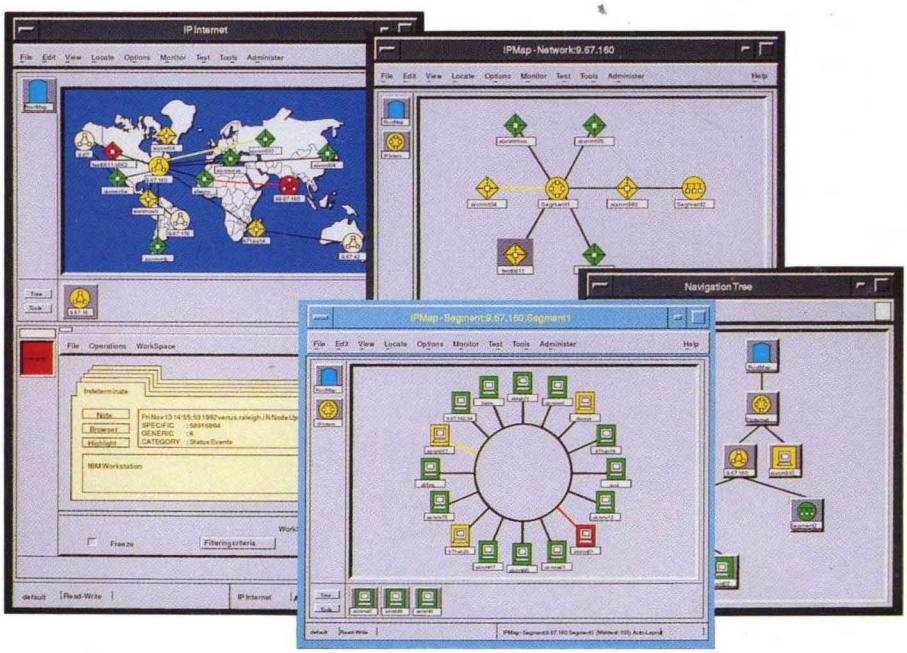
AIX SystemView NetView/6000

SC31-6178-00

And the Host Connection

Version 2



AIX SystemView NetView/6000

SC31-6178-00

And the Host Connection

Version 2

IBM

First Edition (May 1993)

This document applies to the IBM AIX NetView/6000 network management product (5696-362) which runs under the AIX operating system for RISC System/6000 Version 3 Release 2 (5756-030).

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 E15
P.O. Box 12195
Research Triangle Park, North Carolina 27709-9990
U.S.A.

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

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. Changes are made periodically to the information herein; before you use this document in connection with the operation of IBM systems, consult the latest *Task Index and Glossary for IBM RISC System/6000*, GC23-2201, for the editions that are applicable and current.

Any reference to an IBM licensed program or other IBM product in this document is not intended to state or imply that only IBM's program or other IBM product may be used.

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 inquiries, in writing, to the IBM Director of Commercial Relations, International Business Machines Corporation, Purchase, New York, 10577.

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.

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:

AIX	IBM	MVS
NETCENTER	NetView	RISC System/6000
SystemView	System/390	VM
VSE		

The following terms, denoted by a double asterisk (**) at their first occurrences in this publication, are trademarks of other companies in the United States or in other countries:

SynOptics	SynOptics Communications, Inc.

About This Book

This book provides an overview of the AIX* SystemView* NetView*/6000 (AIX NetView/6000) host connection and contains instructions on how to implement and maintain the connection between the host and the AIX NetView/6000 program. Through the connection, the NetView program, and optionally the NETCENTER program, can use the facilities of the AIX NetView/6000 program in managing SNMP devices.

Who Should Use This Book

Anyone responsible for using and implementing the AIX SystemView NetView/6000 host connection should read this book. The intended audience is system administrators. The reader is presumed to have an understanding of the NetView, NETCENTER, and AIX NetView/6000 programs, the AIX Operating System, and the Systems Network Architecture (SNA) and TCP/IP networking environments.

How to Use This Book

This book explains the steps involved in setting up, testing, and using the AIX NetView/6000 host connection. Use this book as a procedural guide or as a reference.

This document contains four chapters and two appendixes.

- Chapter 1, "Understanding the Host Connection" on page 1 provides a general overview of the connection.
- Chapter 2, "Establishing and Maintaining the Host Connection" on page 7 provides a detailed description of the process involved in the connection.
- Chapter 3, "Working with the Host Program" on page 35 describes considerations in working with the NetView program.
- Chapter 4, "Using the Host Connection" on page 41 provides examples of how the connection is used.
- Appendix A, "Reference Information" on page 47 lists the options for the daemons involved in the connection.
- Appendix B, "Subvectors Included in SNA MS Major Vectors" on page 49 lists the subvectors that are included in the SNA Major Vectors

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 AIX NetView/6000 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:

```
Options..Event Configuration..Trap-to-Alert Filter Control:  SNMP...
```

In this example, `Options` is a menu bar or context menu option, `Event Configuration` is an operation available from the Options submenu, `Trap-to-Alert Filter Control` is a second submenu, and `SNMP` is a function that is available when you click on Event Configuration.

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

Terms and Abbreviations

The term *host program* refers to the program, the NetView and optionally, the NETCENTER program, residing on the host 390 portion of the connection.

Where to Find More Information

The Bibliography describes publications that can be helpful when using the AIX NetView/6000 program. The Internet Request for Comments (RFC) documents listed are shipped on the AIX NetView/6000 program installation media and are installed in the /usr/OV/doc directory.

The following list contains the names and order numbers of the publications in the AIX NetView/6000 Version 2 library:

Diagnosis

AIX SystemView NetView/6000 Problem Determination, SC31-7021

General Information

AIX SystemView NetView/6000 Concepts: A General Information Manual, GC31-6179

Installation and Configuration

AIX SystemView NetView/6000 Installation and Configuration, SC31-7020

Usage and Administration

AIX SystemView NetView/6000 User's Guide, SC31-7024
AIX SystemView NetView/6000 and the Host Connection, SC31-6178

Programming

AIX SystemView NetView/6000 Programmer's Reference, SC31-7023
AIX SystemView NetView/6000 Programmer's Guide, SC31-7022
AIX SystemView NetView/6000 Application Design and Style Guide, SC31-7019

Online Information

The information in these books is also available online through the InfoExplorer* program.

Related Sources of Information

The following sources provide specific information that is not documented in the AIX SystemView NetView/6000 Version 2 library:

- The /usr/lpp/nv6000/README file provides additional information about the AIX NetView/6000 program.
- The online help facility provides task, dialog box, operation, 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, 1989 (ISBN 0-13-812611-9)

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. Understanding the Host Connection

Using the AIX NetView Service Point program in conjunction with the AIX SystemView NetView/6000 (AIX NetView/6000) and the NetView programs, you can cooperatively manage both SNA networks and TCP/IP networks. As an option, you can use the NETCENTER program to graphically present and manage your IP-addressable devices. The AIX NetView Service Point program acts as a bridge between the AIX NetView/6000 program and the host enabling the NetView or the NETCENTER program to use the facilities of the AIX NetView/6000 program in managing SNMP devices.

This chapter gives an overview of the connection between the AIX NetView/6000 and the NetView and NETCENTER environments. It explains how the AIX NetView Service Point and the AIX NetView/6000 programs combine to enable the NetView and NETCENTER programs to react to events in a TCP/IP environment. This chapter also explains how the AIX NetView/6000 program transfers information between a TCP/IP environment and a Systems Network Architecture (SNA) environment.

What Are the Software Requirements?

To use the host connection, you need the following software programs:

- NetView Version 1 Release 3 or above
  - (Version 1 Release 2 or above for VSE)
- AIX NetView/6000 Version 2 Release 1
- AIX NetView Service Point Version 1 Release 2
- SNA Services/6000 Version 1 Release 2
- NETCENTER Version 1 (optional)
  - See *NETCENTER Service Point Interface Operation, Installation and Reference* for a list of the hardware and software requirements.

What Are the Uses of the Host Connection?

One use of the host connection is to inform the host program of certain events in a TCP/IP network by converting selected traps into alerts and forwarding them to the host program. The host program can respond to the alert by returning a RUNCMD command that contains an appropriate response to the event.

The host connection also enables the NetView, and optionally, the NETCENTER operator to issue a command for execution in the SNMP environment. The command will be enclosed in a RUNCMD and sent to

the SNMP environment for execution. The results will then be returned to the host program in another RUNCMD.

Use the SMIT Set Options for Host Connection Daemons to specify whether you will be connecting to the NETCENTER program. This process is illustrated in Figure 1.

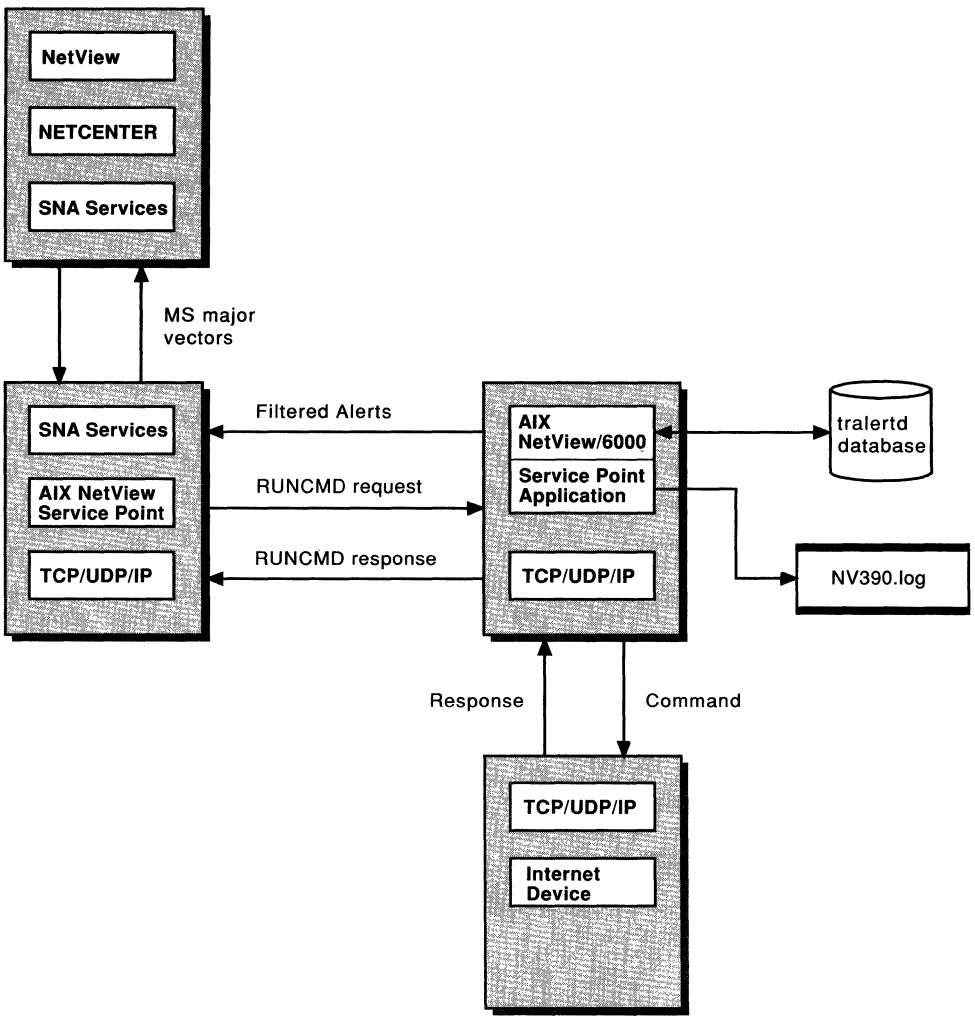


Figure 1. Principal Components in Cooperative Management

The tralertd daemon receives the traps that have met the filtering criteria and uses the NetView Service Point APIs to convert the traps into alerts (NMVTs). The NetView Service Point program then forwards the alerts to the host program.

The host program responds to the alert by enclosing an appropriate command in a RUNCMD command. The RUNCMD command is executed by the AIX NetView/6000 program, which then returns a response

to the host program. An overview of the process is shown in "Understanding the Relationship Between the Daemons" on page 4

Figure 1 on page 2 shows the AIX NetView/6000 and the NetView Service Point programs residing in separate RISC System/6000 systems. Both programs can reside in a single RISC System/6000 if adequate storage is available.

Understanding the Relationship Between the Daemons

The AIX NetView/6000 processes used in the host connection are:

- The ovesmd daemon
- The tralertd daemon
- The spappld daemon

Figure 2 shows the interrelationship of the processes and functions used in the connection.

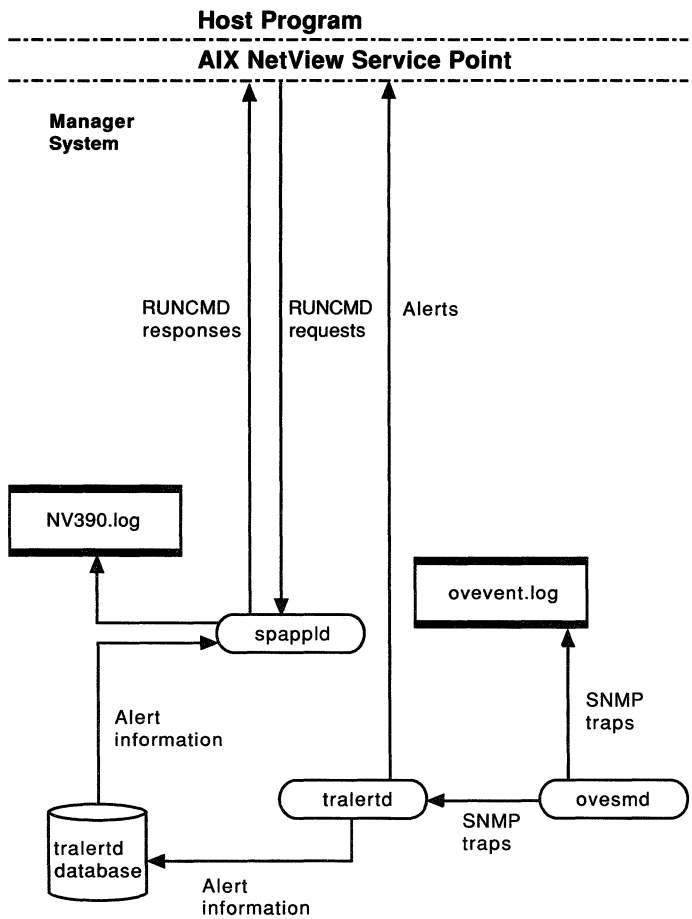


Figure 2. AIX NetView/6000 Processes and Functions Used in the Host Connection

The tralertd daemon receives the incoming SNMP traps, which have met the event filtering criteria, and uses the Service Point program APIs to convert them to alerts."Filtering Events" on page 7 explains how to set the event filtering criteria.

The AIX NetView Service Point program then forwards the alerts to the host program as network management vector transports (NMVTs).

The spappld daemon acts as a command interface between the host and the AIX NetView/6000 program. The spappld daemon receives a RUNCMD command, uses the facilities of the AIX NetView/6000 program to execute the contents of the RUNCMD command, and sends the response back to the host program as RUNCMD NMVTs. If a RUNCMD command requests trap information for an incomplete alert sent by the tralertd daemon, the spappld daemon queries the tralertd.log, and uses the **gettrap** command to retrieve the remaining trap information.

Use the Tools..Filter Editor and the Options.Event Configuration.Trap Customization menu items to determine which traps will be converted to alerts and forwarded to the host program. Use the Options.Event Configuration.Trap Customization.SNMP operations to configure the trap-to-alert mapping and to control what is displayed at the host program.

Chapter 2. Establishing and Maintaining the Host Connection

The process for establishing and maintaining the host connection involves the following activities:

- Using the event filter to limit the number of events forwarded to the tralertd daemon
- Converting the filtered events to alerts
- Sending the alerts to the host program
- Using RUNCMDs to respond to the alerts and to operator-initiated commands.

This chapter also describes the default process used in configuring alerts and the considerations for working with the NetView Service Point and NETCENTER programs.

Filtering Events

The AIX NetView/6000 program uses the event filter to identify which traps will be converted to alerts and to reduce the number of events that will be forwarded to the tralertd daemon. Traps are a type of event in which agents send information to the manager without an explicit request from the manager. Traps inform the manager about changes that occur on the agent system, such as restarting the system.

To create the filtering criteria, you can use the Filter Editor entry in the Tools menu or the default filter (**/usr/OV/conf/tralertd.default**). You can then use the **selectfilter** command or the graphical interface to dynamically vary the filtering criteria. Both methods provide an interface to the AIX **cron** command to specify when a filter will be activated and deactivated.

Defining a Simple Filter

This section describes the process of defining a filter for a link-down trap from an IBM 6611 router. If the tralertd daemon detects a link-down trap from an IBM 6611 router, it will convert the trap into an alert and forward the alert to the host program.

To create a simple filter:

Step 1. Click on the Filter Editor entry in the Tools menu. The Filter Editor dialog box will appear.

Step 2. From the Filter Editor dialog box, enter the path name of the filter file. The default is **/usr/OV/filters/filter.samples**. If you are not sure of the path name, click on the File List... button

and the File Selection dialog box will appear. Select the desired filter file.

Figure 3 shows the Filter Editor dialog box.

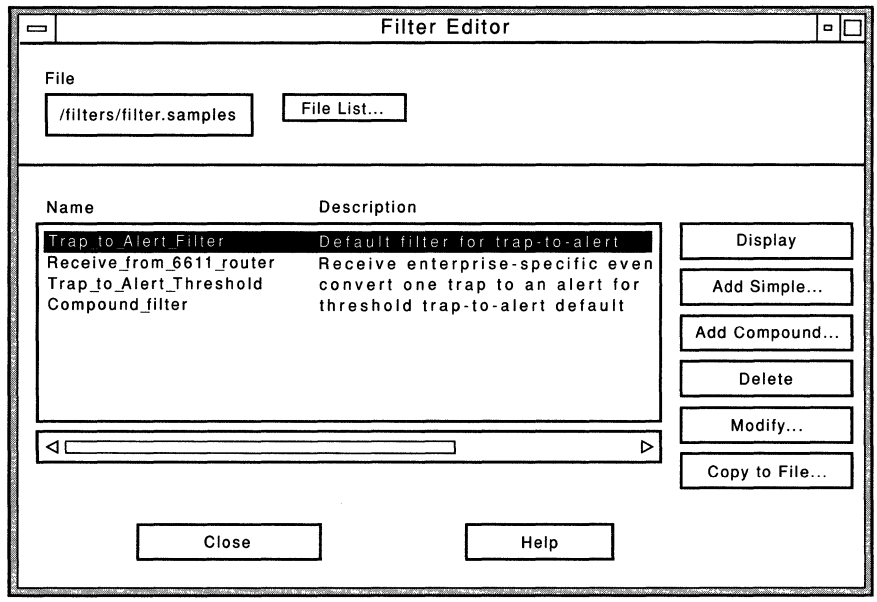


Figure 3. Filter Editor Dialog Box

Step 3. Click on the Add Simple... button. The Simple Filter Editor dialog box will appear.

Figure 4 on page 9 shows the Simple Filter Editor dialog box.

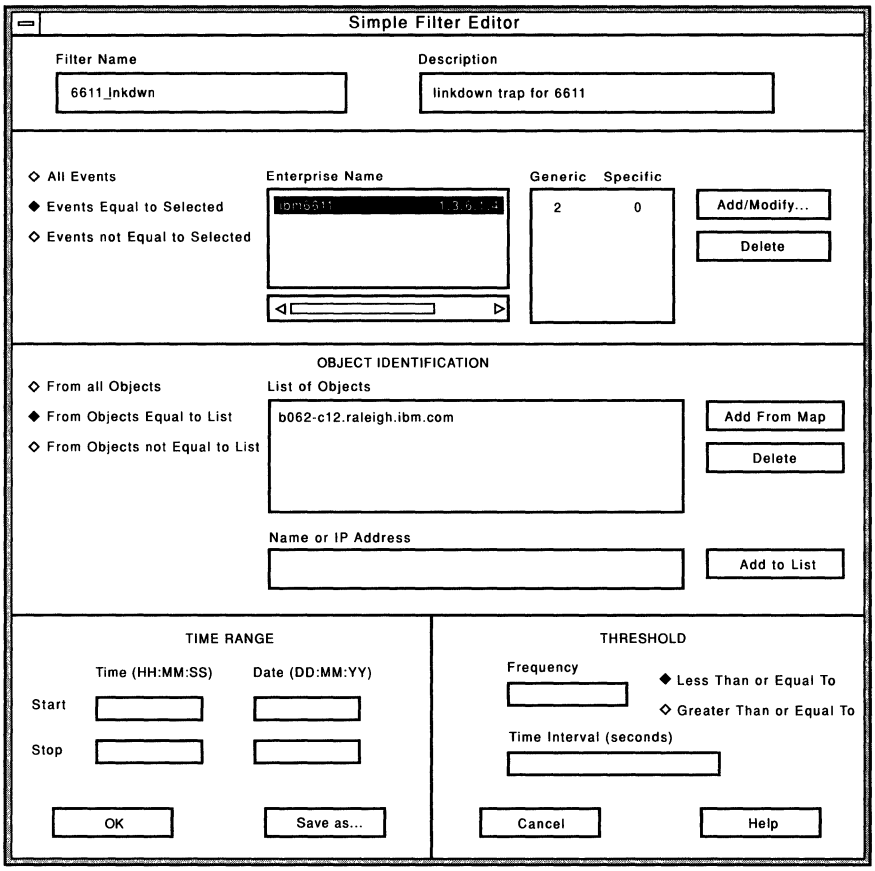


Figure 4. Simple Filter Editor Dialog Box

Step 4. Click on the Events Equal to Selected button and click on the Add/Modify... button. The Enterprise Specific Trap Selection dialog box will appear.

Figure 5 on page 10 shows the Enterprise Specific Trap Selection Dialog box.

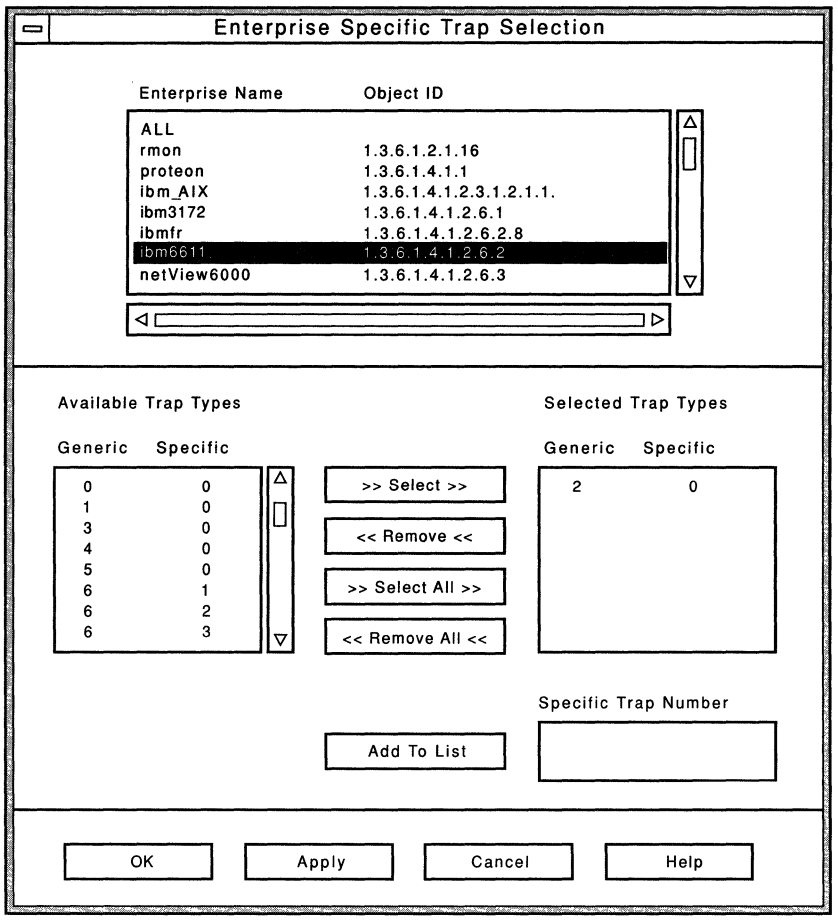


Figure 5. Enterprise Specific Trap Selection Dialog Box

Step 5. Select the appropriate Enterprise Name and desired generic trap type. In this example, a generic trap type of 2 (link-down trap) was selected for the ibm6611 enterprise.

Step 6. Click on the OK button. The Simple Filter Editor dialog box will appear with the selected events.

Figure 4 on page 9 shows the selected events.

Step 7. Click on the Locate function from the main menu and then the Locate By Symbol Type function to locate the 6611 routers. When the 6611 routers have been located, click on the Select button.

Step 8. From the Simple Filter Editor dialog box, click on the From Objects Equal to List and then the Add From Map buttons to move the selected items into the Object Identification window, click on the Add from Map button. You can also enter the IP addresses of the routers in the Object Identification field.

Step 9. Click on the OK button.

Activating the Filter

Use the Trap to Alert Filter Control dialog box to set the activation criteria for a filter. This dialog box is reached through the Options...Event Configuration...Trap to Alert Filter Control:SNMP menu item. (You must be a root user to perform this function.)

Step 1. Select the name of the filter from the Filter/Description window.

Step 2. To activate the filter immediately, click on the Activate button.

Step 3. To select the times and dates that the filter will be activated or deactivated, click on the appropriate buttons and entering the times (in 24–hour format) in the Activation and Deactivation windows.

Step 4. Click on the Add to cron button to update the AIX **cron** table.

Figure 6 shows the Trap to Alert Filter Control dialog box.

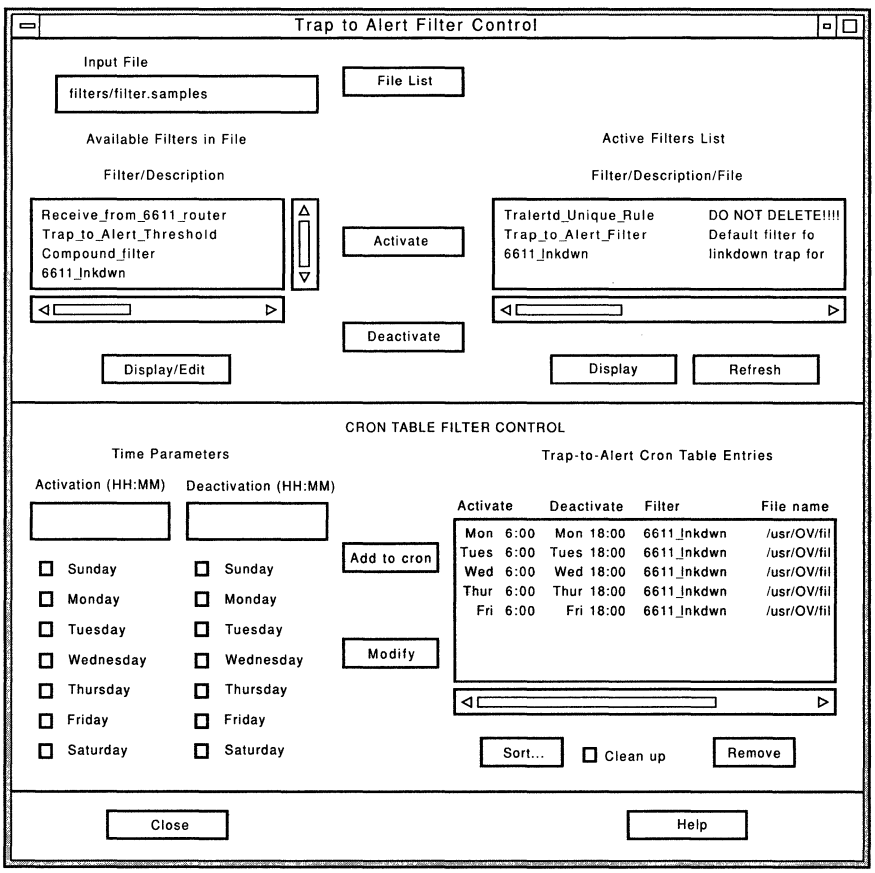


Figure 6. Trap to Alert Filter Control Dialog Box

Using the Alert Editor to Define an Alert

The Alert Editor enables you to define an alert for a particular event. When the particular event occurs and passes through the trap to alert filter the tralertd daemon uses the values stored in tralertd.conf to generate the alert and send the alert to the host.

The Alert Editor is accessed through the Event Configuration dialog box. This box is reached through the Options..Event Configuration.. Trap Customization:SNMP menu item. After selecting this entry from the menu bar, the Event Configuration dialog box becomes available.

The following sections describe how the Alert Editor is used to add a trap for a SynOptics** agent. The trap is defined as follows:

```
chassisPowerSupply Failure     TRAP-TYPE
       ENTERPRISE              SynOptics
       VARIABLES               { s3ChassisPsStatus }
       STATUS                  mandatory for all SynOptics agents
       DESCRIPTION
                               "Concentrator power supply failure"
       ::= 0                    --  0x00
```

Figure 7. Example of a SynOptics Trap

The steps of defining an alert and sending it to the host include:

- Adding a New Enterprise
- Adding a New Trap
- Changing the Generic Alert Subvector
- Changing the Probable Cause Subvector
- Sending Qualifiers with the Alert
- Changing the Causes and Actions Subvectors

These sections show how to define an alert for when a SynOptics agent experiences a concentrator power supply failure. The trap is an enterprise specific trap with a generic trap number of 6 and a specific trap number of 0 (zero).

Adding a New Enterprise

To add a new enterprise:

Step 1. Click on the Add New Enterprise button of the Event Configuration dialog box. A dialog box similar to that shown in Figure 8 will appear.

Step 2. Enter the Enterprise Name and the Enterprise ID. In this example, the Enterprise Name is `SynOptics` and the Enterprise ID is `1.3.6.1.4.1.10`.

Step 3. Click on the Add button to complete the change.

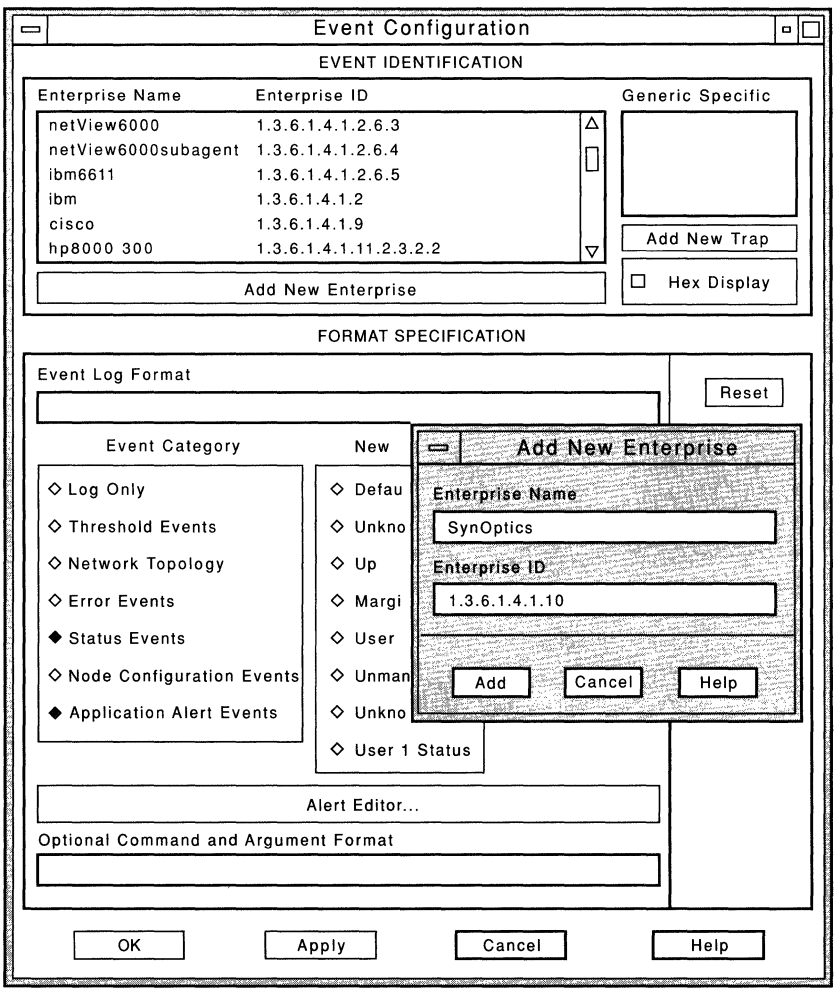


Figure 8. Add New Enterprise Dialog Box

Adding a New Trap

To add a new trap:

Step 1. Click on the Add New Trap button of the Event Configuration dialog box. A dialog box similar to that shown in Figure 9 will appear.

Step 2. Select the appropriate trap type and enter the specific trap number. This example shows an EnterpriseSpecific trap number of zero (0).

Step 3. Click on the Add button to complete the change.

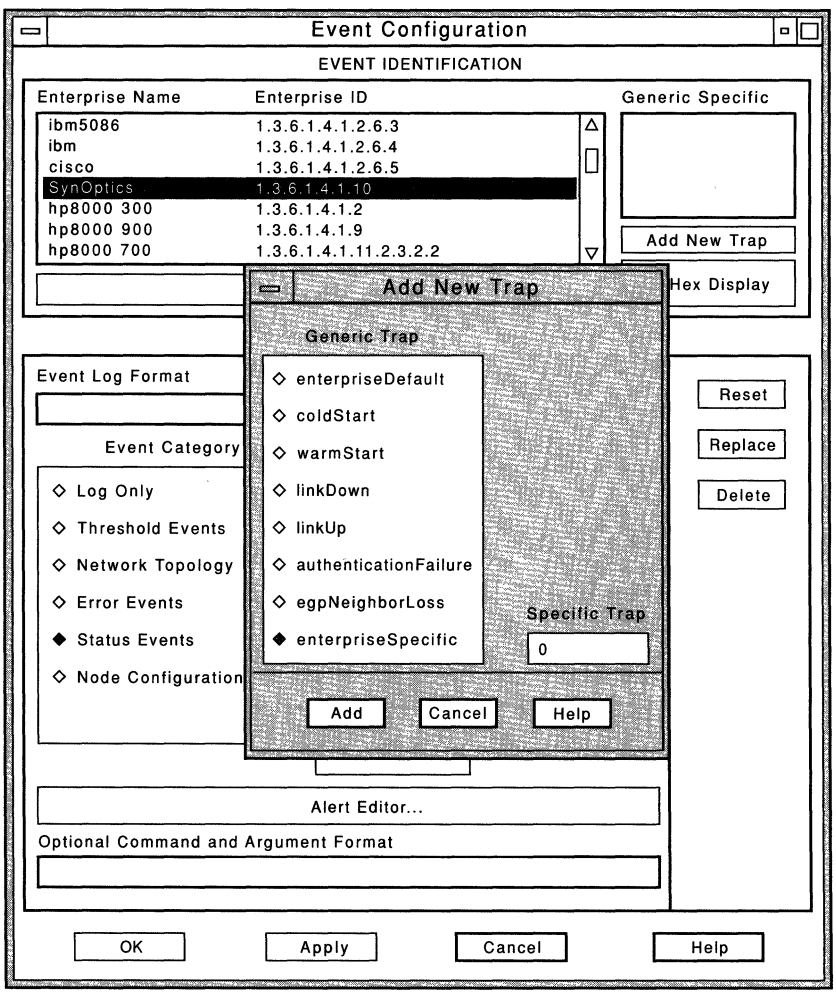


Figure 9. Add New Trap Dialog Box

Changing the Generic Alert Subvector

To change the Generic Alert subvectors (X'92'):

Step 1. Select the desired alert from the Generic Alert subfield in the Event Configuration dialog box. The alert will be highlighted and the Alert Editor... button becomes available.

Step 2. Click on the Alert Editor... button. The Alert Editor dialog box will appear.

Figure 10 illustrates the Alert Editor dialog box.

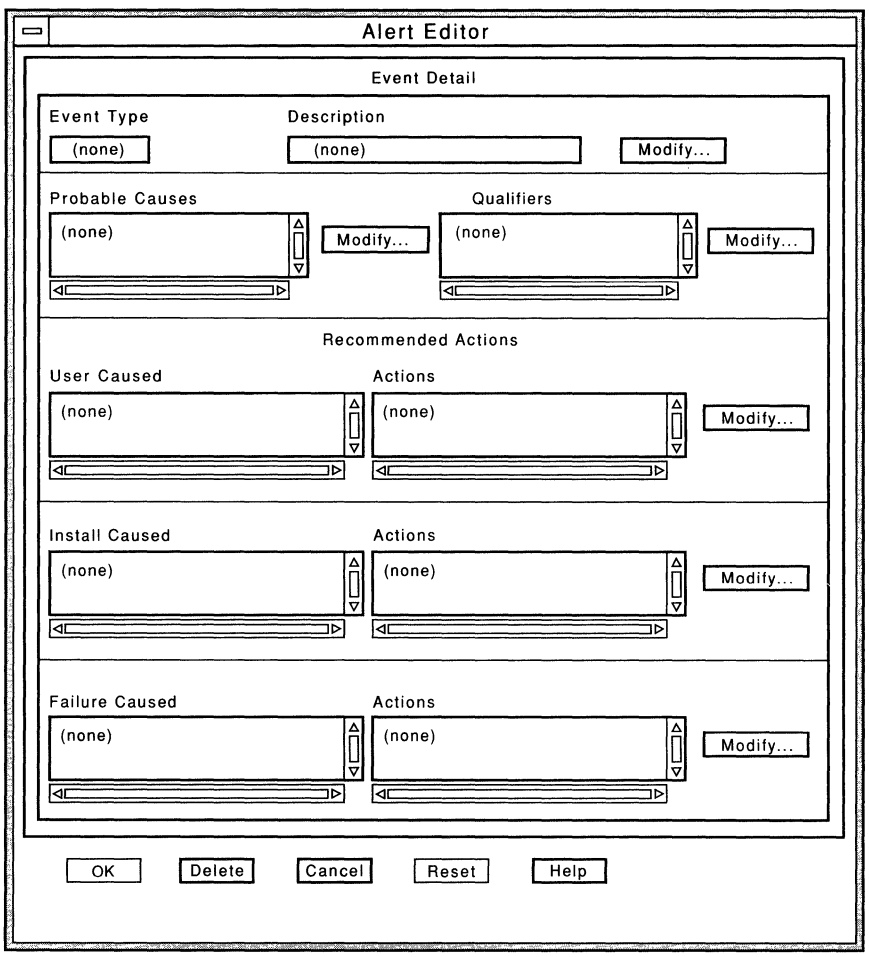


Figure 10. Alert Editor Dialog Box

The Alert Editor dialog box is divided into two portions; the top portion shows the information that is displayed on the NetView Event Detail screen, and the bottom portion shows the information that is displayed on the NetView Recommended Actions panel.

The Event Detail portion of the dialog box shows the Event Type and the description of the event and contains the following subvectors:

Generic Alert Data Subvector ('X'92'')

Probable Causes Alert Subvector ('X'93'')

Detailed Data Alert Subvector ('X'98'')

The Recommended Actions portion of the dialog box contains fields for the following subvectors:

User Caused ('X'94'')	User Actions ('X'81'')
Install Caused ('X'95'')	Install Actions ('X'81'')
Failure Causes ('X'96'')	Failure Actions ('X'81'')

All fields can be modified by clicking on the appropriate Modify button.

Step 3. On the Event Detail portion of the dialog box, click on the Modify... button that is next to the Description field. The Generic Alert dialog box shown in Figure 11 will appear.

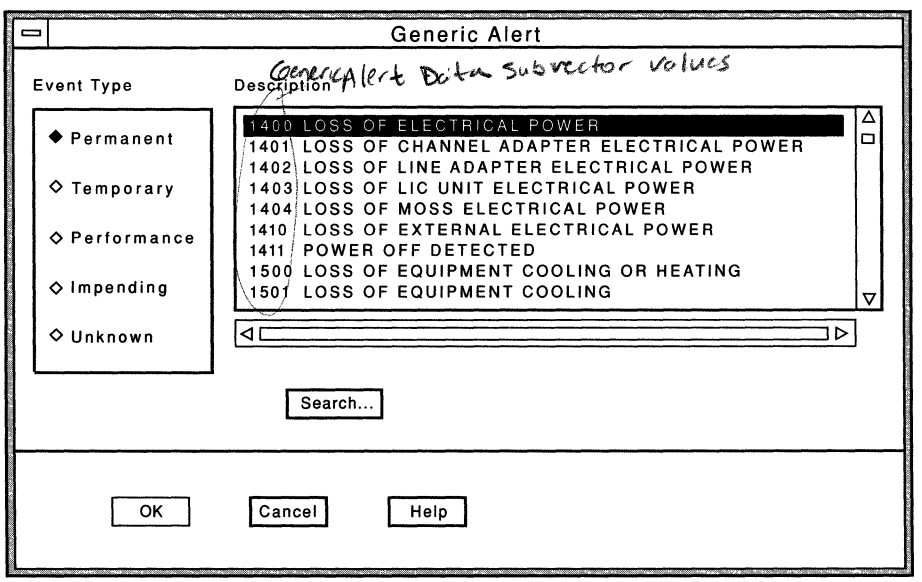


Figure 11. Generic Alert Dialog Box

Step 4. Select the description that contains the desired code point and text string. Use the Search function to find the desired code point and text string. This example shows a code point of `1400` with an accompanying text string of `LOSS OF ELECTRICAL POWER`.

Step 5. Select the type of event. This example shows a type of Permanent.

Step 6. Click on the OK button to complete the change.

Changing the Probable Cause Subvector

To change the probable cause subvector (X'93'):

Step 1. Click on the Modify... button next to the Probable Causes field of the Alert Editor dialog box. The dialog box shown in Figure 12 will appear.

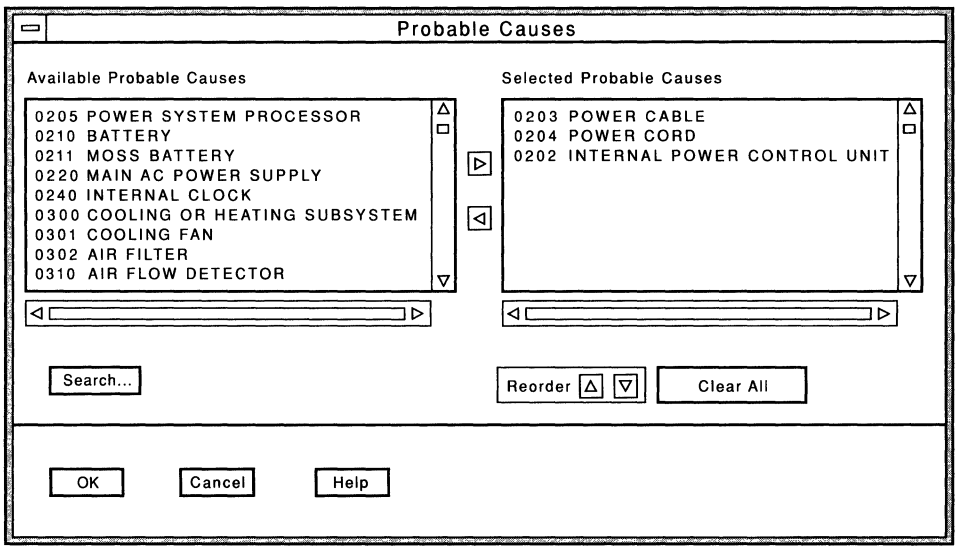


Figure 12. Probable Causes Dialog Box

The left portion of the dialog box shows the available code points and messages, and the right portion shows the code points and messages that have been selected for the sub-vector.

Step 2. Select an available code point and use the right arrow button to move it to the chosen field. You can use the Search function to find a code point.

Step 3. Use the right and left arrow keys to add or remove selections from the selected field. Up to 15 selections can be added to the list.

Step 4. Use the Reorder buttons to arrange the selections by putting the most likely cause at the top of the list and the least likely cause at the bottom of the list.

Step 5. Click on the OK button to complete the change.

Sending Qualifiers (Detailed Data)

To send detailed data (textual information that appears on NetView panels) with the alert:

Step 1. Click on the Modify... button next to the Qualifiers field of the Alert Editor dialog box. A dialog box similar to that shown in Figure 13 will appear.

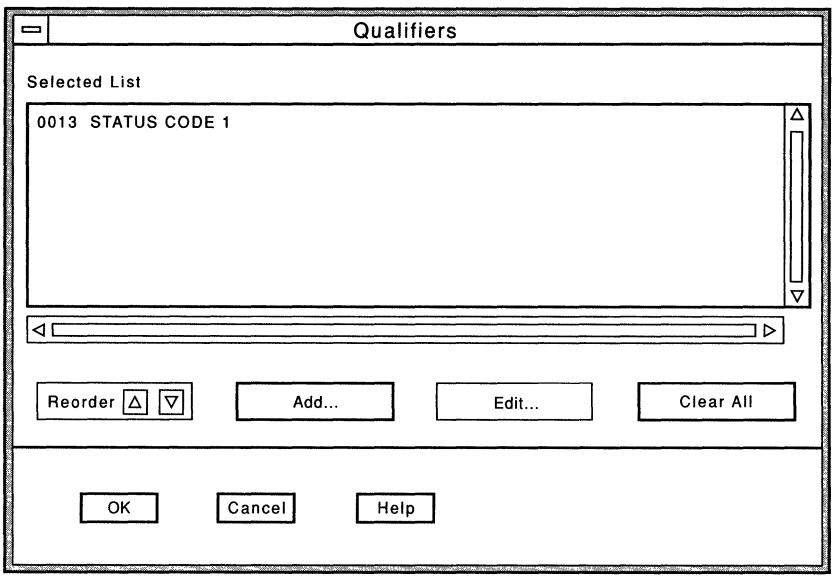


Figure 13. Qualifiers Dialog Box

Step 2. Use the buttons to reorder the list, add detailed data to the list, edit specific entries in the list, or to clear the list. If you click on the Add...button, a dialog box similar to that shown in Figure 14 on page 19 will appear.

Step 3. Use the Search function to find the desired code point or text string. Enter the appropriate qualifiers in the Data field. This example shows a qualifier for a status code.

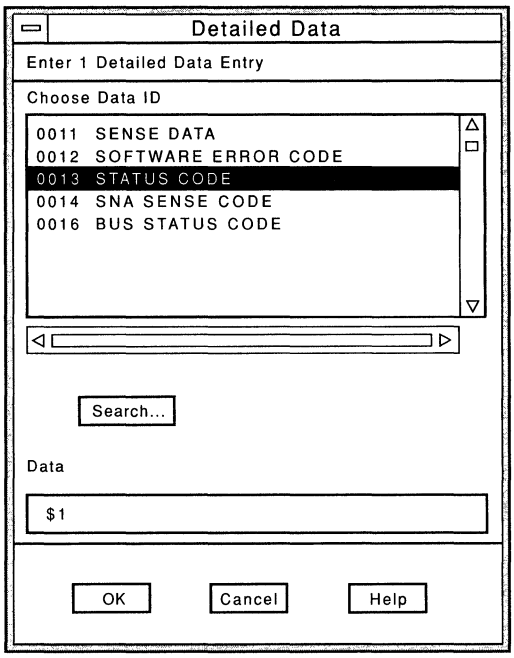


Figure 14. Detailed Data Dialog Box

Step 4. Click on the OK button to complete the change.

Changing the Causes/Actions Subvectors

To change the User Caused, Install Caused, or the Failure Caused subvectors:

Step 1. Click on one of the Modify buttons in the Recommended Actions section of the Alert Editor dialog box. You will see a dialog box similar to that shown in Figure 15 on page 20.

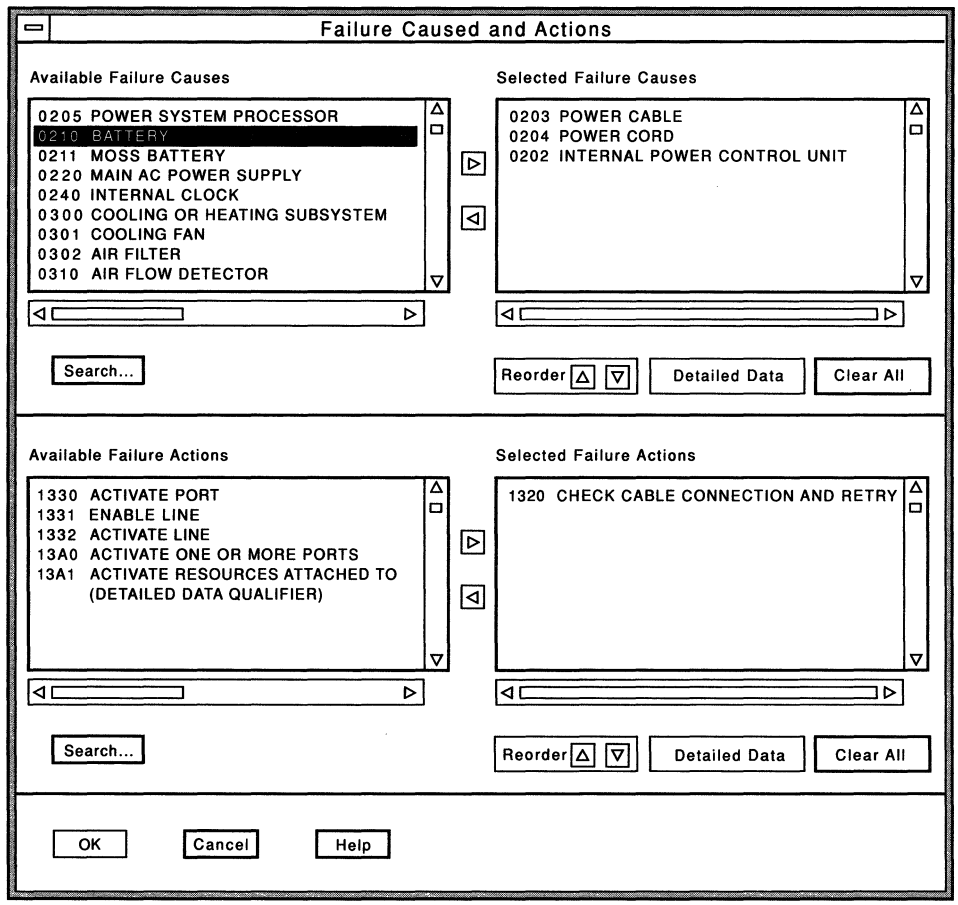


Figure 15. Failure Caused and Actions Dialog Box

The top left portion of the dialog box shows the list of available failure causes code points and messages. The top right portion of the dialog box shows the list of failure causes code points and messages that have been selected for the particular subvector.

The bottom left portion of the dialog box shows the list of available failure actions code points and messages. The bottom right portion of the dialog box shows the list of failure actions code points and messages that have been selected for the particular subvector.

Step 2. Add or remove entries from the selected list by using the right and left arrow buttons, respectively. Clicking on the right button adds the entry to the selected list and clicking on the left button removes the entry from the selected list.

Step 3. Place the most probable entries at the top of the list and the least likely entries at the bottom of the list. Use the up and down buttons to reorder the entries.

Step 4. If the subvector requires additional detailed data, one set of code points and messages is displayed in the Detailed Data dialog box for each unit of detailed data. The detailed data associated with the code points can be edited by clicking on the Detailed Data button.

Step 5. Click on the OK button to complete the change.

Putting It All Together

This section describes what is displayed on the NetView Alerts-Dynamic, Recommend Actions, and Event Detail panels when the SynOptics trap is issued.

Figure 16 contains an example of the Alerts-Dynamic panel. It shows the generic alert and primary cause that were defined in the Generic Alert and Probable Cause dialog boxes, respectively.

```
N E T V I E W          SESSION DOMAIN: NTV7A    OPER3     12/04/92 10:09:27
NPDA-30A                      * ALERTS-DYNAMIC *

    DOMAIN RESNAME  TYPE TIME  ALERT DESCRIPTION:PROBABLE CAUSE

    NTV7A NV6000    DEV  10:09 LOSS OF ELECTRICAL POWER:POWER CABLE
    NTV7A NV6000    DEV  10:09 OPERATOR NOTIFICATION:UNDETERMINED
    NTV7A NV6000    DEV  10:09 OPERATOR NOTIFICATION:UNDETERMINED
    NTV7A NV6000    DEV  09:50 LINK ERROR:LINE/REMOTE NODE
    NTV7A NV6000    DEV  09:36 LINK ERROR:LINE/REMOTE NODE
    NTV7A NV6000    DEV  09:36 OPERATOR NOTIFICATION:UNDETERMINED
    NTV7A NV6000    DEV  09:36 OPERATOR NOTIFICATION:UNDETERMINED
    NTV7A NV6000    DEV  09:35 NO COMM WITH REMOTE NODE:LINE/REMOTE NODE
    NTV7A NV6000    DEV  09:35 OPERATOR NOTIFICATION:UNDETERMINED
    NTV7A NV6000    DEV  09:35 OPERATOR NOTIFICATION:UNDETERMINED
    NTV7A NV6000    DEV  09:35 LINK ERROR:LINE/REMOTE NODE
    NTV7A NV6000    DEV  09:34 CONFIG/CUSTOMIZATION ERR:SOFTWARE PROGRAM
    NTV7A ADRIAN    DEV  09:34 OPERATOR NOTIFICATION:UNDETERMINED
    NTV7A GFHANDEL  DEV  09:34 OPERATOR NOTIFICATION:UNDETERMINED
    NTV7A REBECCA   DEV  09:34 OPERATOR NOTIFICATION:UNDETERMINED

  DEPRESS ENTER KEY TO VIEW ALERTS-STATIC
```

Figure 16. Alerts-Dynamic Screen

Figure 17 on page 23 contains an example of the Recommended Actions panel. It shows what was defined in the Failure Causes and Actions dialog box.

```
N E T V I E W          SESSION DOMAIN: NTV7A    OPER3     12/04/92 10:12:08
NPDA-45A           * RECOMMENDED ACTION FOR SELECTED EVENT *     PAGE  1 OF  1
 NTV7A       NTFFPU04     A1234567     NV6000     NV6000
            +--------+   +--------+   +--------+   +--------+
 DOMAIN     | SP     |---| TP     |---| DEV    |---| DEV    |
            +--------+   +--------+   +--------+   +--------+

USER    CAUSED - NONE

INSTALL CAUSED - NONE

FAILURE CAUSED - POWER CABLE
                 POWER CORD
                 INTERNAL POWER CONTROL UNIT
       ACTIONS - I174 - CHECK CABLE CONNECTION AND RETRY




ENTER ST (MOST RECENT STATISTICS), DM (DETAIL MENU), OR D (EVENT DETAIL)
```

Figure 17. Recommended Actions Screen

Figure 18 and Figure 19 on page 24 contain examples of the Event Detail panel. They show the event type, the description, the chosen probable causes, and the qualifiers.

```
N E T V I E W          SESSION DOMAIN: NTV7A    OPER3     12/04/92 10:13:02
NPDA-43S                        * EVENT DETAIL *                PAGE  1 OF  2

 NTV7A       NTFFPU04     A1234567     NV6000     NV6000
            +--------+   +--------+   +--------+   +--------+
 DOMAIN     | SP     |---| TP     |---| DEV    |---| DEV    |
            +--------+   +--------+   +--------+   +--------+

DATE/TIME: RECORDED - 12/04 10:09    CREATED - 12/04/92 09:58:15

OTHER RESOURCES ASSOCIATED WITH THIS EVENT:
   DEV  NV6000.RALEIGH.IBM.COM

EVENT TYPE: PERMANENT

DESCRIPTION: LOSS OF ELECTRICAL POWER

PROBABLE CAUSES:
   POWER CABLE

ENTER  A  (ACTION) OR  DM  (DETAIL MENU)
```

Figure 18. Event Detail Screen

```
N E T V I E W          SESSION DOMAIN: NTV7A    OPER3     12/04/92 10:13:38
NPDA-43S                      * EVENT DETAIL *                  PAGE  2 OF  2

 NTV7A       NTFFPU04     A1234567     NV6000     NV6000
            +--------+   +--------+   +--------+   +--------+
 DOMAIN     |  SP    |---|  TP    |---|  DEV   |---|  DEV   |
            +--------+   +--------+   +--------+   +--------+

PROBABLE CAUSES (CONTINUED):
   POWER CORD
   INTERNAL POWER CONTROL UNIT

QUALIFIERS:
   1)  STATUS CODE 1



UNIQUE ALERT IDENTIFIER: PRODUCT ID - 5696-3620  ALERT ID - A9DBF0C3

ENTER  A  (ACTION) OR  DM  (DETAIL MENU)
```

Figure 19. Event Detail Screen (continued)

Default Process for Configuring Alerts

This section describes how the AIX NetView/6000 program configures an alert if the Alert Editor has not been used to define the alert. When a trap is detected, and passes the event filtering criteria, the tralertd daemon converts the trap to an SNA alert. If the MIB bindings for the alert cannot be transmitted in a single subvector, the original trap is saved in the tralertd.log. This log contains the trap and a unique log ID, which is sent in the alert. The host program then uses the log ID to issue a RUNCMD command containing the **gettrap** command, requesting the complete trap information for the incomplete alert.

The information sent to the host for a trap differs, based on whether the trap is IBM enterprise-specific, non-IBM enterprise-specific, or generic.

IBM Enterprise-Specific Traps

Certain IBM enterprise-specific traps are alertable errors logged by the error logging facilities provided by the AIX Version 3 Release 2 Operating System for the RISC System/6000.

These errors are processed by the trap-notify process and converted to SNMP traps by the trapgend daemon. They are based on MIB extensions carrying valid SNA code points and are logged in templates that include variable-bindings, which contain all relevant values for the trap. During conversion by the tralertd daemon, these bindings are decoded, and the resulting code points are put in the appropriate subvector.

The error template includes the following variable-bindings:

- Err_type
- Class
- Report
- Log
- Alert
- Err_Desc
- Prob_Causes (from 0 to 4 code points)
- User_Causes (from 0 to 4 code points)
- User_Actions (from 0 to 4 code points)
- Fail_Causes (from 0 to 4 code points)
- Fail_Actions (from 0 to 4 code points)
- Inst_Causes (from 0 to 4 code points)
- Inst_Actions (from 0 to 4 code points)
- Detail_Data (length, code point, encoding)

When the Alert field in the error template is set to **True**, an enterprise-specific trap is built.

Generic and Non-IBM Enterprise-Specific Traps

Table 1 shows the SNMP trap information that is included in an SNA Alert Management Services major vector as a result of a trap. The location of each piece of data within the alert is also shown. The AIX NetView/6000 trap-to-alert conversion provides, in the SNA alert, all SNMP information in the originating trap.

See Appendix B, "Subvectors Included in SNA MS Major Vectors" on page 49 for additional information on the alert components listed.

Table 1 (Page 1 of 2). Location of SNMP Data in NMVTs Generated from Traps

Data	Alert Component
Contents of the *sysObjectID* MIB variable of trap sender	Detailed Data (X'98') subvector, Detailed Data (X'82') Network Alert Common subfield
Contents of the *agent-addr* MIB variable of the agent generating the trap	Cause Undetermined (X'97') subvector, Recommended Actions (X'81') Network Alert Common subfield
Contents of the *ifIndex* MIB variable[1]	Detailed Data (X'98') subvector, Detailed Data (X'82') Network Alert Common subfield
Contents of the *egpNeighbor* MIB variable[2]	Detailed Data (X'98') subvector, Detailed Data (X'82') Network Alert Common subfield
Contents of the *generic-trap* trap field	Detailed Data (X'98') subvector, Detailed Data (X'82') Network Alert Common subfield
Contents of the *specific-trap* trap field	Detailed Data (X'98') subvector, Detailed Data (X'82') Network Alert Common subfield (if enterprise specific)

Table 1 (Page 2 of 2). Location of SNMP Data in NMVTs Generated from Traps

Data	Alert Component
MIB variable names and values[3]	Detailed Data (X'98') subvector, Detailed Data (X'82') Network Alert Common subfield
Log ID (trap/major vector identifier)[3]	Detailed Data (X'98') subvector, Detailed Data (X'82') Network Alert Common subfield

Note:

1. For link-up and link-down traps.
2. For EGP neighbor loss traps.
3. For enterprise-specific traps. If names or values are 44 bytes or less, they are included in the alert. If names or values are more than 44 bytes, or there are more variables than the alert can hold, the information is logged in the tralertd database. A log ID is assigned to the trap record.

MIB II Agents

Additional information is included for agents supporting MIB-II. This information includes:

- The name of a contact for the trap sender in the *sysContact* MIB variable
- The physical location of the device in the *sysLocation* MIB variable

This information is sent in a Recommended Actions (X'81') Network Alert Common subfield of the Cause Undetermined (X'97') subvector. If available, the first 44-bytes of each MIB variable is sent.

Limit the data for the contact, device name, and location to codes, numbers, or internationally recognized terms. Following these guidelines provides consistent MIB data throughout a managed network and satisfies the requirements for textual data.

Provide specific information. For example, instead of specifying `Contact System Administrator`, provide a name and telephone number. Instead of specifying `2nd floor wiring closet`, provide a specific location including room, building, and city.

Internal Events

The AIX NetView/6000 program's internally generated events are treated as non-IBM enterprise-specific traps. These events include the following information:

- Description of the event in the sysDescr MIB variable
- Host name

A node name with the value *<none>* refers to the manager station that is running the AIX NetView/6000 program.

Support for the IBM 6611 Router

The AIX NetView/6000 program incorporates support for IBM 6611 router. Information about the router is contained in the Extended Detailed Data subfield (X'85'). NetView V2R3 includes support for this subfield as part of the base product. NetView V2R2 MVS/XA and MVS/ESA users need to apply the following APARs to obtain the support:

- MVS/ESA (APAR OY51850)
  - UY80062
  - UY83063
  - UY83064
  - UY83065
  - UY83066
- MVS/XA (APAR OY51858)
  - UY83061
  - UY83065
  - UY83068
  - UY83069
  - UY83072

Working with the NetView Service Point Program

The AIX NetView Service Point program enables the host program and the AIX NetView/6000 program to exchange SNA MS major vectors over SNA services. The AIX NetView/6000 program supplies the spappld daemon as a service point application and starts it as a part of the AIX NetView/6000 program initialization process. The resulting connection enables a host operator to send SNA MS Execute (X'8061') Major Vectors, containing RUNCMD commands, enabling the AIX NetView/6000 program to execute the contents of the RUNCMD in the SNMP environment.

Naming the Service Point Application

You have the option of choosing a name for the service point application or using the name automatically generated by SMIT. SMIT's naming algorithm is based on the address of the node, thereby assigning each application a unique name.

Each service point application's name must be unique within the scope of the AIX NetView Service Point program with which the application is registered to ensure that the RUNCMD commands are properly routed. If you provide the service point application name, use a scheme that prevents duplication of service point application names and conforms to the host program naming requirements. Use SMIT to verify that the service point names for the tralertd and spappld daemons match.

Note: If you are using the NETCENTER program, the name you select must be exactly eight characters long.

Preventing Case Conversion

The AIX operating system is sensitive to the case of the command string. The NetView and NETCENTER programs automatically convert all commands to upper-case characters. Unless specifically directed otherwise, the spappld daemon automatically converts all commands to lower-case characters. To prevent case conversion, indicate that the host program and the service point application are not to perform case conversion.

In the NetView program, you can prevent case conversion by:

- Issuing RUNCMD commands in command lists, which use the keywords **ADDRESS NETVASIS**, on machines supporting the REXX language.
- Writing command lists in the NetView command list language supported on the NetView program issuing the RUNCMD command.

To prevent the service point application from performing case conversion, use the keyword **asis** as the first four characters of the *command string* in the command list.

Note: Neither the NetView nor the NETCENTER programs support all AIX operating system Version 3 Release 2 characters. Some AIX special characters will not appear correctly, such as the square brackets used in MIB variables on the AIX Operating System.

Service Point Application Logs

Two logs are used by each service point application. One log, with the default name of **/usr/OV/log/NV390.log**, records application interactions with the host and is used to diagnose configuration and connectivity problems between the AIX NetView/6000 program and the host program.

The other log, located in /usr/OV/databases/tralertd, stores SNMP traps whose contents cannot be transmitted in a single alert. Each record contains the original trap information and an associated log ID sent in the alert. With this log ID, you can access the original trap information by using the **gettrap** command. You should not change the name of this database.

Working with the NETCENTER Program

This section describes the items that are needed to establish and maintain communication between the AIX NetView/6000 and NETCENTER programs. The following files are a key part of the communication between the NETCENTER and the AIX NetView/6000 programs:

- The batch network definition file
- The nc.seed file
- The nc.objects file

The batch network definition file (nc.objects.bdf) is a sequential file that the NETCENTER program uses to define the non-SNA IP-addressable devices it will manage in its connection with the AIX NetView/6000 program. The AIX NetView/6000 program creates the file and stores it as /usr/OV/conf/nc.objects.bdf. After the AIX NetView/6000 program generates the file from the nc.objects file, you need to transfer the file to the host so it can be used in the NETCENTER configuration. The nc.objects file is based on the contents of nc.seed file.

Note: If you use doswrite for the transfer process, do not use the –a option. This will prevent formatting problems in the files that you transfer.

Creating the nc.seed File

The AIX NetView/6000 program uses the device types and hostnames listed in /usr/OV/conf/nc.seed as a basis for defining which devices and hosts will communicate with the NETCENTER program. You can edit this file to list the device types and hostnames that will be used in the connection with the NETCENTER program. This file must be present for the connection to work. The following example shows the seed file that is sent with the AIX NetView/6000 program. The symbol (#) indicates that the line is a comment.

```
#
# COMPONENT_NAME: spappld
#
# Licensed Program Product:  AIX NetView/6000 V2R1
#
# (C) COPYRIGHT International Business Machines Corp. 1992, 1993
# All Rights R
# Licensed Material - Property of IBM
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
#
# Information provided in this file will be used to extract objects from
# the NetView/6000 database of network objects and to generate the NETCENTER
# batch definition file.
#
# After the line containing "TYPES:", enter any of the following types of
# NetView/6000 managed devices that can be managed by the NETCENTER program.
# Allowable types are:
#                 node
#                 device
#                 computer
#                 connector
#                 bridge
#                 router
#                 hub
#                 repeater
#                 PC
#                 workstation
#                 mini
#                 mainframe
#                 printer
#                 server.
#
# Each entry must be placed on a separate line.
TYPES:
  router
  node


# After the line containing "HOSTNAMES:", enter the fully qualified hostname
# of the individual NetView/6000 managed hosts that will be managed by the
# NETCENTER program.

HOSTNAMES:
  aixnm004.raleigh.ibm.com
  aixnmt05.raleigh.ibm.com
```

Figure 20. The nc.seed file specifies the objects and the hosts used in the connection with the NETCENTER program.

In the previous example, the seed file causes the spappld daemon to survey the topology database and to extract all information about routers, servers, printers, and hosts aixnm004 and aixnmt05.

Creating the nc.objects File

If the batch network definition file does not exist when the spappld daemon is started, but an nc.objects file does exist, the spappld daemon uses the objects listed there rather than the ones listed in the current database in its creation of the file. If no nc.objects file exists, the spappld daemon uses the current contents of the topology database to generate a new nc.objects file. The daemon then uses that file in its generation of the batch network definition file. The following example shows the nc.objects file that the spappld daemon generated from the nc.seed file in the previous example:

```
#
# COMPONENT_NAME:  spappld
#
# Licensed Program Product:  AIX NetView/6000 V2R1
#
# (C) COPYRIGHT International Business Machine Corp. 1992, 1993
# All Rights Reserved
# Licensed Material - Property of IBM
#
# US Government Users Restricted Rights - Use, duplication or
# or disclosure restricted by GSA ADP Schedule Contract with IBM
#
#
# HostName                                IPAddress(es)  NETCENTER    Field(s)
#                                                        name

aixnm004.raleigh.ibm.com                  9.67.160.211   0943A0D3
ralname4.raleigh.ibm.com                    9.67.160.3   0943A003  isNode
nm3ps2.raleigh.ibm.com                     9.67.160.36   0943A024  isNode
daveys.raleigh.ibm.com                     9.67.160.31   0943A01F  isNode
aixnmt02.raleigh.ibm.com                  9.67.160.224   0943A0E0  isNode
aixnm012.raleigh.ibm.com                  9.67.160.221   0943A0DD  isNode
rocketeer.raleigh.ibm.com                 9.67.160.216   0943A0D8  isNode
aixnmt07.raleigh.ibm.com                  9.67.160.228   0943A0E4  isNode
aixnm015.raleigh.ibm.com                  9.67.160.246   0943A0F6  isNode
aixkanji.raleigh.ibm.com                  9.67.161.250   0943A1FA  isNode
aixnmt06.raleigh.ibm.com                  9.67.160.227   0943A0E3  isNode
client.raleigh.ibm.com                    9.67.161.113   0943A171  isNode
aixnmmib.raleigh.ibm.com                    192.2.1.81   C0020151  isRouter, isNode
                                            192.1.0.66
                                           9.67.161.78
```

Figure 21. The nc.objects file is used to generate the batch network definition file.

The nc.objects file contains the host name, IP addresses, the NETCENTER name, and the description of the devices that are shown at the NETCENTER program. You can use this information in determining how the devices will be represented.

Creating the Batch Network Definition File

The next example contains the batch network definition file that the spappld daemon generated from the previous nc.objects file. The NETCENTER name of the devices being shown at the NETCENTER program is represented in eight hexadecimal digits (4 bytes).

```
NV6000  SNMP    SNMP                                5A
NV6000  SNMP    0943A0D3                            08 9.67.160.211    SNMP
NV6000  SNMP    0943A003                            08 9.67.160.3      SNMP
NV6000  SNMP    0943A024                            08 9.67.160.36     SNMP
NV6000  SNMP    0943A01F                            08 9.67.160.31     SNMP
NV6000  SNMP    0943A0E0                            08 9.67.160.224    SNMP
NV6000  SNMP    0943A0DD                            08 9.67.160.221    SNMP
NV6000  SNMP    0943A0D8                            08 9.67.160.216    SNMP
NV6000  SNMP    0943A0E4                            08 9.67.160.228    SNMP
NV6000  SNMP    0943A0F6                            08 9.67.160.246    SNMP
NV6000  SNMP    0943A1FA                            08 9.67.161.250    SNMP
NV6000  SNMP    0943A0E3                            08 9.67.160.227    SNMP
NV6000  SNMP    0943A171                            08 9.67.161.113    SNMP
NV6000  SNMP    C0020151                            08 192.2.1.81      SNMP
```

Figure 22. The spappld daemon generates the batch network definition file from the nc.objects file.

For more information on coding and the contents of a batch network definition file see *NETCENTER Service Point Installation and Reference*.

Updating the Batch Network Definition File

Because the batch network definition file is a static file and the AIX NetView/6000 topology database is updated dynamically, the objects listed in the batch network definition file may not be the same as those known to the AIX NetView/6000 program.

To update the batch network definition file:

Step 1. Stop the spappld daemon.

Step 2. Delete the current batch network definition file.

Step 3. Update the nc.seed file.

Step 4. Delete the current nc.objects file.

Step 5. Restart the spappld daemon

Step 6. Transfer the updated batch network definition file to the host.

NETCENTER Options on spappld and tralertd

The –C flag on the spappld and tralertd daemons specifies that the alerts will be formatted for a connection to the NETCENTER program.

The –a flag specifies the value for the standalone alert timeout interval. The default value is 90 seconds. The standalone timeout interval is for alerts that do not have a corresponding opposite (such as ON/OFF).

The standalone timeout interval specifies the time period that the objects affected by the standalone alert are to remain in the critical (red) state. After the time interval has elapsed, the AIX NetView/6000 program turns the objects back to the normal (green) state by returning a problem resolved alert to the NETCENTER program. The change is also reflected on the NetView Alerts Dynamic screen.

Note: The domain name on spappld must be SNMP.

Chapter 3. Working with the Host Program

This chapter describes key items to consider when you use the AIX NetView/6000 program with the NetView program and, optionally, the NETCENTER program. It provides information about:

- "Responding to RUNCMD Commands"
- "Creating User-Defined Generic Code Points" on page 37
- "Restricting the Host Operator to a Subset of AIX Commands" on page 38
- "Diagnosing Host Connection Problems" on page 39

Responding to RUNCMD Commands

The AIX NetView Service Point program routes a RUNCMD command from the host program to a specific AIX NetView/6000 program. The service point application that resides on that AIX NetView/6000 program then executes the contents of the RUNCMD. The connection that results enables a NetView or NETCENTER operator to issue commands to be executed in a TCP/IP environment.

A RUNCMD command is the content of the Self-Defining Text (X'31') subvector of the Execute (X'8061') SNA MS major vector. It can be sent from the host to AIX NetView/6000 in the following ways:

- Automatically through automation table-invoked programs
- Automatically as part of the NETCENTER NSI1 protocol exchange
- Manually by an operator

With NetView Version 2 Release 2 and later, the NetView program can respond to trap-prompted SNA Alert MS major vectors through automation facilities by taking the following actions:

- Generating a message that characterizes the condition at the trap sender for a NetView operator.
- Sending a RUNCMD command to the spappld daemon to issue a command or request the complete trap information for an alert in which partial information was sent.

This information is sent to the specified AIX NetView Service Point program. The AIX NetView Service Point program extracts the RUNCMD command from the NMVT, passes the command string to the specified application, and waits for a response.

An example of the RUNCMD syntax is as follows:

```
RUNCMD SP=NVSP, APPL=A1234567, ECHO SYSTEM SHUTDOWN IN FIVE MINUTES
```

Where the variables indicate the following:

SP	Specifies the SNA name of the AIX NetView Service Point program that is to convert the command and forward it to the manager system. In this example, `NVSP` is the SNA name.
APPL	Specifies the name of the service point application registered with the AIX NetView Service Point program that is to receive and execute the command. In this example, `A1234567` is the service point application name.
command string	Specifies the command to be executed. In this example, `ECHO SYSTEM SHUTDOWN IN FIVE MINUTES` is the command string.

Refer to *AIX NetView Service Point Installation, Operation, and Programming Guide* for information about setting up and configuring the AIX NetView Service Point program.

Upon receiving a command string from the AIX NetView Service Point program, the spappld daemon executes the command and returns the results to the AIX NetView Service Point program. In turn, the AIX NetView Service Point program returns the results to the host in one or more Reply to Execute (X'0061') Major Vectors containing a RUNCMD response. If the executed program did not return a message, the RUNCMD response carries a message informing the host operator the command has completed its task.

If a message is not returned, check the /usr/OV/log/NV390.log file for a record of the interactions. If further steps are needed, use the AIX Version 3 Release 2 Operating System, the AIX NetView Service Point diagnostic facilities, and the spappld daemon tracing facilities.

Note: The AIX NetView/6000 program recognizes the RUNCMDs that are issued from the NETCENTER program as being in an NSI1 "tokenized" format. This format prohibits the use of any AIX command that begins with two capital letters followed by an equal sign. The NETCENTER program issues RUNCMDs under two conditions: as a part of its initialization protocol and when an operator issues a "point and shoot" command.

Creating User-Defined Generic Code Points

To obtain problem determination support for the NetView program, enter the code points in the seven user tables that are shipped with the NetView program. The user tables code point range, X'E000' through X'EFFF', is reserved for your use. The following section describes the process of defining and link-editing user tables in NetView Version 2 Release 3.

Defining User Tables

For MVS..... Submit the NetView sample CNMSJM08, which allocates the portioned data set, CNM.CODE.POINTS, defined by USERLIB in the CNMSJM07 sample. The CNMSJM08 sample contains the members or tables.

For VM..... Run the NetView sample CNMSVM08 to create the CMS files or tables. The *filetype* is NCCFLST. CNMSVM08 accepts the *filemode* as an input parameter.

For VSE..... Run the NetView sample CNMSHM05, which creates the B books that are defined in CNMSHM04. NetView sample CNMSHM05 contains the tables.

Table Formats

Each table contains a different type of code point. The user tables are:

Table	Description
BNJ81UT	Recommended action code points
BNJ82UTB	Detail data code points
BNJ92UTB	Alert description code points
BNJ93UTB	Probable cause code points
BNJ94UTB	User cause code points
BNJ95UTB	Install cause code points
BNJ96UTB	Failure cause code points

The fourth and fifth characters of the table name identify the subvector or subfield that contains the code points.

Link-Editing the User Tables

For MVS ...

NetView sample CNMSJM07 checks the user tables for validity and link-edits them into a user-defined load data set. Concatenate this data set in the STEPLIB of the NetView start procedure and place it before the SYS1.NPDALIB statement.

For VM ...

NetView sample CNMSVM07 checks the user tables for validity and link-edits them into a user-defined LOADLIB. This LOADLIB precedes the NPDA LOADLIB in the GLOBAL LOADLIB statement in the NETSTRT GCS file.

For VSE ...

NetView sample CNMSHM04 parses the user tables for validity and link-edits them into a user-defined configuration library. Put this library in the search chain of the NetView startup procedure before the NetView phase library.

Refer to *NetView Samples* for a copy of the desired job. The comments within the sample explain the operands and how the table is used. If no errors are found, the user table is link-edited into the appropriate data set. If errors are found, the job ends and a list of the errors is written to SYSPRINT.

Note: Use the AIX **errinstall** command to add any additional code points. The new code points are recognized by the AIX NetView/6000 program the next time you invoke the Alert Editor.

Restricting the Host Operator to a Subset of AIX Commands

System administrators can use the AIX restricted shell (Rsh) to define a subset of AIX commands that can be entered by a NetView or NETCENTER operator. To do this, set the operator's profile to point to the /usr/rbin directory. This directory should contain the AIX commands the operator is permitted to use.

For example, assume a system administrator created a directory for a workstation that is used by novice NetView operators, and the /usr/rbin directory contained only the **ps** command. (The **ps** command enables the operator to list the processes running on the system.) If David, a novice NetView operator, issued a **kill** command to terminate any or all of the processes he found with the **ps** command, he would receive a message the **kill** command could not be found. If he tried to issue any command other than the **ps** command, he would receive a similar message.

Diagnosing Host Connection Problems

If alerts from the AIX NetView/6000 program are not reaching the host program, or if RUNCMDs or their responses are not moving between the tralertd and spappld daemons:

Step 1. Verify the daemons are running. Both daemons are dependent on the following daemons: ovemsd, ovelmd, pmd, ovwdb, and trapd.

If any of the daemons are not running, restart them through SMIT or by executing **/usr/OV/bin/ovstart**.

Step 2. Verify that the dlctoken is available by executing the AIX command **lsdev -C -l dlctoken**.

Step 3. Check the entries in /etc/services to see that the port numbers are correct.

Step 4. If multiple RISC System/6000 systems are using a single AIX NetView Service Point program, verify that each RISC System/6000 processor has the AIX NetView Service Point Application Interface Library installed on it.

Step 5. If the daemons are running, check the connection to the AIX NetView Service Point program.

To check the connectivity, use the AIX **rpcinfo** command. Use this command to verify the AIX NetView Service Point program is available, and to determine the asynchronous serial communications port used by your session. If multiple users are listed as using the same port number, change the port number to a unique number.

Refer to the AIX **rpcinfo** online man page for more information about using this command.

Step 6. Ensure the AIX NetView Service Point customization shell script was executed. If you are not sure, stop the AIX NetView Service Point program, execute **/usr/lpp/nvix/scripts/nvix_customize_sp**, and restart the AIX NetView Service Point program.

Step 7. Ensure the port mapper is running before you start the AIX NetView Service Point program. To restart the port mapper:

Step a. Stop the AIX NetView Service Point program from SMIT. (/usr/lpp/nvix/scripts/nvix_control stop)

Step b. Issue the **stopsrc -s portmap** command to stop the portmap process.

Step c. Issue the **startsrc -s portmap** command to start the portmap process.

Step d. Start the AIX NetView Service Point program from SMIT. (/usr/lpp/nvix/scripts/nvix_control start)

Step 8. Verify that if multiple service point applications are using the same AIX NetView Service Point program each application has a name that is unique within the scope of that AIX NetView Service Point program. To do this execute **/usr/lpp/nvix/script/nvix_control status**

Step 9. Check the service point application log to determine what activity the spappld daemon has recorded. The default log file is **/usr/OV/log/NV390.log**

Step 10. Ensure that adequate paging space is available. If needed, increase paging space by using the following sequence of SMIT options from the Administer menu:

Step a. Select Physical & Logical Storage from the System Management menu.

Step b. Select Paging Space from the Physical & Logical Storage menu.

Refer to the associated SMIT help entries for more information about using these options.

Refer to the *AIX NetView Service Point Installation, Operation, and Programming Guide* for more information about assigning ports.

Chapter 4. Using the Host Connection

This chapter provides examples of using the NetView program with the AIX NetView/6000 program. The following section describes suggestions on how to optimize communication between the AIX NetView/6000 and the NetView programs.

Optimizing Communication

The NetView automation facilities can be utilized to optimize communication between the NetView and AIX NetView/6000 programs. The examples reflect the algorithmic approach adopted by the AIX NetView/6000 program for converting traps to alerts.

This section shows examples of NetView automation table segments and command lists initiated by NetView automation facilities. These examples include the following functions:

- Selecting and highlighting alerts from an SNMP device
- Selecting SNA Alerts for a key event
- Selecting SNA Alerts for incomplete trap information
- Sending a RUNCMD command with mixed-case characters

Note: The NetView automation facilities are available in all NetView environments that are Version 1 Release 3 or later.

Selecting and Highlighting Alerts from an SNMP Device

The following example shows a NetView automation table segment designed to select and highlight SNA alerts from a critical SNMP device according to the original SNMP trap type. The critical SNMP device sent SNMP traps to the AIX NetView/6000 program where they were converted to SNA alerts and forwarded to the NetView program.

```
IF ((MSUSEG(0000.97.81(1)) = . HEX('00B0') . ) &
    (MSUSEG(0000.97.82(1) 4) = HEX('FE') . ) &
    (MSUSEG(0000.97.82(1) 6) = HEX('F94BF6F74BF54BF1F2F0'). )) THEN
  BEGIN ;
   IF MSUSEG(0000.98.82(2) 4) = HEX('FA') . THEN BEGIN ;
    IF ((MSUSEG(0000.98.82(2)) = . 'COLD START' .) |
        (MSUSEG(0000.98.82(2)) = . 'WARM START' .) |
        (MSUSEG(0000.98.82(2)) = . 'LINK UP' .)) THEN
       COLOR(GRE) ;
    IF ((MSUSEG(0000.98.82(2)) = . 'LINK DOWN' .)) THEN
       COLOR(RED) ;
    IF ((MSUSEG(0000.98.82(2)) = . 'EGP NEIGHBOR LOSS' .)) THEN
       COLOR(YEL) ;
   END ;
END ;
```

The IP address of the trap origin in all AIX NetView/6000-converted SNA alerts is found in a Recommended Actions (X'81') Network Alert Common subfield of the Cause Undetermined (X'97') subvector. Most of the important information from the SNMP MIB variable bindings portion of the trap are found in the Detailed Data (X'98') subvector of the alert. The following list describes the previous example.

- The first Recommended Actions (X'81') Network Alert Common subfield in the Cause Undetermined (X'97') subvector contains the code point `X'00B0'`.
- A Recommended Actions (X'81') Network Alert Common subfield with this code point in it is accompanied by a Detailed Data (X'82') Network Alert Common subfield with the code point `X'FE'`, which indicates that an IP address is the data in the subfield.
- The IP address of the highlighted node is `9.67.5.120`.
- The type of SNMP trap that prompted the alert is found in the second Detailed Data (X'82') Network Alert Common subfield of the Detailed Data (X'98') subvector.

Selecting SNA Alerts for a Key Event

The following example shows a NetView automation table segment designed to extract information from an SNA alert enabling the NetView program to automatically issue a RUNCMD response to a given alert.

In this example, the automation table segment detects SNA alerts prompted by the receipt of a link-down trap from IP address `9.67.5.120`. This example initiates the execution of the command list, `FNDROUTE`, to determine if, after the loss of an interface on this device (router), there remains a route between `ROUTER2` and `ROUTER3`.

```
IF ((MSUSEG(0000.97.81(1)) = . HEX('00B0') . ) &
    (MSUSEG(0000.97.82(1) 4) = HEX('FE') . ) &
    (MSUSEG(0000.97.82(1) 6) = HEX('F94BF6F74BF54BF1F2F0') . )) THEN
   BEGIN ;
     IF ((MSUSEG(0000.98.82(2) 4) = HEX('FA') . )  &
         (MSUSEG(0000.98.82(2)) = . 'LINK DOWN' . )) THEN
       EXEC(CMD('FNDROUTE ')) ;
   END;
```

The selection of alerts in the previous example is based on the following:

- Action is to be taken only if the alert was prompted by a link-down trap. The second Detailed Data (X'82') Network Alert Common subfield of the Detailed Data (X'98') subvector of the SNA alert contains the trap type.
- If the automation table segment determines that the link-down trap originated from the device at IP address `9.67.5.120`, it initiates the command list. The command list determines whether two devices that previously used the trap sender as a gateway can still communicate.

  The IP address of the trap sender is always sent in the first Recommended Actions (X'81') Network Alert Common subfield in the Cause Undetermined (X'97') subvector with code point X'00B0'.

In the next example, the NetView command list, `FNDROUTE`, issues an AIX NetView/6000 **findroute** command to determine whether there is a route between two internet devices, `router1` and `router2`, that support SNMP.

The command list automatically retrieves the SNA name of the AIX NetView Service Point program and the service point application name from the SNA alert to create a RUNCMD command. These names are needed to correctly address the RUNCMD command.

```
   SERVPT= HIER(1)
   SERVPT = SUBSTR(SERVPT, 1, 8)
   SPAPPL = HIER(2)
   SPAPPL = SUBSTR(SPAPPL, 1, 8)
   CMD = 'findroute router1 router2 '
   'RUNCMD SP='SERVPT',APPL='SPAPPL','CMD
  EXIT
```

Selecting SNA Alerts for Incomplete Trap Information

This example shows a NetView automation table segment designed to select SNA alerts for incomplete SNMP trap information. The automation table segment extracts a log ID from the SNA alert, enabling the NetView program to automatically issue a response to a given alert.

In this example, the automation table segment illustrates selecting SNA alerts that were prompted by an SNMP trap sent by the host program at 9.67.5.120. The automation table segment checks for SNA alerts that do not contain the entire contents of the SNMP trap.

Incomplete SNMP trap information is indicated by the presence of a log ID as the first Detailed Data (X'82') Network Alert Common subfield in the Detailed Data (X'98') subvector. The ID is the key for the trap record in the tralertd database. Its presence indicates that the AIX NetView/6000 program has logged the trap in the tralertd database and that all the information in the trap could not be forwarded to the NetView program.

The automation table segment extracts the log ID and passes it to a command list, GETTRAP, that retrieves the complete trap record.

```
IF ((MSUSEG(0000.97.81(1)) = . HEX('00B0') . ) &
    (MSUSEG(0000.97.82(1) 4) = HEX('FE') . ) &
    (MSUSEG(0000.97.82(1) 6) = HEX('F94BF6F74BF54BF1F2F0'). ) &
    (MSUSEG(0000.98.82(1) 4) = HEX('DA') HEX('00') HEX(ID))) THEN
   EXEC(CMD('GETTRAP ' ID)) ;
```

In the following example, the NetView command list, GETTRAP, automatically issues a command to retrieve the trap information for an SNMP trap that was logged in the manager system's /usr/OV/databases/tralertd database. Trap information is stored in this database for SNMP traps that are converted to SNA alerts, but cannot completely fit in the SNA alert sent to the NetView program.

In this example, the command list automatically issues a **gettrap** command on the manager system that is managing the SNMP device 9.67.5.120; this device generated an SNMP trap. The SNMP trap was converted to an SNA alert, but all the information could not fit in the SNA alert. The trap information was logged in the tralertd database, and the record was assigned a log ID. The incomplete SNA alert containing the log ID was sent to the NetView program. This command list issues the AIX NetView/6000 **gettrap** command to retrieve this trap information, using the unique log ID to identify the trap record.

```
Parse Arg ID
  SERVPT = HIER(1)
  SERVPT = SUBSTR(SERVPT, 1, 8)
  SPAPPL = HIER(2)
  SPAPPL = SUBSTR(SPAPPL, 1, 8)
 'RUNCMD SP='SERVPT', APPL='SPAPPL', GETTRAP ' ID
```

Sending RUNCMDs with Mixed-Case Characters

This example shows a NetView command list that automatically issues a command containing mixed-case characters. The command list contains keywords that enables a mixed-case command to be issued.

In the following example, the command list automatically issues a AIX NetView/6000 **snmpget** command to obtain the sysDescr MIB variable binding from the host, `aixnm004`.

Note that the keywords `asis` and `ADDRESS NETVASIS` are used to prevent case conversion from being performed by the NetView program and the service point application.

The keyword `asis` precedes the **snmpget** command so that the service point application on the AIX NetView/6000 program will not perform case conversion on the received command. The service point application automatically converts commands to lower-case alphabetical characters.

The keywords `ADDRESS NETVASIS` precedes the RUNCMD string so that the NetView program will not perform case conversion on the RUNCMD command string. The NetView program automatically converts commands to upper-case alphabetic characters.

```
SERVPT= HIER(1)
SERVPT = SUBSTR(SERVPT, 1, 8)
SPAPPL = HIER(2)
SPAPPL = SUBSTR(SPAPPL, 1, 8)
CMD = "asissnmpget aixnm004 public system.sysDescr.0"
ADDRESS NETVASIS "RUNCMD SP="SERVPT","APPL="SPAPPL","CMD
EXIT
```

Appendix A. Reference Information

This appendix provides reference information about the following topics:

- "Options for the tralertd and spappld Daemons"
- "Events Automatically Converted to Alerts" on page 48

Options for the tralertd and spappld Daemons

The following table lists the daemons involved in the NetView connection, their options, and their defaults:

Table 2. AIX NetView/6000 Daemon Options

Daemon	Option	Default
tralertd	Tracing mask	0
	Full path name of trace file	/usr/OV/log/tralertd.trace
	Service point application name	A943A2BE
	Are you using NETCENTER	no
	If yes, DOMAIN name	SNMP
	If yes, standalone timeout	90 seconds
spappld	Service point application name	A943A2BE
	Execute shell state	bsh (Bourne)
	Execute shell path	/bin:/usr/bin:/usr/OV/bin
	Log service point transactions?	yes
	Full path name of log file	/usr/OV/log/NV390.log
	Tracing mask	0
	Full path name of trace file	/usr/OV/log/NV390.trace
	Are you using NETCENTER	no

Note: The name you choose for the service point application is used for the value of `appl` in the RUNCMD. SMIT automatically generates a unique name based on the address of the IP interfaces of the manager system. The following is an example of a RUNCMD command that a NetView operator can issue; the `sp=` variable indicates the service point application name.

```
RUNCMD SP=NTFFPU04,APPL=REGION1, gettrap 0123456789ABCDEF > /tmp/test
```

Events Automatically Converted to Alerts

The AIX NetView/6000 program supports generic traps 0-to-5 for all enterprises and the following specific traps for the AIX NetView/6000 enterprise. (The traps have a enterprise ID of `1.3.6.1.4.2.6.3` and a specific trap number of 6.) By default, the following enterprise-specific events are automatically converted to alerts.

Table 3. Events Automatically Converted to Alerts

Event Number	Event Name	Event Description
58720256	CPU_EV	CPU Load
58720257	DSPU_EV	Disk Space Percentage Used
58720258	IPD_EV	Interface Percent Deferred
58720259	IPC_EV	Interface Percent Collisions
58720260	ICE_EV	Interface CRC Errors
58720261	IPIE_EV	Interface Percent Input Errors
58720262	IPOE_EV	Interface Percent Output Errors
58720263	DCOL_EV	Data Collector Detected Threshold
58720264	DCRA_EV	Data Collector Rearm Event
58851330	FERR_EV	Fatal Errors
58916864	NUP_EV	Node Up
58916865	NDWN_EV	Node Down
58916866	IUP_EV	Interface Up
58916867	IDWN_EV	Interface Down
58916868	SC_EV	Segment Critical
58916869	NC_EV	Network Critical

The AIX NetView/6000 program, by default, also converts and forwards the following enterprise-specific traps:

- netView6000subagent
- ibm_aix
- ibm6611

Appendix B. Subvectors Included in SNA MS Major Vectors

The following sections identify the subvectors included in an SNA Alert Management Services (MS) major vector prompted by a trap from the AIX NetView/6000 program or a managed device running SNMP protocol. The subvectors included in an Alert MS major vector and the data carried are:

Table 4. SNA Alert MS Major Vector Subvectors

Subvector	Description
Hierarchy/Resource List (X'05')	Provides hierarchy of the resources involved in the trap conversion and the host name (if available) or IP address (first 8-characters) of the node originating the trap.
Product Set ID (X'10')	Identifies products that implement a network component as hardware or software.
Product Identifier (X'11')	Identifies a product, hardware or software, as IBM or non-IBM, and includes detailed product information.
Supporting Data Correlation (X'48')	Provides a log ID for an alertable error from the system error log if the alert was converted to an SNMP trap by the trapgend daemon.
Generic Alert Data (X'92')	Provides alert type and description text.
Probable Causes (X'93')	Provides a possible cause for the trap.
User Caused (X'94')	Provides a possible user cause for the alert condition, and recommended actions to be taken. This is forwarded from the AIX error log.
Install Causes (X'95')	Provides a possible installation cause for the alert condition, and recommended actions to be taken. This is forwarded from the AIX error log.
Failure Causes (X'96')	Provides a possible failure cause for the alert condition, and recommended actions to be taken. This is forwarded from the AIX error log.
Cause Undetermined (X'97')	Provides recommended actions for further inquiries.
Detailed Data (X'98')	Provides additional information from the trap, and a unique log ID for the trap that allows further information inquiries (if the trap was logged).

Hierarchy/Resource List (X'05') Subvector

The Hierarchy/Resource List (X'05') subvector indicates the hierarchy of the AIX NetView Service Point, service point application, SNMP manager, and SNMP agent participating in the trap conversion.

This subvector carries the following subfields:

- Hierarchy Name List (X'10') subfield
- Associated Resources (X'11') subfield

Hierarchy Name List (X'10') Subfield

The Hierarchy Name List (X'10') subfield will contain the instances shown in Table 5. This information appears on the NetView Event Detail (NPDA-43S) and Recommended Actions (NPDA-45A) screens, showing the hierarchy of the domain.

Table 5 (Page 1 of 2). Hierarchy Name List (X'10') Subfield

Resource Identifier	Display Resource Name Indicator	Name of Resource
X'81' SERVICE POINT	0	SNA name of the AIX NetView Service Point sending the NMVT. This is the SNA name entered through SMIT. If you are using the NETCENTER program, the name must be exactly eight characters long.
X'18' TRANSACTION PROGRAM	0	The registered name of the service point application.
X'00' UNSPECIFIED DEVICE	0	Either SNMPMNGR or the name of the SNMP manager doing the trap to NMVT conversion, if it is 8-bytes or less in length. This name must reside in the /etc/hosts file on the AIX NetView Service Point so that RUNCMDs can be routed to the intended device.

Table 5 (Page 2 of 2). Hierarchy Name List (X'10') Subfield

Resource Identifier	Display Resource Name Indicator	Name of Resource
X'00' UNSPECIFIED DEVICE	1	The name (if available), or IP address of the device sending the trap, if the name meets the same specifications given for the name of the SNMP manager. The first 8-characters of the name or IP address (in dot notation) are included.

Note: When the trap is internally generated by AIX NetView/6000, the first device in the hierarchy indicates the name of the SNMP manager or SNMPMNGR, and the second device indicates the host name or IP address of the node about which the event is concerned.

Associated Resources (X'11') Subfield

The Associated Resources (X'11') subfield provides the host name or IP address of the node originating the alertable error that was logged in the AIX error log.

This information appears on the NetView Event Detail (NPDA-43S) screen, in the Other Resources Associated With This Event field.

Product Set ID (X'10') Subvector and Product Identifier (X'11') Subvector

The Product Set ID (X'10') subvector identifies the product generating the event as either hardware (a RISC System/6000) or software (AIX). Defaults values are provided when data is not available. The Product Identifier (X'11') subvector provides details about the product, including whether the product is an IBM or non-IBM product.

Four Product Identifier (X'11') subvectors are sent for each event. Two provide product identification information for the machine (hardware and software) running AIX NetView/6000 and sending the event to the host program. Two provide product identification information for the machine (hardware and software) generating the event.

For events not processed by the trapgend daemon, the generating machine product information includes the first 30-characters of the sysDescr MIB variable (if available) for the hardware. The software is indicated as unknown.

For an event generated by a failing RISC System/6000 that was logged as an alertable error in the AIX error log and processed by the trapgend daemon, the product information is retrieved from the RISC System/6000

Vital Product Data database. In this instance, the RISC System/6000 product information is always included in the subvectors. For product set information about a failing component within the RISC System/6000, use the AIX **errpt** command, with the log ID supplied in the Supporting Data Correlation (X'48') subvector, to retrieve this information.

For hardware products, the subfields carried include the following:

Table 6. Subfields Carried for Hardware Products

Subfield	Data and Comments
Hardware Product Identifier (X'00') Product ID	The machine type, machine model number, plant of manufacturer, and the sequence number.
Hardware Product Common Name (X'0E') Product ID	The name commonly used to identify the hardware product.
Vendor Identification (X'0F') Product ID	Identifies the name of the product vendor, such as IBM.

For software products, the subfields carried include the following:

Table 7. Subfields Carried for Software Products

Subfield	Data and Comments
Software Product Common Level (X'04') Product ID	The common version, release, and modification level numbers as given in the software product announcement documentation.
Software Product Common Name (X'06') Product ID	The name commonly used to identify the software product.
Software Product Program Number (X'08') Product ID	The program product number as assigned by distribution personnel, or a substitute value supplied by a user-written software program.
Vendor Identification (X'0F') Product ID	Identifies the name of the product vendor, such as IBM.

Supporting Data Correlation (X'48') Subvector

This subvector forwards a log ID for an alertable error from the system error log if the alert was converted to an SNMP trap by the trapgend daemon.

Use the AIX **errpt** command and this log ID to retrieve additional data related to the event reported. The log ID is transported in the Detailed Data (X'82') Network Alert Common subfield.

Generic Alert Data (X'92') Subvector

This subvector identifies the event type and provides an event description.

For an event that was generated by a failing RISC System/6000, logged as an alertable error in the AIX error log, and processed by the trapgend daemon, this subvector provides an error type and error description as contained in the AIX error log.

For events not processed by the trapgend daemon, this subvector provides an alert type and code points that correspond to strings of text from the trap.

The Alert Type field is set according to the received trap. The settings for the various generic traps are shown in Table 8. This information appears on the NetView Event Detail (NPDA-43S) screen in the Event Type field.

Table 8. Alert Type Field in the Generic Alert Data (X'92') Subvector

SNMP Trap	Type	Meaning
Cold start	X'12'	Unknown
Warm start	X'12'	Unknown
Link up	X'12'	Unknown
Link down	X'01'	Permanent loss of availability
Authentication failure	X'11'	Impending problem
EGP neighbor loss	X'01'	Permanent loss of availability
Enterprise-specific	X'12'	Unknown (Default)

The code points used in the Generic Alert Data (X'92') subvector are shown in Table 9. This information appears in the Description field of the NetView Alerts-Dynamic (NPDA-30A), Alerts-Static (NPDA-30B), and Event Detail (NPDA-43S) screens.

Table 9 (Page 1 of 2). Generic Alert Data (X'92') Subvector Code Points

SNMP Trap	Code Point	Text
Cold start	X'A000'	PROBLEM RESOLVED
Warm start	X'A000'	PROBLEM RESOLVED
Link up	X'A000'	PROBLEM RESOLVED
Link down	X'3300'	LINK ERROR
Authentication failure	X'C00A'	AUTHORIZATION FAILURE

Table 9 (Page 2 of 2). Generic Alert Data (X'92') Subvector Code Points

SNMP Trap	Code Point	Text
EGP neighbor loss	X'3305'	UNABLE TO COMMUNICATE WITH REMOTE NODE
Enterprise-specific (*)	X'B00C'	SNMP RESOURCE PROBLEM

Note: * For enterprise-specific traps not designed for NMVT conversion.

Probable Causes (X'93') Subvector

The Probable Causes (X'93') subvector contain a general indication of the cause of the trap. The probable causes appear in order of descending probability.

For an event that was generated by a failing RISC System/6000, logged as an alertable error in the AIX error log, and processed by the trapgend daemon, the subvector provides probable causes as contained in the AIX error log.

For events not processed by the trapgend daemon, the code points used are shown in Table 10.

This information appears in the Probable Causes field of the NetView Alerts-Dynamic (NPDA-30A), Alerts-Static (NPDA-30B), and Event Detail (NPDA-43S) screens.

Table 10. Probable Causes (X'93') Subvector Code Points

SNMP Trap	Code Point	Text
Cold start	X'FE00'	UNDETERMINED
Warm start	X'FE00'	UNDETERMINED
Link up	X'2132'	LINE/REMOTE NODE
Link down	X'2132'	LINE/REMOTE NODE
Authentication failure	X'6700'	SECURITY PROBLEM
EGP neighbor loss	X'2200'	REMOTE NODE
Enterprise-specific	X'FE00'	UNDETERMINED

User Caused (X'94') Subvector

The User Caused (X'94') subvector transports code points for stored text detailing the probable user causes and the recommended actions to be taken. This subvector includes the following subfields:

- User Causes (X'01') subfield
- Recommended Actions (X'81') Network Alert Common subfield
- Detailed Data (X'82') Network Alert Common subfield

This subvector is included for alertable errors logged in the AIX error log and processed by the trapgend daemon. AIX NetView/6000 forwards this information as it is defined in the AIX error log.

These subfields are shown in Table 11.

Table 11. User Caused (X'94') Subvector Subfields

Subfield	Data and Comment
User Caused (X'01')	A user cause is defined as a condition that an operator can resolve without contacting a service organization. It includes one or more code points indicating the probable user causes of the alert condition.
Recommended Actions (X'81')	Actions to be taken to resolve the alert condition.
Detailed Data (X'82')	Additional information regarding the causes or recommended actions.

Install Caused (X'95') Subvector

The Install Caused (X'95') subvector transports code points for stored text detailing the probable installation causes and the recommended actions to be taken.

This subvector includes the following subfields:

- Install Causes (X'01') subfield
- Recommended Actions (X'81') Network Alert Common subfield
- Detailed Data (X'82') Network Alert Common subfield

This subvector is included for alertable errors logged in the AIX error log and processed by the trapgend daemon. AIX NetView/6000 forwards this information as it is defined in the AIX error log.

These subfields are shown in Table 12 on page 56.

Table 12. Install Causes (X'95') Subvector Subfields

Subfield	Data and Comment
Install Causes (X'01')	An installation cause is defined as a condition that results from the initial installation or setup of some equipment. Includes one or more code points denoting the probable installation causes of the alert condition.
Recommended Actions (X'81')	Recommended actions to be taken to resolve the alert condition.
Detailed Data (X'82')	Additional information regarding the causes or recommended actions.

Failure Causes (X'96') Subvector

The Failure Causes (X'96') subvector transports code points for stored text detailing the probable installation causes and the recommended actions to be taken. This subvector includes the following subfields:

- Failure Causes (X'01') subfield
- Recommended Actions (X'81') Network Alert Common subfield
- Detailed Data (X'82') Network Alert Common subfield

This subvector is included for alertable errors logged in the AIX error log and processed by the trapgend daemon. AIX NetView/6000 forwards this information as it is defined in the AIX error log.

These subfields are shown in Table 13.

Table 13. Failure Causes (X'96') Subvector Subfields

Subfield	Data and Comment
Failure Causes (X'01')	A failure cause is defined as a condition that results from the failure of a resource. Includes one or more code points listing the probable failure causes of the alert condition.
Recommended Actions (X'81')	Recommended actions to be taken to resolve the alert condition.
Detailed Data (X'82')	Additional information regarding the causes or recommended actions.

Cause Undetermined (X'97') Subvector

The Cause Undetermined (X'97') subvector provides recommended action information for alerts that indicate existing, impending, or resolved conditions. This information is in the Recommended Actions subfields.

If the agent generating the trap supports MIB-II, additional information about a person responsible for that agent's host device, the location of the agent device, and the name of the agent device will be provided.

When defining this information, it is recommended that you limit the data for the contact, system name, and location subfields to codes, numbers, or internationally recognized terms that do not require translation. While SNMP does not restrict the data you send in this subvector, SNA does impose these restrictions. Following these restrictions facilitates interactions with the host program and provides consistency in MIB variables.

The data from the Recommended Actions subfields appears in the Actions field of the NetView Recommended Action For Selected Event (NPDA-43S) screen.

Recommended Actions for Link-Down, Authentication Failure, and EGP Neighbor Loss Traps

The Recommended Actions subfields shown in Table 14 are for SNA Alert major vectors that indicate an existing or impending problem.

Table 14. Alert Major Vectors: Recommended Actions Subfield Code Points

Code Point	Text
X'00B0'	PERFORM PROBLEM DETERMINATION PROCEDURES FOR (detailed data qualifier). The detailed data for this code point is in Detailed Data (X'82') Network Alert Common subfield type data ID X'FE'.[1]
X'31D0'	IF REQUIRED, QUERY (detailed data qualifier) AT (detailed data qualifier) ABOUT (detailed data qualifier). The detailed data for this code point is in Detailed Data (X'82') Network Alert Common subfield type data ID X'F9', X'4B', and X'33'.[1, 2]

Note:

1. See Table 16 on page 58 for detailed data.
2. Only included when the agent sending the trap supports MIB-II.

Recommended Actions for Cold Start, Warm Start, and Link-Up Traps

The Recommended Actions subfields shown in Table 15 are for SNA Alert major vectors that indicate a resolved condition.

Table 15. Resolution Major Vectors: Recommended Actions Subfield Code Points

Code Point	Text
X'0700'	NO ACTION NECESSARY
X'3302'	IF PROBLEM CONTINUES TO OCCUR REPEATEDLY THEN DO THE FOLLOWING
X'00B0'	PERFORM PROBLEM DETERMINATION PROCEDURES FOR (detailed data qualifier). The detailed data for this code point is in Detailed Data (X'82') Network Alert Common subfield type data ID X'FE'.[1]
X'31D0'	IF REQUIRED, QUERY (detailed data qualifier) AT (detailed data qualifier) ABOUT (detailed data qualifier). The detailed data for this code point is in Detailed Data (X'82') Network Alert Common subfield type data ID X'F9', X'4B', and X'33'.[1, 2]

Note:

1. See Table 16 for detailed data.
2. Included only when the agent sending the trap supports MIB-II.

Detailed Data (X'82') Network Alert Common Subfield for Recommended Actions Subfields

The Detailed Data (X'82') Network Alert Common subfield shown in Table 16 may be provided in a Cause Undetermined (X'97') subvector.

Table 16 (Page 1 of 2). Detailed Data (X'82') Network Alert Common Subfield

Data ID	Data Type	Data and Comment
X'F9'	CONTACT ID	The *sysContact* binding. The system contact information from the MIB of the agent sending the trap.
X'FE'	INTERNET PROTOCOL ADDRESS	The IP address of an adjacent node for the EGP Neighbor Loss trap. This data is from the *agent addr* field in the original trap. This data may also appear in the Detailed Data (X'82') Network Alert Common subfield of the Detailed Data (X'98') subvector.
X'33'	COMPONENT ID	The *sysName* binding. The component ID from the MIB of the agent sending the trap.

Table 16 (Page 2 of 2). Detailed Data (X'82') Network Alert Common Subfield

Data ID	Data Type	Data and Comment
X'4B'	LOCATION NAME	The *sysLocation* binding. The location name from the MIB of the agent sending the trap.

Detailed Data (X'98') Subvector

The Detailed Data (X'98') subvector consists of a series of Detailed Data (X'82') Network Alert Common subfields, containing additional information from the trap. This subvector carries either the variable binding or the variable name of all variables whose values are sent in a trap.

The unique log ID (in X'DA') associates a SNA Alert MS major vector with a specific trap when the entire contents of the alert could not be transported to the host program. The host program can use this log ID, along with the **gettrap** command, to identify and retrieve the complete trap information for a specific trap. This trap-to-major vector identifier is stored in the tralertd database. The log ID is used as the key to the required variable bindings.

The contents of the Detailed Data (X'98') subvector, when the Detailed Data (X'82') Network Alert Common subfield are sent, as shown in Table 17. This information appears in the Qualifiers list of the NetView Event Detail (NPDA-43S) screen.

Table 17 (Page 1 of 2). Contents of the Detailed Data (X'98') Subvector

Data ID	Data Type	Data and Comment
X'DA'	LOG ID	The number identifying trap-to-alert conversion. Provides a key to the tralertd database. At times, an entire trap cannot be included in an alert. This log ID lets the host program get the MIB variable bindings that were sent in a trap but were not included in the alert.
X'F2'	INTERFACE	The *ifIndex* binding. Sent minimally for link-up and link-down traps.
X'F8'	ENTERPRISE	The *sysObjectID* binding.
X'FA'	SNMP GENERIC TRAP NUMBER	The *generic trap* binding. Either COLD START, WARM START, LINK UP, LINK DOWN, AUTHENTICATION FAILURE, EGP NEIGHBOR LOSS, or ENTERPRISE SPECIFIC for 0, 1, 2, 3, 4, 5, or 6 traps, respectively, is sent.

Table 17 (Page 2 of 2). Contents of the Detailed Data (X'98') Subvector

Data ID	Data Type	Data and Comment
X'FB'	SNMP SPECIFIC-TRAP NUMBER	The *specific trap* binding. The enterprise-specific trap number. When the trap is not enterprise-specific, this instance of the sub-field may be omitted. If it is present under these circumstances, its value is zero (0).
X'FC'	SNMP MIB VARIABLE NAME	The MIB variable name. This variable name may be from either the standard MIB (I or II) or from an enterprise-specific extension to the MIB. This data may be available, if it was in the original trap.
X'FD'	SNMP MIB VARIABLE VALUE	The SNMP MIB variable value. This detailed data is sent when the value of the MIB variable will fit in the allocated space and when the name of the variable is sent in the immediately preceding the Detailed Data subfield. This data may be available if it was in the original trap.
X'FE'	INTERNET PROTOCOL ADDRESS	The IP address of an adjacent node for the EGP Neighbor Loss trap. This data is from the *agent addr* field in the original trap. The address of the trap sender will always be in the Recommended Actions subfields of the Cause Undetermined (X'97') subvector.

Glossary, Bibliography, and Index

Glossary

This glossary defines important AIX NetView/6000 and AIX NetView Service Point terms. It includes definitions from the *Dictionary of Computing*, SC20-1699, which are identified by an asterisk (*). Definitions from draft proposals and working papers under development by the International Standards Organization, Technical Committee 97, Subcommittee 1 are identified by the symbol (TC97). Definitions from the *IBM RISC System/6000 Task Index and Glossary* are identified by the symbol (R). Definitions from the *CCITT Sixth Plenary Assembly Orange Book, Terms and Definitions* and working documents published by the Consultative Committee on International Telegraph and Telephone of the International Telecommunication Union, Geneva, 1980 are identified by the symbol (CCITT/ITU). Definitions from published sections of the *ISO Vocabulary of Data Processing*, developed by the International Standards Organization, Technical Committee 97 Subcommittee 1 and from published sections of the *ISO Vocabulary of Office Machines*, developed by subcommittees of ISO Technical Committee 95, and identified by the symbol (ISO).

This glossary may also include terms and definitions from the following sources:

- The *American National 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 42 Street, New York, New York 10036. Definitions are identified by the symbol (A).
- 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).
- 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). Definitions from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T), indicating that final agreement has not yet been reached among the participating National Bodies of SC1.

For abbreviations, the definition usually consists only of the words represented by the letters; for complete definitions, see the entries for the words.

Reference Words Used in the Entries

The following cross-references are used in this glossary:

Contrast with: Refers to a term that has an opposed or substantively different meaning.

Deprecated term for: Indicates that the term should not be used. It refers to a preferred term, which is defined.

Synonymous with: Appears in the commentary of a preferred term and identifies less desirable or less specific terms that have the same meaning.

Synonym for: Appears in the commentary of a less desirable or less specific term that has the same meaning.

See: Refers to multiple-word terms that have the same last word.

See also: Refers to related terms that have similar (but not synonymous) meanings.

A

action. (1) 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. * (2) An operation on a managed object, the semantics

of which are defined as part of the managed object class definition.

address. See *internet address*.

agent. In the TCP/IP environment, a process running on a network node that responds to requests and sends information.

AIX. Advanced Interactive Executive.

AIX Operating System. (1) IBM's implementation of the UNIX Operating System. The AIX Operating System runs on the RISC System/6000 system. (2) See *UNIX Operating System.*

AIX NetView/6000. An abbreviated name for AIX SystemView NetView/6000.

AIX SystemView NetView/6000. A comprehensive management tool for heterogeneous devices on Transmission Control Protocol/Internet Protocol (TCP/IP) networks. The AIX SystemView NetView/6000 program can use the IBM AIX Service Point program to communicate with the NetView and NETCENTER programs.

alert. (1) An error message sent to the system services control point (SSCP) at the host system. (R) (2) In the AIX SystemView NetView/6000 program, selected traps are converted to alerts that are then forwarded to the NetView or NETCENTER programs for handling. (3) In the NetView and NETCENTER programs, a high-priority event that warrants immediate attention.

APPL. Application program. *

B

background process. (1) In the AIX Operating System, a mode of program execution in which the shell does not wait for program completion before prompting the user for another command. * (2) A process that does not require operator intervention but can be run by the computer while the workstation is used to do other work. * (3) Contrast with *foreground process*. * (4) See also *daemon*.

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) In the connection of local loops, channels, or rings, the equipment and techniques used to match circuits and to facilitate accurate data transmission. * (3) See also *gateway*.

button. A word or picture on the screen that can be selected. Once selected and activated, a button begins an action in the same manner that pressing a key on the keyboard can begin an action. (R)

C

class. 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 mouse button.

client. (1) In an AIX distributed file system environment, a system that is dependent on a server to provide it with programs or access to programs. (2) See also *server*. *

CMIP. Common Management Information Protocol.

CMOT. Common Management Information Protocol over TCP/IP.

code point. In the NetView and NETCENTER programs, a 1- or 2-byte hexadecimal value that indexes a text string stored at an alert receiver and is used by the alert receiver to create displays of alert information.

command. (1) A request from a terminal for the performance of an operation or the execution of a particular program. * (2) A request to perform an operation or run a program. When parameters, values, flags, or other operands are associated with a command, the resulting character string is a single command. (R)

command list. A list of program commands and statements designed to perform a specific function for the user. *

Common Management Information Protocol (CMIP). The protocol elements used to provide the operational and notification services defined by Common Management Information Services. CMIP is part of the Organization for Standardization (ISO) and Open Systems Interconnection (OSI) specification.

Common Management Information Services (CMIS). A suite of operational and notification services used for the management of systems. CMIS is a part of the International Organization for Standardization (ISO) and Open Systems Interconnection (OSI) specification.

Common Management Information Protocols over TCP/IP (CMOT). A protocol interface defined by the Internet Engineering Task Force (IETF) that enables the use of CMIP over a TCP/IP protocol stack.

component. Hardware or software that is part of a functional unit. *

compound status. (1) The compound status scheme determines how status is propagated from symbols in child submaps to symbols of the parent object. The combined status of symbols determines the resulting compound status. Compound status can propagate up through multiple levels of submaps in the network map. The compound status setting applies to the entire map. In effect, the status of specific nodes propagates up to a symbol on a higher-level submap. Compound status is configured by using one of three schemes:

- Default
- Propagate Most Critical
- Propagate at Threshold Value

(2) See *default compound status.*

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. * (3) The act of organizing and interconnecting the components of an information processing system.

connection. (1) In system communications, a line over which data can be passed between two systems or between a system and a device. * (2) A physical or logical link between objects that appears as a line between them on the topology map. For example, the connection line between a gateway and network represents an interface on that network. Multiple connections appear as one line. (3) Synonym for *physical connection.*

context menu. (1) A menu (also known as a pop-up menu) that provides no visual cue to its presence, but pops-up when operators perform a menu selection with button 3 of a three-button mouse.

copy. (1) In the AIX SystemView NetView/6000 program, a menu item function that copies selected symbols and objects to the cut buffer. To complete the copy operation, select the Paste menu item. (2) See *cut, cut buffer,* and *paste.*

critical status. (1) In the AIX SystemView NetView/6000 program, the status state, displayed by a symbol, that indicates a problem with the object. If the status is compound status, it reflects a critical condition in the parent object's child submap. If the status is direct status, it may reflect a critical condition for the symbol or the object. The default color for critical status is red. (2) See *normal status, marginal status,* and *compound status.*

cut. (1) A function used to cut (delete) objects and place them in the cut buffer. The Cut Button can be used in conjunction with the Paste menu item to move objects by pasting them from the cut buffer to a submap (cut-and-paste). (2) See *copy, cut buffer,* and *paste.*

cut buffer. (1) A memory area where symbols and objects that are cut or copied are temporarily stored. The cut buffer enables cut and paste, or copy and paste, operations. (2) See *copy, cut,* and *paste.*

D

daemon. (1) A background process usually started at system initialization that runs continuously and performs a function required by other processes. (2) In the AIX Operating System, a program that runs unattended to

perform a standard service. Some daemons are triggered automatically to perform their task; others operate periodically. * (3) See also *background process*.

data. A representation of facts, concepts, or instructions in a form suitable for communication, interpretation, or processing by human or automatic means. Data includes constants, variables, arrays, and character strings. *

data set. The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access. *

default. An initial configuration setting. Defaults are supplied when the AIX SystemView NetView/6000 program is first run to reduce the amount of time required to start actively managing systems on a network. Users and applications can alter many default settings.

default compound status. When a new map is created, compound status is set to a default value. The default value for compound status causes the graphical interface to propagate status.

delete. (1) An Edit menu function that deletes symbols and objects. A confirmation box is displayed before the deletion is performed. Some objects may be rediscovered and their symbols can be hidden. The Delete function is available for maps, submaps, and snapshots. (2) See also *hide symbol* and *edit menu*.

device. A mechanical, electrical, or electronic contrivance with a specific purpose. *

dialog box. (1) A dialog box provides data fields and buttons for setting controls, selecting from lists, choosing from mutually exclusive options, entering data, and presenting the user with messages. The AIX SystemView NetView/6000 dialog boxes are defined by OSF/Motif. (2) A pop-up window that is used primarily to gather user input.

discovery. The automatic detection of network topology changes (for example, new and deleted nodes, new and deleted interfaces).

display. (1) A visual presentation of data. (I) (A) (2) To present data visually. (I) (A) (3) A device or medium on which information is presented, such as a terminal screen. (4) Deprecated term for *panel*. *

DOC. Documentation. *

domain. (1) That part of a network in which the data processing resources are under common control. (T) (2) In a database, all the possible values of an attribute or a data element. * (3) In TCP/IP, the naming system used in hierarchical networks. The domain naming system uses the DOMAIN protocol and the named daemon. (4) In a domain system, groups of hosts are administered separately within a tree-structured hierarchy of domains and subdomains. *

dynamic. (1) In programming languages, pertaining to properties that can be established only during the execution of a program; for example, the length of a variable-length data object is dynamic. (I) (2) Pertaining to an operation that occurs at the time it is needed rather than at a predetermined or fixed time. * (3) In AIX SystemView NetView/6000, the contents of windows in the event display function are either dynamic or static. In the dynamic display (workspace), events continue to be added to the cards/list. (4) Contrast with *static*. *

E

echo. In data communication, a reflected signal on a communications channel. On a communications terminal, each signal is displayed twice, once when entered at the local terminal and again when returned over the communications link. This allows the signals to be checked for accuracy. *

edit menu. An action bar menu that contains items that enable the user to edit symbols and objects in an open map or submap. Editing includes tasks, such as adding, deleting, and copying.

Enhanced X-Windows Toolkit. (1) In the AIX Operating System, a collection of basic functions for developing a variety of application environments. Toolkit functions manage Toolkit initialization, widgets, memory, events, geometry, input focus, selections, resources, translation of events, graphics contexts, pixmaps, and errors. * (2) See also *X-Window System*.

enterprise. An entire business organization. An enterprise may consist of one or more establishments, divisions, plants, warehouses, and so on that require an information system.

enterprise-specific MIB. (1) An SNMP management Information Base (MIB) developed by individual vendors for specific products. Vendors register their private MIBs under the enterprise object identifier subtree. (2) See *MIB*.

entity. (1) In the AIX SystemView NetView/6000 program, an element on a network that has semantic attributes. (2) See also *object*.

enterprise-specific trap. (1) An enterprise-defined SNMP trap indicated by generic trap number 6 and a unique specific trap number that denotes an enterprise-unique event.

error. A discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition. (I) (A)

error log. (1) A data set or file in the AIX Operating System where error information is stored. Applications write to the AIX error log in response to hardware and software errors. (2) A form in a maintenance library that is used to record error information about a product or system. * (3) A record of machine checks, device errors, and volume statistical data. *

event. (1) An occurrence of significance to a task, such as an SNMP trap or an AIX SystemView NetView/6000 internal event. (2) In the AIX SystemView NetView/6000 program, an unsolicited notification from the managed object or SNMP agent that at least one of the following has occurred:

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

(3) In the NetView and NETCENTER programs, a record indicating irregularities of operation in physical elements of a network. * (4) A CMIP event report.

EXEC. (1) In the AIX Operating System, to overlay the current process with another executable program. * (2) See also *fork*.

F

field. Fields are the building blocks 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 which describe how the field is treated by AIX SystemView NetView/6000. A field can contain data only when it is associated with an object.

filter. (1) In the AIX Operating System, a command that reads standard input data, modifies the data, and sends it to the display screen. * (2) A device or program that separates data, signals, or material in accordance with specified criteria. (A) (3) In the AIX SystemView NetView/6000 program, a set of criteria that determines which events are received by registered applications, selected for displaying, or forwarded to the NetView and NETCENTER programs as alerts. (4) In the NetView program, a function that limits the data that is to be recorded on the database and displayed at the terminal. See *recording filter* and *viewing filter*. *

filtering. In the AIX SystemView NetView/6000 program, a process that applies tests to previously identified objects to extract a subset.

foreground process. (1) In the AIX Operating System, a process that must run to completion before another command is issued to

the shell. The foreground process is in the foreground process group, which is the group that receives the signals generated by a terminal. (2) In the AIX SystemView NetView/6000 program, the xnm application and the applications running under it. (3) Contrast with *background process.*

fork. (1) In the AIX Operating System, to create and start a child process. * (2) See also *EXEC.*

G

gateway. (1) 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. * (2) 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) (3) In TCP/IP, a device used to connect two systems that use either the same or different communication protocols. *

generic alert. (1) A product-independent method of encoding alert data by means of both (a) code points indexing short units of stored text and (b) textual data. (2) Encoded alert information that uses code points (defined by IBM and possibly customized by users or application programs) stored at an alert receiver, such as the NetView program. *

H

help menu. An action bar menu to provides detailed help information about the AIX SystemView NetView/6000 graphical interface. It also provides information about registered applications that are integrated with the graphical interface.

help panel. Information displayed by a system in response to a help request from a user. See *task panel.* *

hide symbol. (1) An operation that enables users to prevent symbols from being displayed on a submap. The symbols still exist but are not visible.

highlighting. (1) In the AIX SystemView NetView/6000 program, a visual cue showing the nodes or connections that are the output of certain operations. (2) Emphasizing a display element or segment by modifying its visual attributes. (I) (A)

host. (1) The primary or controlling computer in the communications network. (R) (2) A computer attached to a network. (R) (3) In TCP/IP, any system that has at least one Internet address associated with it. A host with multiple network interfaces may have multiple Internet addresses associated with it. * (4) See also *host processor.* *

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 access method for the network resides. *

I

ID. Identification. *

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)

Internet. A wide-area network connecting thousands of disparate networks in industry, education, government, and research. The Internet network uses TCP/IP as the standard protocol for transmitting information. *

internet address. The numbering system used in TCP/IP Internetwork communications to specify a particular network, or a particular host on that network, with which to communicate. Internet addresses are denoted in dotted decimal form. *

internet-level submap. The highest level of the topology map that shows how internet protocol networks or subnets are connected by gateways.

IP. Internet Protocol. *

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. * (3) A name or symbol that identifies a parameter. * (4) Part of a command operand that consists of a specific character string, such as DSNAME=. *

L

label. A label is used to distinguish a symbol from other symbols on a submap and map. The label is displayed below a symbol. Labels can be assigned or modified at any time by using the Symbol Description dialog box.

link. (1) In data communications, a transmission medium and data link control component that together transmit data between adjacent nodes. (R) (2) In TCP/IP, a communications line. A TCP/IP link may share the use of a communications line with SNA. *

local. Pertaining to a device, file, or system that is accessed directly from your system, without the use of a communications line. Contrast with *remote*. (R)

M

mainframe. A large computer, particularly one to which other computers can be connected so that they can share facilities the mainframe provides. The term usually refers to hardware only. *

managed object. (1) An object that is being actively managed. Applications can monitor and manage objects for topology, status, and configuration changes. When you choose to manage an object, the objects in child submaps of the managed object also become managed. An object can be toggled between managed and unmanaged. You can choose which objects to manage, thereby, customizing the management region for any map. (2) See *unmanaged object* and *management region*.

managed object class. A named set of managed objects sharing the same (named) sets of attributes, notifications, management operations (packages), and which share the same conditions for presence of those packages. (I)

management region. 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.

manager. The part of a distributed management application that issues requests and receives notifications; that is, uses the services of one or more agents.

menu. 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)

menu bar. 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. (R)

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 context. (2) Information from the system that informs the user of a condition that may affect further processing of a current program. (R)

MIB. Management Information Base.

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*.

N

NETCENTER program. An IBM licensed program that enables network operators to use sophisticated online graphics and menus to work with images of a network.

NetView program. An IBM licensed program used to monitor a network, manage it, and diagnose network problems. *

NetView command list language. An interpretive language unique to the NetView program that is used to write command lists. *

network. (1) An arrangement of nodes and interconnecting branches. (T) (2) A configuration of data processing devices and software connected for information interchange. *

network operator. (1) A person who controls the operation of all or part of a network. * (2) In a multiple-domain network, a person or program responsible for controlling all domains. *

NFS. Network File System. (R)

NMVT. Network management vector transport. *

node. (1) An end point of a link, or a junction common to two or more links in a network. Nodes can be processors, controllers, or workstations, and they can vary in routing and other functional capabilities. (R) (2) The portion of a hardware component, along with its associated software components, that implements the functions of the seven architectural layers (SNA). (3) In a tree structure, a point at which subordinate items of data originate. (R)

node name. In the AIX SystemView NetView/6000 program, the symbolic name assigned to a specific node during network definition.

node-level submap. Contains the addressable resources of a network, such as a gateway, router, workstation, and personal computer.

normal status. (1) Indicates that a network object is functioning normally. The default icon symbol color for normal status is green. The default connection symbol color for normal status is black. (2) See *critical status* and *marginal status*.

notification. Information emitted by a managed object relating to an event that has occurred within the managed object. (I)

O

object. (1) In the AIX SystemView NetView/6000 program, a generic term for any entity that AIX SystemView NetView/6000 discovers and displays on the topology map, or any entity that you add to the topology map. (2) In the AIX object data manager, an instance or member of an object class, conceptually similar to a structure that is a member or array of structures. * (3) In the AIX SystemView NetView/6000 program, objects convey to the symbol various semantic attributes that represent an entity. (4) See *managed object*. (5) See also *entity* and *symbol*.

object class. (1) In AIX SystemView NetView/6000, objects are divided into four classes: computer, connector, device, software, location, and cards. (2) In the AIX object data manager, a stored collection of objects with the same definition. Conceptually similar to an array of structures. * (3) See also *object class, symbol class*, and *managed object class*.

OK button. Saves and cancels the value of the dialog box.

online. (1) Pertaining to the operation of a functional unit when it is under the direct control of the computer. (T) (2) Pertaining to a user's ability to interact with a computer. *

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)

operator. (1) A person who operates a device. * (2) A person or program responsible for managing activities controlled by a given piece of software such as MVS, the NetView program, or IMS. * (3) A person who keeps a system running. (4) See *network operator.*

OSF. Open Software Foundation.

OSF/Motif. (1) A graphical interface that contains a tool kit, presentation description language, window manager, and style guideline. (2) See also *Open Software Foundation.*

OSI. Open systems interconnection.

P

page. The information displayed at the same time on the screen of a display device. *

panel. (1) A formatted display of information that appears on a terminal screen. * (2) In computer graphics, a display image that defines the locations and characteristics of display fields on a display surface. * (3) See *help panel.* Contrast with *screen.*

paste. (1) Used in conjunction with the Cut and Copy menu item to complete a cut-and-paste operation or a copy operation. It retrieves items from the cut buffer and places symbols of objects on a submap of your choice. (2) See also *copy and cut buffer.*

physical connection. (1) A connection that establishes an electrical circuit. (2) In the AIX SystemView NetView/6000 program, a point-to-point connection or multipoint connection. Synonymous with *connection.*

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) In TCP/IP, a 16-bit number used to communicate between TCP and a higher-level protocol or application. Some protocols, such as the File Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP), use the same port number in all TCP/IP implementations. (4) The representation of a physical connection to the link hardware. A port is sometimes referred to as an adapter. There may be one or more ports controlled by a single DLC process.

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)

R

recommended action. Procedures suggested by the NetView program that can be used to determine the causes of network problems. *

record. (1) In programming languages, an aggregate that consists of data objects, possibly with different attributes, that usually have identifiers attached to them. In some programming languages, records are called structures. (I) (2) A set of data treated as a unit. (TC97) (3) A set of one or more related data items grouped for processing. *

recording filter. In the NetView program, the function that determines which events, statistics, and alerts are stored on a database. *

remote. (1) Pertaining to a system, program, or device that is accessed through a telecommunication line. * (2) A device that does not use the same protocol and is, therefore, unknown. (3) 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)

resource. Any facility of the 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 communications, 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*.

RISC. Reduced instruction-set computer. *

root-level submap. Contains the highest level of the submap hierarchy. Multiple networks can be placed within the root level submap.

route. An ordered sequence of nodes and transmission groups (TGs) that represents a path from an origin node to a destination node traversed by the traffic exchanged between them.

router. See Internet router. *

S

screen. (1) In the AIX extended curses library, a window that is as large as the display screen of the workstation. * (2) Deprecated term for display panel. *

seed file. In the AIX SystemView NetView/6000 program, 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 group of display elements. * (2) A contiguous area of virtual storage allocated to a job or system task. A program segment can be run by itself, even if the whole program is not in main storage. (3) A portion of a computer program that may be executed without the entire program being resident in main storage. * (4) In AIX Enhanced X Windows, one or more lines that are drawn but not necessarily connected at the end points. * (5) In the IBM Token-Ring Network, a section of cable between components or devices on the network. A segment may consist of a single patch cable, multiple patch cables connected together, or a combination of building cable and patch cables connected together. *

segment-level submap. Represents the topology of a segment of a network. A segment submap contains network nodes and connectors.

select. (1) In the AIX Operating System, to choose a button on the display screen. * (2) To place the cursor on an object (name or command) and press a button on the mouse or the appropriate key on the keyboard.

server. (1) In the AIX Operating System, an application program that usually runs in the background and is controlled by the system program controller. (2) In Enhanced X Windows, provides the basic windowing mechanism. It handles IPC connections from clients, demultiplexes graphics requests onto screens, and multiplexes input back to clients. * (3) See also *client*. *

shell script. A synonym for shell procedure.

Simple Network Management Protocol (SNMP). A protocol running above the User Datagram Protocol (UDP) used to exchange network management information.

SMIT. System Management Interface Tool

SNA. Systems Network Architecture. *

SNA network. The part of a user-application network that conforms to the formats and protocols of Systems Network Architecture. It enables reliable transfer of data among end users and provides protocols for controlling the resources of various network configurations. The SNA network consists of network addressable units (NAUs), boundary function, gateway function, and intermediate session routing function components; and the transport network. *

SNMP. Simple Network Management Protocol.

SP. Service point. *

spappld daemon. A background process that receives the RUNCMD command from the host system that is running NetView and executes those commands on the AIX SystemView NetView/6000 management station.

static. (1) In programming languages, pertaining to properties that can be established before execution of a program; for example, the length of a fixed length variable is static.

(T) (2) In AIX SystemView NetView/6000, static workspace contains only certain events. The static workspace is not updated. (3) Pertaining to an operation that occurs at a predetermined or fixed time. * (4) Contrast with *dynamic*. *

station. An input or output point of a system that uses telecommunications 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. (1) The current condition or state of a program or device. (R) (2) In the AIX SystemView NetView/6000 program, the condition of a node or portion of a network as represented by the color of a symbol on a submap.

submap. (1) A particular view of some aspect of a network that displays symbols that represent objects. Some symbols may explode into other submaps, usually having a more detailed view than their parent submap. The application that creates a submap determines what part of the network the submap displays. (2) See also *root-level submap, internet-level submap, node-level submap,* and *segment-level submap*.

subvector. A subcomponent of the network management vector transport (NMVT) major vector. *

symbol. (1) In the AIX SystemView NetView/6000 program, a picture or icon that represents an object. Each symbol has an outside and inside component.

- The outside component differentiates the object classes.
- The inside component differentiates the objects within the class. (2) See also *object class* and *symbol class*.

symbol class. (1) A collection of symbols that have the same or similar properties. A symbol class is represented by the shape of the symbol. Each symbol subclass in a given class contains the same shape. Each symbol class has a unique set of subclasses associated with it. Applications may register additional symbol classes. Some of the registered symbol classes provided with the AIX SystemView NetView/6000 program include:

- Computer
- Connector
- Device
- Software
- Location
- Cards

You can view all the registered classes from the Display Legend panel, or from the Add Object Palette. (2) See also *symbol subclass* and *symbol type*.

symbol subclass. (1) A set of symbols that is in a given symbol class. A particular subclass in a given class defines the type of the symbol. For example, in the symbol class called Computer, the subclasses consist of PC, workstation, mini, and mainframe. All symbols in the subclass of the same class contain the same outline (shape). The AIX SystemView NetView/6000 program displays the symbol subclass as the graphic inside the outer shape of the symbol. (2) See also *symbol class* and *symbol type*.

symbol type. (1) The symbol type consists of the symbol class and the symbol subclass. A specific symbol type is defined by the concatenation of a symbol class and a symbol subclass within that class. The symbol class is identified on submaps by the outer shape of the symbol and the symbol subclass by the graphic inside the shape. (2) See also *symbol class* and *symbol subclass*.

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. *

SystemView. The IBM systems management strategy for planning, coordinating, and operating open, heterogeneous, enterprise-wide information systems.

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 index. (1) An index that provides online help entries for a variety of tasks that are available in the AIX SystemView NetView/6000 program and applications that are integrated with the AIX SystemView NetView/6000 program. The Task Index can be accessed from the Help menu. (2) See also *help menu.*

TCP. Transmission Control Protocol. *

TCP/IP. Transmission Control Protocol/Internet Protocol. *

threshold. In the AIX SystemView NetView/6000 program, 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, SNMPCollect 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) A sequence of bits passed from one device to another along the token ring. When the token has data appended to it, it becomes a frame.

tralertd daemon. A background process that receives SNMP traps, converts the traps to NMVT alerts, and sends the alerts to the host system that is running the NetView and NETCENTER programs.

trap. An unsolicited event generated by an agent and forwarded to a manager. Traps inform the manager of changes that occur in the network.

trapgend daemon. An SNMP subagent that communicates with the AIX Operation System Version 3 Release 2 snmpd daemon through the Single multiplexer (SMUX) protocol. The subagent converts alertable AIX system errors into SNMP traps and sends them to the AIX SystemView NetView/6000 program.

U

UNIX Operating System. An operating system developed by Bell Laboratories that features multiprogramming in a multiuser environment. The UNIX Operating System was originally developed for use on minicomputers but has been adapted for mainframes and microcomputers. *

Note: The AIX Operating System is IBM's implementation of the UNIX operating system. See *AIX.*

unknown status. (1) The status of an object that is not yet known or does not actually exist in the network. The default icon symbol color for unknown status is Blue. The default connection symbol color is Black. (2) See *critical status, normal status, unknown status, unmanaged status,* and *status.*

unmanaged object. (1) An object that is not actively managed. An unmanaged object displays status as Unmanaged. It does not display active status (normal, marginal, critical). Unmanaged objects do not display compound status nor do they contribute to compound status. Objects can be kept in an unmanaged state if they are not of interest. An object may be toggled between a managed and unmanaged state. (2) See *managed object* and *unmanaged status.*

unmanaged status. (1) The status that indicates that an object is unmanaged. The default icon symbol color displayed to indicate unmanaged status is Wheat. The default connection symbol color displayed is Black. (2) See *critical status, normal status, compound status, unknown status,* and *status.*

user. Any person or anything that may issue commands and messages to or receive com-

mands and messages from the information processing system. (T)

V

value. (1) A specific occurrence of an attribute, for example, "blue" for the attribute color. (TC97) (2) A quantity assigned to a constant, a variable, a parameter, or a symbol. *

variable. (1) A name used to represent a data item whose value can change while the program is running. * (2) 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. * (3) A quantity that can assume any of a given set of values. (A)

view. See *submap*.

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. *

W

window. A portion of a visual display surface in which display images pertaining to a particular application can be presented. Different applications can be displayed simultaneously in different windows. (A)

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. (1) A network-transparent windowing system developed by the Massachusetts Institute of Technology. It is the basis for Enhanced X-Windows, which runs on the AIX Operating System. (2) See also *Enhanced X-Windows Toolkit*.

Bibliography

AIX SystemView NetView/6000 Publications

The following paragraphs briefly describe the publications for Version 2 of the AIX SystemView NetView/6000 program:

AIX SystemView NetView/6000 Application Design and Style Guide (SC31-7019)

This book provides guidelines for system programmers who develop applications that will integrate with the AIX SystemView NetView/6000 program.

AIX SystemView NetView/6000 Concepts: A General Information Manual (GC31-6179)

This book provides an overview of the AIX SystemView NetView/6000 program that business executives can use to evaluate the product. System planners can also use this information to learn how the AIX SystemView NetView/6000 manages heterogeneous networks.

AIX SystemView NetView/6000 Installation and Configuration (SC31-7020)

Provides installation and configuration steps for the system programmer who will install and configure the AIX SystemView NetView/6000 program.

AIX SystemView NetView/6000 And the Host Connection (SC31-6178)

Provides information for System/390, NetView and NETCENTER users who want to manage TCP/IP and SNA networks.

AIX SystemView NetView/6000 Problem Determination (SC31-7021)

This book is intended to help the reader classify and resolve problems related to the operation of the AIX SystemView NetView/6000 program and its individual components.

AIX SystemView NetView/6000 Programmer's Guide (SC31-7022)

Provides information for programmers about creating network management applications. This book also contains information about the AIX SystemView NetView/6000 program server, commands, function calls, and object classes.

AIX SystemView NetView/6000 Programmer's Reference (SC31-7023)

This book is intended for programmers and contains reference information about the AIX SystemView NetView/6000 program and its server, commands, function calls, and object classes.

AIX SystemView NetView/6000 User's Guide (SC31-7024)

This book contains "how-to" information that provides network operators the help they need to accomplish networking and customization tasks. This book explains network management principles and describes how the AIX SystemView NetView/6000 program's components work together to help network operators and administrators perform network management tasks.

In addition to these printed books, hypertext documentation of the AIX SystemView NetView/6000 library is available through InfoExplorer. An online Help Index is also available from the AIX SystemView NetView/6000 Help pull-down window. The Help Index provides dialog box help, function help, and task help.

IBM RISC System/6000 Publications

In addition to the AIX SystemView NetView/6000 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 publications apply to NetView Version 2 Release 2:

NetView At a Glance (GC31-6123)

NetView Installation and Administration Guide (SC31-6051)

NetView Customization Guide (SC31-6048)

NetView Operation (SC31-6053)

NetView Problem Determination and Diagnosis (LY43-0005)

NetView Automation Planning: Planning (SC31-6101)

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)

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)

RT/PC Interface Program for TCP/IP (SC23-0812)

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:

Using AIX SNA Services/6000 (SC31-7002)

AIX SNA Services/6000 Reference (SC31-7014)

AIX SNA Services/6000: Writing SNA Transaction Programs (SC31-7003)

NETCENTER Publications

The following NETCENTER publications are available:

NETCENTER Operator Tutorial (GC75-0109)

NETCENTER Service Point Interface Installation and Reference (SC75-0111)

Internet Request for Comments Documents

The following documents describe Internet standards supported by the AIX SystemView NetView/6000 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: A Simple Network Management Protocol (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: A Convention for Defining Traps for Use with 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

Related Publications

The following publications are closely related to or referenced by the AIX SystemView NetView/6000 Library:

AIX Trouble Ticket/6000 Publications

For information about the AIX Trouble Ticket/6000 program, consult the following publications:

AIX Trouble Ticket/6000 at a Glance (GC31-7054)

AIX Trouble Ticket/6000 User's Guide (SC31-7034)

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)

IBM Local Area Network Technical Reference (SC30-3383).

MVS/DFP Version 3 Release 3: Using the Network File System Server (SC26-4732)

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)

IBM AIX X-Windows Programmer's Reference (SC23-2118)

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 document:

X/Open OSI-Abstract-Data Manipulation (XOM) API, CAE Specification

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 AIX SystemView NetView/6000 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 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

T

U

V

Communicating Your Comments to IBM

AIX SystemView NetView/6000
And the Host Connection
Version 2

Publication No. SC31-6178-00

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!

AIX SystemView NetView/6000
And the Host Connection
Version 2

Publication No. SC31-6178-00

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!
SC31-6178-00

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

International Business Machines Corporation
Information Development
Department E15
PO BOX 12195
RESEARCH TRIANGLE PARK, NORTH CAROLINA 27709-9990

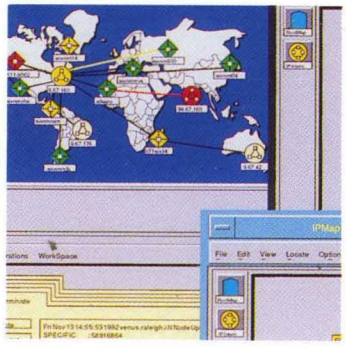
Fold and Tape **Please do not staple** Fold and Tape

SC31-6178-00

Cut or Fold
Along Line

Program Number: 5696-392

Printed in U.S.A.



SC31-6178-00