object or disclosing information about an object.

operator. (1) A person or program responsible for managing activities controlled by a given piece of software such as MVS, the NetView program, or IMS. (2) A person who operates a device. (3) A person who keeps a system running.

ORS. Object registration service.

OS. Operating system.

OSF. Open Software Foundation.

OSF/Motif. A graphical interface that contains a toolkit, a presentation description language, a window manager, and a style guideline.

OSI. Open Systems Interconnection.

output. Pertaining to a device, process, or channel involved in an output process, or to the associated data or states. The word "output" may be used in place of "output data," "output signal," "output process," when such a usage is clear in a given context. (T)

P

packet. In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. The data, control signals, and, possibly, error control information are arranged in a specific format. (I)

packet internet groper (PING). (1) In Internet communications, a program used in TCP/IP networks to test the ability to reach destinations by sending the destinations an Internet Control Message Protocol (ICMP) echo request and waiting for a reply. (2) In communications, a test of reachability.

packet switching. The process of routing and transferring data by means of addressed packets so that a channel is occupied only during transmission of a packet. On completion of the transmission, the channel is made available for transfer of other packets. (I)

page. (1) In a virtual storage system, a fixed-length block that has a virtual address and is transferred as a unit between real storage and auxiliary storage. (I) (A) (2) The information displayed at the same time on the screen of a display device.

panel. (1) See *window*. (2) A formatted display of information that appears on a display screen. See *help panel* and *task panel*. (3) In computer graphics, a display image that defines the locations and characteristics of display fields on a display surface.

path. The route used to locate files; the storage location of a file. A fully qualified path lists the drive identifier, directory name, subdirectory name (if any), and file name with the associated extension.

pattern-matching character. A special character such as an asterisk (*) or a question mark (?) that can be used to represent one or more characters. Any character or set of characters can replace a pattern-matching character. Synonymous with *global character* and *wildcard character*.

physical connection. (1) A connection that establishes an electrical circuit. (2) A point-to-point or multipoint connection. (3) Synonymous with *connection*.

PING. Packet internet groper.

polling. (1) On a multipoint connection or a point-to-point connection, the process whereby data stations are invited, one at a time, to transmit. (I) (2) Interrogation of devices for such purposes as to avoid contention, to determine operational status, or to determine readiness to send or receive data. (A)

port. (1) An access point for data entry or exit. (2) A connector on a device to which cables for other devices such as display stations and printers are attached. (3) The representation of a physical connection to the link hardware. A port is sometimes referred to as an adapter; however, there can be more than one port on an adapter. There may be one or more ports controlled by a single DLC process. (4) In the Internet suite of protocols, a 16-bit number used to communicate between TCP or the User Datagram Protocol (UDP) and a higher-level protocol or application. Some protocols, such as File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP), use the same well-known port number in all TCP/IP implementations. (5) An abstraction used by transport protocols to distinguish among multiple destinations within a host machine. (6) Synonymous with *socket*.

postmaster. In NetView for AIX, a process (daemon) that directs network management information between multiple application programs and agents running concurrently. The postmaster determines the route by using specified addresses or a routing table that is configured in the object registration service.

problem determination. The process of determining the source of a problem; for example, a program component, machine failure, telecommunication facilities, user or contractor-installed programs or equipment, environmental failure such as a power loss, or user error.

process identification number (process ID). A unique number assigned to a process by the operating system. The number is used internally by processes to communicate.

processor. In a computer, a functional unit that interprets and executes instructions. A processor consists of at least an instruction control unit and an arithmetic and logic unit. (T)

program temporary fix (PTF). A temporary solution or bypass of a problem diagnosed by IBM in a current unaltered release of the program.

protocol. (1) A set of semantic and syntactic rules that determine the behavior of functional units in achieving communication. (I) (2) In Open Systems Interconnection architecture, a set of semantic and syntactic rules that determine the behavior of entities in the same layer in performing communication functions. (T)

proxy agent. A process or entity that is both an agent to its manager and a manager for one or more objects. It satisfies requests from its manager by relaying those requests and translating them for the objects that it manages.

PTF. Program temporary fix.

pull-down menu. See *menu*.

push button. A button, labeled with text, graphics, or both, that represents an action that will be initiated when a user selects it.

R

radio button. A circle with text beside it. Radio buttons are combined to show a user a fixed set of choices from which the user can select one. The circle becomes partially filled when a choice is selected.

recording filter. In the NetView program, the function that determines which events, statistics, and alerts are stored on a database.

redirect. To define or use a logical device name as a reference to another device or file that may be local or remote.

reduced instruction-set computer (RISC). A computer that uses a small, simplified set of frequently used instructions for rapid execution.

registration file. See *application registration file*, *field registration file*, *local registration file (LRF)*, and *symbol registration file*.

relation. In a relational database, a set of entity occurrences that have the same attributes. (T)

relational database. A database in which the data are organized and accessed according to relations. (T)

remote. (1) Pertaining to a system, program, or device that is accessed through a telecommunication line.
(2) Contrast with *local*.

repeater. A node of a local area network, a device that regenerates signals in order to extend the range of transmission between data stations or to interconnect two branches. (T)

Request for Comments (RFC). In Internet communications, the document series that describes a part of the Internet suite of protocols and related experiments. All Internet standards are documented as RFCs.

resource. Any facility of a computing system or operating system required by a job or task, and including main storage, input/output devices, the processing unit, data sets, and control or processing programs.

response. (1) In data communication, a reply represented in the control field of a response frame. It advises the primary or combined station of the action taken by the secondary or other combined station to one or more commands. (2) See also *command*.

RFC. Request for Comments.

ring. See *ring network*.

ring network. (1) A network in which every node has exactly two branches connected to it and in which there are exactly two paths between any two nodes. (T)
(2) A network configuration in which devices are connected by unidirectional transmission links to form a closed path.

RISC. Reduced instruction-set computer.

root user. See *superuser authority.*

route. (1) An ordered sequence of nodes and transmission groups (TGs) that represent a path from an origin node to a destination node traversed by the traffic exchanged between them. (2) The path that network traffic uses to get from source to destination.

router. (1) A computer that determines the path of network traffic flow. The path selection is made from several paths based on information obtained from specific protocols, algorithms that attempt to identify the shortest or best path, and other criteria such as metrics or protocol-specific destination addresses. (2) An attaching device that connects two LAN segments, which use similar or different architectures, at the reference model network layer. (3) In OSI terminology, a function that determines a path by which an entity can be reached. (4) In TCP/IP, synonymous with *gateway*. (5) Contrast with *bridge*.

routine. A program, or part of a program, that may have some general or frequent use. (T)

S

screen. (1) The physical surface of a display device upon which information is shown to users. (2) In the AIX extended curses library, a window that is as large as the display screen of the workstation. (3) Deprecated term for *display panel*.

seed file. In NetView for AIX, a file that contains a list of nodes within an Administrative Domain, which the automatic discovery function uses to accelerate the generation of the network topology map.

segment. (1) A portion of a computer program that may be executed without the entire computer program being resident in main storage. (T) (2) A group of display elements. (3) A section of cable between components or devices. A segment may consist of a single patch cable, several patch cables that are connected, or a combination of building cable and patch cables that are connected. (4) In the Enhanced X-Windows Toolkit, one or more lines that are drawn but not necessarily connected at the endpoints. (5) In LANs or WANs, a subset of nodes in a network or subnet that are connected by a common physical medium.

select. To explicitly identify one or more objects to which a subsequent choice will apply.

selection. The process of explicitly identifying one or more objects to which a subsequent choice will apply.

server. (1) A functional unit that provides shared services to workstations over a network; for example, a file server, a print server, a mail server. (T) (2) In a network, a data station that provides facilities to other stations; for example, a file server, a print server, a mail server. (A) (3) In the AIX operating system, an application program that usually runs in the background and is controlled by the system program controller. (4) In the Enhanced X-Windows Toolkit, a program that provides the basic windowing mechanism. It handles interprocess communication (IPC) connections from clients, demultiplexes graphics requests onto screens, and multiplexes input back to clients.

service point (SP). (1) An entry point that supports applications that provide network management for resources not under the direct control of itself as an entry point. Each resource is either under the direct control of another entry point or not under the direct control of any entry point. A service point accessing these resources is not required to use SNA sessions (unlike a focal point). A service point is needed when entry point support is not yet available for some network management function. (2) In NetView for AIX, see *NetView for AIX Service Point*.

shared. Pertaining to the availability of a resource for more than one use at the same time.

shell procedure. In the AIX operating system, a series of commands, combined in a file, that carry out a particular function when the file is run or when the file is specified as a value to the SH command. Synonymous with *shell script*.

shell script. Synonym for *shell procedure*.

shutdown. The process of ending operation of a system or a subsystem, following a defined procedure.

Simple Network Management Protocol (SNMP). In the Internet suite of protocols, a network management protocol that is used to monitor routers and attached networks. SNMP is an application layer protocol. Information on devices managed is defined and stored in the application's Management Information Base (MIB).

SMIT. System Management Interface Tool.

SMUX. SNMP multiplexer.

SNA. Systems Network Architecture.

snapshot. In NetView for AIX, a copy of a map that reflects the topology and status of the map's nodes and links at a given moment in time.

SNMP. Simple Network Management Protocol.

SNMP multiplexer (SMUX). A protocol that is used by a subagent to provide local and remote system monitoring using the Simple Network Management Protocol (SNMP).

socket. (1) An endpoint for communication between processes or application programs. (2) Synonym for *port*.

softcopy. (1) A nonpermanent copy of the contents of storage in the form of a display image. (T) (2) One or more files that can be electronically distributed, manipulated, and printed by a user. (3) Contrast with *hardcopy*.

spin button. A component used to display, in sequence, a ring of related but mutually exclusive choices. A user can accept the value displayed in the entry field or can type a valid choice into the entry field.

SSCP. System services control point.

station. An input or output point of a system that uses telecommunication facilities; for example, one or more systems, computers, terminals, devices, and associated programs at a particular location that can send or receive data over a telecommunication line.

status. The condition or state of hardware or software, usually represented by a status code.

subagent. In the Simple Network Management Protocol (SNMP), something that provides an extension to the utility provided by the SNMP agent.

submap. In NetView for AIX, a particular view of some aspect of a network that displays symbols representing objects. The application program that creates a submap determines what part of the network the submap displays.

subnet. (1) In TCP/IP, a part of a network that is identified by a portion of the IP address. (2) Synonym for *subnetwork*.

subnet mask. Synonym for *address mask*.

subnetwork. (1) Any group of nodes that have a set of common characteristics, such as the same network ID. (2) In the AIX operating system, one of a group of multiple logical network divisions of another network, such as can be created by the Transmission Control Protocol/Internet Protocol (TCP/IP) interface program. (3) Synonymous with *subnet*.

subnetwork mask. Synonym for *address mask*.

subsystem. A secondary or subordinate system, usually capable of operating independently of, or asynchronously with, a controlling system. (T)

superuser authority. In the AIX operating system, the unrestricted authority to access and modify any part of the operating system, usually associated with the user who manages the system.

symbol. In NetView for AIX, a picture or an icon on a submap that represents an object (a network resource or an application). Each symbol belongs to a class, represented by the symbol's shape, and to a subclass, represented by the design within the shape. The symbol reflects characteristics of the object it represents, such as its status; it also has characteristics of its own, such as behavior.

symbol registration file. In NetView for AIX, a file used to define symbol classes and subclasses.

System Management Interface Tool (SMIT). An interface tool of the AIX operating system for installing, maintaining, configuring, and diagnosing tasks.

system services control point (SSCP). A component within a subarea network for managing the configuration, coordinating network operator and problem determination requests, and providing directory services and other session services for end users of the network. Multiple SSCPs, cooperating as peers with one another, can divide the network into domains of control, with each SSCP having a hierarchical control relationship to the physical units and logical units within its own domain.

system services control point (SSCP) domain. The system services control point, the physical units (PUs), the logical units (LUs), the links, the link stations, and all the resources that the SSCP has the ability to control by means of activation and deactivation requests.

Systems Network Architecture (SNA). The description of the logical structure, formats, protocols, and operational sequences for transmitting information units through, and controlling the configuration and operation of, networks. The layered structure of SNA allows the ultimate origins and destinations of information, that is, the end users, to be independent of and unaffected by the specific SNA network services and facilities used for information exchange.

T

task. In a multiprogramming or multiprocessing environment, one or more sequences of instructions treated by a control program as an element of work to be accomplished by a computer. (I) (A)

task panel. Online display from which you communicate with the program in order to accomplish the program's function, either by selecting an option provided on the panel or by entering an explicit command. See also *help panel*.

TCP. Transmission Control Protocol.

TCP/IP. Transmission Control Protocol/Internet Protocol.

Telnet. In the Internet suite of protocols, a protocol that provides remote terminal connection service. It allows users of one host to log on to a remote host and interact as directly attached terminal users of that host.

terminal. A device, usually equipped with a keyboard and a display device, that is capable of sending and receiving information.

threshold. In NetView for AIX, a setting that specifies the maximum value a statistic can reach before notification that the limit was exceeded. For example, when a monitored MIB value has exceeded the threshold, the data collector generates a threshold event.

token. (1) In a local area network, the symbol of authority passed successively from one data station to another to indicate the station temporarily in control of the transmission medium. Each data station has an opportunity to acquire and use the token to control the medium. A token is a particular message or bit pattern that signifies permission to transmit. (T) (2) In LANs, a sequence of bits passed from one device to another along the transmission medium. When the token has data appended to it, it becomes a frame.

token ring. (1) According to IEEE 802.5, network technology that controls media access by passing a token (special packet or frame) between media-attached stations. (2) A FDDI or IEEE 802.5 network with a ring topology that passes tokens from one attaching ring station (node) to another. (3) See also *local area network (LAN)*.

topology. In communications, the physical or logical arrangement of nodes in a network, especially the relationships among nodes and the links between them.

trace. A record of the execution of a computer program. It exhibits the sequences in which the instructions were executed. (A)

transaction program (TP). (1) A program that processes transactions in an SNA network. There are two kinds of transaction programs: application transaction programs and service transaction programs. See also *conversation*. (2) In VTAM, a program that performs services related to the processing of a transaction. One or more transaction programs may operate within a VTAM application program that is using the VTAM application program interface (API). In that situation, the transaction program would request services from the application program, using protocols defined by that application program. The application program, in turn, could request services from VTAM by issuing the APPCCMD macroinstruction.

Transmission Control Protocol (TCP). A communications protocol used in the Internet and in any network that follows the U.S. Department of Defense standards for internetwork protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It uses the Internet Protocol (IP) as the underlying protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP). A set of communications protocols that support peer-to-peer connectivity functions for both local and wide area networks.

trap. In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

U

UDP. User Datagram Protocol.

user. (1) Any person or any thing that may issue or receive commands and messages to or from the information processing system. (T) (2) Anyone who requires the services of a computing system.

User Datagram Protocol (UDP). In the Internet suite of protocols, a protocol that provides unreliable, connectionless datagram service. It enables an application program on one machine or process to send a datagram to an application program on another machine or process. UDP uses the Internet Protocol (IP) to deliver datagrams.

V

value. (1) A specific occurrence of an attribute; for example, “blue” for the attribute “color.” (T) (2) A quantity assigned to a constant, a variable, a parameter, or a symbol.

variable. (1) In programming languages, a language object that may take different values, one at a time. The values of a variable are usually restricted to a certain data type. (I) (2) A quantity that can assume any of a given set of values. (A) (3) A name used to represent a data item whose value can be changed while the program is running. (4) In the Simple Network Management Protocol (SNMP), a match of an object instance name with an associated value.

version. A separately licensed program that usually has significant new code or new function.

viewing filter. In the NetView program, the function that allows a user to select the alert data to be displayed on a terminal. All other stored data is blocked.

virtual machine (VM). (1) A virtual data processing system that appears to be at the exclusive disposal of a particular user, but whose functions are accomplished by sharing the resources of a real data processing system. (T) (2) In VM/ESA, the virtual processors, virtual storage, virtual devices, and virtual channel subsystem allocated to a single user. A virtual machine also includes any expanded storage dedicated to it.

VM. Virtual machine.

W

WAN. Wide area network.

wide area network (WAN). (1) A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. (T) (2) A data communication network designed to serve an area of hundreds or thousands of miles; for example, public and private packet-switching networks, and national telephone networks. (3) Contrast with *local area network (LAN)* and *metropolitan area network (MAN).*

wildcard character. Synonym for *pattern-matching character.*

window. (1) A portion of a display surface in which display images pertaining to a particular application can be presented. Different applications can be displayed simultaneously in different windows. (A) (2) An area with visible boundaries that presents a view of an object or with which a user conducts a dialog with a computer system.

workstation. (1) A functional unit at which a user works. A workstation often has some processing capability. (T) (2) One or more programmable or nonprogrammable devices that allow a user to do work. (3) A terminal or microcomputer, usually one that is connected to a mainframe or to a network, at which a user can perform applications.

X

X Window System. A software system, developed by the Massachusetts Institute of Technology, that allows the user of a display to concurrently use multiple application programs through different windows of the display. The application programs may execute on different computers.

X.25. (1) An International Telegraph and Telephone Consultative Committee (CCITT) recommendation for the interface between data terminal equipment and packet-switched data networks. (2) See also *packet switching.*

X.25 interface. An interface consisting of a data terminal equipment (DTE) and a data circuit-terminating equipment (DCE) in communication over a link using the procedures described in the CCITT Recommendation X.25.

Bibliography

NetView for AIX Publications

The following paragraphs briefly describe the publications for Version 4 of the NetView for AIX program:

NetView for AIX Concepts: A General Information Manual (GC31-8160)

This book provides an overview of the NetView for AIX program that business executives can use to evaluate the product. System planners can also use this information to learn how NetView for AIX manages heterogeneous networks.

NetView for AIX Database Guide (SC31-8167)

This book provides information for system administrators and database administrators to configure the NetView for AIX program to work with the following relational database management systems: DB2/6000, INFORMIX, INGRES, ORACLE, and SYBASE. This book also describes how to transfer IP topology, trapdlog, and snmpCollect data to the relational database and how to manipulate the data.

NetView for AIX Installation and Configuration (SC31-8163)

This book provides installation and configuration steps for the system programmer who will install and configure the NetView for AIX program.

NetView for AIX User's Guide for Beginners (SC31-8158)

This book contains “how-to” information that provides network operators the help they need to get acquainted with NetView for AIX and accomplish some basic networking tasks. It is written for the user who is unfamiliar with the NetView for AIX program.

NetView for AIX Administrator's Guide (SC31-8168)

This book explains network management principles and describes how the NetView for AIX program's components work together. It is for the advanced user. Most of the tasks require root authority. This book includes tasks such as customizing the graphical interface, filtering events, configuring events, and managing network performance and configuration.

NetView for AIX Administrator's Reference (SC31-8169)

This book contains reference information for commands, daemons, and files. It is used primarily when performing administrative tasks.

NetView for AIX Diagnosis Guide (SC31-8162)

This book is intended to help you classify and resolve problems related to the operation of the NetView for AIX program.

NetView for AIX Application Interface Style Guide (SC31-6240)

This book provides guidelines for system programmers who develop applications that will be integrated with the NetView for AIX program.

NetView for AIX Programmer's Guide (SC31-8164)

This book provides information for programmers about creating network management applications. This book also contains information about the NetView for AIX program server, commands, function calls, and object classes.

NetView for AIX Programmer's Reference (SC31-8165)

This book is intended for programmers and contains reference information about the NetView for AIX program and its server, commands, function calls, and object classes.

NetView for AIX and the Host Connection (SC31-8161)

This book provides information for System/390 and NetView users who want to manage TCP/IP and SNA networks.

Quick Reference Card (SX75-0113)

This summary provides a brief description of each NetView for AIX daemon. The card also lists the menu items and the submenu items below them.

In addition to these printed books, online documentation of the NetView for AIX library is available. An online Help Index is also available from the NetView for AIX Help pull-down window. The Help Index provides dialog box help and task help.

IBM RISC System/6000 Publications

In addition to the NetView for AIX documentation, the following publications may also be helpful to users:

AIX Quick Reference (SC23-2401)

Task Index and Glossary for IBM RISC System/6000 (GC23-2201)

IBM RISC System/6000 Problem Solving Guide (SC23-2204)

AIX Communications Concepts and Procedures for IBM RISC System/6000 (GC23-2203)

AIX Commands Reference for IBM RISC System/6000 (GC23-2366, GC23-2367, GC23-2376, GC23-2393)

AIX Files Reference for IBM RISC System/6000 (GC23-2200)

NetView Publications

The following list contains selected NetView Version 2 Release 3 publications:

NetView Administration Reference (SC31-6128)

NetView At a Glance (GC31-7016)

NetView Automation Planning (SC31-6141)

NetView Customization Guide (SC31-6132)

NetView Installation and Administration Guide (MVS: SC31-6125) (VM: SC31-6182) (VSE: SC31-6182)

NetView Operation (SC31-6127)

NetView Problem Determination and Diagnosis (LY43-0014)

NetView Resource Alerts Reference (SC31-6136)

NetView Samples (MVS: SC31-6126) (VM: SC31-6183) (VSE: SC31-6184)

The following list contains selected NetView Version 2 Release 4 publications:

NetView Administration Reference (SC31-7080)

NetView Automation Planning (SC31-7082)

NetView Customization Guide (SC31-7091)

NetView General Information (GC31-7098)

NetView Installation and Administration Facility/2 Guide (SC31-7099)

NetView Installation and Administration Guide (SC31-7084)

NetView Operation (SC31-7066)

NetView Problem Determination and Diagnosis (LY43-0101)

NetView Resource Alerts Reference (SC31-7097)

TCP/IP Publications for AIX (RS/6000, PS/2, RT, 370)

The following list shows the books available for TCP/IP in the AIX Operating System library:

AIX Operating System TCP/IP User's Guide (SC23-2309)

AIX PS/2 TCP/IP User's Guide (SC23-2047)

TCP/IP for IBM X-Windows on DOS (SC23-2349)

AIX SNA Services/6000 Publications

The following list of publications are for use with the AIX Operating System:

AIX SNA Server/6000 User's Guide (SC31-7002)

AIX SNA Server/6000 Configuration Reference (SC31-7014)

AIX SNA Server/6000 Transaction Program (SC31-7003)

Internet Request for Comments (RFCs)

The following documents describe Internet standards supported by the NetView for AIX program. Copies of these documents are shipped on the AIX SystemView NetView/6000 product installation media. They are installed in the /usr/OV/doc directory.

RFC 1095: The Common Management Services and Protocol over TCP/IP (CMOT)

RFC 1155: Structure and Identification of Management Information for TCP/IP-Based Internets

RFC 1157: Simple Network Management Protocol (SNMP)

RFC 1187: Bulk Table Retrieval with the SNMP

RFC 1189: The Common Management Information Services and Protocols for the Internet (CMOT and CMIP)

RFC 1212: Concise MIB Definitions

RFC 1213: Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II

RFC 1215: Convention for Defining Traps for Use with the SNMP

RFC 1229: Extensions to the Generic-Interface MIB

RFC 1230: IEEE 802.4 Token Bus MIB

RFC 1231: IEEE 802.5 Token Bus MIB

RFC 1232: Definitions of Managed Objects for the DS1 Interface Type

RFC 1233: Definitions of Managed Objects for the DS3 Interface Type

RFC 1239: Reassignment of Experimental MIBs to Standard MIBs

RFC 1243: AppleTalk Management Information Base

RFC 1253: OSPF Version 2 Management Information Base

RFC 1269: Definitions of Managed Objects for the Border Gateway Protocol (Version 3)

RFC 1271: Remote Network Monitoring Management Information Base

RFC 1284: Definitions of Managed Objects for the Ethernet-like Interface Types

RFC 1285: FDDI Management Information Base

RFC 1286: Definitions of Managed Objects for Bridges

RFC 1289: DECnet Phase IV MIB Extensions

RFC 1304: Definition of Managed Objects for the SIP Interface Type

RFC 1315: Management Information Base for Frame Relay DTEs

RFC 1316: Definitions of Managed Objects for Character Stream Devices

RFC 1317: Definitions of Managed Objects for RS-232-like Hardware Devices

RFC 1318: Definitions of Managed Objects for Parallel-printer-like Hardware Devices

RFC 1450: Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)

RFC 1452: Coexistence between Version 1 and Version 2 of the Internet-Standard Network Management Framework

Related Publications

The following publications are closely related to or referenced by the NetView for AIX Library:

AIX Trouble Ticket/6000 Publications

For information about the AIX Trouble Ticket/6000 program, consult the following publications:

AIX Trouble Ticket/6000 Brochure (GC31-7161)

AIX Trouble Ticket/6000 User's Guide (SC31-7162)

Service Point Publication

AIX NetView Service Point Installation, Operation, and Programming Guide (SC31-6120)

Other IBM TCP/IP Publications

The following list shows other available IBM TCP/IP publications:

Introducing IBM Transmission Control Protocol/Internet Protocol Products for OS/2, VM, and MVS (GC31-6080)

IBM TCP/IP Version 2 for VM and MVS: Diagnosis Guide (LY43-0013)

MVS/DFP Version 3 Release 3: Using the Network File System Server (SC26-4732)

SNMP Information

You can use the following sources for detailed SNMP information:

The Simple Book, M.T. Rose, Prentice-Hall, 1991 (ISBN 0-13-812611-9)

The *Windows SNMP Manager API Specification*, the *WinSNMP/MIB API Specification*, and other information on Windows SNMP are available through anonymous FTP from the host sunsite.unc.edu under the directory path /pub/micro/pc-stuff/ms-windows/WinSNMP

These Internet standards provide SNMP information:

RFC 1901: Introduction to Community-based SNMPv2

RFC 1902: Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)

RFC 1903: Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)

RFC 1904: Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)

RFC 1905: Protocol Operation for Version 2 of the Simple Network Management Protocol (SNMPv2)

RFC 1906: Transport Mapping for Version 2 of the Simple Network Management Protocol (SNMPv2)

RFC 1907: Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)

RFC 1908: Coexistence between Version 1 and Version 2 of Internet-standard Network Management Framework

RFC 1909: An Administrative Infrastructure for SNMPv2 (SNMPv2USEC)

RFC 1910: User-based Security Model for SNMPv2 (SNMPv2USEC)

X Window System Publications

The following list shows selected X Window System publications:

Introduction to the X Window System, Oliver Jones, Prentice-Hall, 1988 (ISBN 0-13-499997)

X Window System Technical Reference, Steven Mikes, Addison-Wesley, 1990 (ISBN 0-201-52370)

X Window System: Programming and Applications with Xt, Douglas A. Young, Prentice-Hall, 1989 (ISBN 0-13-972167)

X Window System: Programming and Applications with Xt, OSF/Motif Edition, Douglas A. Young, Prentice-Hall, 1990 (ISBN 0-13-497074)

X/Open Specification

For information about the X/Open OSI-Abstract-Data Manipulation (XOM) application programming interface (API), consult the following X/Open documents:

X/Open OSI-Abstract-Data Manipulation (XOM) API, CAE Specification

X/Open Preliminary Specification. Systems Management: GDMO to XOM Translation Algorithm

OSF/Motif Publications

The following list contains selected OSF/Motif publications:

OSF/Motif Series (5 volumes), Open Software Foundation, Prentice Hall, Inc. 1990

OSF/Motif Application Environment Specifications, (AES) (ISBN 0-13-640483-9)

OSF/Motif Programmer's Guide (ISBN 0-13-640509-6)

OSF/Motif Programmer's Reference,
(ISBN 0-13-640517-7)

OSF/Motif Style Guide (ISBN 0-13-640491-X)

OSF/Motif User's Guide, (ISBN 0-13-640525-8)

ISO/IEC Standards

For information about the ISO/IEC standards on which the NetView for AIX program is based, refer to the following publications:

ISO IS 7498-4, Open Systems Interconnection–Basic Reference Model–Part 4: Management Framework

ISO 8824, Open Systems Interconnection–Specification of Abstract Syntax Notation One (ASN.1)

ISO 8825, Open Systems Interconnection– Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)

ISO IS 9595, Common Management Information–Service Definition

ISO IS 9596-1, Common Management Information–Protocol Specification

ISO DIS 9899, Information Processing–Programming Language C

ISO 10040, Systems Management Overview

The ISO/IEC standards can be obtained from the following address:

OMNICOM
243 Church St. NW
Vienna, VA 22180-4434

(800) OMNICOM
(703) 281-1135
(703) 281-1505 (FAX)

Index

Communicating Your Comments to IBM

NetView for AIX
Installation and Configuration
Version 4

Publication No. SC31-8163-01

If you especially like or dislike anything about this book, please use one of the methods listed below to send your comments to IBM. Whichever method you choose, make sure you send your name, address, and telephone number if you would like a reply.

Feel free to comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. However, the comments you send should pertain to only the information in this manual and the way in which the information is presented. To request additional publications, or to ask questions or make comments about the functions of IBM products or systems, you should talk to your IBM representative or to your IBM authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

If you are mailing a readers' comment form (RCF) from a country other than the United States, you can give the RCF to the local IBM branch office or IBM representative for postage-paid mailing.

- If you prefer to send comments by mail, use the RCF at the back of this book.
- If you prefer to send comments by FAX, use this number:

  United States and Canada: **1-800-227-5088**
- If you prefer to send comments electronically, use this network ID:
  - IBM Mail Exchange: **USIB2HPD at IBMMAIL**
  - IBMLink: **CIBMORCF at RALVM13**
  - Internet: **USIB2HPD@VNET.IBM.COM**

Make sure to include the following in your note:

- Title and publication number of this book
- Page number or topic to which your comment applies.

Help us help you!

NetView for AIX
Installation and Configuration
Version 4

Publication No. SC31-8163-01

We hope you find this publication useful, readable and technically accurate, but only you can tell us! Your comments and suggestions will help us improve our technical publications. Please take a few minutes to let us know what you think by completing this form.

Overall, how satisfied are you with the information in this book?	Satisfied	Dissatisfied
	□	□

How satisfied are you that the information in this book is:	Satisfied	Dissatisfied
Accurate	□	□
Complete	□	□
Easy to find	□	□
Easy to understand	□	□
Well organized	□	□
Applicable to your task	□	□

Specific Comments or Problems:

____

____

____

Please tell us how we can improve this book:

____

____

____

Thank you for your response. When you send information to IBM, you grant IBM the right to use or distribute the information without incurring any obligation to you. You of course retain the right to use the information in any way you choose.

Name	Address
Company or Organization	
Phone No.	

Help us help you!
SC31-8163-01

Cut or Fold
Along Line

Fold and Tape | **Please do not staple** | Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

Information Development
Department CGMD
International Business Machines Corporation
PO BOX 12195
RESEARCH TRIANGLE PARK NC 27709-9990

Fold and Tape | **Please do not staple** | Fold and Tape

Cut or Fold
Along Line

Program Number: 5765-527

Printed in U.S.A.

SC31-8163-01

```
DSMKPO653E POSTSCRIPT FILE '@E@P@S' NOT FOUND.
DSMMOM395I '.EDFPO' LINE 70: .po @E@P@S
DSMMOM397I '.EDFPO' WAS IMBEDDED AT LINE 910 OF '.EDFAWRK'
DSMMOM397I '.EDFAWRK' WAS IMBEDDED AT LINE 2330 OF '.EDF#CV'
DSMMOM397I '.EDF#CV' WAS IMBEDDED AT LINE 120 OF '.EDF#FCV5'
DSMMOM397I '.EDF#FCV5' WAS IMBEDDED AT LINE 330 OF '.EDFCOVER'
DSMMOM397I '.EDFCOVER' WAS IMBEDDED AT LINE 41 OF 'LBUL0MST'
DSMKPO653E POSTSCRIPT FILE '@E@P@S' NOT FOUND.
DSMMOM395I '.EDFPO' LINE 70: .po @E@P@S
DSMMOM397I '.EDFPO' WAS IMBEDDED AT LINE 910 OF '.EDFAWRK'
DSMMOM397I '.EDFAWRK' WAS IMBEDDED AT LINE 37 OF 'LBUL0C2'
DSMMOM397I 'LBUL0C2' WAS IMBEDDED AT LINE 187 OF 'EDFPRF40'
DSMBEG323I STARTING PASS 2 OF 4.
DSMKPO653E POSTSCRIPT FILE '@E@P@S' NOT FOUND.
DSMMOM395I '.EDFPO' LINE 70: .po @E@P@S
DSMMOM397I '.EDFPO' WAS IMBEDDED AT LINE 910 OF '.EDFAWRK'
DSMMOM397I '.EDFAWRK' WAS IMBEDDED AT LINE 2330 OF '.EDF#CV'
DSMMOM397I '.EDF#CV' WAS IMBEDDED AT LINE 120 OF '.EDF#FCV5'
DSMMOM397I '.EDF#FCV5' WAS IMBEDDED AT LINE 330 OF '.EDFCOVER'
DSMMOM397I '.EDFCOVER' WAS IMBEDDED AT LINE 41 OF 'LBUL0MST'
DSMKPO653E POSTSCRIPT FILE '@E@P@S' NOT FOUND.
DSMMOM395I '.EDFPO' LINE 70: .po @E@P@S
DSMMOM397I '.EDFPO' WAS IMBEDDED AT LINE 910 OF '.EDFAWRK'
DSMMOM397I '.EDFAWRK' WAS IMBEDDED AT LINE 37 OF 'LBUL0C2'
DSMMOM397I 'LBUL0C2' WAS IMBEDDED AT LINE 187 OF 'EDFPRF40'
DSMBEG323I STARTING PASS 3 OF 4.
DSMKPO653E POSTSCRIPT FILE '@E@P@S' NOT FOUND.
DSMMOM395I '.EDFPO' LINE 70: .po @E@P@S
DSMMOM397I '.EDFPO' WAS IMBEDDED AT LINE 910 OF '.EDFAWRK'
DSMMOM397I '.EDFAWRK' WAS IMBEDDED AT LINE 2330 OF '.EDF#CV'
DSMMOM397I '.EDF#CV' WAS IMBEDDED AT LINE 120 OF '.EDF#FCV5'
DSMMOM397I '.EDF#FCV5' WAS IMBEDDED AT LINE 330 OF '.EDFCOVER'
DSMMOM397I '.EDFCOVER' WAS IMBEDDED AT LINE 41 OF 'LBUL0MST'
DSMKPO653E POSTSCRIPT FILE '@E@P@S' NOT FOUND.
DSMMOM395I '.EDFPO' LINE 70: .po @E@P@S
DSMMOM397I '.EDFPO' WAS IMBEDDED AT LINE 910 OF '.EDFAWRK'
DSMMOM397I '.EDFAWRK' WAS IMBEDDED AT LINE 37 OF 'LBUL0C2'
DSMMOM397I 'LBUL0C2' WAS IMBEDDED AT LINE 187 OF 'EDFPRF40'
DSMBEG323I STARTING PASS 4 OF 4.
DSMKPO653E POSTSCRIPT FILE '@E@P@S' NOT FOUND.
DSMMOM395I '.EDFPO' LINE 70: .po @E@P@S
DSMMOM397I '.EDFPO' WAS IMBEDDED AT LINE 910 OF '.EDFAWRK'
DSMMOM397I '.EDFAWRK' WAS IMBEDDED AT LINE 2330 OF '.EDF#CV'
DSMMOM397I '.EDF#CV' WAS IMBEDDED AT LINE 120 OF '.EDF#FCV5'
DSMMOM397I '.EDF#FCV5' WAS IMBEDDED AT LINE 330 OF '.EDFCOVER'
DSMMOM397I '.EDFCOVER' WAS IMBEDDED AT LINE 41 OF 'LBUL0MST'
DSMKPO653E POSTSCRIPT FILE '@E@P@S' NOT FOUND.
DSMMOM395I '.EDFPO' LINE 70: .po @E@P@S
DSMMOM397I '.EDFPO' WAS IMBEDDED AT LINE 910 OF '.EDFAWRK'
DSMMOM397I '.EDFAWRK' WAS IMBEDDED AT LINE 37 OF 'LBUL0C2'
DSMMOM397I 'LBUL0C2' WAS IMBEDDED AT LINE 187 OF 'EDFPRF40'
```