Tivoli IBM Tivoli NetView for z/OS

IBM

Version 5 Release 3

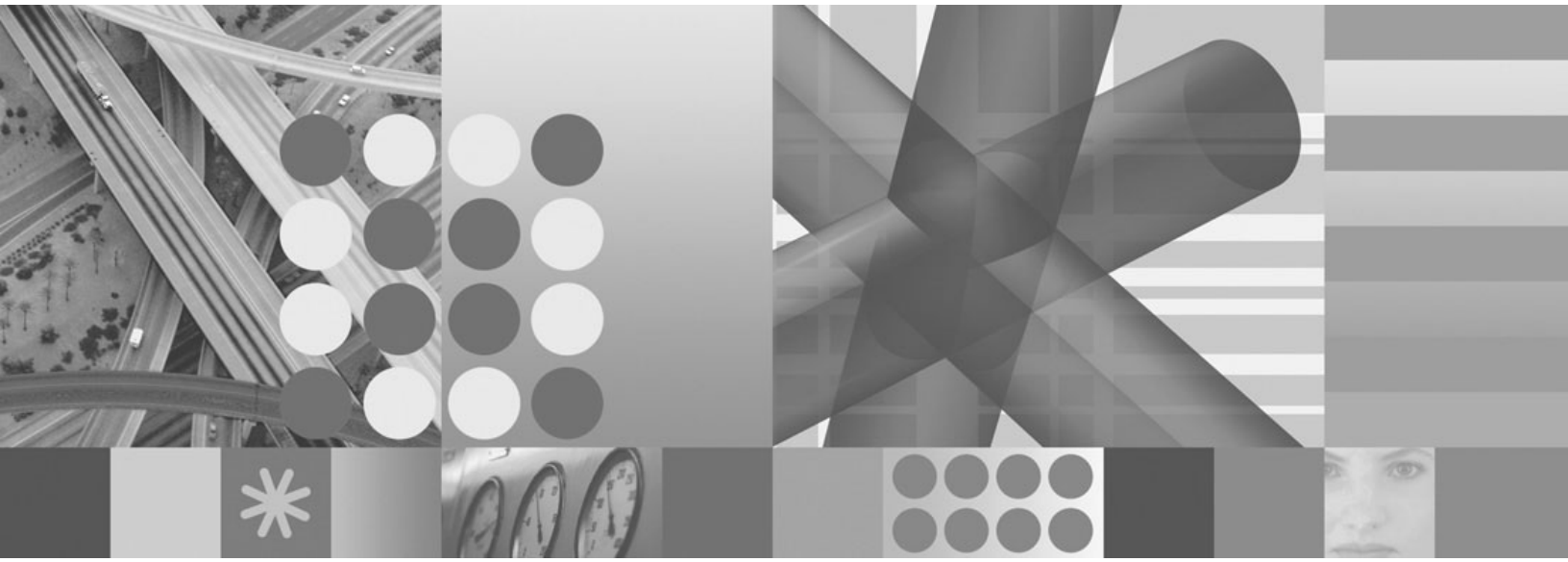
User's Guide

GC31-8849-02

Tivoli® IBM Tivoli NetView for z/OS

IBM

Version 5 Release 3



User's Guide

GC31-8849-02

Note
Before using this information and the product it supports, read the information in "Notices" on page 399.

This edition applies to version 5, release 3 of IBM Tivoli NetView for z/OS (product number 5697-ENV) and to all subsequent versions, releases, and modifications until otherwise indicated in new editions. Make sure you are using the correct edition for the level of the product.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Figures

About this publication

The IBM® Tivoli® NetView® for z/OS® product provides advanced capabilities that you can use to maintain the highest degree of availability of your complex, multi-platform, multi-vendor networks and systems from a single point of control. This publication, the *IBM Tivoli NetView for z/OS User's Guide* provides information for the operator and system programmer on using the NetView program as the central point to manage their networks and systems.

Intended audience

This publication is for system console operators, network operators, and system programmers. Specific operator procedures are defined by the individual installation to meet local requirements.

Publications

This section lists publications in the IBM Tivoli NetView for z/OS library and related documents. It also describes how to access Tivoli publications online and how to order Tivoli publications.

IBM Tivoli NetView for z/OS library

The following documents are available in the Tivoli NetView for z/OS library:

- *Administration Reference*, SC31-8854, describes the NetView program definition statements required for system administration.
- *Application Programmer's Guide*, SC31-8855, describes the NetView program-to-program interface (PPI) and how to use the NetView application programming interfaces (APIs).
- *Automated Operations Network Customization Guide*, SC31-8871, describes how to tailor and extend the automated operations capabilities of the NetView Automated Operations Network (AON) component, which provides event-driven network automation.
- *Automated Operations Network User's Guide*, GC31-8851, describes how to use the Automated Operations Network component to improve system and network efficiency.
- *Automation Guide*, SC31-8853, describes how to use automated operations to improve system and network efficiency and operator productivity.
- *Command Reference Volume 1*, SC31-8857, and *Command Reference Volume 2*, SC31-8858, describe the NetView commands, which can be used for network and system operation and in command lists and command procedures.
- *Customization Guide*, SC31-8859, describes how to customize the NetView product and points to sources of related information.
- *Data Model Reference*, SC31-8864, provides information about the Graphic Monitor Facility host subsystem (GMFHS), SNA topology manager, and MultiSystem Manager data models.
- *Installation: Configuring Additional Components*, SC31-8874, describes how to configure NetView functions beyond the base functions.
- *Installation: Configuring Graphical Components*, SC31-8875, describes how to install and configure the NetView graphics components.

- *Installation: Getting Started*, SC31-8872, describes how to install and configure the NetView base functions.
- *Installation: Migration Guide*, SC31-8873, describes the new functions provided by the current release of the NetView product and the migration of the base functions from a previous release.
- *Installation: Configuring the Tivoli NetView for z/OS Enterprise Agents*, SC31-6969, describes how to install and configure the Tivoli NetView for z/OS enterprise agents.
- *Messages and Codes Volume 1 (AAU-DSI)*, SC31-6965, and *Messages and Codes Volume 2 (DUI-IHS)*, SC31-6966, describe the messages for the NetView product, the NetView abend codes, the sense codes that are shown in NetView messages, and generic alert code points.
- *MultiSystem Manager User's Guide*, GC31-8850, describes how the NetView MultiSystem Manager component can be used in managing networks.
- *NetView Management Console User's Guide*, GC31-8852, provides information about the NetView management console interface of the NetView product.
- *Programming: Assembler*, SC31-8860, describes how to write exit routines, command processors, and subtasks for the NetView product using assembler language.
- *Programming: Pipes*, SC31-8863, describes how to use the NetView pipelines to customize a NetView installation.
- *Programming: PL/I and C*, SC31-8861, describes how to write command processors and installation exit routines for the NetView product using PL/I or C.
- *Programming: REXX and the NetView Command List Language*, SC31-8862, describes how to write command lists for the NetView product using the Restructured Extended Executor language (REXX™) or the NetView command list language.
- *Resource Object Data Manager and GMFHS Programmer's Guide*, SC31-8865, describes the NetView Resource Object Data Manager (RODM), including how to define your non-SNA network to RODM and use RODM for network automation and for application programming.
- *Security Reference*, SC31-8870, describes how to implement authorization checking for the NetView environment.
- *SNA Topology Manager Implementation Guide*, SC31-8868, describes planning for and implementing the NetView SNA topology manager, which can be used to manage subarea, Advanced Peer-to-Peer Networking®, and TN3270 resources.
- *Troubleshooting Guide*, LY43-0093, provides information about documenting, diagnosing, and solving problems that might occur in using the NetView product.
- *Tuning Guide*, SC31-8869, provides tuning information to help achieve certain performance goals for the NetView product and the network environment.
- *User's Guide*, GC31-8849, describes how to use the NetView product to manage complex, multivendor networks and systems from a single point.
- *Web Application User's Guide*, SC32-9381, describes how to use the NetView Web application to manage complex, multivendor networks and systems from a single point.
- *Licensed Program Specifications*, GC31-8848, provides the license information for the NetView product.

Prerequisite publications

To read about the new functions offered in this release, see the *IBM Tivoli NetView for z/OS Installation: Migration Guide*.

For information about how the NetView for z/OS product interacts with the IBM Tivoli Monitoring product, see the following IBM Tivoli Monitoring publications:

- *Introducing IBM Tivoli Monitoring*, GI11-4071, introduces the components, concepts, and function of IBM Tivoli Monitoring.
- *IBM Tivoli Monitoring: Upgrading from Tivoli Distributed Monitoring*, GC32-9462, provides information on how to upgrade from IBM Tivoli Distributed Monitoring.
- *IBM Tivoli Monitoring: Installation and Setup Guide*, GC32-9407, provides information about installing and setting up IBM Tivoli Monitoring.
- *IBM Tivoli Monitoring User's Guide*, SC32-9409, which complements the IBM Tivoli Enterprise™ Portal online help, provides hands-on lessons and detailed instructions for all Tivoli Enterprise Portal functions.
- *IBM Tivoli Monitoring Administrator's Guide*, SC32-9408, describes the support tasks and functions required for the IBM Tivoli Enterprise Portal Server and clients.
- *Configuring IBM Tivoli Enterprise Monitoring Server on z/OS*, SC32-9463, describes how to configure and customize the IBM Tivoli Enterprise Monitoring Server running on a z/OS system.
- *IBM Tivoli Monitoring Problem Determination Guide*, GC32-9458, provides information and messages to use in troubleshooting problems with the software.
- *Exploring IBM Tivoli Monitoring*, SC32-1803, provides a series of exercises for exploring IBM Tivoli Monitoring.
- *IBM Tivoli Universal Agent User's Guide*, SC32-9459, introduces the IBM Tivoli Universal Agent.
- *IBM Tivoli Universal Agent API and Command Programming Reference Guide*, SC32-9461, explains how to implement the IBM Tivoli Universal Agent APIs and describes the API calls and command-line interface commands.

Related publications

For information about the NetView Bridge function, see *Tivoli NetView for OS/390 Bridge Implementation*, SC31-8238-03 (available only in the V1R4 library).

You can find additional product information on the NetView for z/OS Web site:

http://www.ibm.com/software/tivoli/products/netview-zos/

Accessing terminology online

The *Tivoli Software Glossary* includes definitions for many of the technical terms related to Tivoli software. The *Tivoli Software Glossary* is available at the following Tivoli software library Web site:

http://publib.boulder.ibm.com/tividd/glossary/tivoliglossarymst.htm

The IBM Terminology Web site consolidates the terminology from IBM product libraries in one convenient location. You can access the Terminology Web site at the following Web address:

http://www.ibm.com/software/globalization/terminology/

For a list of NetView for z/OS terms and definitions, refer to the IBM Terminology Web site. The following terms are used in this library:

NetView
For the following products:
- Tivoli NetView for z/OS version 5 release 3
- Tivoli NetView for z/OS version 5 release 2
- Tivoli NetView for z/OS version 5 release 1
- Tivoli NetView for OS/390® version 1 release 4

MVS™ For z/OS operating systems

MVS element
For the BCP element of the z/OS operating system

CNMCMD
For CNMCMD and its included members

CNMSTYLE
For CNMSTYLE and its included members

PARMLIB
For SYS1.PARMLIB and other data sets in the concatenation sequence

The following IBM names replace the specified Candle® names:

IBM Tivoli Monitoring Services
For OMEGAMON® platform

IBM Tivoli Enterprise Monitoring Agent
For Intelligent Remote Agent

IBM Tivoli Enterprise Monitoring Server
For Candle Management Server

IBM Tivoli Enterprise Portal
For CandleNet Portal

IBM Tivoli Enterprise Portal Server
For CandleNet Portal Server

Unless otherwise indicated, references to programs indicate the latest version and release of the programs. If only a version is indicated, the reference is to all releases within that version.

When a reference is made about using a personal computer or workstation, any programmable workstation can be used.

Using LookAt to look up message explanations

LookAt is an online facility that you can use to look up explanations for most of the IBM messages you encounter, as well as for some system abends (an abnormal end of a task) and codes. Using LookAt to find information is faster than a conventional search because in most cases LookAt goes directly to the message explanation.

You can use LookAt from the following locations to find IBM message explanations for z/OS elements and features, z/VM®, VSE/ESA™, and Clusters for AIX® and Linux®:

- The Internet. You can access IBM message explanations directly from the LookAt Web site at http://www.ibm.com/eserver/zseries/zos/bkserv/lookat/.

- Your z/OS TSO/E host system. You can install code on your z/OS or z/OS.e systems to access IBM message explanations, using LookAt from a TSO/E command line (for example, TSO/E prompt, ISPF, or z/OS UNIX® System Services running OMVS).
- Your Microsoft® Windows® workstation. You can install code to access IBM message explanations on the *z/OS Collection* (SK3T-4269), using LookAt from a Microsoft Windows DOS command line.
- Your wireless handheld device. You can use the LookAt Mobile Edition with a handheld device that has wireless access and an Internet browser (for example, Internet Explorer for Pocket PCs, Blazer, or Eudora for Palm OS, or Opera for Linux handheld devices). Link to the LookAt Mobile Edition from the LookAt Web site.

You can obtain code to install LookAt on your host system or Microsoft Windows workstation from a disk on your *z/OS Collection* (SK3T-4269), or from the LookAt Web site (click **Download**, and select the platform, release, collection, and location that suit your needs). More information is available in the LOOKAT.ME files available during the download process.

Accessing publications online

The documentation CD contains the publications that are in the product library. The publications are available in Portable Document Format (PDF), HTML, and BookManager® formats. Refer to the readme file on the CD for instructions on how to access the documentation.

An index is provided on the documentation CD for searching the Tivoli NetView for z/OS library. If you have Adobe Acrobat on your system, you can use the Search command to locate specific text in the library. For more information about using the index to search the library, see the online help for Acrobat.

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli Information Center Web site at http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp.

In the Tivoli Information Center window, click **Tivoli product manuals**. Click the letter that matches the first letter of your product name to access your product library. For example, click **N** to access the Tivoli NetView for z/OS library.

Note: If you print PDF documents on other than letter-sized paper, set the option in the **File → Print** window that enables Adobe Reader to print letter-sized pages on your local paper.

Ordering publications

You can order many Tivoli publications online at the following Web address:

http://www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss

You can also order by telephone by calling one of these numbers:
- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order Tivoli publications. To locate the telephone number of your local representative, perform the following steps:

1. Go to the following Web address:

   http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi
2. Select your country from the list and click **Go**. The Welcome to the IBM Publications Center window is displayed.
3. On the left side of the window, click **About this site** to see an information page that includes the telephone number of your local representative.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. Standard shortcut and accelerator keys are used by the product and are documented by the operating system. Refer to the documentation provided by your operating system for more information.

For additional information, see Appendix G, "Accessibility," on page 397.

Tivoli technical training

For Tivoli technical training information, refer to the following IBM Tivoli Education Web site at http://www.ibm.com/software/tivoli/education.

Support information

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

Online
Go to the IBM Software Support site at http://www.ibm.com/software/support/probsub.html and follow the instructions.

IBM Support Assistant
The IBM Support Assistant (ISA) is a free local software serviceability workbench that helps resolve questions and problems with IBM software products. The ISA provides quick access to support-related information and serviceability tools for problem determination. To install the ISA software, go to http://www.ibm.com/software/support/isa.

Problem determination guide
For more information about resolving problems, see the *IBM Tivoli NetView for z/OS Troubleshooting Guide*.

Downloads

Clients and agents, demonstrations of the NetView product, and several free NetView applications that you can download are available at the NetView for z/OS Web site:

http://www.ibm.com/software/tivoli/products/netview-zos/

These applications can help with the following tasks:

- Migrating customization parameters from earlier releases to the current style sheet

- Getting statistics for your automation table and merging the statistics with a listing of the automation table
- Displaying the status of a job entry subsystem (JES) job or canceling a specified JES job
- Sending alerts to the NetView program using the program-to-program interface (PPI)
- Sending and receiving MVS commands using the PPI
- Sending Time Sharing Option (TSO) commands and receiving responses

Conventions used in this publication

This publication uses several conventions for special terms and actions, operating system-dependent commands and paths, and command syntax.

Typeface conventions

This publication uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as **Tip:**, and **Operating system considerations**:)
- Keywords and parameters in text

Italic

- Citations (examples: titles of publications, diskettes, and CDs
- Words defined in text (example: a nonswitched line is called a *point-to-point line*)
- Emphasis of words and letters (words as words example: "Use the word *that* to introduce a restrictive clause."; letters as letters example: "The LUN address must start with the letter *L*.")
- New terms in text (except in a definition list): a *view* is a frame in a workspace that contains data.
- Variables and values you must provide: ... where *myname* represents...

`Monospace`

- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

Operating system-dependent variables and paths

For workstation components, this publication uses the UNIX convention for specifying environment variables and for directory notation.

When using the Windows command line, replace **$***variable* with **%***variable***%** for environment variables and replace each forward slash (**/**) with a backslash (\) in directory paths. The names of environment variables are not always the same in

the Windows and UNIX environments. For example, %TEMP% in Windows environments is equivalent to $TMPDIR in UNIX environments.

Note: If you are using the bash shell on a Windows system, you can use the UNIX conventions.

Syntax Diagrams

Syntax diagrams start with double arrowheads on the left (►►) and continue along the main syntax line until they end with two arrowheads facing each other (►◄). When more than one line is needed for a syntax diagram, the continued lines end with a single arrowhead (►).

Position and Appearance of Syntax Elements

Syntax diagrams do not rely on highlighting, brackets, or braces. In syntax diagrams, the position of the elements relative to the main syntax line indicates the required, optional, and default values for keywords, variables, and operands as shown in the following table.

Table 1. Position of Syntax Elements

Element Position	Meaning
On the main syntax line	Required
Above the main syntax line	Default
Below the main syntax line	Optional

Keywords and operands are shown in uppercase letters. Variables are shown in lowercase letters and are either italicized or, for NetView help and BookManager online publications, shown in a differentiating color. The appearance of syntax elements indicates the type of element as shown in the following table.

Table 2. Appearance of Syntax Elements

Element	Appearance
Keyword	CCPLOADF
Variable	*resname*
Operand	MEMBER=*membername*
Default	*today* or INCL

Required Syntax Elements

The command name and the required keywords, variables, and operands are shown on the main syntax line. Figure 1 shows that the *resname* variable must be used for the CCPLOADF command.

CCPLOADF

Figure 1. Required Syntax Elements

Optional Syntax Elements

Optional keywords, variables, and operands are shown below the main syntax line. Figure 2 on page xxv shows that the ID operand can be used for the DISPREG

command but is not required.

DISPREG

Figure 2. Optional Syntax Elements

Default Keywords and Values

Default keywords and values are shown above the main syntax line.

If the default is a keyword, it is shown only above the main line. You can specify this keyword or allow it to default. Figure 3 shows the default keyword STEP above the main line and the rest of the optional keywords below the main line.

If an operand has a default value, the operand is shown both above and below the main line. A value below the main line indicates that if you specify the operand, you must also specify either the default value or another value shown. If you do not specify the operand, the default value above the main line is used. Figure 3 shows the default values for operands `MODNAME=*` and `OPTION=*` above and below the main line.

RID

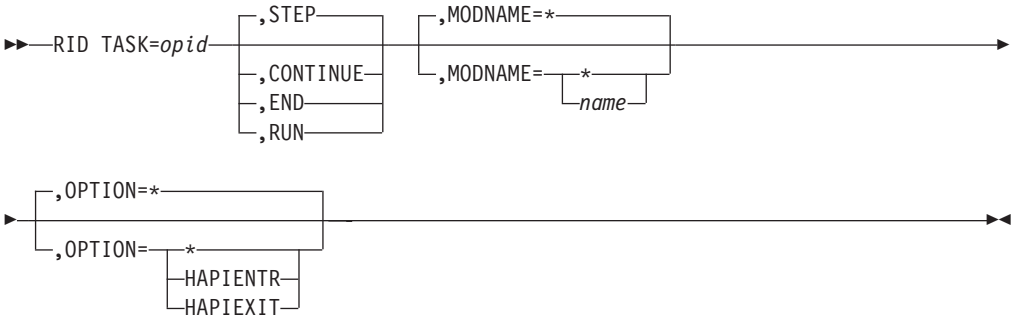


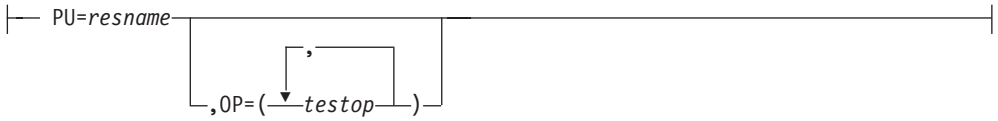
Figure 3. Default Keywords and Values

Syntax Fragments

Commands that contain lengthy sections of syntax or a section that is used more than once in a command are shown as separate fragments following the main diagram. The fragment name is shown in mixed case. Figure 4 on page xxvi shows a syntax diagram with the fragments `Pu`, `PurgeAll`, and `PurgeBefore`.

CSCF

Pu



PurgeAll

PurgeBefore

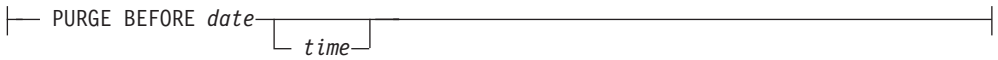


Figure 4. Syntax Fragments

Commas and Parentheses

Required commas and parentheses are shown in the syntax diagram.

When an operand can have more than one value, the values are typically enclosed in parentheses and separated by commas. For example, in Figure 4, the OP operand contains commas to indicate that you can specify multiple values for the *testop* variable.

If a command requires positional commas to separate keywords and variables, the commas are shown before the keyword or variable, as in Figure 3 on page xxv.

Commas are also used to indicate the absence of a positional operand. In the following example of the BOSESS command, the second comma indicates that an optional operand is not being used:

```
NCCF BOSESS applid,,sessid
```

You do not need to specify the trailing positional commas. Trailing positional and non-positional commas either are ignored or cause a command to be rejected. Restrictions for each command state whether trailing commas cause the command to be rejected.

Abbreviations

Command and keyword abbreviations are listed in synonym tables after each command description.

Part 1. About NetView

Chapter 1. Introduction

This chapter provides an overview of the IBM Tivoli NetView for z/OS program, including information about the NetView components. It also describes key programs with which the NetView program interoperates and provides an overview of networking concepts.

NetView for z/OS Overview

The NetView for z/OS program provides functions to help maintain the highest degree of availability for IBM System z™ networks. It has an extensive set of tools for managing and maintaining complex, multi-vendor, multi-platform networks and systems from a single point of control. It provides advanced correlation facilities to automate any network or system event, support for both TCP/IP and SNA networks, a set of user interfaces to meet the needs of every user, and management functions that work in conjunction with other products.

The NetView program includes the following benefits:

- Increased network and system efficiency and availability
- Centralized management for TCP/IP and SNA network environments, which helps reduce the need for duplicate network management systems
- Enhanced operations and message management support to improve and simplify operator interactions and to provide more control in automating and managing day-to-day operations
- Management of larger networks, more resources, and more systems with fewer resources and personnel

With open application programming interfaces, the NetView program can be an integration point for both z/OS and distributed vendors. The NetView program enables the management of networks and systems through graphical display and automation. It reduces the need for manual resource definition and complex automation setup through production-ready automation and extends centralized management into multiple network environments. The NetView program can be used in an enterprise as a centralized manager, a mid-level manager, or a z/OS management endpoint.

The NetView for z/OS program helps maintain system availability and streamline support by consolidating TCP/IP and SNA information from across your enterprise and providing a single platform for automating problem diagnosis. The NetView program can quickly guide support personnel to an appropriate response or even respond automatically.

Enterprise Integration

For coordinated management of availability and performance and for making z/OS data available for broader enterprise management, NetView data is available in the Tivoli Enterprise Portal, which is part of a common infrastructure, known as Tivoli Management Services, that is provided with the IBM Tivoli Monitoring product. You can use this infrastructure to monitor and manage availability and performance across your enterprise from a single point of control.

A wide variety of NetView data, including DVIPA, sysplex, packet traces, the NetView log, and IP connection data, is available through the Tivoli Enterprise Portal and is correlated with information from Tivoli OMEGAMON XE products. The NetView for z/OS program focuses on availability management, while the OMEGAMON XE products focus on performance management. Using the Tivoli Enterprise Portal, you can integrate these solutions for a complete view of network performance and availability data to improve efficiency and to reduce the time needed for problem resolution.

The NetView program also supports Common Base Events, a highly flexible, industry-standard event architecture. Standardized information facilitates automation and enables products to more easily work together.

IP Management

TCP/IP management is an integral part of the NetView for z/OS program and includes the following functions:

- Management of SNA over IP. With the Enterprise Extender technology, you can transport SNA traffic over an IP network. This technology routes SNA path information units (PIUs) over Advanced Peer-to-Peer Networking nodes using high-performance routing (HPR) and subsequently across IP using User Datagram Protocol (UDP). The routing provided by Enterprise Extender is more complex and requires additional information about the paths to session partners. The NetView DIS command provides additional data for this routing. Although the information is primarily for local Enterprise Extender-connected resources, some information is also provided about other HPR-connected resources and about physical units (PUs) that are associated with an active, Enterprise Extender-connected logical unit (LU). Operators can use the DIS command to perform TRACERTE and EEDIAG analysis for these resources and can browse the data provided to discover congestion or broken links. The NLDM SESS command supports referenced (non-endpoint) resources. In addition, the session monitor can display all SNA sessions across an Enterprise Extender connection.
- Support for dynamic virtual IP addressing (DVIPA). The following information is available through the Tivoli Enterprise Portal and the 3270 console:
  - DVIPA definition and status, including summary data for IPv4 DVIPA interfaces of a stack for which a DVIPADAT=Y statement is coded on a TCP390 statement in CNMPOLCY
  - Summary data for all DVIPA sysplex distributors that are currently defined for the local system and for which a DVIPADAT=Y statement is coded on a TCP390 statement in CNMPOLCY, including the number of sysplex distributor target stacks for each DVIPA across the sysplex
  - Information about the DVIPA distributor targets currently defined for the local system, including summary data for each target stack for a given distributed DVIPA and port, the DVIPA workload for each destination host, and the DVIPA and corresponding DVIPA ports that have the worst server acceptance percentages
  - Information about the DVIPA connections for which a DVIPADAT=Y statement is coded on a TCP390 statement in CNMPOLCY, including the number of active DVIPA connections, summary data for all DVIPA connections, and a list of all connections with no traffic flowing
- Dynamic IP resource discovery. The MultiSystem Manager topology manager dynamically discovers the topology and status of IP resources in your network, including resources running in a z/OS environment, and stores the information in the Resource Object Data Manager (RODM). After the information is in RODM, you can view your network resources from the NetView management

console. Topology correlation automatically ties together resources managed by different types of topology functions such as IP and Tivoli management region. Topology correlation is provided for MultiSystem Manager topology functions, for the NetView SNA Topology Manager, and for customer or vendor applications that use the Graphic Monitor Facility host subsystem data model.

- Connection management. The NetView program provides both real-time and historical connection information, including stack name, local and remote addresses and ports, start time, end time (for connections that ended), sent and received byte and segment counts, retransmit counts, and information about connection state, interface, host, TN3270, and application transparent transport layer security (AT-TLS), if applicable. Data is available both in a form for humans to read and in binary form for programming use. Host name translation and IPv4 or IPv6 addresses are supported. In addition, the cross-domain capabilities of the NetView program enable the viewing of connection data at remote z/OS hosts.
- Packet trace collection and formatting. The examination of packet content is sometimes necessary to debug a problem. The NetView program provides real-time capture and formatting of IP packet trace data, including both headers and payloads. The formatting is the same as that under IPCS, so you do not need to learn a new format. Because the formatter is directly integrated with the IP stack, no translation mismatches can occur. Highly flexible tracing and formatting options are available so that you can filter out unwanted data. Both IPv4 and IPv6 packets are supported, and the data is also available in binary (unformatted) form for use by automation routines.
- Command support. The NetView program provides extensive support for IP-related commands, providing users the control capabilities needed to manage IP resources. Commands can be issued directly from the NetView command line, and in REXX procedures and other automation routines. The following commands are commonly used:
  - PING. Test connectivity to an IP host.
  - TRACERTE. Trace the routes of data packets to a specified IP host from the IP stack on the host on which the NetView program is running. Use this command to determine connectivity with or routing to a particular endpoint, roundtrip times between the NetView and target hosts, and routers along the way.
  - TN3270. Log in to remote TCP/IP-connected systems, either from the NetView command line or from the NetView management console.
  - SNMP commands. Send an SNMP request to a network device to set or obtain information about the device.
  - SOCKET. Request IP services, to obtain information about the TCP/IP stack being used or to manage client or server applications (or both).
  - Any UNIX command
  - REXEC. Send a command over IP to a remote host for processing and display the resulting output. The standard UNIX RSH protocol is used. The remote host must have an REXEC server listening at the specified or default port for the command to work.
  - RSH. Send a command over IP to a remote host for processing. The output can be displayed as line-mode output or in a panel that is placed on the NetView roll stack. If the remote host supports it, additional commands can be issued from the panel where the output is displayed.
- Automated responses to intrusions. Firewalls are not impenetrable. Even within a firewall, systems can be vulnerable to attack or misuse, whether accidental or

malicious. In conjunction with the Intrusion Detection Services of z/OS Communications Server, the NetView program offers several kinds of automated responses to an intrusion:

  - Notification. Send an e-mail to security administrators, an alert to the NetView console, a message to designated NetView operators, or a Tivoli Enterprise Console® event to Tivoli Risk Manager for enterprise-wide correlation and analysis.
  - Commands. Issue UNIX, NetView, or z/OS commands to collect more data or take other actions.
  - Statistics. Collect statistics and generate trmdstat reports to send by e-mail to security administrators.

- IPv6 support. This support provides for IPv6 connectivity. It also enables IPv6 addresses to be accepted as input for commands and to be displayed in messages, views, and most places where an IP address can be shown.
- SNMP. In addition to the long-standing support for SNMPv1, the NetView program provides the following SNMP support:
  - Commands. The NetView SNMP command sends an SNMP request to a network device to set or retrieve information about the device. This command supports SNMPv3 authentication and encryption from the command line, REXX, and command lists, with switches for the following settings:
    - The authentication protocol (MD5 or SHA) used for authenticating SNMPv3 messages
    - The authentication pass phrase used for authenticating SNMPv3 messages
    - The privacy pass phrase used for encrypted SNMPv3 messages.
  - Traps. The NetView program can process SNMPv3 traps and also SNMPv2c traps, and can both receive and emit traps. Conversion of SNMP traps is provided either by Event/Automation Service (E/AS) services (see "Event/Automation Service" on page 12) or by base NetView services independent of E/AS.
- Network address translation. For a resource reported through the Tivoli NetView program and for which the IP address has changed as packets related to it are routed from one network to another, the translated addresses are flagged with a special symbol for easy recognition and the corresponding original address is provided in NetView graphical displays.

Automation

Automated operations enable corrections to occur without human intervention. The automation capabilities of the NetView program facilitate and simplify operator interactions and include the following functions:

- Automation of responses to messages and events, which is enabled by the NetView automation table.
- Event correlation using a correlation engine that enables messages and management services units (MSUs) to be correlated according to user-specified criteria.
- Message revision, which enables user-defined modification of attributes such as color, route code, descriptor code, display and syslog settings, and text of original z/OS messages (rather than copies). For example, you can take the following actions:
  - Revise messages before they are presented to the system log, console or automation.
  - Treat a message differently depending on its source.
  - Suppress messages entirely.

– Automate only.

The message revision table can override actions taken by the z/OS message processing facility (MPF) and can generally replace the MPF. It also provides statistics and usage information, includes a test mode, and is active even when the NetView program is not. Finally, the message revision table is under the control of the NetView system programmer rather than the z/OS system programmer.

- Command lists and command processors, which are user-written programs that can be used as if they are NetView commands. A command list or command processor can be used by an operator to accomplish a complex operation with a single command or can perform an entire, complex procedure without operator intervention.
- Timer commands, which initiate automated actions. Both operators and automation procedures can issue timer commands to schedule other commands, command lists, and command processors at a specified time, after a specified delay, repeatedly after specified intervals or in complex, timed combinations.
- Autotasks, which are operator station tasks (OSTs) that do not require a terminal or operator. Like other OSTs, autotasks can receive messages and issue commands. Autotasks are limited only in that they cannot run full-screen applications.

  You can define one or more autotasks for automation and have them started during NetView initialization. Then, the automation table, command lists, command processors, and timer commands can all issue commands under the autotasks. The autotasks can receive messages and present them to the automation table or to installation-exit routines. Thus, many of the other automation facilities can use autotasks.
- Installation exits, which are user-written routines that take control of processing at certain points to alter the usual course of NetView processing.
- MVS command management, which can be used to examine, modify, or reject an MVS command.

Sysplex Monitoring

Sysplex monitoring eases management of complex system configurations and interactions and maximizes operations effectiveness. To help manage the increasing complexity of sysplexes, the NetView program automatically discovers all z/OS images in a sysplex and all IP stacks on each of those images, and displays a topology showing the relationships.

Problem Management

To improve your IT service management process, you can use the NetView browser interface to create incident records (trouble tickets) directly in the following service desk products:

- IBM Tivoli Information Management for z/OS and Web Access for Information Management product suite
- Peregrine ServiceCenter

Security

The NetView for z/OS program includes many provisions to ensure that only authorized personnel gain access to the product and its capabilities, and thereby to the networks, systems, and data it controls. These include user IDs and passwords; limitations on scope of authority; terminal access restrictions; authorization through an SAF product for commands, views and data sets; and other mechanisms.

Beginning with z/OS version 1.7, RACF® supports mixed-case passwords. To support that capability and to reduce the already remote likelihood of a successful random logon attempt, the NetView program also accepts mixed-case passwords. If the RACF mixed-case password function is active, and passwords are defined in mixed case, the NetView program leaves them unchanged. Otherwise, NetView passwords are converted to uppercase. This processing applies to all password handling.

NetView for z/OS Components

The NetView program provides a comprehensive set of management functions from a z/OS host and several graphical interfaces. For the mainframe components, see Figure 5. For the distributed components and the NetView operating environment, including other programs that work with the NetView program, see Figure 6 on page 14.

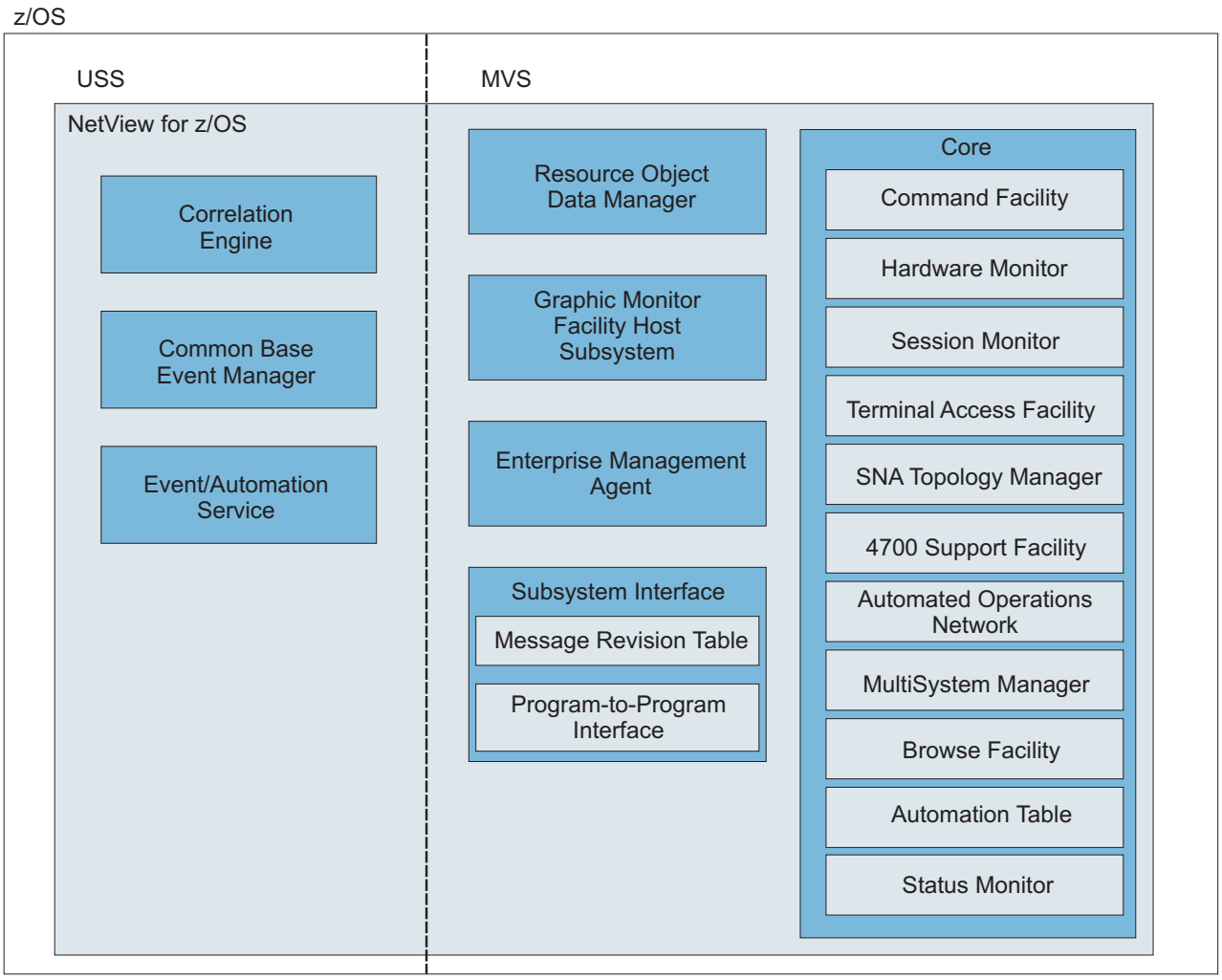


Figure 5. NetView Mainframe Components

Core Components

The core NetView components run under the MVS element in a z/OS system.

Command Facility

The command facility is used to send commands and receive messages. It also provides base functions and services for other components, such as intercomponent communication, presentation services, database services, and automation facilities.

Hardware Monitor

The hardware monitor component collects and displays events and statistical data for both hardware and software to identify failing resources in a network. It provides probable cause and recommended actions that operators can use to perform problem determination more efficiently.

Session Monitor

The session monitor component provides information about SNA sessions (subarea and Advanced Peer-to-Peer Networking) including session partner identification, session status, connectivity of active sessions, and response time data. The session monitor also provides session trace data, route data, and Virtual Telecommunications Access Method (VTAM®) sense code information for problem determination. It can display all SNA sessions across an Enterprise Extender connection.

Terminal Access Facility

The terminal access facility (TAF) provides operator control of any combination of CICS®, IMS™, TSO, and other subsystems from one terminal. The operator does not have to log off or use a separate terminal for each subsystem. The subsystem can be in the same domain or in another domain.

The two types of TAF sessions are operator-control sessions and full-screen sessions. In operator-control sessions, TAF acts like an LU type-1 terminal; that is, any transaction that can be entered from a 3767 terminal attached directly to one of these subsystems can also be entered from the command facility panel. Operator-control sessions are also called 3767-type sessions or LU1 sessions.

In full-screen sessions, TAF acts like an LU type-2 terminal. TAF lets full-screen applications operating on these subsystems use a NetView panel. The NetView operator can also enter commands and data as if the terminal is directly connected to the subsystem. Full-screen sessions are also called 3270-type sessions or LU2 sessions.

SNA Topology Manager

The SNA topology manager dynamically collects topology and status of Advanced Peer-to-Peer Networking and subarea resources. This data is stored in RODM for display by the NetView management console.

The topology agent supplies information consisting of the SNA nodes in a network, the Advanced Peer-to-Peer Networking transmission groups (TGs) between them, and the underlying logical links and ports supporting the TGs, in response to requests from the manager application.

4700 Support Facility

The 4700 Support Facility provides information about and management of the 47xx Finance Communications Systems.

Automated Operations Network

Automated Operations Network (AON) uses NetView automation facilities to automate the monitoring and recovery of both TCP/IP and SNA network resources. AON can monitor messages and alerts, and then automatically perform

recovery actions. AON also provides an automated help desk to assist with resolving network problem, and generates reports so that you can monitor how well your automation is working.

AON provides default policy definitions that enable automation, without lengthy configuration, as soon as AON is enabled.

For more information about using AON, see the *IBM Tivoli NetView for z/OS Automated Operations Network User's Guide*.

MultiSystem Manager

MultiSystem Manager provides for the management of distributed resources from the NetView program. The NetView operator can use MultiSystem Manager to view and manage resources that are identified and managed locally by products such as Tivoli NetView and the Tivoli framework. The topology and status of these resources are dynamically managed through RODM and the graphical workstation components of the NetView program. See the *IBM Tivoli NetView for z/OS MultiSystem Manager User's Guide* for more detailed information.

Browse Facility

The browse facility is used to view local or remote NetView data set members including the NetView log, NetView parameter files, and NetView panels.

Automation Table

With the NetView automation table, you can specify processing options for incoming messages and MSUs and issue automatic responses. The table contains a sequence of statements that define the actions that the NetView program can take in various circumstances. The automation table is one of several components that provide automation capabilities; for more information about automation, see "Automation" on page 6.

Status Monitor

The status monitor component provides status information about SNA subarea network resources.

Resource Object Data Manager

Resource Object Data Manager (RODM) is an object-oriented data cache. Objects in RODM can represent resources in your network. The data cache is located entirely in the memory of the host processor for fast access to data and high transaction rates. RODM can contain approximately 2 million objects, providing support for large and growing networks.

The MultiSystem Manager and SNA topology manager components of the NetView program populate RODM with information such as topology and status about resources they monitor, and maintain that information as changes occur. Using data in RODM, the Graphic Monitor Facility host subsystem component dynamically builds graphical views for display by the NetView management console. When the topology or status changes in RODM, methods automatically update the views that include the affected resources.

Additionally, authorized operators can use the RODMView command to display, create, update, and delete classes, objects, fields, and relationships in RODM.

RODM also provides application programming interfaces (APIs) that can be used by any application running in the host processor. A user API allows a properly authorized address space to access the data contained in the RODM address space

and data spaces. Through this user API, objects can be created, organized into hierarchies, or deleted. The user API can also query the value of a field associated with an object or alter the value in that field. It can be called from NetView command processors and from applications written in any programming language that meets the parameter passing conventions of RODM. A method API enables methods that reside in the RODM address space to be called by user applications, by changes to fields in RODM, by other methods, and at RODM initialization.

Graphic Monitor Facility Host Subsystem

The NetView Graphic Monitor Facility host subsystem (GMFHS) component supplies the NetView management console with views and information about RODM resources. It works with RODM and the NetView management console to display graphical views of networks and to route commands to resources that you select from a NetView management console view.

IBM Tivoli NetView for z/OS Enterprise Management Agent

The IBM Tivoli NetView for z/OS Enterprise Management Agent enables management of your network from the Tivoli Enterprise Portal using sampled and real-time data. The sampled data can provide information about network resources and outages, using situations and expert advice. It can also indicate trends in your network when historical data is used. Additionally, NetView, VTAM, and z/OS commands can be issued directly from the Tivoli Enterprise Portal to provide instant display and troubleshooting capabilities. The NetView for z/OS Enterprise Management Agent enables management of both availability and performance data from the Tivoli Enterprise Portal using cross-product links to selected z/OS OMEGAMON XE V4.1.0 agents.

Subsystem Interface

The subsystem interface is used to receive system messages and enter system commands. With extended multiple console support (EMCS) consoles, the subsystem interface is used to receive commands, but not messages. In a single system, multiple NetView programs can use the subsystem interface. Each NetView program that uses the subsystem interface requires a NetView subsystem address space in addition to the NetView application address space.

Using the subsystem interface is optional. If you do not need to use the PPI, receive system messages, or enter system commands from a NetView program, then that NetView program does not need to use the subsystem interface.

Message Revision Table

You can use the message revision table to intercept z/OS messages before they are displayed, logged, automated, or routed through your sysplex. With this table, you can make decisions about a message based on its message ID, job name, and other properties and can revise or suppress a message or take certain actions. The message revision table is one of several components that provide automation capabilities. For more information about the message revision table and about automation, see “Automation” on page 6.

Program-to-Program Interface

The program-to-program interface (PPI) enables application programs to communicate with the NetView program and other applications running in the same host. When an application calls the PPI using its application program interface (API), the request is synchronous.

For more information about the PPI , see the *IBM Tivoli NetView for z/OS Application Programmer's Guide*.

Correlation Engine

The correlation engine correlates multiple events over time, based on duplicates, thresholds, presence or absence of specific events, and other user-specified criteria. The correlation engine is one of several components that provide automation capabilities. For more information about automation, see "Automation" on page 6.

Common Base Event Manager

Events based on the Common Base Event specification are used with the Common Event Infrastructure to automate activities. The Common Event Infrastructure is an IBM component technology that is used to manage events, providing a server to store generated Common Base Events and forward them as needed.

The common base event manager serves as the intermediary between the NetView program running under z/OS and a WebSphere® Application Server client that interacts with the Common Event Infrastructure server. It receives Common Base Events from the client and forwards them to the NetView program to be automated. It receives Common Base Events created by the NetView program from messages and MSUs and sends them to the correlation engine.

When appropriate (for example, when correlation is being bypassed or correlation rules require submitting the event to the Common Base Event database), the common base event manager sends a Common Base Event to the WebSphere Application Server client, which submits the event to the database. The common base event manager accepts connections from any number of clients for forwarding Common Base Events to the NetView program. For additional information about automating using Common Base Events, see the *IBM Tivoli NetView for z/OS Automation Guide*.

Event/Automation Service

The Event/Automation Service (E/AS) serves as a gateway for event data between the NetView for z/OS management environment, Tivoli management regions, and SNMP managers and agents. With this gateway function, you can manage all network events from the management platform of your choice.

If you manage network events using the Tivoli Enterprise Console program, the E/AS can convert NetView for z/OS alerts and messages into Tivoli Enterprise Console events before forwarding the event data to a Tivoli Enterprise Console server in the Tivoli management region. For more information about the Tivoli Enterprise Console program, see the *Tivoli Enterprise Console User's Guide*.

If you choose to manage events at the NetView program, the E/AS can convert Tivoli Enterprise Console events from a Tivoli management region into alerts before forwarding the alerts to the NetView for z/OS program through the Alert Receiver PPI mailbox.

The E/AS can convert SNMP traps from SNMP managers into alerts before forwarding the alerts to the NetView for z/OS program through the Alert Receiver PPI mailbox. The E/AS also converts NetView for z/OS alerts into SNMP traps before forwarding the trap data to an SNMP manager. The E/AS performs the function of an SNMP subagent and sends the converted alert data to an SNMP

agent for eventual forwarding to an SNMP manager. Note that these functions are also available as base NetView services, independent of E/AS.

Integrated TCP/IP Services Component

The Integrated TCP/IP Services Component (ITSC), shown in Figure 6 on page 14, discovers TCP/IP resources, which are then managed using the MultiSystem Manager IP agent.

User Interfaces to the NetView for z/OS Program

Access to the NetView for z/OS program is provided by several user interfaces, which are described in this section. Distributed components are shown in Figure 6 on page 14.

Tivoli Enterprise Portal

Availability data from the NetView for z/OS program is correlated with performance data from OMEGAMON XE products in the Tivoli Enterprise Portal to provide consolidated console for managing availability and performance. For example, you can use this data to understand the performance impact of a network problem or to locate a resource causing a performance problem.

3270 Session

3270 sessions provide access to the core components and the command-line interface of the NetView for z/OS program.

NetView Management Console

The NetView management console, which consists of a client based on Java™ technology and a server, uses interactive graphics to display color-coded views that represent network resources being monitored. The views show the statuses of the resources and the relationships of the resources to each other. From the views, you can interactively control resources and see the status changes reflected in the view updates. For additional information about the NetView management console, see the *IBM Tivoli NetView for z/OS NetView Management Console User's Guide*.

Web Application

The NetView for z/OS Web application provides a browser interface to the NetView program. Use the NetView for z/OS Web application to manage your IP connections, view events, issue NetView commands, and more. For additional information about the Web application, see the *IBM Tivoli NetView for z/OS Web Application User's Guide*.

Help

NetView for z/OS mainframe online help is available for the following areas, depending on your installation and configuration:

- General help and component information
- Command help
- Message help
- Sense code information
- Recommended actions
- Help desk

The following types of online help are available in workstations running NetView for z/OS components, depending on your installation and configuration:

- Tivoli Enterprise Portal help
- Web application help
- NetView management console help

- NetView information center, which includes the NetView for z/OS online library

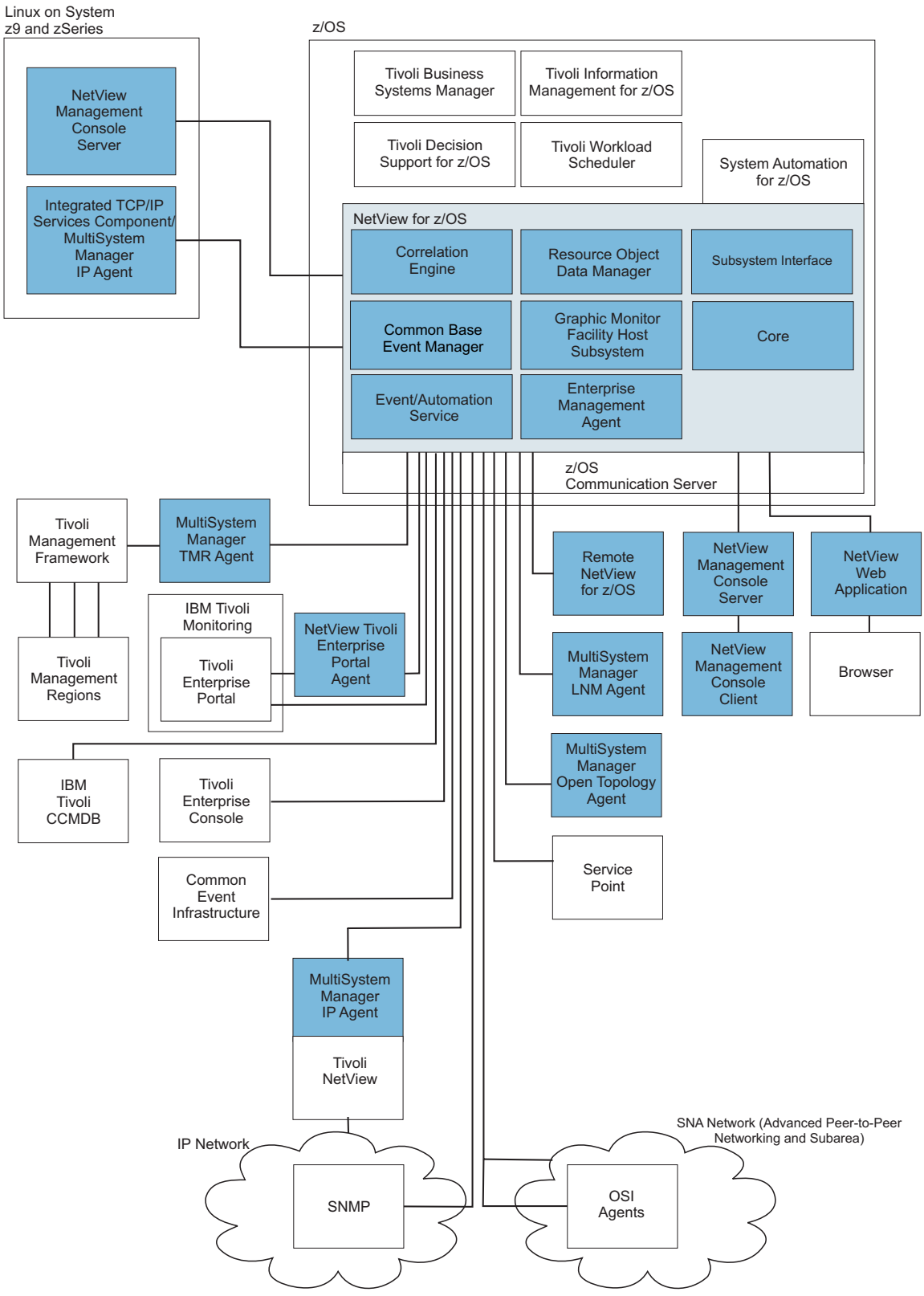


Figure 6. NetView Operating Environment. NetView components are shaded.

Programs That Interact with the NetView for z/OS Program

The NetView for z/OS program is the foundation for enterprise management, serving as the focal point for systems and distributed network managers. The NetView automation table and RODM provide a strong automation platform for managing systems, networks, workstations, and LANs.

Other products that work with the NetView program include the following programs:

- System Automation for z/OS. The NetView for z/OS program provides the automation services, graphic topology services, and other underlying services for System Automation for z/OS, which enables automated management of z/OS and OS/390 systems and applications.
- Tivoli NetView. The NetView for z/OS program can receive discovered TCP/IP resource topology from the Tivoli NetView program running on a Microsoft Windows, AIX, Solaris, HP-UX, or Linux system to show an enterprise-wide view of the network, track resource status, and issue commands to the discovered resources.
- Tivoli Enterprise Console. The NetView for z/OS program can forward collected z/OS management information to other management applications. For example, z/OS messages and events can be sent to the Tivoli Enterprise Console program as events for end-to-end correlation, action, and display.
- Tivoli Business Systems Manager. The NetView for z/OS program delivers management services to Tivoli Business Systems Manager for handling of z/OS and OS/390 subsystems such as the CICS, DB2®, and IMS subsystems.

Many other products complement the NetView for z/OS program to provide a comprehensive set of enterprise management functions. Figure 6 on page 14 shows a graphical representation of the NetView operating environment, including the distributed NetView for z/OS components and other products that can be used with the NetView for z/OS program. NetView for z/OS components are shaded. The other programs are described briefly in this section. For more information, see the documentation for these programs.

z/OS Operating System

The z/OS operating system is a widely used mainframe operating system. It offers a stable, secure, and continuously available environment for applications running on the mainframe. The z/OS operating system of today is the result of decades of technological advancement, having evolved from an operating system that could process a single program at a time to an operating system that can handle many thousands of programs and interactive users concurrently.

MVS

MVS services and functions are provided by the Base Control Program (BCP), a base element and the backbone of the z/OS system. These essential services enable reliable, secure workload processing with complete data integrity and without interruption.

UNIX System Services

The NetView for z/OS program uses UNIX System Services for the following functions:

- UNIX command server
- AON/TCP functions
- Event/Automation Service

- Event correlation and, optionally, the Common Event Infrastructure interface

NetView operators or programs can interact with z/OS UNIX System Services in the following ways:

- The PIPE UNIX stage, which transfers a command to a UNIX command server where the command is to be processed and from which the results are returned.
- The IPCMD command, which provides a generic API for processing any IP command in a UNIX or TSO environment. The command is issued from the NetView program and correlated responses are returned to the user.
- The UNIX command server, which enables UNIX commands to be entered from the NetView command line and command output to be returned to the NetView console. Running UNIX for z/OS commands from the NetView program requires a dedicated PPI receiver (CNMEUNIX) to receive commands and data from the NetView program. A server process running in a UNIX System Services address space waits on this PPI receiver for incoming commands and data.

z/OS Communication Server

z/OS Communications Server, which is a component of the z/OS operating system, implements the SNA and TCP/IP protocols. SNA applications and transaction servers (such as CICS) can use SNA or TCP/IP to send and receive data. Industry-standard internet applications can use TCP/IP to send and receive data. z/OS Communications Server provides a set of communications protocols that support connectivity functions for both local- and wide-area networks, including the Internet.

z/OS Communications Server includes the following major components:

- The TCP/IP protocol stack. NetView operators or programs can interact with z/OS Communication Server IP using the NetView TSO and UNIX PIPE stages. z/OS Communication Server IP also supports several NetView functions, such as the Java client and the Web server. The IPCMD command can be used to issue any line-mode z/OS Communication Server IP command from the NetView program.
- The SNA protocol stack accessed through the Virtual Telecommunications Access Method (VTAM) API. The VTAM API provides communication facilities for the NetView for z/OS program and other applications. It provides status information and control facilities for SNA resources. It also provides the topology agent information for SNA resources, both subarea and Advanced Peer-to-Peer Networking.
- The communications storage manager, which provides a shared I/O buffer area for both TCP/IP and VTAM data flow. The communications storage manager allows authorized host applications to share data without having to physically move the data.

TSO

Operators, administrators, programmers, and others who access z/OS can use Time Sharing Option/Extensions (TSO/E or simply TSO) to create an interactive session with the z/OS system. TSO provides a single-user logon capability and a basic command prompt interface to the z/OS operating system.

Most users work with TSO through the menu-driven interface, Interactive System Productivity Facility (ISPF). This collection of menus and panels offers a wide range of functions to assist users in working with data files on the system.

NetView operators or programs can interact with TSO using the NetView TSO PIPE stage. For more information, see the help for PIPE TSO.

Linux on the IBM System z Platform

Linux on the IBM System z platform combines the scalability and reliability of IBM mainframe systems with the flexibility and open standards of the Linux operating systems. It can provide an environment for efficient and effective infrastructure simplification, application deployment and business integration.

System Automation for z/OS

System Automation for z/OS is a comprehensive automation product for z/OS applications. It centralizes operations such as initial microcode load (IML), initial program load (IPL), automation of system resources, and reconfiguring local or remote target systems, of z/OS processors and operating systems. With this platform, an operator at a focal point host can control and monitor multiple target systems such as z/OS, VM, VSE, and TPF systems, concurrently.

System Operations

The system operations component provides comprehensive, out-of-the-box automation for the CICS, IMS, DB2, Tivoli Workload Scheduler, and SAP R/3 products. It automates many system console operations and selected operator tasks, such as startup, monitoring, recovery, and shutdown of z/OS and OS/390 subsystems, components, applications, UNIX System Services (USS) and sysplex resources. This component also provides the ability to automate operator console messages, initiate timer-based actions, and prevent critical z/OS resource shortages, such as Write To Operator (WTO) buffers, log, and spool.

Processor Operations

The processor operations component centralizes operations of System z processors and operating systems, such as initial microcode load (IML), recycling operating systems (IPL), automation, and reconfiguring local or remote target systems. The processor operations component is used to start or stop systems; the system operations component is used to manage applications that run on the systems that the processor operations component starts or stops.

With the processor operations component, an operator at a focal point host can control and monitor multiple target systems, such as z/VM, VSE, TPF, and Linux, concurrently. In a parallel sysplex environment, the processor operations component supports the coupling facility at a target system, both with coupling links and with the Integrated Coupling Migration Facility.

The processor operations component provides built-in automation that can be extended by user-written automation routines and by its integration with the system operations component on the operator views of the System Automation for z/OS graphical interface.

I/O Operations

I/O operations inherits and enhances the functions of ESCON® Manager. With I/O operations, you can make multisystem operational changes to channels, ESCON Directors, and devices while protecting access to critical system resources. I/O Operations provides NetView management console monitoring of I/O resource exceptions and text and multisystem graphical displays of active I/O configurations. I/O Operations also supports interaction with ESCON Manager at the level of function provided in that product.

Tivoli Business Systems Manager

IBM Tivoli Business Systems Manager is an enterprise management product that monitors the data processing resources that are critical to a business application.

Mission-critical business systems typically span host and distributed environments; include many interconnected application components, both commercial and custom; and rely on diverse middleware, databases, and supporting platforms.

Tivoli Business Systems Manager provides end-to-end business systems management to organize related components and give business context to management decisions. A unique, configurable business system view enables management and control of the multiple integrated software components required to deliver a specific business service. The product also shows and allows the manipulation of the relationships between applications, so that you can more easily detect inefficiencies or diagnose problems in critical business systems.

Tivoli Decision Support for z/OS

Tivoli Decision Support for z/OS provides a uniform way to collect and process performance data from multiple resources in the managed environment. This application provides performance data collection and reporting functions for z/OS or VM systems, IMS, CICS, networks, and more. Tivoli Decision Support for z/OS can control the selection and collection of data, provide predefined reports to present the data, and include documentation to help with performance analysis. Data provided by Tivoli Decision Support for z/OS can be used to fine tune the performance of the NetView for z/OS program.

Tivoli Information Management for z/OS

Tivoli Information Management for z/OS can record and maintain information for problems as they recur, and subsequently use this information to address problem areas before problems recur. Using the NetView for z/OS Web application, you can open incident records (problem tickets) directly in Tivoli Information Management.

Note: You can also use the NetView for z/OS Web application to open incident records directly in the Peregrine ServiceCenter.

Tivoli Workload Scheduler for z/OS

Tivoli Workload Scheduler for z/OS can be used to schedule and control workloads in any operating environment where communication with z/OS can be established. It increases the opportunities for centralized control of product workload across your environment. For example, you can use Tivoli Workload Scheduler with the NetView for z/OS program to schedule activities by business cycle or dependencies, control real resources, automatically report and respond to unusual workload conditions, or manage your disaster recovery plan.

Tivoli NetView

The Tivoli NetView program is a comprehensive management tool for heterogeneous, multivendor devices on TCP/IP networks. It uses the AIX NetView service point program to support non-SNA data flows between the NetView for z/OS program and any supported resource. This program also provides status of any type resource, such as non-IBM hardware and software, to be converted into an SNA format or into a format that is recognized by the NetView for z/OS program.

When used with the MultiSystem Manager IP agent, the MultiSystem Manager component of the NetView for z/OS program can gather topology and status information about the resources managed by the Tivoli NetView program. This information is then stored in RODM and can be displayed graphically using the NetView management console.

IBM Tivoli Enterprise Console

The IBM Tivoli Enterprise Console product is a rule-based event management application that integrates system, network, database, and application management to provide a centralized, global view of your computing enterprise. It collects, processes, and automatically responds to common management events, such as a database server that is not responding, a lost network connection, or a successfully completed batch processing job. It acts as a central collection point for alarms and events from a variety of sources, including those from other Tivoli software applications, Tivoli partner applications, custom applications, network management platforms, and relational database systems.

The Tivoli Enterprise Console product helps in processing the high volume of events in an IT environment by prioritizing, filtering, or correlating events; by determining who should view and process specific events; and by initiating automatic corrective actions, when appropriate.

IBM Tivoli Change and Configuration Management Database

The NetView for z/OS program extracts data about TCP/IP resources and relationships from the NetView for z/OS RODM data cache and sends the managed resource information to IBM Tivoli Change and Configuration Management Database (IBM Tivoli CCMDB) to be stored in the configuration management database (CMDB). Information about resources discovered by other providers in a TCP/IP network is also stored in the configuration management database. Operators and network analysts can use the correlated resource information in this database to solve outages and to improve configuration and change management.

Tivoli Management Regions

A Tivoli management region is a logical representation of a group of resources that share a common policy region and are managed by a single server. Policy regions are logical groups that are based on the shared characteristics of their members. For example, a region might be geographically based (all the systems in Detroit) or application-based (all the users of a set of software applications) or use some other common defining principle. Policy regions mask the operating system and hardware differences or resources when a management function is processing across Tivoli management regions.

The NetView hardware monitor component can display events related to Tivoli management region resources, and the Tivoli Enterprise Console can integrate information about resources managed by the NetView for z/OS program with information about Tivoli management region resources.

When used with the MultiSystem Manager Tivoli management region agent, the MultiSystem Manager component of the NetView for z/OS program can gather topology and status information about the resources managed by Tivoli management region. This information is then stored in RODM and can be displayed graphically using the NetView management console.

LAN Network Manager

With LAN Network Manager (LNM), you can manage multisegment IBM token-ring networks, broadband and baseband IBM PC networks, and IBM 8209 LAN Bridge that interconnects a token-ring segment and an Ethernet segment. You can manage your LAN centrally using the NetView for z/OS program or locally using the operator interface at the LAN workstation.

The MultiSystem Manager component of the NetView for z/OS program communicates with an agent in LNM to gather topology and status information about resources managed by LNM. MultiSystem Manager displays this information graphically using the NetView management console, and in a text format using the NetView 3270 interface. MultiSystem Manager can also correlate information from LNM with information provided by other MultiSystem Manager agents, such as IP, letting you view system information and network connectivity from a single interface.

MultiSystem Manager Open Topology Agents

Any customer-written or vendor-written manager-agent application that follows the rules established by the NetView for z/OS MultiSystem Manager component can be used to extend the management capability of MultiSystem Manager to resources not already supported. This includes storing them in RODM for display and management using the NetView management console.

Service Points

Any service point product that supports an architected data flow and can be monitored by the NetView for z/OS program can be used.

Open Systems Interconnection Agents

Open Systems Interconnect (OSI) is a standardized architecture that establishes a framework for interconnection of computer systems, based on the manager/agent model. OSI agents can perform management operations on managed objects and send notifications to a manager on behalf of those managed objects. An agent application provided by VTAM gathers topology information about SNA and Advanced Peer-to-Peer Networking resources.

What Are Network Management Tasks?

The tasks required to manage a complex network fall into the following categories:

- Learn the network management concepts
- Monitor and control the network and system
- Investigate and solve problems
- Control the NetView program

In a multiple-host environment, you can automate the NetView program so that many operation tasks are automatically performed in distributed hosts. Significant events that require intervention can be forwarded to a NetView operator at the focal point host. You can design systems so that little or no intervention is required at the distributed hosts.

Table 3 on page 21 describes these categories of tasks, and the remaining chapters of this book further divide these categories into subcategories and actual tasks that make up network management.

Note: For information about automating the NetView program, see the *IBM Tivoli NetView for z/OS Automation Guide*.

Table 3. Major NetView Tasks

Task	Task Description
Monitoring and Controlling the Network and System This management task is described in the following chapters: • Chapter 3, "Monitoring and Controlling Your Network from a Workstation," on page 45 • Chapter 4, "Monitoring and Controlling Your Network Using the IBM Tivoli NetView for z/OS Enterprise Management Agent," on page 51 • Chapter 5, "Monitoring and Controlling Network Configuration," on page 75 • Chapter 6, "Managing Network and System Status," on page 135 • Chapter 7, "Monitoring Hardware and Software Problems," on page 139 • Chapter 8, "Managing Network Inventory," on page 169 • Chapter 9, "Controlling Remote Processors," on page 173 • Chapter 10, "Controlling Operating System Resources," on page 183	Monitoring, controlling, and accounting are three major tasks of daily NetView operation. You monitor resources, control them to prevent or correct problems, and track network usage for billing purposes.*Monitoring* is the examination of the entire network and system for changes in the status of individual components from satisfactory to a status requiring attention. The NetView program achieves this through receipt of status changes, alerts, and messages, which are displayed for analysis. You can explicitly request this status information or the NetView program can present it automatically. You can control the amount of information collected, and you can request more information such as network and system definitions to help you analyze changes in status. *Controlling* is the taking of specific actions against individual network and system components to change their status from unsatisfactory to satisfactory. This includes controlling the configuration and definition of the resources. The NetView program provides controls to limit the functions you can use and the resources you can access. *Accounting* involves recording information about the length of sessions and the amounts of data processed for sessions, such as the amount of session data, the number of PIUs, and the number of bytes. This information can be used to charge end users for their use of network resources.
Controlling the NetView Environment This management task is described in the following chapters: • Chapter 11, "Maintaining the NetView Program," on page 193 • Chapter 12, "Controlling NetView Operation," on page 201 • Chapter 13, "Managing NetView Data," on page 217	*Controlling* the NetView program is the continual adjustment of the NetView environment to achieve the goals of monitoring, investigating, analyzing, and controlling of network and system components.
Automating the Network or System This management task is described in the following chapters: • Chapter 14, "Using the NetView Automation Table," on page 235 • Chapter 15, "Controlling Message Routing Using the ASSIGN Command," on page 245 • Chapter 16, "Starting an Autotask to Handle Automation," on page 247 • Chapter 17, "Scheduling Commands," on page 249 • Chapter 18, "Debugging Automation," on page 273	*Automating* is the understanding of a consistent relationship between an event and the normal reaction to that event, and storing a procedure to automatically recognize the event as well as taking appropriate action. One way of doing this is through analysis of messages and alerts, and the operator actions taken in response to them.

Table 3. Major NetView Tasks (continued)

Task	Task Description
Diagnosing Problems This management task is described in the following chapters: • Chapter 19, "Proactive Investigating," on page 287 • Chapter 20, "Reactive Investigating," on page 299 • Chapter 21, "Managing Problems," on page 333	*Investigating* is the requesting of additional information so that you can further analyze the cause of a status change from satisfactory to unsatisfactory. This can involve requesting more detailed status information or initiating a test on a failing resource. *Solving* is completing the analysis of the problem situation and deciding on the proper action to bypass or resolve the unsatisfactory condition. This can also include logging the problem and its resolution to make future analysis of similar problems more efficient.

Chapter 2. Getting Started

This chapter describes how to get started using the IBM Tivoli NetView for z/OS program and briefly describes the NetView for z/OS interfaces and functions. It also provides an overview of the types of online information available.

Starting the NetView Program

The NetView host environment consists of the following MVS address spaces:

- NetView program
- NetView subsystem
- Resource Object Data Manager (RODM)
- Graphic Monitor Facility host subsystem (GMFHS)
- Event/Automation Service (E/AS)
- NetView for z/OS Enterprise Management Agent

To start the address spaces manually, enter the following commands from the system console:

- To start the NetView program, enter the following command:

  ```
  s procname
  ```

  Where *procname* is the name that your system programmer assigned to the cataloged procedure for the NetView program, such as CNMPROC. When the NetView program starts, certain functions can be specified to start automatically. See Chapter 12, "Controlling NetView Operation," on page 201 for more information.
- To start the NetView subsystem, enter the following command:

  ```
  s procname
  ```

  Where *procname* is the name that your system programmer assigned to the cataloged procedure for the NetView subsystem, such as CNMPSSI.
- To start the Event/Automation Service, enter the following command:

  ```
  s procname
  ```

  Where *procname* is the name your system programmer assigned to the cataloged procedure for the Event/Automation Service, such as IHSAEVNT. The Event/Automation Service depends on the following programs being active:
  - TCP/IP
  - NetView subsystem
- The RODM program can be started with, or without, using the checkpoint data set. Use the *procname* that your system programmer assigned to the cataloged procedure for the RODM program, such as EKGXRODM.
  - To cold-start the RODM program, without using the checkpoint data set, enter the following command:

    ```
    s procname,type=c,name=rodmname
    ```

    Where *rodmname* is the name of the RODM program to be started. If you do not enter a value for *rodmname*, the NetView program defaults to *procname*.

    You get the following message requesting confirmation not to use the checkpoint data sets:

```
EKG1918D  EKGXRODM: RODM rodm WILL COLD START.
          ENTER '1' TO CONTINUE OR '2' TO TERMINATE.
```

Enter 1 to cold-start RODM. The first time you start RODM for NetView V3 or later, specify `TYPE=C` to cold start RODM.

– To warm-start the RODM program, using the latest checkpoint data set, enter the following command:

```
s procname,type=w
```

This is the default for the NetView-supplied RODM procedure (if you do not specify `TYPE=C`).

See "Copying the Contents of RODM to a Checkpoint Data Set" on page 231 for information about how to copy the data from the RODM data cache to a checkpoint data set.

- To start the GMFHS program, enter the following command:

```
s procname.id
```

- To start the NetView for z/OS Enterprise Management Agent, enter the following command:

```
s procname
```

Where *procname* is the name that your system programmer assigned in the **Agent started task** field on the Specify Agent Address Space Parameters panel in the Configuration Tool during agent configuration.

Replying to a Message

If the DSIWTOMT task is started, the NetView program issues a write-to-operator with reply (WTOR) message to the system console when initialization is complete. This WTOR message is outstanding while the NetView program is active. The message ID is either DSI802A or DSI803A. You can use the REPLY command to issue NetView commands from the system console. For example, if you see the following WTOR message on your system console:

```
*07 DSI802A CNM01 REPLY WITH VALID NCCF SYSTEM OPERATOR COMMAND
```

You can enter the following command:

```
r 07,command
```

Where *command* is any of the following commands:

- CLOSE DUMP
- CLOSE IMMED
- CLOSE NORMAL
- CLOSE STOP
- MSG *operid*,*text*
- MSG LOG,*text*
- MSG SYSOP,*text*
- MSG ALL,*text*
- REPLY P*nn*,*text*
- REPLY L*nn*,*text*

Stopping NetView

To stop the NetView address spaces, enter the following commands from the system console:

- To stop the NetView program, enter the following command:

```
p procname
```

Where *procname* is the name that your system programmer assigned to the cataloged procedure for the NetView program, such as CNMNETV.

You can also stop the NetView program by replying to the NetView outstanding WTOR in the following way:

```
r nn,close
```

Where *nn* is the reply identifier for the WTOR message DSI802A or DSI803A. This stops the NetView program after all operators have logged off. If you do not want to wait for all operators to log off, use the CLOSE STOP command.

- To stop the NetView subsystem, enter the following command:

  ```
  p procname
  ```

  Where *procname* is the name that your system programmer assigned to the cataloged procedure for the NetView subsystem, such as CNMPSSI.
- To stop the Event/Automation Service, enter one of the following commands:

  ```
  f procname,term
  p procname
  ```

  Where *procname* is the name your system programmer assigned to the cataloged procedure for Event/Automation Service such as IHSAEVNT.
- To stop the RODM program, enter the following command:

  ```
  f procname,term
  ```

  Where *procname* is the name that your system programmer assigned to the cataloged procedure for the RODM program, such as EKGXRODM.
- To stop the GMFHS program, enter one of the following commands:

  ```
  f procname,term
  p procname
  ```

  Where *procname* is the name that your system programmer assigned to the cataloged procedure for the GMFHS program, such CNMGMFHS.
- To stop the NetView for z/OS Enterprise Management Agent, enter the following command:

  ```
  p procname
  ```

  Where *procname* is the name that your system programmer assigned in the **Agent started task** field on the Specify Agent Address Space Parameters panel in the Configuration Tool during agent configuration.

Issuing a NetView Command from MVS

If you have an autotask associated with the system console, you can enter NetView commands from the console using the following MVS MODIFY command:

```
f procname,command
```

Where *procname* is the name that your system programmer assigned to the cataloged procedure for the NetView program, such as CNMNETV, and *command* is the NetView command you want to issue. For example, to display the MVS console names and IDs used by the NetView program, enter the following command:

```
f procname,disconid
```

When the NetView subsystem is active, you can also enter NetView commands by prefixing the command with a designator that identifies the command as belonging to the NetView program. The default command designator is the 4-character subsystem name. For example, if job T130TEST is the NetView subsystem address space job, the designator is T130. To display the MVS console names and IDs used by the NetView program, enter the following command:

```
t130 disconid
```

You can register the command designator with the MVS system on which the subsystem address space job runs or you can register the prefix for the entire sysplex. This is done when you start the NetView subsystem address space.

Note: If you use the MVS MODIFY command, a designator character for the NetView program is not required.

Topic:	Reference:
CNMSJ009 and CNMSJ010 (NetView start procedure)	*IBM Tivoli NetView for z/OS Installation: Getting Started*
NetView commands	NetView online help
Associating an autotask with an MVS console	AUTOTASK command in the NetView online help
NetView cataloged procedures	*IBM Tivoli NetView for z/OS Installation: Getting Started*
Activating VTAM, NetView, SSI, RODM, and GMFHS	*IBM Tivoli NetView for z/OS Installation: Getting Started*

Using NetView from a 3270 Session

This section describes the following topics:

- How to log on to the NetView program
- The parts of a NetView panel
- How to move between the NetView components
- How to issue commands
- How to list your program function key definitions
- How to control the NetView screen

Logging on to NetView from a 3270 Session

To log on to the NetView program from a 3270 session:

1. To establish a session with the NetView program, enter the following command:

   ```
   logon applid(applid) logmode(logmode) data(data)
   ```

   Where *applid* is the name of the NetView application to which you are logging on. LOGMODE and DATA are optional parameters, where *logmode* specifies information about your terminal session, and *data* specifies information that is inserted in the `OPERATOR ID` and `PASSWORD` fields of the NetView logon panel. The password is accepted only on the VTAM LOGON command when the NetView program has enabled the function through the LOGONPW command. In this case *data* is entered in the form *userid/password*.

   When you log on, the NetView program queries the device for screen size and color attributes if the logmode specifies to issue the query. Otherwise, the NetView program uses the screen size specified in the logmode. The command facility adapts to use the entire width and depth of the screen. The

hardware monitor and session monitor adapt to use the screen depth, but limit the display to 80 characters in width. All components of the NetView program support color where the display is capable of displaying color.

When a session is established, a NetView logon panel similar to the one shown in Figure 7 is displayed.

```
 NN    NN                     VV         VV
 NNN   NN   EEEEEE  TTTTTTTT  VV       VV   II   EEEEEE  WW         WW  TM
 NNNN  NN   EE         TT      VV     VV    II   EE      WW    W    WW
 NN NN NN   EEEE       TT       VV   VV     II   EEEE     WW  WWW  WW
 NN  NNNN   EE         TT        VV VV      II   EE        WWWW WWWW
 NN   NNN   EEEEEE     TT         VVV       II   EEEEEE     WW   WW
 NN    NN                        V

 5697-ENV (C) Copyright IBM Corp. 1986,2007 - All Rights Reserved
U.S. Government users restricted rights - Use, duplication, or disclosure
      restricted by GSA ADP schedule contract with IBM corporation.
         Licensed materials - Property of Tivoli Systems.
 Domain = NTVE1                     Tivoli NetView V5R3

        OPERATOR ID ==>             or LOGOFF
           PASSWORD ==>
            PROFILE ==>             Profile name, blank=default
       HARDCOPY LOG ==>             device name, or NO, default=NO
RUN INITIAL COMMAND ==>             YES or NO, default=YES
   Takeover session ==>             YES, NO, or FORCE, default=NO



       Enter logon information or PF3/PF15 to logoff
```

Figure 7. Example of NetView Logon Panel

Note:

- NetView provides the option of specifying whether password checking is performed by NetView or by an SAF security product such as RACF. The method of checking is specified by the SECOPTS.OPERSEC setting, described in the *IBM Tivoli NetView for z/OS Administration Reference*. If you specified in that setting that password checking is to be performed by NetView, be aware that any password defined to NetView is automatically converted to uppercase and stored in uppercase. If you specified that password checking is to be performed by using an SAF security product, you can use the mixed-case password function that is available in z/OS version 1.7.
- If the NetView program is using a system authorization facility (SAF) product to define its operators (OPERSEC=SAFDEF) or passwords (OPERSEC=SAFPW or OPERSEC=SAFCHECK), your logon panel is slightly different.
- In the PROFILE ==> field, system symbolic substitution is performed on records read from the DSIOPF member in the DSIPARM data set and the specified profile member in the DSIPRF data set. The NetView-supplied symbolic is also included in the substitution process. The substitution is performed after comment removal but prior to record processing. After substitution, comments are also removed. Substitution is always performed on the symbolic, unless substitution was disabled when NetView was started. For MVS and

user-defined system symbolics, substitution is performed only when your MVS system is running MVS Version 5 Release 2 or later.

2. Type your operator identification (for example, OPER1) in the space next to the OPERATOR ID field, where the cursor is located. If you specified a DATA parameter when you established the session, the OPERATOR ID field contains the value you specified.

   Blanks entered in the NetView logon fields are treated as null characters. For example, OPER 1 entered in the OPERATOR ID field of the NetView logon screen is treated as OPER1 because the blank between "R" and "1" is treated as a null character.

3. Enter your password. You do not see your password on the screen as you type it. If you are using a system authorization facility (SAF) security product, such as Resource Access Control Facility (RACF), and want to change your password, leave this field blank.

   If you are using OPERSEC=SAFDEF, you can log on to the NetView program using a PassTicket rather than a password if you use the Network Security Program/Secure Logon Coordinator product (NetSP/SLC V1.2) with an SAF product which supports PassTickets, such as RACF Version 2 Release 1.

4. If operators are defined in NetView profiles, and you must specify a profile at logon, move to the PROFILE field and type the information you were given. The profile defines operator attributes, such as which commands you have authorization to use and which resources you can control.

   If operators are defined in an SAF product, you cannot enter a profile value because no PROFILE field is displayed. Instead, the operator attributes are specified in the NETVIEW segment of the SAF product.

5. If you are using a printer (also called a hardcopy log device) to record your session, you can also type the name of the printer in the HARDCOPY LOG field.

6. If you do not want to use an initial command, type no in the RUN INITIAL COMMAND field. If you want to use an initial command, leave this field blank or type yes. The initial command is set up by your system programmer to eliminate some manual procedures.

7. If the operator ID is already logged on and you want to take over the session, enter YES as the takeover value. If you receive message DSI045I indicating that takeover is blocked, and if you log on to NetView via VTAM, you can enter FORCE as the takeover value. When FORCE is entered, NetView always tries to take over the session without abnormally ending the operator first. If that fails, NetView issues a user abend X'101'. If that also fails also, NetView issues a STOP FORCE on the operator ID and continues the logon processing. As a result of the STOP FORCE, the operator ID takes an X'EC4' abend. Storage and other resources might be lost. Data sets can be corrupted.

8. Press Enter.

   If you left the PASSWORD field blank and the NetView program is using an SAF product such as RACF to check passwords, the panel shown in Figure 8 on page 29 is displayed.

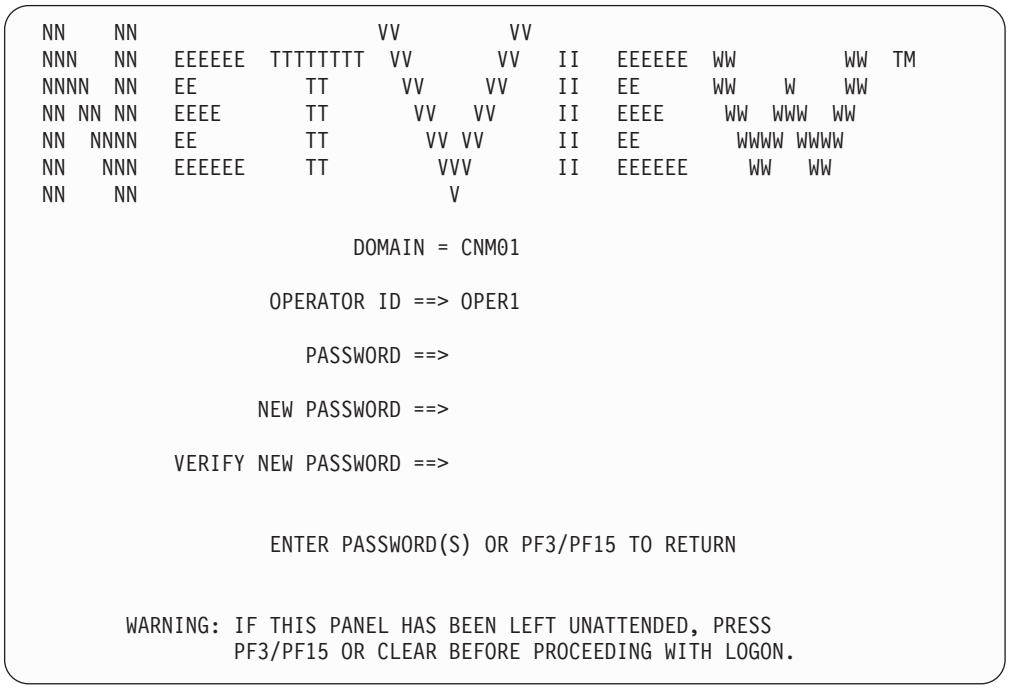


Figure 8. New Password Panel

9. Fill in the fields as appropriate. If an operator tries to change a password, but the logon attempt is not successful because of a bad parameter and the password is valid, then the password is changed and message DSI757 is sent to the NetView log, but the operator is not logged on.

   For example, if the operator specifies values for profile, HCL, or INITCMD that are not valid, even if the password change is valid, the operator is not logged on, and does not receive a message at the console. However, at the next logon attempt, the operator needs to use the new password. For security reasons, do not leave your display unattended while this panel is active. If you have any question about what was entered in the non-displayed fields, press either CLEAR or PF3/PF15 before proceeding.
10. Press Enter. A panel similar to Figure 9 on page 30 is displayed.

```
NetView V5R3             Tivoli NetView   NTVE1 OPER4    04/22/07 10:05:45
- NTVE1    DSI020I OPERATOR OPER4 LOGGED ON FROM TERMINAL NTE1L704 USING
           PROFILE (DSIPROFA ), HCL ( )
- NTVE1    DSI083I AUTOWRAP STOPPED
C NTVE1    CNM357I PFKDEF : PF KEY SETTINGS NOW ESTABLISHED. 'DISPFK' TO SEE
           YOUR PF KEY SETTINGS
| NTVE1

    Enter LOG  or LOGOFF to terminate session.
    Enter HELP to obtain help.
    Lead operator has been notified of your logon.
    To obtain help from the NETWORK CONTROL CENTER, enter

        MSG PPT, your question here

| NTVE1
News for April 22, 2007

   Tivoli NetView for z/OS V5R3 contains the following enhancements and
   more.  For additional NetView information, point your browser to
   http://www.ibm.com/software/tivoli/products/netview-zos/

??? ***
```

Figure 9. NetView News Panel

11. Press the **Clear** or **Enter** key to clear the screen and go to the NetView Main Menu. After the NetView program processes the operator profile, the following panel is displayed.

```
 CNM1NETV          Tivoli NetView for z/OS Version 5 Release 3         Main Menu

                   Operator ID = OPER4     Application = NTVE1030

    Enter a command (shown highlighted or in white) and press Enter.

        Browse Facility                BROWSE command
        Command Facility               NCCF command
        News                           NEWS command
        PF Key Settings                DISPFK command
        Help Facility                  HELP command
        Index of help topics           INDEX command
        Help Desk                      HELPDESK command
        Hardware Monitor               NPDA command
        Session Monitor                NLDM command
        Automated Operations Network   AON command




        To log off or disconnect       LOGOFF command or DISC command

 TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
 Action===>
```

Figure 10. NetView Main Menu

If the NetView Main Menu panel is not displayed:

a. Press **Enter** to access the command facility screen.
b. Type `mainmenu`.
c. Press **Enter**.

The NetView Main Menu automatically recognizes whether an option on the menu is active or inactive. The NetView Main Menu displays only active options. For example, if the Automated Operations Network and System Automation for z/OS are not active, those options are not displayed on the menu.

If a command on the NetView Main Menu is backlit, it is only partially available. That means that some functions are available using the command, but not all functions. For example, if the BROWSE command is backlit, only partial use of the command is available. You can use the BROWSE *member* command, but not the BROWSE NETLOGA command.

The panel in Figure 11 shows these examples. However, the size of the white space and the backlit commands in the menu might vary. If the status of an option changes, you can update the Main Menu by pressing Enter.

```
CNM1NETV          Tivoli NetView for z/OS Version 5 Release 3         Main Menu

                  Operator ID = OPER4     Application = NTVE1030

   Enter a command (shown highlighted or in white) and press Enter.

       Browse Facility                 BROWSE command
       Command Facility                NCCF command
       News                            NEWS command
       PF Key Settings                 DISPFK command
       Help Facility                   HELP command
       Index of help topics            INDEX command
       Help Desk                       HELPDESK command
       Hardware Monitor                NPDA command
       Session Monitor                 NLDM command
       Automated Operations Network    AON command




       To log off or disconnect        LOGOFF command or DISC command

TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
Action===>
```

Figure 11. NetView Main Menu

Understanding the Panel Layout

Type `nccf` and Press **Enter** to access the command facility.

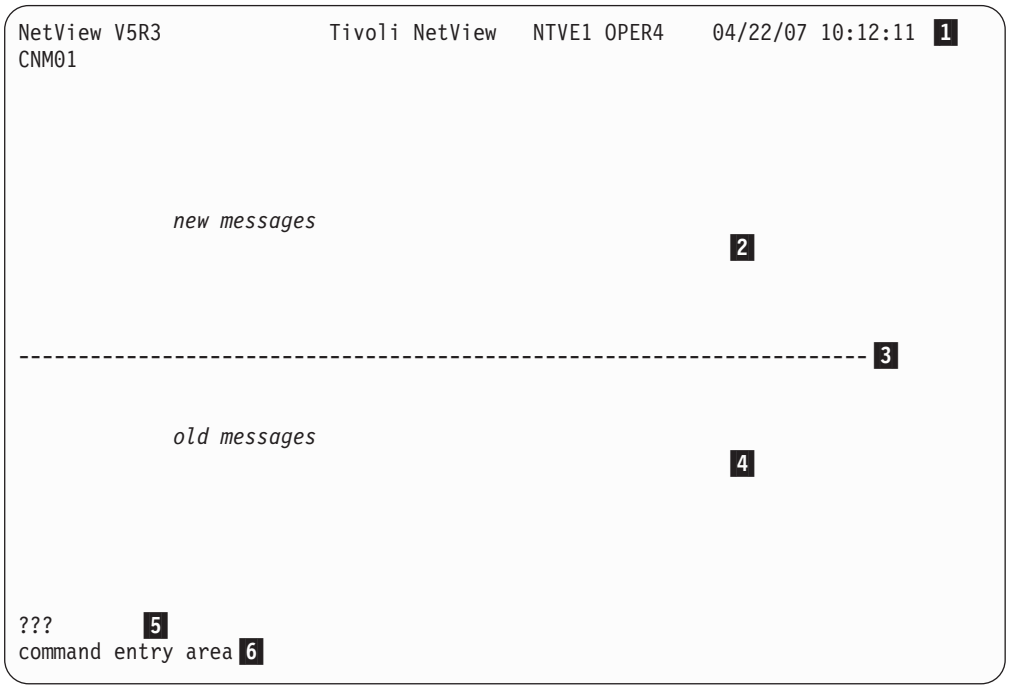


Figure 12. Sample Command Facility Console

You can customize this panel for your needs.For additional information about changing the format of the NetView panel, see sample CNMSCNFT and "Changing the NetView Screen Layout" on page 207.

Session Identification Line

The first line of the panel, identified with 1 , shows the name of the panel and the name of the system (NetView). The next field lists the application identifier (CNM01) and your operator identifier (OPER1). The next two fields list the current date and time. The last two fields contain a combination of A, H, P, W, or a blank, which indicates whether messages can be written to the panel. The A, H, P, and W indicators are described in the following list:

A The autowrap indicator means that AUTOWRAP is active. If autowrap is on and the display is full of data, it is automatically overlaid with new data. If autowrap is not on, press the Clear or Enter key to allow new data to overlay the display screen.

H The held-screen indicator means that the screen does not roll forward unless it is unlocked by the operator. You can use this indicator if you need time to read the screen before it is erased, or to freeze the screen while you mark messages for deletion or enter a command.

P The pause status indicator. A command list running on the operator task is pausing for operator input and does not continue until the operator enters information.

W The wait indicator. A command list running on the operator task is waiting for messages or other events, such as for a specified amount of time to elapse.

Message Area

The message area displays commands, responses, and messages from the system. Figure 13 on page 33 shows a sample display screen.

```
NCCF                     Tivoli NetView       CNM01 OPER1    04/22/07 21:41:49
T ORIGIN   OPER/JOB
* CNM01    OPER1    D NET,ID=NCP98
  CNM01    OPER1    IST097I  DISPLAY  ACCEPTED
' CNM01    OPER1
IST075I  NAME = NCP98            , TYPE = PU T4/5
IST486I  STATUS= ACTIV     , DESIRED STATE= ACTIV
IST247I  LOAD/DUMP PROCEDURE STATUS = RESET                2
IST484I  SUBAREA =         98
IST391I  ADJ LINK STATION = 014-S   , LINE = 014-L   , NODE = NTC0VTAM
IST654I  I/O TRACE = OFF, BUFFER TRACE = OFF
IST077I  SIO = 00040374 CUA = 014
IST675I  VR =  0, TP =  2
IST314I  END
------------------------------------------------------------------------ 3
IST080I  J0032055 ACTIV      J0032057 ACTIV      J0032059 ACTIV 4
IST080I  J003205B ACTIV      J003205D ACTIV      J003205F ACTIV
IST080I  J0032061 ACTIV      J0032063 ACTIV      J0032065 ACTIV
IST080I  J0032067 ACTIV      J0032069 ACTIV      J003206B ACTIV
IST080I  J003206D ACTIV      A19CA01  ACTIV----E A19CA02  ACTIV----E
IST080I  A19CA03  ACTIV----E A19CA04  ACTIV----E
IST314I  END
???
```

Figure 13. Sample Display Screen

The dashed line, indicated by **3** separates the latest messages from the older ones. The messages are continually updated. You can use this line to locate the most recent messages. The most recent messages are the ones directly above the line, in the area indicated by **2** . The oldest messages displayed on the screen are at the bottom of the screen, below the line, in the area indicated by **4** .

You can use message suppression to limit the number of messages sent to the screen, as described in the *IBM Tivoli NetView for z/OS Automation Guide*. See Appendix A, "Message Format," on page 341 for additional information on message formats.

To rearrange the messages on the screen, press the Enter key. This redisplays the messages in sequential order and removes the dashed line. If you type a command and press Enter before you rearrange the messages on the screen, you might have to press Enter again to see the full response.

Generally, messages are no longer displayed as the screen scrolls. Examples of exceptions include reply messages, held messages, and windowed responses.

Reply messages are messages to which you need to reply before you delete them from the display screen. These messages are displayed in high intensity on your display screen with a P*number* or L*number* and the message number, where *number* is a 2- or 4-digit number. Unsolicited reply messages received on the system console remain outstanding even after a reply is given. Delete these messages manually using the MVS control (K) command.

Held messages are messages that are defined to be held on the screen. These messages are displayed in high intensity (or are otherwise highlighted) and are shown at the top of the message area. Specific action must be taken to remove them, such as the following actions:

- Specifically deleting them (by the operator)
- De-emphasizing them with a Delete Operator Messages (DOM) command

The DOM command causes messages to lose highlighting immediately. This means they can now scroll off the screen. If more messages are being held than can be displayed on your type of terminal, message DSI151I is displayed and the messages are queued. The queued messages are displayed only when existing ones are deleted.

To delete one or more held messages:

1. Move the cursor to the message line, using either the cursor keys or the TAB key.
2. To delete a single message, press Enter. The cursor returns to the command entry area.
3. To delete multiple messages, erase the first line of each message to be deleted (you can use the Erase EOF key) and press Enter. The cursor returns to the command entry area.

Attention: If an autowrap timeout occurs while you are typing over message text, that text might be moved or refreshed, thus destroying the typing that you did.

To avoid losing information from the command entry area, you can take either of the following actions:

- Turn autowrap off, using the AUTOWRAP NO command.
- Use the HOLD command.

Windowed responses are messages that are displayed in a scrollable window using the NetView WINDOW command. This prevents the message responses from being overwritten by subsequent messages; you can also navigate through the information using standard BROWSE commands. For a description of the behavior of windowed responses, refer to the WINDOW command in the NetView online help.

Response Area

Near the bottom of the screen is a line that begins with the `???` indicator. This line is the response area, indicated by **5** in Figure 12 on page 32. Look here for error messages.

The `=X=` indicator is displayed in place of the `???` indicator when messages are arriving (prior to entering or after leaving a panel). This indicator means that only a limited set of commands can be used. The following commands are some of the commands you can use:

- AUTOWRAP
- CLOSE
- GO
- HOLD
- LOGOFF
- RESET

Hint: In general, commands that are specified as TYPE=I or TYPE=B in CNMCMD can be used when the `=X=` indicator is displayed.

Most of these commands change how quickly new information is presented. If you enter any other command, you get message DSI596I, which reads `WAITING TO DISPLAY A PANEL, COMMAND NOT PROCESSED. HIT ENTER.`

Command Entry Area

The cursor is located in the command entry area, indicated by **6** in Figure 12 on page 32. You communicate with the NetView program by entering commands here or you can call another NetView component. If you press a key on a terminal that has no keyboard buffering capability, and the controller is already processing a request from the host, the key is rejected, and the keyboard can lock up. You can then press **RESET** to unlock the keyboard and enable input to proceed.

The length of the command entry area is limited to three lines of 80 characters each. For input modes of two or three lines, on screens wider than 80 characters, the NetView program indicates the end of the input area with three less-than symbols (<<<). When you press any action key (Enter, PF, PA, or Clear), the command area is erased.

Moving between the Components

To move from one component to another, enter the component name. See the following table for information about moving between the various NetView components.

Table 4. Moving between Components

To move to this component:	Enter:
Automated Operations Network	`aon`
Browse facility	`browse` *`logname`*
Command facility	`nccf`
Hardware monitor	`npda`
Help facility	`help`
4700 Support Facility	`tara`
Session monitor	`nldm`
Status monitor	`statmon`

For example, to move to the hardware monitor initial screen (or the last panel viewed if the hardware monitor component is still active), enter `npda`.

In the NetView program, you can have multiple components active at the same time. Use the ROLL function to move among active components in a continuous loop. The NetView-supplied PF key for ROLL is PF6. If your PF key settings have PF6 set to ROLL, then pressing PF6 returns you to the last panel you viewed in an active component.

To display a list of the active components, enter the following command:

```
LIST ROLL
```

To return to a specific component, enter the following command:

```
RESUME component_name
```

For additional information on the hierarchy of panels within the session monitor, hardware monitor, status monitor, and 4700 Support Facility, see Appendix B, “NetView Component Hierarchies,” on page 343. This information also includes the command that you can use to enter the hierarchy at a specific point.

If you are in a component other than command facility with a panel displayed, you can be interrupted by a message from another component. This message is displayed on the command facility screen. After the message is displayed, the NetView program displays *** at the bottom of the command facility screen. You can press Enter to return to the panel you were using when the interrupt occurred.

Issuing Commands

You can direct commands to explicit destinations in the NetView environment. Table 5 shows the possible destinations and how to direct commands to those destinations.

Table 5. Directing Commands

To direct a command to:	**Use:**
Current operator task	*command_name*
VTAM	*VTAM_command_name*
Another task on this NetView program	EXCMD command or command prefix label
Remote NetView program	RMTCMD command or command prefix label
Service point	RUNCMD command
MVS	MVS command

To direct a command to the session monitor, hardware monitor, or 4700 Support Facility from another component, type the component name followed by the command. For example, to view the total statistics information in the hardware monitor from the session monitor, enter the following command:

```
npda tot st
```

To direct a command to the status monitor, type the command without prefixing it with the component name. For example, to start automatic node reactivation for all applicable nodes from the session monitor, enter the following command:

```
monit start all
```

Using Program Function and Program Access Keys

You can use program function (PF) or program access (PA) keys to send commands to the system. Doing so can save time because you do not have to type a command and then press the Enter key.

Most PF and PA keys have already been set for you, with unique settings by component. They are set to commands that you frequently need to use.

To display the current settings for command facility PF and PA keys, enter the following command:

```
dispfk nccf
```

A scrollable window similar to the following one is displayed, showing the NetView-supplied default values. Your system might have different values, and each operator can change PF key values, both in a profile and interactively.

```
CNMKWIND OUTPUT FROM  DISPFK                                  LINE 1    OF 33
DISPLAY OF PF/PA KEY SETTINGS FOR NCCF
KEY   ----TYPE----   -----------COMMAND------------  SET-APPL
PA1   IMMED,IGNORE   RESET                          NETVIEW
PA2   IMMED,IGNORE   AUTOWRAP TOGGLE                NETVIEW
PA3   IMMED,IGNORE   RETRIEVE AND EXECUTE           NETVIEW
PF1   IMMED,APPEND   HELP                           NETVIEW
PF2   IMMED,APPEND   GO                             NCCF
PF3   IMMED,IGNORE   RETURN                         NETVIEW
PF4   IMMED,APPEND   DISPFK                         NETVIEW
PF5   IMMED,IGNORE   BROWSE NETLOGA                 NETVIEW
PF6   IMMED,IGNORE   ROLL                           NETVIEW
PF7   IMMED,APPEND   TASKUTIL                       NCCF
PF8   IMMED,IGNORE   PIPE NETVIEW LIST STATUS=      NCCF
                     OPS|COL|CONS ONLY
PF9   DELAY,IGNORE   PIPE HELDMSG | CONSOLE DELETE  NCCF
PF10  IMMED,APPEND   WINDOW                         NETVIEW
PF11  IMMED,IGNORE   HOLD                           NCCF
PF12  IMMED,IGNORE   RETRIEVE                       NETVIEW
PF13  IMMED,APPEND   CMD HELP                       NETVIEW
PF14  IMMED,APPEND   STATIONS                       NETVIEW
PF15  IMMED,IGNORE   LINES                          NETVIEW
PF16  IMMED,IGNORE   PFKDEF CNMKEYS2                NETVIEW
PF17  IMMED,IGNORE   BROWSE NETLOGI                 NETVIEW
PF18  IMMED,APPEND   NCCF                           NETVIEW
PF19  IMMED,APPEND   TASKUTIL                       NCCF
PF20  IMMED,APPEND   TS                             NCCF
PF21  DELAY,IGNORE   PIPE HELDMSG | CONSOLE DELETE  NCCF
PF22  IMMED,APPEND   PIPE NETVIEW LIST STATUS=      NCCF
                     TASKS | LOCATE 55.10 /NOT
                     ACTIVE/ | COLLECT | CONSOLE
                     ONLY
PF23  IMMED,APPEND   NPDA                           NETVIEW
PF24  IMMED,IGNORE   RETRIEVE                       NETVIEW
TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
CMD==>
```

Figure 14. List of NetView-Supplied Default Command Facility PF Keys

You can also display PF key settings for other components, such as status monitor, hardware monitor, and log browse by specifying their component abbreviations on the DISPFK command or a PF key set to that command. For example, the NetView defaults specify the DISPFK command with the APPEND keyword as PF4; you can type a component name on the command line and press PF4 to see the PF keys for that component. Browse the CNMKEYS member or enter `dispfk all` to display all PF key settings. As an example of other NetView-supplied default settings, see Figure 69 on page 118.

If you need only a single PF key definition, enter the following command:

`list key=pf`*`nn`*

Where *nn* is the PF key number. See "Defining Program Function Keys" on page 203 for information on changing the settings of PF key defaults across components, or for individual components such as the command facility, hardware monitor, 4700 support facility, and session monitor.

Controlling the NetView Screen

When you are familiar with the initial setup of your screen, you might want to change the way it looks and functions. For example, you can change the PF key

settings, the screen colors, the rate at which the screen wraps when full, and the overall screen layout. See “Controlling the NetView Screen Contents and Format” on page 203 for more information.

Using NetView from the NetView 3270 Management Console

The NetView 3270 management console provides access through TCP/IP to the NetView program using a Java virtual machine. Using the NetView 3270 management console, you can access both the command facility and full-screen applications that are available to the NetView program.

This section describes the following topics:
- Logging on to the NetView 3270 management console
- Customizing your console
- Accessing NetView components from the NetView 3270 management console
- Logging off the NetView 3270 management console

Logging on to NetView from the NetView 3270 Management Console

To log on to the NetView program from the NetView 3270 management console:

1. Enter a valid operator ID and password. To change your password, also enter the new password.
2. As appropriate, enter the name of an operator profile, whether you want to print the log, and whether you want to run the initial command list.
3. If your operator ID is already logged on, enter **Y** in the `Takeover` field to disconnect from the current terminal and reconnect at the terminal where this logon is requested.
4. Press Enter. You specified a new password. You are prompted to reenter it for verification. A command facility panel is then displayed.

Customizing Your Console

You can customize your console in the following ways:
- Change the font size
- Change the text and background colors
- Change the function associated with a particular key

You can do this using the toolbar push buttons. You can move the mouse pointer to the various push buttons on the toolbar for tooltips.

Using the Command Facility Panel

Use the Command Facility panel to issue commands and view messages. You can move the mouse pointer to various push buttons or areas on the screen for tooltips. To issue a command, either press a function key or type the command in the command area and press **Enter**.

Using a Full-Screen Session Panel

Use a full-screen session panel to access NetView components such as the session monitor, status monitor, hardware monitor, help, browse, and TAF. You can also use the full-screen session panel to access other full-screen sessions or applications.

To select a full-screen session panel:

1. If the full-screen session panel is active, select its index tab to bring it to the foreground; otherwise, start the session using the following steps:
   a. Select Session Services on the menu bar.
   b. Select the session that you want to start.
   c. If you selected TAF, edit the command in the command area and press **Enter** to send the command to the host. A message at the bottom of the message area provides instructions.
2. To enter a command, press its function key or enter it in the command area and press **Enter**.

To add a full-screen session panel:

1. From the menu bar, select **Session Services**, then select **Add/Delete Session** from the menu. A dialog box is displayed.
2. Enter the name of the full-screen session to be added.
3. Enter the initial command to call the session from the command line in the Start command String field.
4. Click the Immediate push button if the command is to be issued immediately. Click **Delay** if the command is to be displayed on the command line when the new session panel is opened. Then, you can modify the command before it is sent.
5. Select any of the following session options:
   - Start the session automatically when the console is started.
   - Show the tool bar at the top of the session panel.
   - Show the keypad at the bottom of the session panel.
6. Select the terminal size for the session.
7. If desired, enter the fully qualified class name of an HACL application to be started as part of the application.
8. Click **Add**.
9. Click **Save** to save changes and**Done** to close the dialog. If you do not click **Save**, the changes are in effect only for the current session.

To modify a full-screen session:

1. From the menu bar, select **Session Services**, then select **Add/Delete Session** from the menu. A dialog box is displayed.
2. Select the name of the full-screen session to modify from the list of session listed in the Delete Sessions list.
3. Modify any options as appropriate, then click **Modify**.
4. Click **Save** to save changes and **Done** to close the dialog. If you do not click **Save**, the changes are in effect only for the current session.

To delete a full-screen session:

1. From the menu bar, select **Session Services**, then select **Add/Delete Session** from the menu. A dialog box is displayed.
2. Select the name of the full-screen session to be deleted from the list of session listed in the Delete Sessions list.
3. Click **Delete**.
4. Click **Save** to save changes and **Done** to close the dialog. If you do not click on **Save**, the changes are in effect only for the current session.

Logging Off

To log off the NetView program:

1. Select **Connection Services** on the menu bar.
2. Select **Logoff** from the menu. You can also type LOGOFF on the command facility panel. In either case, the panels remain open so you can review the final messages.

To close the workspace:

1. Select **File** on the menu bar.
2. Click **Close** on the menu. This logs you off the NetView program if you have not already logged off and ends the NetView 3270 management console session.

Accessing the NetView Program from the NetView Management Console

The NetView management console graphically displays systems and networking information provided by the NetView program. You can monitor and control the network, view the topology and connectivity of the network, display events or status changes for a selected resource, issue commands, and build custom views and resource collections. For more information about using the NetView management console, see "Using the NetView Management Console" on page 45; for detailed information, see the *IBM Tivoli NetView for z/OS NetView Management Console User's Guide*.

Accessing the NetView Program from the Tivoli Enterprise Portal

You can send commands to the NetView program from the Tivoli Enterprise Portal using take action commands or situations, including Reflex Automation and Policy. The commands can be sent using the NetView for z/OS Enterprise Management Agent or the NetView APSERV receiver. Command and command responses, along with audit trail messages, are displayed in the NetView for z/OS Enterprise Management Agent workspaces. For more information about using the NetView for z/OS Enterprise Management Agent, see Chapter 4, "Monitoring and Controlling Your Network Using the IBM Tivoli NetView for z/OS Enterprise Management Agent," on page 51. For more information about APSERV, see the *IBM Tivoli NetView for z/OS Application Programmer's Guide*.

Accessing the NetView Program from a Web Browser

Using the NetView Web application, you can access a specific set of NetView functions from a Web browser. For information about using the NetView Web application, see the *IBM Tivoli NetView for z/OS Web Application User's Guide*; for detailed information, see the Task Assistant in the Web application.

Part 2. Monitoring and Controlling the Network and System

Chapter 3. Monitoring and Controlling Your Network from a Workstation

This chapter provides an overview of how to manage your network from a workstation using the following components:

- NetView management console, described in "Using the NetView Management Console"
- NetView Resource Manager, described in "Monitoring Resource Utilization Using NetView Resource Manager" on page 47
- SNA topology manager, described in "Using the SNA Topology Manager" on page 48
- System Automation for z/OS, described in "Monitoring Resources Using System Automation for z/OS" on page 49

Monitoring is the examination of the entire network and system for changes in the status of individual components from satisfactory to a status requiring attention.

Controlling is the taking of specific actions against individual network and system components to change their status, make them available for monitoring, or to manipulate the use of the resources.

Using the NetView Management Console

The NetView management console runs on Windows systems and uses interactive graphics to display pictures (*views*) that represent a network, a portion of a network, or a group of networks at various levels of detail. These views show the network resources that you are monitoring. When you monitor a network, resource status changes are reflected graphically in the views.

Using the NetView management console, you can perform the following tasks:

- Monitor and control large portions of complex communication networks, including SNA subarea and Advanced Peer-to-Peer Networking resources, and non-SNA resources. In addition, you can see the status of resources in several domains.
- View your network topology and connectivity graphically.
- View a history of status updates for resources.
- Use exception views to quickly see all problem resources in one view.
- Monitor the overall state of a network or portion of a network using aggregate resources, which represent the combined status of a group of related resources.
- Use the **Locate Failing Resources** function to navigate quickly from an aggregate resource to a real resource that is failing.
- Mark resources for your own purposes; for example, to show that they are being serviced.
- View a history of alerts generated by resources in your network that are managed by the NetView Graphic Monitor Facility host subsystem (GMFHS)
- Use items in the context menu to issue predefined commands, or access a NetView or non-SNA command line to issue your own commands.

The NetView management console topology server workstation communicates with host NetView through either an LU 6.2 or IP session. The NetView management console topology server is installed on the server workstation and receives topology changes and resource status changes from host NetView.

The NetView management console collects topology information from SNA topology manager, or other applications. Status information is sent to the focal point by resource status collectors. Or, if you are using the SNA topology manager, status information is collected by Open Systems Interconnection (OSI) agents and sent to the SNA topology manager, which puts that information in the Resource Object Data Manager (RODM) so the NetView management console can display it. The NetView management console topology server forwards topology and status information collected from these sources to all signed-on client workstations.

Figure 15 illustrates the connection between host NetView and the NetView management console.

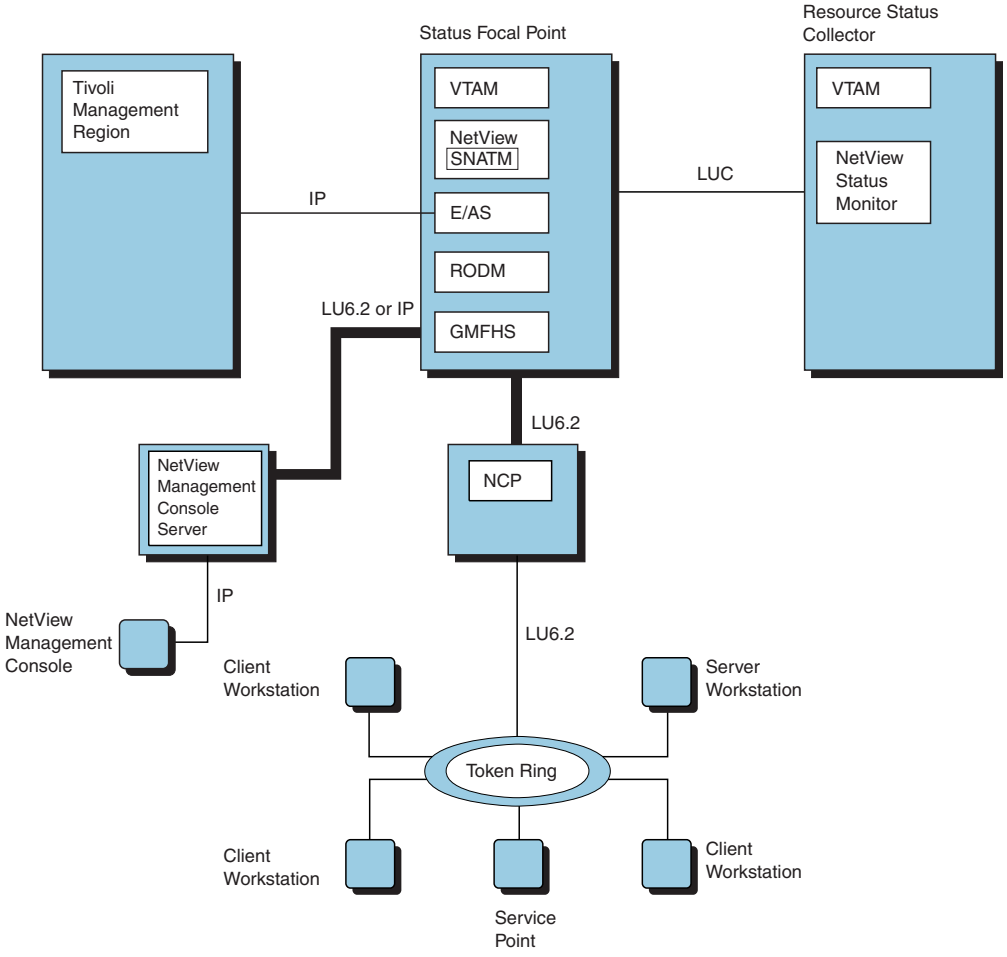


Figure 15. Host-to-Workstation Connection

The service point in Figure 15 collects information about RODM-defined SNA and non-SNA resources. Status information from the service point travels as an alert to the host NetView system and then to the GMFHS. GMFHS updates the status for the resources stored in RODM, then sends the status information to the server workstation through the LU 6.2 or IP session. The server workstation distributes the information to the attached clients as a system status update.

Topic:	Reference:
Examples of non-SNA networks attached to service points	*IBM Tivoli NetView for z/OS Resource Object Data Manager and GMFHS Programmer's Guide*
Information about the NetView management console	The NetView management console online help and *IBM Tivoli NetView for z/OS NetView Management Console User's Guide*

Monitoring Resource Utilization Using NetView Resource Manager

Use NetView Resource Manager to graphically monitor and manage NetView tasks for resource utilization and status using the NetView management console. You can monitor all NetView programs in your enterprise using one NetView management console.

NetView Resource Manager includes manager and agent NetView hosts. The agent host forwards local resource utilization information to one or more manager hosts. The manager host then processes resource utilization information for agent hosts (including itself), and provides a graphical interface (NetView management console) to monitor all of your NetView programs. A manager host can also forward data to one or more manager hosts. You can use TCP/IP or SNA to communicate between these NetView programs.

NetView Resource Manager is started with the `INITNRM` command, manually or at NetView initialization. `CNMSTYLE` and its included members contain all of the values that can be customized for NetView Resource Manager.

`AUTONRM` is the default autotask used for NetView Resource Manager processing. You can specify a different autotask for the NetView Resource Manager function by changing the following statement in CNMSTYLE or its included members:

```
function.autotask.NRM=AUTORNM
```

Use NetView Resource Manager to set thresholds for the following types of resources:

- Processor
- I/O
- MQS rates
- Storage
- Message queue count

When a resource reaches a threshold, a status change is sent to NetView management console. Reaching a threshold does not cause any action to be taken on the task. The NetView Resource Manager NetView uses the following functions:

- RODM
- RMTCMD
- Hardware Monitor
- TCP/IP Alert Receiver (if your communication method is TCP/IP)

The NetView Resource Manager agent NetView uses the RMTCMD function.

For more information about setting up and using NetView Resource Manager, refer to the following documents:

- *IBM Tivoli NetView for z/OS Installation: Configuring Graphical Components*

- *IBM Tivoli NetView for z/OS Resource Object Data Manager and GMFHS Programmer's Guide*

Using the SNA Topology Manager

The NetView program can manage SNA subarea and Advanced Peer-to-Peer Networking resources using the NetView SNA topology manager. SNA topology manager collects topology information from VTAM agents.

The VTAM agent collects topology information from SNA resources, both subarea and Advanced Peer-to-Peer Networking.

The SNA topology manager provides a dynamic, centralized network management system for SNA subarea and Advanced Peer-to-Peer Networking networks. It uses existing NetView components, including RODM and GMFHS, to manage and display SNA subarea and Advanced Peer-to-Peer Networking topology data at the NetView management console workstation. Data is stored in RODM dynamically and can be used for automation.

The SNA topology manager application works with one or more agent applications to gather topology data about SNA subarea and Advanced Peer-to-Peer Networking networks. The agent application supplies topology information about nodes and links in response to requests from the manager application. VTAM V4R3 and later releases provide a topology agent for Advanced Peer-to-Peer Networking and subarea topology information. The SNA topology manager is controlled using the TOPOSNA command.

The SNA topology manager offers the following functions:

- The SNA topology manager gathers topology data for SNA subarea and Advanced Peer-to-Peer Networking nodes in the network. Two types of topology are collected:
  - Network topology which contains information about subarea nodes, network nodes, and transmission groups (TGs) between nodes that are part of an Advanced Peer-to-Peer Networking intermediate routing network.
  - Local topology which contains information about network nodes, end nodes, and low-entry networking nodes; the connections between nodes; and the ports and links that make up the connections.
- SNA topology manager uses the NetView management console to display configuration and status in graphic views. Operators can start network and local topology monitoring dynamically using the NetView management console menus. The topology data can also be monitored automatically using NetView command lists.

  SNA topology manager views are built and updated dynamically, which ensures the most current status and configuration are displayed to the operator. This is especially important for Advanced Peer-to-Peer Networking networks: by their nature, these networks change configuration and status frequently as nodes establish and stop connections. As changes occur in the network, the views are updated. Operators are informed of changes through status color changes and messages, or by failing resources displayed in exception views.
- The SNA topology manager uses RODM to manage the topology data dynamically. Storing objects in RODM allows other applications to make use of the stored data. Objects representing nodes, links, ports, and connections in a network are defined to RODM according to the SNA topology manager data model.

- The SNA topology manager provides several different ways to issue commands. These include:
  - Generic NetView management console commands at the NetView management console workstation
  - Customized command sets at the NetView management console workstation
  - Command line entry using the NetView command interface
- The SNA topology manager provides a sample network to help users become familiar with the SNA topology manager function and to help gain experience with the views in a test environment.

Figure 16 shows an overview of the SNA topology manager environment.

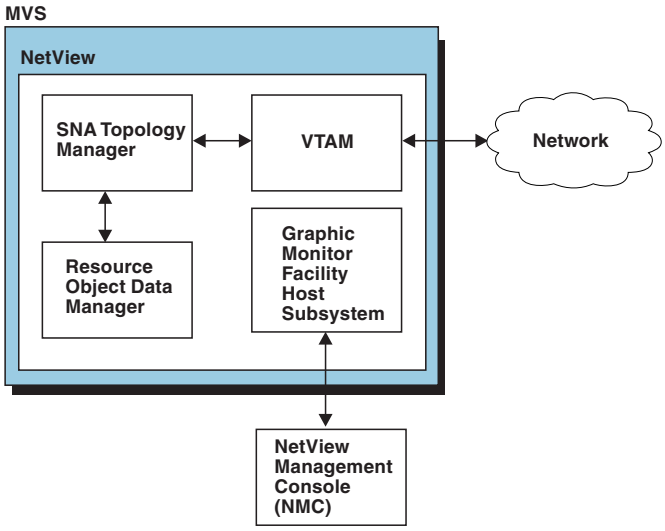


Figure 16. SNA Topology Manager Environment

Monitoring Resources Using System Automation for z/OS

The terminology used here is System Automation for z/OS terminology, not NetView terminology.

The System Automation for z/OS graphical interface works with the NetView management console to provide the following functions:

- Monitor the operational status of your systems
- Temporarily change threshold settings that cause status changes to be reflected in your view of your systems
- Temporarily change the scheduled availability of MVS target systems
- Control the operation of your systems

Figure 17 on page 50 shows the relationships between the windows in the System Automation for z/OS graphical interface and the NetView management console:

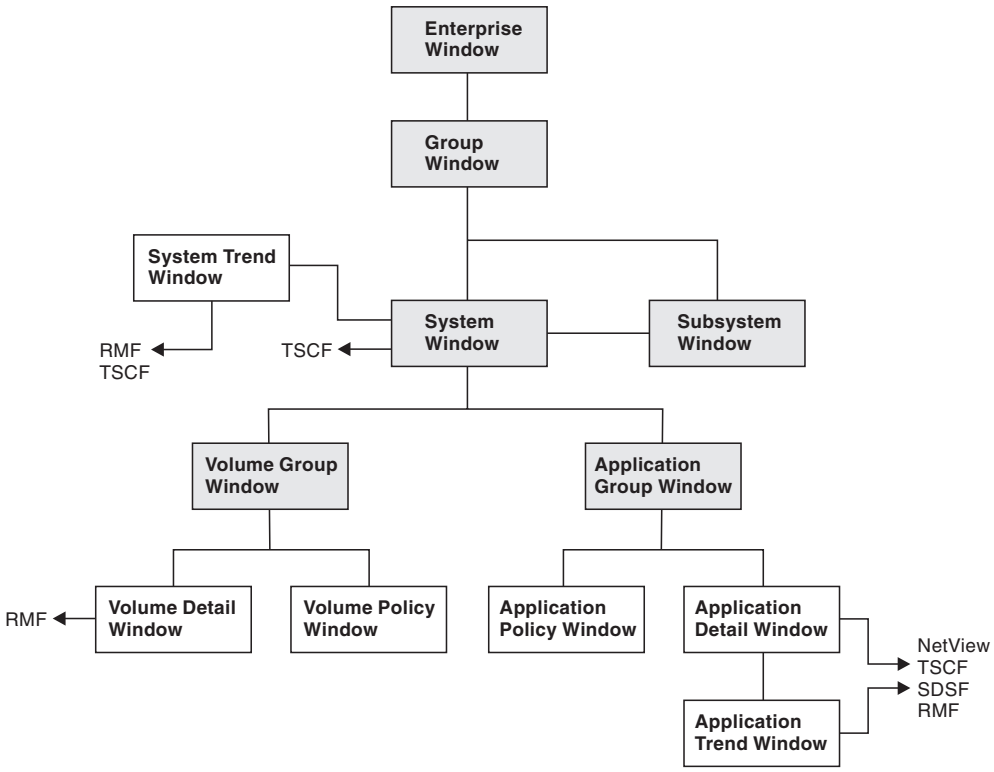


Figure 17. Relationships between the System Automation for z/OS Graphical Interface and NetView Management Console Views

The shaded blocks represent NetView management console views, using System Automation for z/OS terminology

Chapter 4. Monitoring and Controlling Your Network Using the IBM Tivoli NetView for z/OS Enterprise Management Agent

Use the IBM Tivoli NetView for z/OS Enterprise Management Agent to manage your network from the Tivoli Enterprise Portal. Both sampled and real-time NetView data is available in the Tivoli Enterprise Portal with this agent. With the NetView for z/OS Enterprise Management Agent and the OMEGAMON XE performance agents, you can manage and view availability and performance data for your network from a single interface.

You can perform the following kinds of tasks:
- Monitor NetView task status and performance statistics
- Monitor the status of your TCP/IP stacks in a sysplex
- Monitor DVIPA configuration, workload balance, and connections
- Monitor and diagnose problems with TCP/IP connections
- Monitor active SNA sessions
- Diagnose TCP/IP problems with packet trace
- Issue commands to manage your network

NetView for z/OS Enterprise Management Agent Overview

The NetView for z/OS Enterprise Management Agent runs on a z/OS system in its own address space and requires the Tivoli Management Services, which is provided by IBM Tivoli Monitoring V6.1 Fix Pack 5 or later. The NetView program communicates with the NetView for z/OS Enterprise Management Agent using the NetView program-to-program interface (PPI), which provides a secure communication layer between the NetView program and the agent.

The NetView for z/OS Enterprise Management Agent is disabled by default. It is enabled using the TEMA tower and associated subtower statements in the CNMSTYLE member. Note that the CNMSTYLE member contains all of the values that can be customized for the NetView for z/OS Enterprise Management Agent.

Enabling the TEMA tower starts the PPI receiver connection to the NetView for z/OS Enterprise Management Agent by issuing the NACMD command. Enabling TEMA subtowers starts data collection for specific functions. Data collectors provide sampled or real-time data. The collected data is stored in a data space and is retrieved by the NetView for z/OS Enterprise Management Agent when a user requests data for the associated workspace in the Tivoli Enterprise Portal. The PPI receiver is stopped with the STOPNA command.

Tivoli Enterprise Portal Overview

The NetView for z/OS program uses the Tivoli Enterprise Portal to provide a view of your enterprise from which you can drill down to more closely examine components of each system being monitored. The application window for the Tivoli Enterprise Portal consists of a Navigator and a workspace.

The Physical Navigator displays all the systems in your enterprise where Tivoli Enterprise Monitoring Agents are installed. It shows the hierarchy of your monitored enterprise, from the top level (Enterprise) down to individual groupings

of information collected by NetView for z/OS Enterprise Management Agent. When you click an item in the Navigator, the default workspace for that item is displayed.

The workspace is the work area of the Tivoli Enterprise Portal window and consists of one or more views of the resources being monitored. A view is a pane in the workspace, typically a chart or table, showing data collected by the NetView for z/OS Enterprise Management Agent or other Tivoli Enterprise Monitoring Agents. Each view has a set of properties associated with it. You can customize the workspace by using the Properties Editor to change the style and content of each view. You can also add and delete views in a workspace.

Access the Tivoli Enterprise Portal in one of the following modes:

Desktop
The application software is installed on your system.

Browser
The software is downloaded to your system the first time you log on to Tivoli Enterprise Portal, and, after that, whenever the software is updated. Access is through a supported browser using the Web address of the Tivoli Enterprise Portal Server.

For more information about the Tivoli Enterprise Portal, see the Tivoli Enterprise Portal user assistance and the *IBM Tivoli Monitoring: User's Guide*.

Attributes

Use the NetView for z/OS Enterprise Management Agent attributes to build views that display the availability of your network. Attributes can be used to define situations to test for specific conditions. When the conditions for a situation are met, situation event indicators are displayed in the Navigator.

A direct relationship usually exists between the NetView for z/OS Enterprise Management Agent attributes and the table views. An attribute group corresponds to a table view, or, occasionally, to several table views within a workspace. Each attribute group has one or more attribute items, which correspond to the columns in a table view. For general information about an attribute group or to see the names of the attributes in each attribute group, see the NetView for z/OS Enterprise Management Agent online help.

Situations

The NetView for z/OS Enterprise Management Agent provides a set of situations that you can use to monitor the systems in your network. A situation is a logical expression involving one or more system conditions.

Use the provided situations to begin monitoring, or modify the situations to meet your requirements. Before modifying a provided situation, make a backup copy of the situation. You can also create your own situations using the attributes provided by the NetView for z/OS Enterprise Management Agent. For a list of the provided situations, see the NetView for z/OS Enterprise Management Agent online help.

Manage situations in the following ways by using the Situation Editor from the Tivoli Enterprise Portal:

- Display a list of situations running on a specific managed system, the same types of managed systems, or in the enterprise

- Create, edit, save, delete, or display a situation
- Start or stop a situation
- Associate a situation with the current navigator item
- Investigate the event workspace for a situation

Note: If a situation is edited to add an action, the notification about that situation goes to the user who added the action.

The Situation Editor initially lists the situations associated with the selected Navigator item. When you click a situation name or create a new situation, the Situation Editor provides the following information about the situation so that you can further define that situation:

- Condition. See, add to, and edit the condition being tested.
- Distribution. See the systems to which the situation is assigned and assign the situation to systems.
- Expert advice. Write comments or instructions to be read in the event workspace.
- Action. Specify a command to be sent to the system or use or create take action commands.
- Until. Reset a true situation when another situation becomes true or a specified time interval elapses.

Take Action Commands

Use the NetView for z/OS Enterprise Management Agent take action commands to interact with your applications and operating system.

A take action command that is issued from the Tivoli Enterprise Portal is received by the NetView for z/OS Enterprise Management Agent and sent to the NetView program over the PPI. The command is processed, and the command responses are stored in a data space. When the Tivoli Enterprise Portal user selects or refreshes the workspace for the command issued, the data is retrieved from the data space and displayed in the Tivoli Enterprise Portal. If applicable, the displayed data can include graphs.

The following NetView for z/OS Enterprise Management Agent take action commands are provided; for more information about the take action commands, see the NetView for z/OS Enterprise Management Agent online help.

- Browse NetView Logs (AGTBRW). Browse the network log.
- Format Packet Trace (FMTPACKT). Collect and format packet trace entries.
- Issue NetView Commands. Issue commands that can be issued from a NetView for z/OS command line.
- List NetView Task (LIST). Display task status.
- Purge Packet Trace (PKTS PURGE). Purge packet trace data that matches input criteria.
- Start NetView Task (START). Start the specified optional NetView task.
- Stop Force NetView Task (STOP). Stop a task that cannot process normally.
- Stop Immed NetView Task (STOP). Stop the specified NetView task immediately.
- Stop NetView Task (STOP). Stop a task normally.
- View Data Collection Statistics (NACTL LISTINFO). View data collection statistics.

- View DVIPA Connections (CNMSDVPC). View the dynamic virtual IP address (DVIPA) connections.
- View DVIPA Definition and Status (CNMSDVIP). View the status of the DVIPA stack.
- View DVIPA Distributor Targets (CNMSTARG). View information about the DVIPA distributor targets.
- View DVIPA Sysplex Distributors (CNMSPLEX). View information about DVIPA sysplex distributors.
- View Session Configuration Data (SESSC). View session monitor configuration data.
- View Session Data (AGTSESMG). View SNA sessions collected by the session monitor.
- View Stack Configuration and Status (CNMSSTAC). View stack configuration and status.
- View TASKMON Data by Task (TASKMON). View color-coded monitoring of all NetView tasks.
- View TASKUTIL Data by Task (TASKUTIL). View central processing unit utilization and storage use for NetView tasks.
- View TCP/IP Connections (AGTTCPC). View TCP/IP connection data.

Workspaces

The NetView for z/OS Enterprise Management Agent workspaces contain views that report information about enterprise resources that you are monitoring.

Each workspace contains a navigation tree view and at least one other view. Many workspaces contain table views. Table rows can contain links to related workspaces that provide more detailed information. A workspace can contain other views, such as a bar chart, notepad, or take action view. A take action view can be used to send commands to the NetView host.

Many of the agent workspaces provide data that is sampled at an interval, but some of the agent workspaces are real-time workspaces. With the exception of the Stack Configuration and Status workspace, the real-time workspaces require a take action command to be issued to provide data.

The following workspaces contain sampled data:
- "DVIPA Connections Workspace" on page 63
- "DVIPA Definition and Status Workspace" on page 59
- "DVIPA Distributor Targets Workspace" on page 61
- "DVIPA Sysplex Distributors Workspace" on page 60
- "DVIPA Workload by Port Workspace" on page 62
- "Inactive TCPIP Connection Data Workspace" on page 65
- "NetView Task Details Workspace" on page 67
- "NetView Tasks Workspace" on page 66
- "Session Data Workspace" on page 68
- "TCPIP Connection Data Workspace" on page 64

The following workspaces contain real-time data:
- "NetView Audit Log Workspace" on page 71
- "NetView Command Response Workspace" on page 70
- "NetView Log Workspace" on page 69
- "Stack Configuration and Status Workspace" on page 72

All of the workspaces that are included with the NetView for z/OS Enterprise Management Agent are read-only. To change these workspaces, save them using a different name.

This rest of this section provides general information about the NetView for z/OS Enterprise Management Agent workspaces, including how to access them, what cross-product workspace links are available, and how data is collected for the workspaces.

The following sections introduce the NetView for z/OS Enterprise Management Agent workspaces. For detailed information about the workspaces, see the online help. Note that the workspace descriptions in the online help apply to the default settings of the original configuration. Changes and additions that you make to a workspace are not described in the online help.

- "DVIPA Workspaces" on page 58
- "TCP/IP Connection Workspaces" on page 64
- "NetView Health Workspaces" on page 66
- "Other Workspaces" on page 68

Access to Workspaces

To access NetView for z/OS Enterprise Management Agent workspaces from the Navigator in the Tivoli Enterprise Portal, expand **z/OS Systems**, the system, **NetView Agent**, **KNAAGENT**, **NetView**, and the domain name; and then click the workspace name.

Note: To access the Inactive TCPIP Connection Data workspace, expand **z/OS Systems**, the system, **NetView Agent**, **KNAAGENT**, **NetView**, and the domain name; select and right-click **TCPIP Connection Data**; click **Workspace**; and click **Inactive TCPIP Connection Data**.

Filtered workspaces are available for the following workspaces:

- "DVIPA Connections Workspace" on page 63
- "DVIPA Definition and Status Workspace" on page 59
- "DVIPA Distributor Targets Workspace" on page 61
- "Inactive TCPIP Connection Data Workspace" on page 65
- "Session Data Workspace" on page 68
- "TCPIP Connection Data Workspace" on page 64

For the links to some filtered workspaces, a filter window opens. In the filter window, specify or change values for one or more of the fields. For information about the fields, see the online help.

You must specify a value for at least one field. You can include one or more wildcard characters (*) anywhere within a value that you specify. You can also specify a lone wildcard character for one or more fields, but you cannot specify a lone wildcard character for all the fields. Leaving a field blank is the same as specifying a lone wildcard character. Click **OK** to display the filtered data in the target workspace.

Notes:

- When you click **OK**, the values you specified are saved, and the target workspace is displayed using the specified values.
- If you click **Cancel**, any changes that you made are discarded and the target workspace is displayed with no data.

Cross-Product Workspace Links

Dynamic workspace linking provides easy navigation between workspaces for different products. By providing additional information about resources that are being monitored by other monitoring agents, this linking helps in problem determination and improves integration across the monitoring products, so that you can quickly determine the root cause of a problem.

When you right-click a link, a list of links is displayed. The list can contain links to workspaces provided by other monitoring products. For a cross-product workspace link to work, the target product must be installed and configured and your Tivoli Enterprise Portal user ID must be authorized to access the target product.

Choose a workspace from the list to navigate to that workspace. By linking to the target workspace in context, attributes in the source row can be used to locate the target workspace in the navigation tree or to filter the data that is displayed in the target workspace.

If you choose a target workspace that is not available, the following message is displayed; for more information, see the *Troubleshooting Guide*.

```
KFWITM081E The link target can not be found.
```

Table 6 summarizes the cross-product workspace links available when this product shipped. See the workspace descriptions in the online help for information about the predefined links provided with each workspace.

Table 6. Cross-Product Workspace Links

NetView for z/OS Enterprise Management Agent Workspace	Target Application or Monitoring Agent	Workspace in Target Application or Monitoring Agent	Attributes Used to Locate Target Workspace	Attributes Used to Filter Data in Target Workspace
DVIPA Connections	IBM Tivoli OMEGAMON XE for Mainframe Networks version 4.1.0	TCP Connections Link	SMFID	• Local IP Address • Local Port • Remote IP Address • Remote Port
Session Data	IBM Tivoli OMEGAMON XE for Mainframe Networks version 4.1.0	HPR Connections	SMFID	• Primary Name • Secondary Name
TCPIP Connection Data	IBM Tivoli OMEGAMON XE for Mainframe Networks version 4.1.0	TCP Connections Link	SMFID	• Connection Start Time • Local IP Address • Local Port • Remote IP Address • Remote Port
TCPIP Connection Data	IBM Tivoli OMEGAMON XE for CICS on z/OS version 4.1.0	TCPIP Statistics	SMFID	• Local Port (converted to an integer in the link expression)
TCPIP Connection Data	IBM Tivoli OMEGAMON XE on z/OS version 4.1.0	System CPU Utilization	Managed system name (Sysplex Name:System ID:″MVSSYS″)	None

Data Collection for Workspaces

Data collectors for the NetView for z/OS Enterprise Management Agent collect and store data for display in the Tivoli Enterprise Portal. Data collectors are designated by the TEMA subtowers. Except for the TEMA.SYSPLEX subtower, data collection begins after an NACMD command completes successfully. After that, the NetView for z/OS Enterprise Management Agent address space is active and ready for communication.

After communication is established between the NetView program and the agent, data is collected unless an operator action or unexpected error occurs. You might need to change the data collectors that are running at a given time or want to change some of the data collector parameters.

You can manually stop and start any of the NetView for z/OS Enterprise Management Agent data collectors using the NACTL STOP or NACTL START command, if the data collector subtower is enabled. You can specify all data collectors or any subset of data collectors.

You can change any of the data collector statements in the CNMSTYLE (ROWS*xxx* and INT*xxx*) member and issue the RESTYLE NACMD command to pick up the changes. For these changes to take effect, the NACMD command must be stopped and reissued.

Note: If you are changing only the intervals for a subtower, issuing the NACTL STOP and NACTL START commands for the subtower causes the changes to take effect.

Historical Data

Both real-time and historical data are available within the NetView for z/OS Enterprise Management Agent workspaces. After historical data is configured, enabled, and collected, you can display historical reports, which are useful in finding the root cause of problems that evolved over a period of time and debugging problems that occurred in a prior time period. Capacity planners can also use historical reports to identify trends and correct imbalances in network load distribution.

Historical Data Collection

To generate reports containing historical data, historical collection must be configured and enabled and data must be collected. Use the Tivoli Enterprise Portal support to configure and enable collection of data in a historical database. The two types of historical data are short-term and long-term. Short-term historical data collection must be configured and enabled if you want to perform long-term historical data collection.

Short-term historical data is, by default, the most recent 24 hours of data. It is stored in the persistent data store on z/OS systems or in files on distributed systems. The persistent data store is configured using the z/OS Configuration Tool.

Long-term historical data can be defined for as long as you want to store the data: days, weeks, months, or years. It is periodically exported from short-term history and is stored in Tivoli Data Warehouse. The Warehouse Proxy must be installed and configured with a supported database manager (for example, DB2 Universal Database™) before you can configure warehousing using the Historical Collection dialog.

Table 7 shows which workspaces and views can display historical data and the corresponding objects to configure for historical data collection.

Table 7. Workspaces and Views That Display Historical Data

Object	Workspace and Views
NA_DVIPA_Distributor_Targets	DVIPA Distributor Targets: • Server Acceptance • DVIPA Distributor Targets Summary
NA_DVIPA_Sysplex_Distributors	DVIPA Sysplex Distributors: • DVIPA Sysplex Distributors Summary
NA_Inactive_TCPIP_Connection_Data	Inactive TCPIP Connection Data: • All views except Inactive TCPIP Connection Count
NA_NetView_Tasks	NetView Tasks: • All views
NA_Session_Count	Session Data: • Active Session Count
NA_TCPIP_Connection_Count	TCPIP Connection Data: • Active TCPIP Connection Count
NA_TCPIP_Connection_Data	TCPIP Connection Data: • All views except Active TCPIP Connection Count

For more information about configuring historical data collection and reporting, see the *IBM Tivoli Monitoring: Installation and Setup Guide*.

Historical Reports

After historical data collection is enabled, a **Time Span** button (displayed as a clock in front of a calendar) is shown in the upper left corner of qualifying views in Tivoli Enterprise Portal workspaces. Click this icon to extend any existing Tivoli Enterprise Portal view (also called a report) to include historical data. Tivoli Enterprise Portal reports automatically pull data from both short-term and long-term history, based on the time period you specify.

You can create summarization data tables (hourly, daily, weekly, quarterly, monthly, and yearly) to reduce the data overload when creating reports. You can also define pruning intervals to ensure that you save only the data that is needed.

For more information about creating historical reports, see the *IBM Tivoli Monitoring User's Guide*.

DVIPA Workspaces

The DVIPA workspaces provide information about your DVIPA configuration and the use of the configuration within your network. The information displayed in the DVIPA workspaces is determined by the stacks that are specified for monitoring in the CNMPOLCY member.

The DVIPA tower must be enabled for DVIPA data to be collected. The information collected by the DVIPA tower, which is stored in the INSTORE member FKXSDVPT, is the basis for the data collected for the DVDEF, DVTAD, and DVCONN subtowers of the TEMA tower. If the INSTORE member FKXSDVPT contains no data, then the DVIPA workspaces contain no data.

Note: During NetView initialization, an attempt is made to retrieve data for the DVIPA tower. If the attempt is successful, then data collection for the DVDEF, DVTAD, and DVCONN subtowers of the TEMA tower begins. If the attempt is unsuccessful, then two retries occur before data collection for the DVIPA subtowers is allowed to continue; however, no data is collected. The user might need to wait an entire sampling interval before data is available.

The data in the DVIPA workspaces is provided by sampling. You can also issue take action commands to retrieve real-time DVIPA information.

The following DVIPA workspaces are provided:

- "DVIPA Definition and Status Workspace"
- "DVIPA Sysplex Distributors Workspace" on page 60
- "DVIPA Distributor Targets Workspace" on page 61
- "DVIPA Workload by Port Workspace" on page 62
- "DVIPA Connections Workspace" on page 63

DVIPA Definition and Status Workspace

The DVIPA Definition and Status workspace displays the configuration and status information about DVIPA stacks for which you have specified DVIPADAT=Y in the CNMPOLCY member.

The data collection for this workspace is controlled by the TEMA.DVDEF subtower and the associated TEMA.DVDEF statements in the CNMSTYLE member.

The data in this workspace is based on the DVIPSTAT command.

The DVIPA Definition and Status workspace is shown in Figure 18 on page 60.

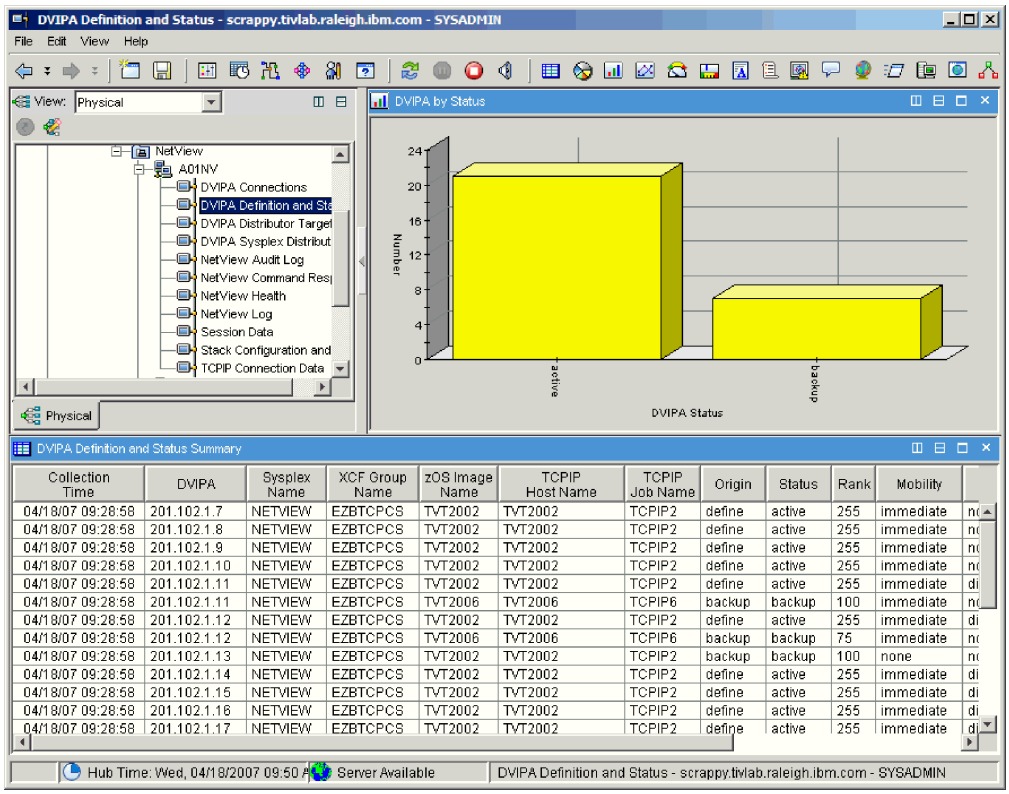


Figure 18. DVIPA Definition and Status Workspace

DVIPA Sysplex Distributors Workspace

The DVIPA Sysplex Distributors workspace displays sysplex distributors for the DVIPAs on this LPAR that are shown in the DVIPA Definition and Status workspace.

The data collection for this workspace is controlled by the TEMA.DVTAD subtower and the associated TEMA.DVTAD statements in the CNMSTYLE member.

Note: If you do not have sysplex distributors in your network, do not enable this subtower.

The data in this workspace is based on the DVIPPLEX command.

The DVIPA Sysplex Distributors workspace is shown in Figure 19 on page 61.

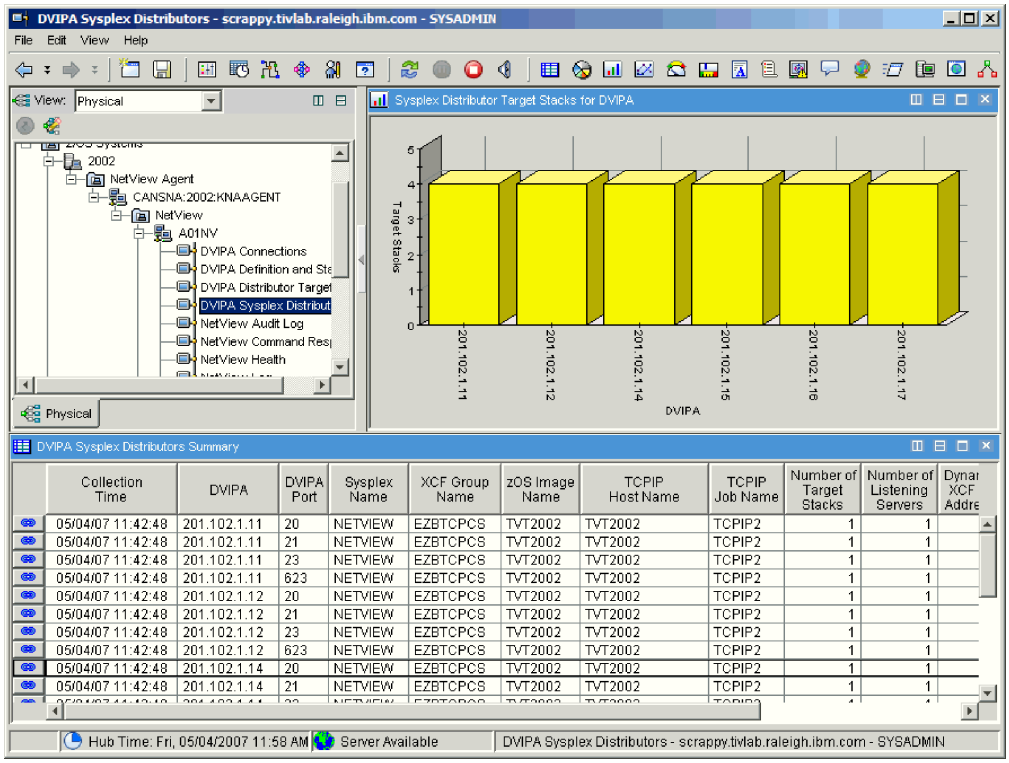


Figure 19. DVIPA Sysplex Distributors Workspace

DVIPA Distributor Targets Workspace

The DVIPA Distributor Targets workspace displays distributor targets for the sysplex distributors on this LPAR that are shown in the DVIPA Sysplex Distributors workspace.

The data collection for this workspace is controlled by the TEMA.DVTAD subtower, and the associated TEMA.DVTAD statements in the CNMSTYLE member.

Note: If you do not have sysplex distributors in your network, do not enable this subtower.

The data in this workspace is based on the DVIPTARG command.

The DVIPA Distributor Targets workspace is shown in Figure 20 on page 62.

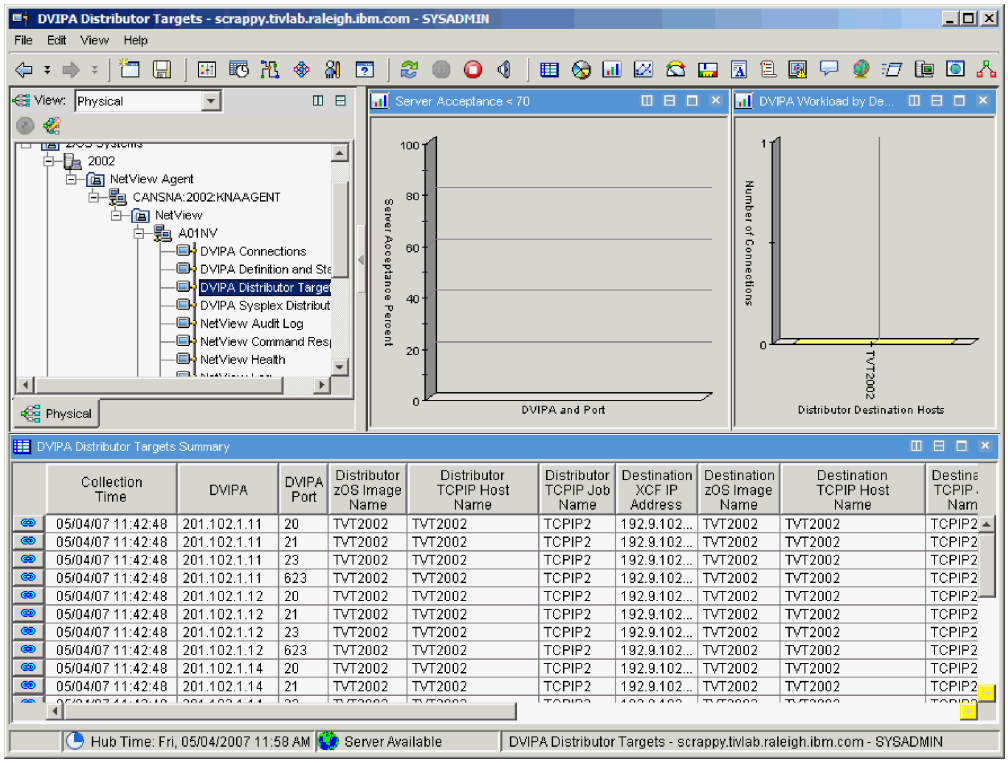


Figure 20. DVIPA Distributor Targets Workspace

DVIPA Workload by Port Workspace

The DVIPA Workload by Port workspace displays the port distribution for DVIPA distributor targets across an LPAR. This workspace can be reached only by using a link in the DVIPA Distributor Targets workspace.

The amount of data that can be displayed in this workspace is determined by the (TEMA.DVTAD)NACMD.ROWSDVTADWP statement in the CNMSTYLE member.

The DVIPA Workload by Port workspace is shown in Figure 21 on page 63.

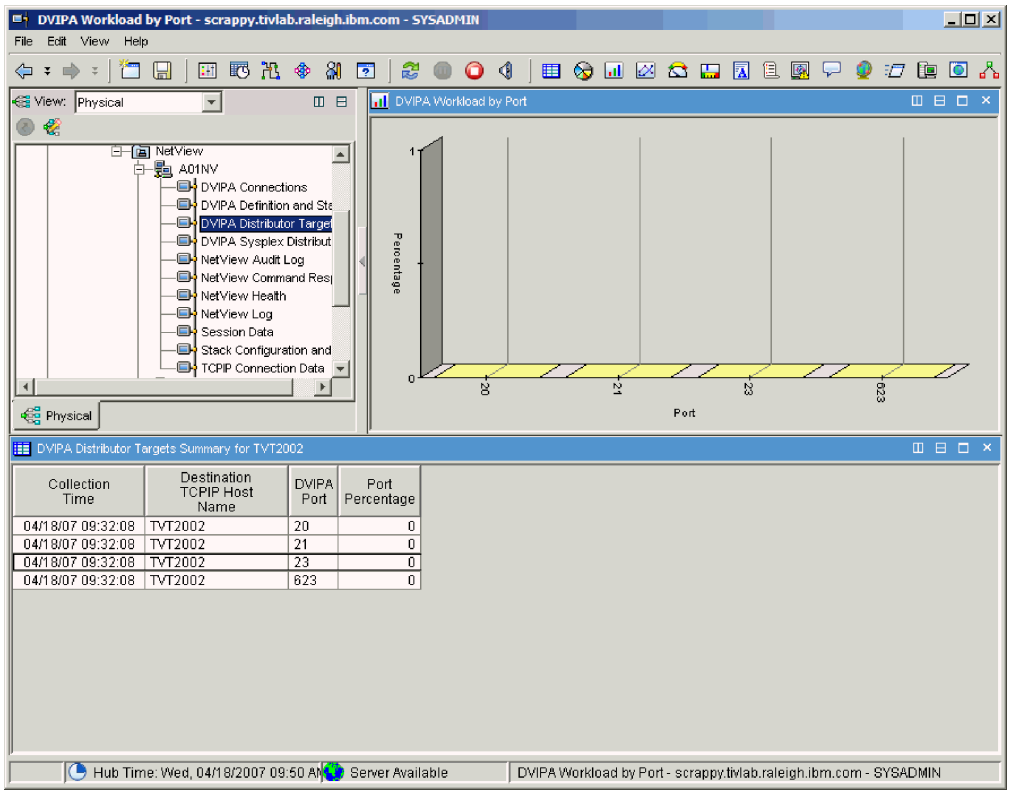


Figure 21. DVIPA Workload by Port Workspace

DVIPA Connections Workspace

The DVIPA Connections workspace displays DVIPA connections for stacks for which you have specified DVIPADAT=Y in the CNMPOLCY member.

The data collection for this workspace is controlled by the TEMA.DVCONN subtower, and the associated TEMA.DVCONN statements in the CNMSTYLE member.

The data in this workspace is based on the DVIPCONN command.

Notes:

1. DVIPA connection data can be collected regardless of whether you are using sysplex distributors.
2. This workspace might be empty if you link to it from the DVIPA Distributor Targets workspace and the Number of Connections attribute in that workspace is 0.

The DVIPA Connections workspace is shown in Figure 22 on page 64.

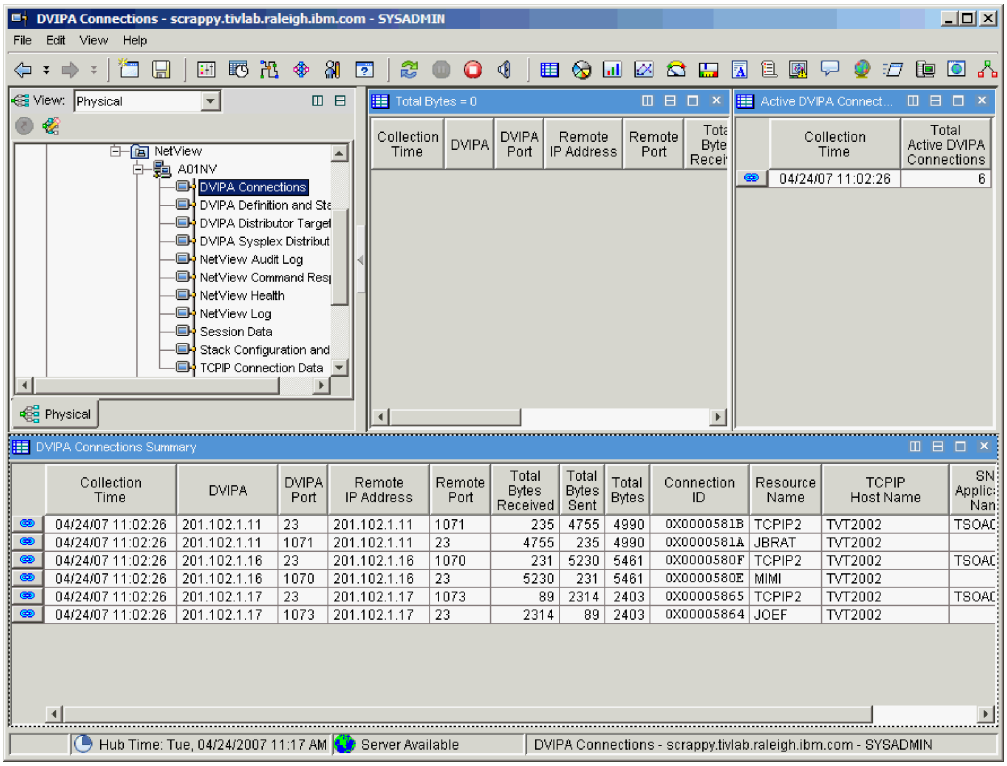


Figure 22. DVIPA Connections Workspace

TCP/IP Connection Workspaces

The TCP/IP connection workspaces provide information about active and inactive TCP/IP connections in your network. The following workspaces for TCP/IP connections are provided:

- "TCPIP Connection Data Workspace"
- "Inactive TCPIP Connection Data Workspace" on page 65

The TCPIPCOLLECT tower must be enabled to collect TCP/IP connection information in the NetView program.

TCPIP Connection Data Workspace

The TCPIP Connection Data workspace displays information about active TCP/IP connections on this LPAR for stacks that you have defined on the TCPCONN.ROWSA.&CNMTCPN statement in the CNMSTYLE member.

Data collection for the TCPIP Connection Data workspace is controlled by the TEMA.CONNACT subtower and the associated TEMA.CONNACT statements in the CNMSTYLE member.

The data in this workspace is provided by sampling. You can issue a take action command to retrieve real-time TCP/IP connection data.

The data in this workspace is based on the TCPCONN QUERYACT command. You do not have to issue a TCPCONN DEFINE or START command (or the CNMSTYLE equivalent) to retrieve this data.

The queries assigned to the views in this workspace use the Byte Rate attribute to filter the rows that can be retrieved for display. Because of the default filter, you might not see all your connections. You can modify the query to display more or fewer connections than the default filter allows.

If you have a large installation, you might not be able to view all the available connections in the Tivoli Enterprise Portal. For more information, see the *IBM Tivoli NetView for z/OS Tuning Guide*.

The TCPIP Connection Data workspace is shown in Figure 23.

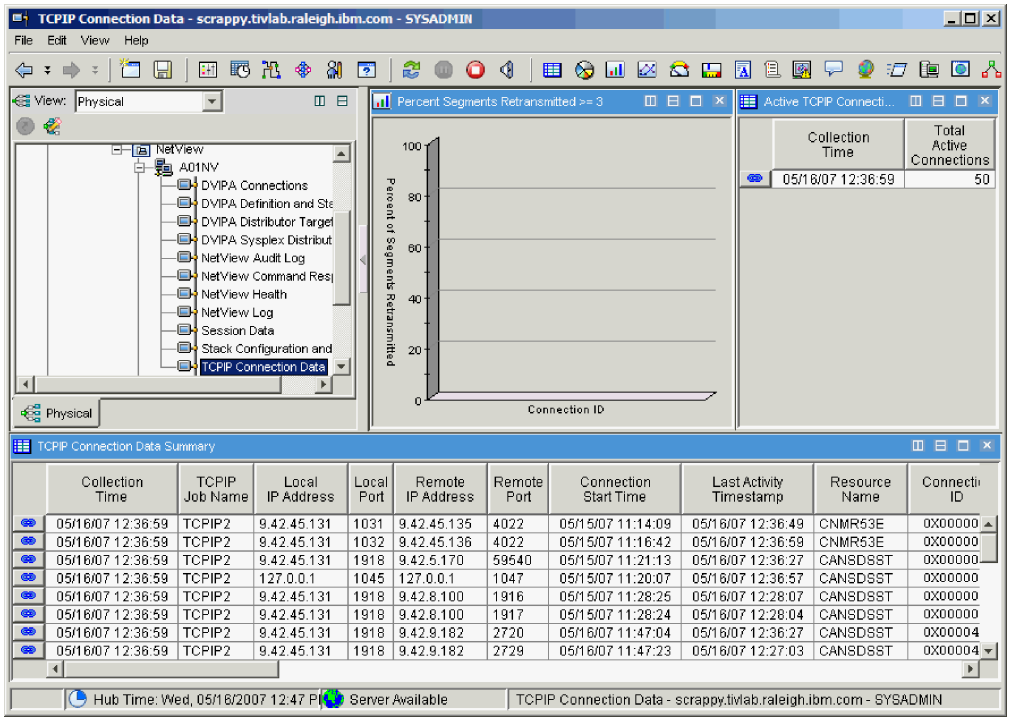


Figure 23. TCPIP Connection Data Workspace

Inactive TCPIP Connection Data Workspace

The Inactive TCPIP Connection Data workspace displays the most recent inactive connections that you specified to keep on DASD for this LPAR. You need to issue the TCPCONN DEFINE and START commands (or the CNMSTYLE equivalent) to keep inactive connection information on DASD.

Data collection for the TCPIP Inactive Connection Data workspace is controlled by the TEMA.CONINACT subtower and the associated TEMA.CONINACT statements in the CNMSTYLE member.

The data in this workspace is provided by sampling. You can issue a take action command to retrieve real-time TCP/IP connection data.

The queries assigned to the views in this workspace use the Byte Rate attribute to filter the rows that can be retrieved for display. Because of the default filter, you might not see all your connections. You can modify the query to display more or fewer connections than the default filter allows.

If you have a large installation, you might not be able to view all the available connections in the Tivoli Enterprise Portal. For more information, see the *IBM Tivoli NetView for z/OS Tuning Guide*.

The Inactive TCPIP Connection Data workspace is shown in Figure 24.

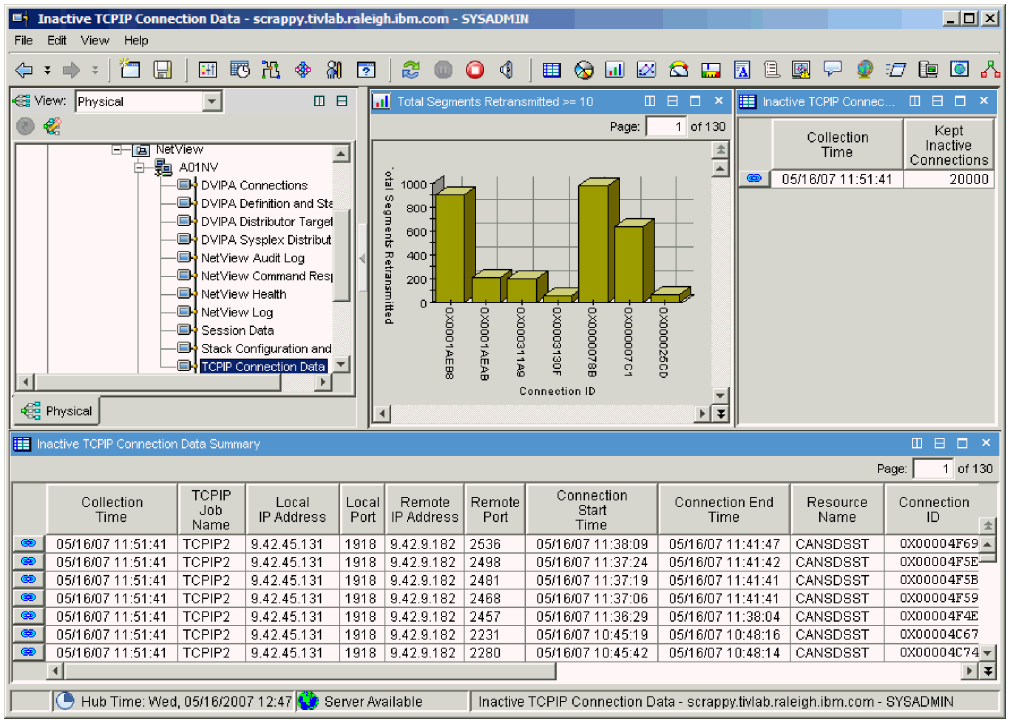


Figure 24. Inactive TCPIP Connection Data Workspace

NetView Health Workspaces

The NetView Health workspaces show the status and performance of NetView tasks. The performance statistics for the tasks can be seen on the sampled interval or historically. The data that is used is from the NetView resource utilization function.

Data collection for the NetView Health workspaces is controlled by the TEMA.HEALTH subtower and the associated TEMA.HEALTH statements in the CNMSTYLE member.

The following workspaces for NetView Health are provided:
- "NetView Tasks Workspace"
- "NetView Task Details Workspace" on page 67

NetView Tasks Workspace

The NetView Tasks workspace provides task status and performance statistics for all NetView tasks.

The data in this workspace is provided by sampling.

The tasks shown in the bar chart views (CPU Utilization >= Critical CPU Util Threshold and Storage >= Critical Storage Threshold) use values defined with the WRNCPU, WRNSTG, MAXCPU, and MAXSTG keywords of the DEFAULTS and

OVERRIDE commands. If you specify one or more values for the WRNCPU or WRNSTG keywords, then the maximum of the specified values is compared to the current CPU or storage statistic for the task. If the current CPU or storage statistic is greater than or equal to the maximum WRNCPU or maximum WRNSTG value, the task is displayed in the appropriate view. If a WRNCPU or WRNSTG value was not specified for the task, then the MAXCPU and MAXSTG values are used to determine whether the task is displayed in the view.

A situation for each performance statistic is provided for critical, warning, and informational levels. To provide a warning that a task is approaching the value when it might be penalized, the values for all of the situations should be below the maximum value specified for these statistics on the DEFAULTS and OVERRIDE commands.

The NetView Tasks workspace is shown in Figure 25.

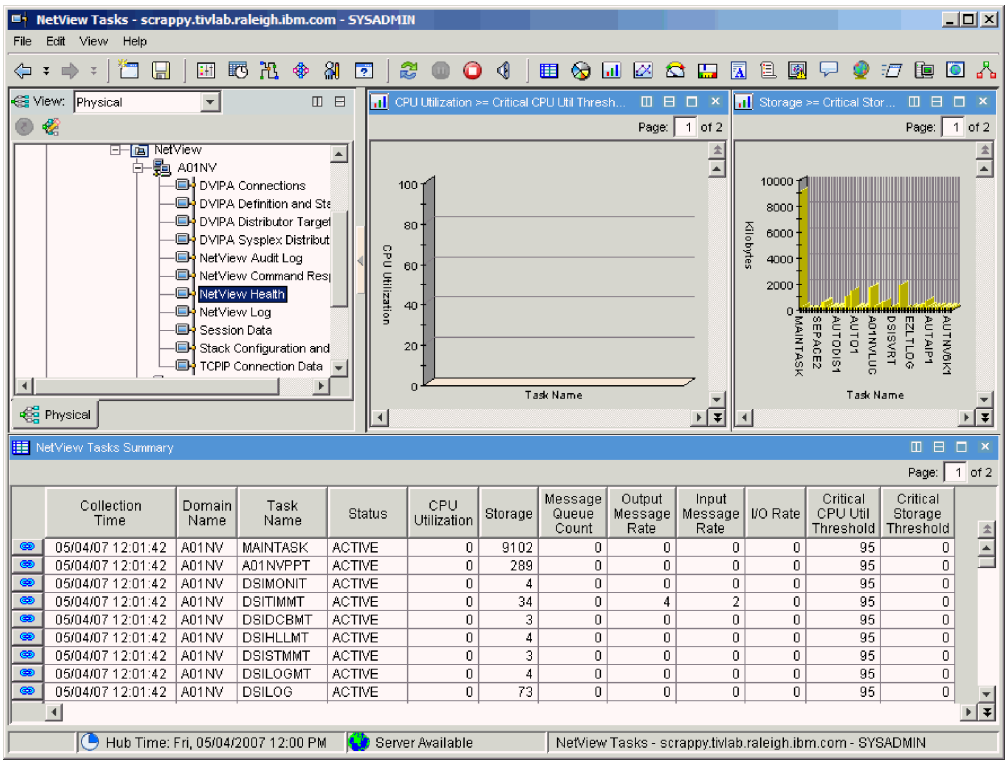


Figure 25. NetView Tasks Workspace

NetView Task Details Workspace

The NetView Task Details workspace displays six performance statistics for the task over time.

The data in this workspace is provided using historical data collection.

The NetView Task Details workspace is shown in Figure 26 on page 68.

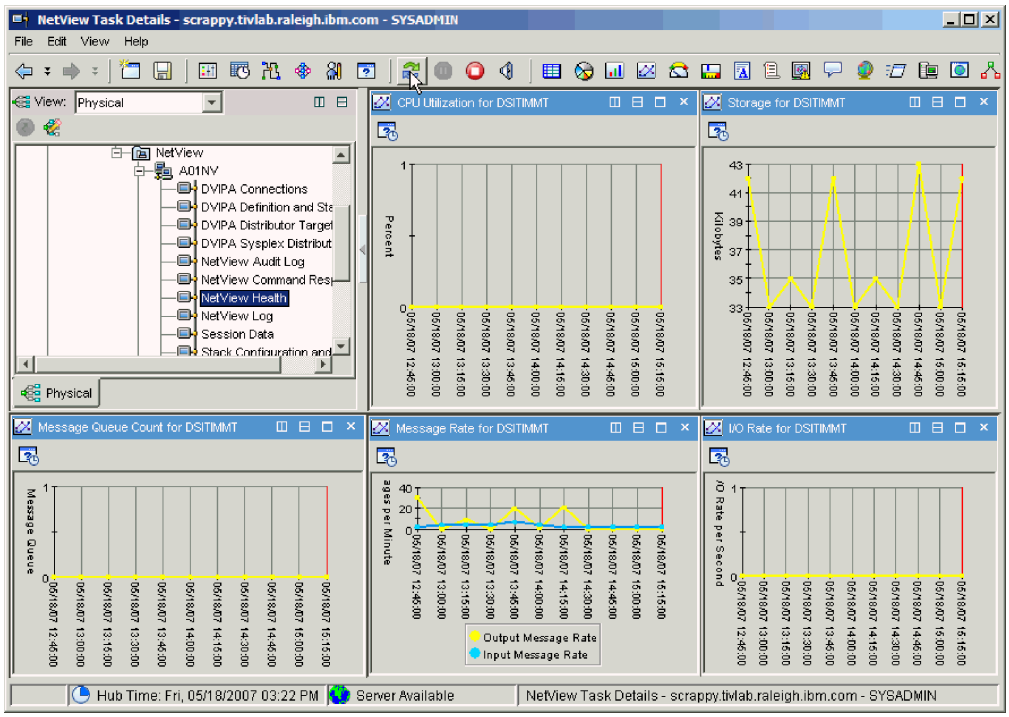


Figure 26. NetView Task Details Workspace

Other Workspaces

The following additional NetView for z/OS Enterprise Management Agent workspaces are provided:

- "Session Data Workspace"
- "NetView Log Workspace" on page 69
- "NetView Command Response Workspace" on page 70
- "NetView Audit Log Workspace" on page 71
- "Stack Configuration and Status Workspace" on page 72

Session Data Workspace

The Session Data workspace displays information about active SNA sessions.

The NLDM tower must be enabled to collect data about SNA sessions. Data collection for the Session Data workspace is controlled by the TEMA.SESSACT subtower and the associated TEMA.SESSACT statements in the CNMSTYLE member.

The data in this workspace is provided by sampling. You can issue a take action command to retrieve real-time session data.

The data in this workspace is based on the SESMGET command.

The queries assigned to the views in this workspace use the Primary Type attribute to filter the rows that can be retrieved for display. Because of the default filter, you might not see all your sessions. You can modify the query to display more or fewer sessions than the default filter allows.

If you have a large installation, you might not be able to view all the available sessions in the Tivoli Enterprise Portal. For more information, see the *IBM Tivoli NetView for z/OS Tuning Guide*.

The Session Data workspace is shown in Figure 27.

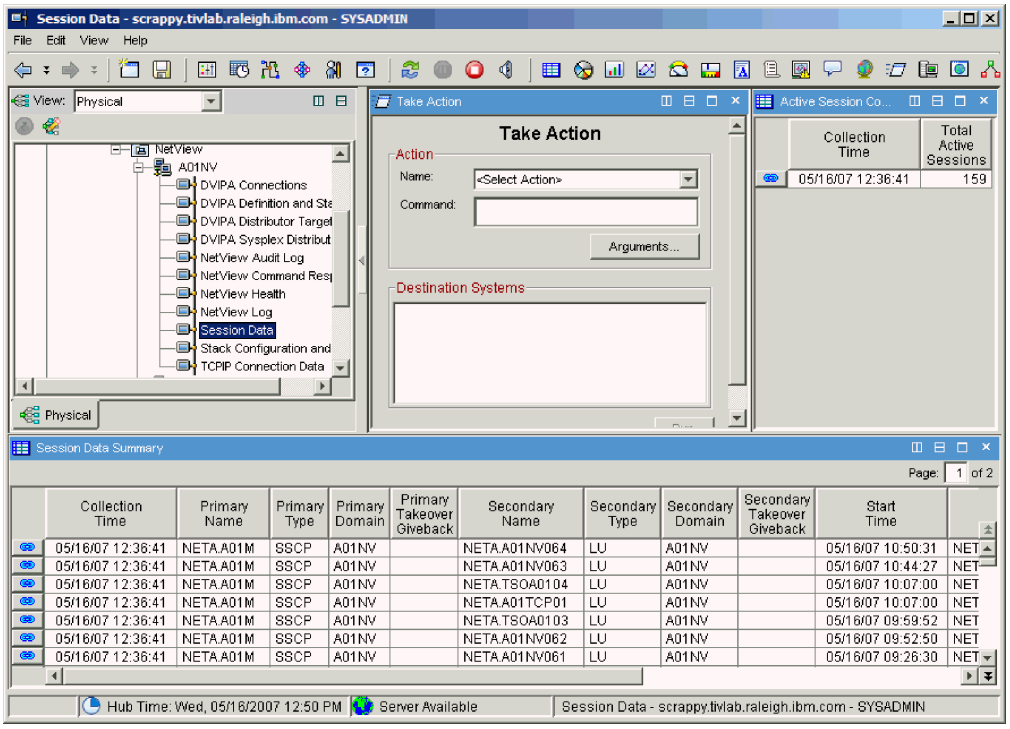


Figure 27. Session Data Workspace

NetView Log Workspace

The NetView Log workspace displays information from the NetView log.

Data in this workspace is present after the Browse NetView Logs take action command is issued and the workspace is refreshed. Error messages related to this take action command are displayed in the NetView Audit Log workspace.

The amount of data that can be displayed in this workspace is controlled by the (TEMA)NACMD.ROWSNVLOG statement in the CNMSTYLE member.

The NetView Log workspace is shown in Figure 28 on page 70.

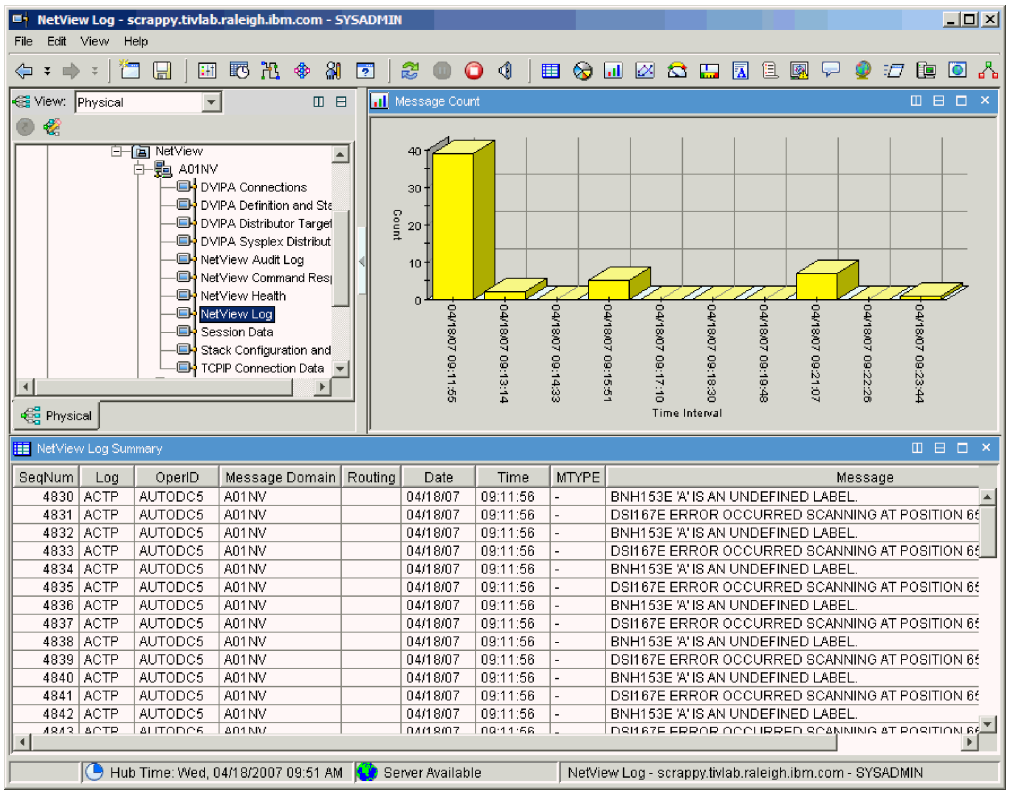


Figure 28. NetView Log Workspace

NetView Command Response Workspace

The NetView Command Response workspace displays the commands and command responses for take action commands using the NetView for z/OS Enterprise Management Agent and the APSERV receiver.

For security reasons, only commands and command responses issued by the current Tivoli Enterprise Portal user can be seen in this workspace.

Data in this workspace is present after a take action command is issued and the workspace is refreshed.

The amount of data that can be displayed in this workspace is controlled by the (TEMA)NACMD.ROWSNVCM statement in the CNMSTYLE member.

The data in this workspace wraps and is not cleared until the NACMD command is stopped and reissued.

To find a text string in this view, click the **Find** icon. In the Find window, type the text you want to find, and click **Find**.

To reverse the order of the command responses in the view, click the **Sort** icon. The default order of the command responses is the oldest at the top and the newest at the bottom.

Notes:

1. The find and sort functions work only on the page that you are viewing. The default view-level page size is 100 rows of data. This value is specified in the properties for the NetView Command Response Summary view. If you are viewing more than 100 rows of data, by default, they are displayed in several pages. To use the find and sort functions for more than 100 rows of data, set the view-level page size to return all rows or increase the number of rows to return.
2. The data for this view can span several pages. If the workspace is refreshed while you are viewing any page other than the first page, the view is reset to display the first page.

The NetView Command Response workspace is shown in Figure 29.

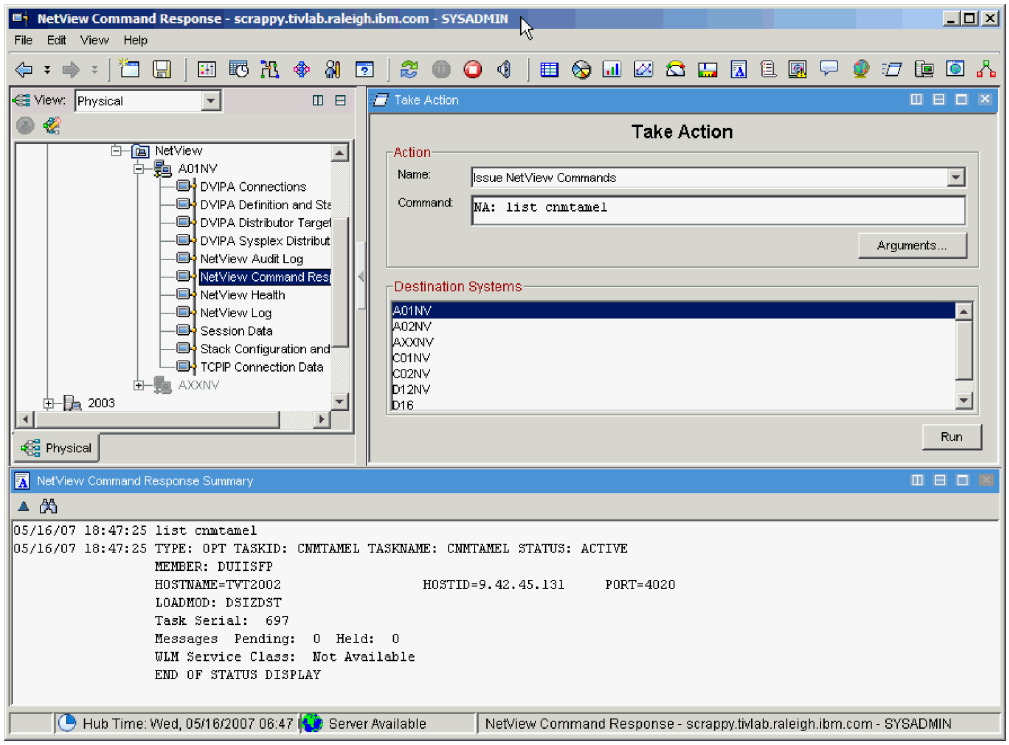


Figure 29. NetView Command Response Workspace

NetView Audit Log Workspace

The NetView Audit Log workspace displays information about take action commands issued using the NetView for z/OS Enterprise Management Agent and the APSERV receiver.

Audit trail messages BNH806I and BNH807I provide information about the command and the NetView task that processed the command.

This workspace is empty unless take action commands are issued. The amount of data that can be displayed in this workspace is controlled by the (TEMA)NACMD.ROWSAVLOG statement in the CNMSTYLE member.

The data in this workspace wraps and is not cleared until the NACMD command is stopped and reissued.

The NetView Audit Log workspace is shown in Figure 30.

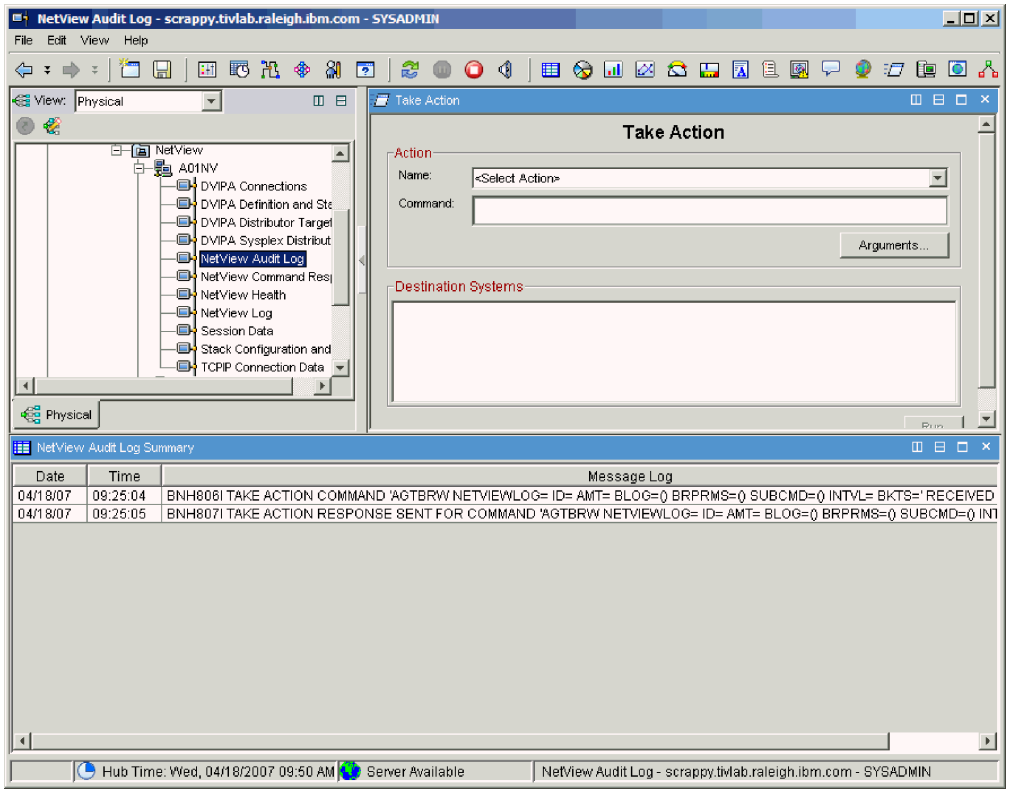


Figure 30. NetView Audit Log Workspace

Stack Configuration and Status Workspace

The Stack Configuration and Status workspace displays information about the z/OS Communications Server stacks.

The data in this workspace is real-time. This workspace is updated for the following conditions:

- When the status of your sysplex changes
- When the status of your TCP/IP stack changes
- When the NetView monitoring agent defined using the RTNDEF.BASE.AGENT statement in CNMSTYLE is not available

Data collection for the Stack Configuration and Status workspace is controlled by the TEMA.SYSPLEX subtower and the associated TEMA.SYSPLEX statements in the CNMSTYLE member.

The data in this workspace is provided by real-time events.

The Stack Configuration and Status workspace is shown in Figure 31 on page 73.

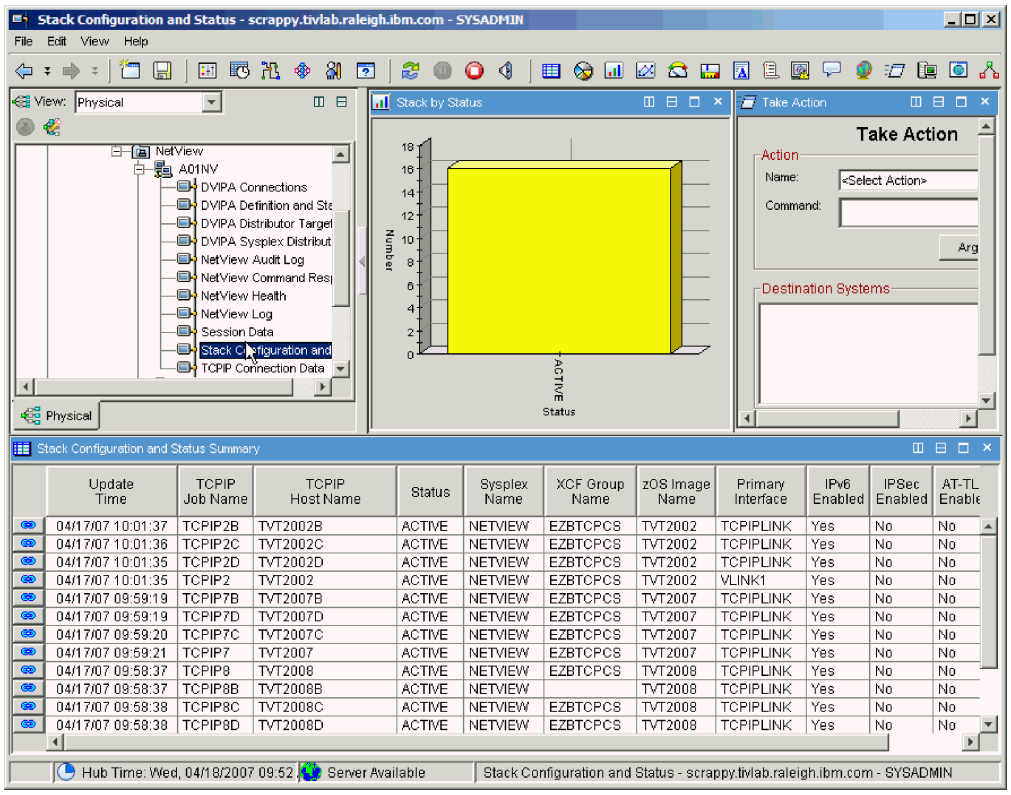


Figure 31. NetView Stack Configuration and Status Workspace

Chapter 5. Monitoring and Controlling Network Configuration

You can monitor your network and system for changes in the status of individual resources. The NetView program lets you track these changes and display the information for any required analysis. You can explicitly request status information or the NetView program can present it automatically. You can control the amount of information collected, and you can request more information, such as network and system definitions, for use in analyzing changes in status.

You can then take specific actions against individual resources to change their status, make them available for monitoring, or to manipulate their usage. This can include controlling the configuration and definition of the resources. The NetView program provides controls to limit the functions you can use and the resources you can access.

Monitoring Network Resources

You can use various programs to monitor your network. You can use some of these programs to monitor only specific types of resources, for example, SNA (subarea and Advanced Peer-to-Peer Networking) or LAN resources.

To monitor your entire network (consisting of hardware and software, SNA and non-SNA resources), use the graphical workstations.

Monitoring SNA (Subarea and Advanced Peer-to-Peer Networking) Resources

To monitor and control the network, use a combination of the following functions:

- Status monitor
- Hardware monitor
- Session monitor
- Graphic Monitor Facility host subsystem
- SNA topology manager
- User-written command lists
- Messages and message indicators
- Alerts
- NetView management console

You can use the NetView program to monitor SNA subarea networks. The NetView hardware monitor and session monitor collect information about events in the network, log this information, and display it. You can use this information to discover network problems and to monitor the performance of the network.

The NetView program can also manage SNA Advanced Peer-to-Peer Networking networks. In an SNA Advanced Peer-to-Peer Networking network, no single resource controls the network. You designate a single network node as the network management focal point so that network management can be centralized. The rest of the network nodes in the SNA Advanced Peer-to-Peer Networking network act as end nodes or entry points and filter and forward network management data to your network management focal point node.

In a multiple-domain environment, you can expand your control through the use of NetView-to-NetView communications or terminal access facility (TAF) sessions.

Monitoring Non-SNA Resources

Monitoring non-SNA resources in the network is more complex than monitoring SNA (subarea and Advanced Peer-to-Peer Networking) resources because of the various places in which the status information can be stored and the many different ways in which this information can be queried. You can monitor the status of non-SNA resource by using the NetView management console and service points.

In general, the status of non-SNA resources can be monitored from a view on an NetView management console workstation. The GMFHS collects alerts from SNA topology manager and service points. You can also send commands through service points that communicate with non-SNA networks. GMFHS stores the status of non-SNA resources in RODM. As status changes are detected by GMFHS they are sent to the workstation, where the color of the resource changes to reflect the new status.

You can also monitor and control non-SNA resources directly through service points. A display command can be sent directly to the service point application by using the NetView RUNCMD command. Depending on the service point application, this can result in an alert being sent to the NetView program or in an alert being sent and a command response being sent in reply to this command. Suppose that you enter the following command:

```
runcmd sp=sppuname,appl=applname,query dom1.resource1
```

The following responses are sent:

```
Resource DOM1.RESOURCE1 is ACTIVE
Alert Sent
```

Managing TCP/IP Connections and IP Packets

You can use NetView to collect and query TCP/IP connection data (including start and stop times, data traffic, and retransmit counts), and IP packet trace data. These functions are available only if you have enabled data collection for TCP/IP connections and IP packet traces. (See *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components* for more information.)

To start collecting connection data, use the TCPCONN START command. (You can also configure NetView to start data collection automatically during startup; see *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components* for more information.) NetView collects real-time connection data for any active connection specified by the TCPCONN.KEEP statements in CNMSTYLE or its included members. In addition, data is stored on DASD for inactive (historical) connections specified by TCPCONN.DASD statements in CNMSTYLE or its included members.

To start collecting packet trace data, use the PKTS START command.

After you have started data collection, you can use the TCPCONN QUERY and PKTS QUERY commands to retrieve the collected data based on filtering criteria you specify. For example, you can view all connections to a particular remote host, or all packets transmitted during a certain period of time.

For more information about the TCPCONN and PKTS commands, see the *IBM Tivoli NetView for z/OS Command Reference Volume 1*.

Note: Information provided by the TCPCONN QUERY command contains all connection data for inactive connections. However, only a subset of this

information is displayed for active connections. Use one of the following methods to display information for active connections:

- The NetView Web application. See Chapter 3, "Monitoring and Controlling Your Network from a Workstation," on page 45.
- The Tivoli Enterprise Portal using the Tivoli NetView for z/OS Enterprise Management Agent. See Chapter 4, "Monitoring and Controlling Your Network Using the IBM Tivoli NetView for z/OS Enterprise Management Agent," on page 51.
- For 3270 display, the TCPCONN QUERYACT command or the CNMSTCPC sample, or, for DVIPA connections, the CNMSDVPC sample. See "Monitoring Network Data using NetView Samples from a 3270 Session."

Monitoring Network Data using NetView Samples from a 3270 Session

NetView commands collect network data for various NetView components. These commands are commonly referred to as data collectors. Several NetView samples use these data collectors to provide the same data in a 3270 session. These samples provide the following data:

- TCP/IP connection data
- Dynamic virtual IP address (DVIPA) data
- TCP/IP stack configuration and status data

Each data collector returns data using one or more NetView messages. The samples that use the data collectors reformat the NetView messages and display the collected data in a more usable format. You can use input parameters with a sample to specify the data to collect. The input parameters for a sample are the same as those for the NetView command that is called by the sample. For information about the data that is returned by the data collectors, the format of the messages returned, the parameters accepted, and general information about the data collectors themselves, see the NetView for z/OS online command and message help.

Notes:

1. Because the data records that are displayed can be quite wide, these samples are based on the WINDOW command. To scroll to the right to view the data that is not currently visible on the screen, use the RIGHT function (F11 by default).
2. These samples are also used by the NetView for z/OS Enterprise Management Agent take action commands.

The following sections describes the samples provided by the NetView program to display this network data.

TCP/IP Connection Data

Table 8 lists the sample that can be used to display TCP/IP connection data.

Table 8. Sample that Displays TCP/IP Connection Data

Sample	NetView Command	Messages Returned by the Collector
CNMSTCPC	TCPCONN	BNH772I or BNH775I

Use the CNMSTCPC sample to view TCP/IP data for active and inactive connections in a 3270 session. To display this TCP/IP connection data in a different format, modify the CNMSTCPC sample or create your own application to format the data returned by the TCPCONN command.

DVIPA Data

Table 9 lists the samples that can be used to display DVIPA data.

Table 9. Samples that Display DVIPA Data

Sample	NetView Command	Messages Returned by the Collector
CNMSDVIP	DVIPSTAT	BNH846I
CNMSDVPC	DVIPCONN	BNH849I
CNMSPLEX	DVIPPLEX	BNH847I
CNMSTARG	DVIPTARG	BNH848I and BNH850I

The NetView program uses four data collectors to collect DVIPA data. Each data collector collects a different type of DVIPA data. DVIPSTAT collects DVIPA address information that is defined to your TCP/IP stack. DVIPPLEX collects information about DVIPA addresses that are defined as sysplex distributors. DVIPTARG collects information about DVIPA distributor targets as they are defined to your TCP/IP. DVIPCONN collects information about TCP/IP connections that are using a DVIPA address.

DVIPA data might or might not exist in your network. These dynamic IP addresses must be defined to a TCP/IP stack in your network. If you define DVIPA addresses in your network, you must then decide whether to configure any DVIPA sysplex distributors. DVIPA sysplex distributors can balance the workload in your sysplex and provide TCP/IP backup capabilities. If sysplex distributors are not configured within your network, DVIPA addresses can still be used to create TCP/IP connections. The need to monitor the DVIPA data in your network depends on how you have configured your network.

Even if you configure DVIPA addresses and DVIPA sysplex distributors in your network, the NetView program might not collect all the DVIPA data in your network. For DVIPA data to be collected by the NetView program, the following conditions must be met:

- The DVIPA tower in the NetView program must be enabled.
- A TCP390 statement must exist in CNMPOLCY for the given TCP/IP stack.
- A DVIPADAT keyword must be coded on the TCP390 statement for the given TCP/IP stack and must have a value of Yes.

Use the CNMSDVIP, CNMSDVPC, CNMSPLEX, and CNMSTARG samples to view DVIPA data in a 3270 session. This information includes details such as the DVIPA address, the current status of a DVIPA address, bytes sent and bytes received in a DVIPA connection, the TCP/IP host name of the TCP/IP stack to which the DVIPA address is defined, and more. To display this DVIPA data in a different format, modify the samples or create your own applications to format the data that is returned by the NetView commands that are used by these samples.

TCP/IP Stack Configuration and Status Data

Table 10 on page 79 lists the sample that can be used to display TCP/IP stack configuration and status data.

Table 10. Sample that Displays TCP/IP Stack Configuration and Status Data

Sample	NetView Command	Messages Returned by the Collector
CNMSSTAC	STACSTAT	BNH845I

Use the CNMSSTAC sample to view configuration and status information about the TCP/IP stacks in your network in a 3270 session. This information contains details such as the host name of the TCP/IP stack and the status of the stack. To display the TCP/IP stack configuration and status data in a different format, modify the CNMSSTAC sample or create your own application to format the data returned by the STACSTAT command.

Using VTAM Commands (SNA Subarea, SNA Advanced Peer-to-Peer Networking)

When VTAM activates a resource, it owns that resource. Session requests and alerts from that resource are delivered to the owning VTAM. With the hierarchical structure used in the resource definition, you can control a group of resources as a single unit. You can then activate a specified resource, the specified resource and other resources associated with it, or the specified resource and all its associated resource nodes with the initial status set to active.

When you use a VTAM DISPLAY, MODIFY, or VARY command, NetView checks your authority to issue the command and your authority to access the resource. This authorization check is either against the original issuer of the command (AUTHCHK=SOURCEID) or against the task under which the VTAM command runs (AUTHCHK=TARGETID). The AUTHCHK keyword is specified either in CNMSTYLE or its included members or on the REFRESH command.

Checking the Status of a Resource

You can use the DISPLAY ID VTAM command to check the status of a resource. For example, to check the status of an application CNM01003, enter:

```
d net,id=cnm01003,e
```

A panel similar to Figure 32 on page 80 is displayed.

```
NCCF                      Tivoli NetView      CNM01 OPER5    04/12/01 09:30:50
* CNM01    D NET,ID=CNM01003,E
  CNM01    IST097I  DISPLAY  ACCEPTED
' CNM01
IST075I  NAME = NETA.CNM01003    , TYPE = APPL
IST486I  STATUS= ACT/S     , DESIRED STATE= ACTIV
IST977I  MDLTAB=***NA*** ASLTAB=***NA***
IST861I  MODETAB=AMODETAB USSTAB=***NA*** LOGTAB=***NA***
IST934I  DLOGMOD=DSILGMOD USS LANGTAB=***NA***
IST597I  CAPABILITY-PLU ENABLED  ,SLU ENABLED  ,SESSION LIMIT NONE
IST231I  APPL     MAJOR NODE = A01APPLS
IST654I  I/O TRACE = OFF, BUFFER TRACE = OFF
IST271I  JOBNAME = E240ECNV, STEPNAME = E240ECNV, DSPNAME = 00002IST
IST1050I MAXIMUM COMPRESSION LEVEL - INPUT = 0   , OUTPUT = 0
IST171I  ACTIVE SESSIONS = 0000000001, SESSION REQUESTS = 0000000000
IST206I  SESSIONS:
IST634I  NAME     STATUS         SID          SEND RECV VR TP NETID
IST635I  A01A701  ACTIV-S    E7F38CE64E947D01 0051 0030  0  0 NETA
IST314I  END
------------------------------------------------------------------------



???
```

Figure 32. Command Facility Display for the D NET,ID Command

Notice that the application CNM01003 is active and currently has one session running. The NetView program supplies command lists (DIS, ACT, INACT, DISG) that can be used instead of the VTAM commands. For more information about these commands, see "Using NetView Commands (SNA Subarea, SNA Advanced Peer-to-Peer Networking)" on page 81, and refer to the NetView online help.

Controlling Resources Defined to VTAM

You can use VTAM commands to control SNA (subarea and Advanced Peer-to-Peer Networking) resources that are defined to VTAM. For example, if a user receives a status code of 695 at the bottom of his terminal screen, you can reset this condition in some cases by changing the status of the SNA subarea resource to inactive and then back to active.

To control SNA resources, complete the following steps from your NetView terminal:

1. To inactivate a resource named NRU0505, enter:

   ```
   v net,id=nru0505,inact
   ```

2. To reactivate the resource, enter:

   ```
   v net,id=nru0505,act
   ```

Reloading and Reactivating an NCP

To activate, inactivate, or load an NCP, complete the following steps from the NetView command facility:

1. To inactivate an NCP named NCP45, enter:

   ```
   v net,id=ncp45,inact
   ```

2. To activate and load the NCP, enter:

   ```
   v net,id=ncp45,act,load=yes
   ```

Using NetView Commands (SNA Subarea, SNA Advanced Peer-to-Peer Networking)

You can use NetView commands to control all or part of a domain by requesting both hardware and software data from network resources. This data can be used to determine when errors occur in the network.

Using the APPLSPEN Command

You can use the APPLSPEN command to list sessions in a specific state for a particular application program. For example, to display all active sessions with the application named a01a701, enter the following command:

```
applspen a01a701,act
```

The system responds with messages similar to the following messages:

```
CNM221I APPLSPEN : NAME = 'A01A701', STATUS = 'ACT/S',
        DESIRED STATE = 'ACTIV'
CNM220I APPLSPEN : ACTIVE SESSIONS = '0000000001',
        SESSION REQUESTS = '0000000000'
CNM311I APPLSPEN : NAME     STATUS    SESSION ID
CNM313I APPLSPEN : TSO0101  ACTIV-P   E7FF38CE6EE8A9AD7
CNM312I APPLSPEN : 1 SESSION(S) IN THE ACT STATE FOR A01A701
```

Using the DISG Command

You can use the DISG command list to display the status of resources and to provide connectivity information for LUs, PUs, lines, network control programs (NCPs), and major nodes.

Note: The DISG command cannot be routed to a remote NetView program. To process the DISG command in a remote NetView program, you must log on to that NetView program either directly or through the use of the terminal access facility (TAF) for NetView.

To issue a DISG command, enter the DISG command followed by the name of the resource. For example, to display the resource status for PU A04P1092, enter the following command:

```
disg a04p1092
```

A panel similar to Figure 33 on page 82 is displayed.

```
CNM0PU01               VTAM DISPLAY : PHYSICAL UNIT               PAGE 1 OF 6
------------      ------------                ------------
|   HOST   |      | LOCAL NCP|    LINE       |    PU    |  --------------------
| HOSTA99  | 0002 | A04B62S  |--- A04N1092 --| A04P1092 |-| LOGICAL UNITS 1-16:
------------      ------------                ------------ |
                  ACTIV        ACTIV          ACTIV

SIO= 02604    DESIRED= ACTIV  DESIRED= ACTIV DESIRED= ACTIV
I/O TRC= OFF  I/O TRC= OFF    TYPE= LEASED   I/O TRC= OFF
BUF TRC= OFF  BUF TRC= OFF    LNCTL= SDLC    BUF TRC= OFF
SUBAREA= 99   SUBAREA= 4
IRN TRC= OFF  NETA            GROUP= A04PGRP1




Select:
  1  NCP       2  Line    3  Link Station



TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
Action===>
```

Figure 33. Display of a Physical Unit

This panel is useful in determining the highest level node that is inactive or disabled. You can then use the highest level inactive resource as your starting point in isolating problems.

Depending on how the resource is connected, you can display detailed information on specific components. In this example, you can display detailed information on the NCP, line, and link station shown in the connectivity diagram. For example, if you choose to display detailed information for the NCPs, a panel similar to Figure 34 on page 83 is displayed.

```
CNM0NCP1                    VTAM DISPLAY : NCP                    PAGE 1 OF 6
------------      ------------   ---------------------------------------------
|   HOST   |      | LOCAL NCP|   | ATTACHED LINES 1 - 32 :
| HOSTA99  | 0002 | A04B62S  |---| A04N1092 ACTIV          J000401D ACTIV
------------      ------------     A04N1093 ACTIV          J000401F ACTIV
                  ACTIV            J0004001 ACTIV          J0004021 ACTIV
                                   J0004003 ACTIV          J0004023 ACTIV
SIO= 02604        DESIRED= ACTIV   J0004005 ACTIV          J0004025 ACTIV
I/O TRC= OFF      I/O TRC= OFF     J0004007 ACTIV          J0004027 ACTIV
BUF TRC= OFF      BUF TRC= OFF     J0004009 ACTIV          J0004029 ACTIV
SUBAREA= 99       SUBAREA= 4       J000400B ACTIV          J000402B ACTIV
IRN TRC= OFF      NETA             J000400D ACTIV          J000402D ACTIV
                                   J000400F ACTIV          J000402F ACTIV
                                   J0004011 ACTIV          J0004031 ACTIV
                                   J0004013 ACTIV          J0004033 ACTIV
                                   J0004015 ACTIV          J0004035 ACTIV
                                   J0004017 ACTIV          J0004037 ACTIV
                                   J0004019 ACTIV          J0004039 ACTIV
                                   J000401B ACTIV          J000403B ACTIV
 LOAD/DUMP PROCEDURE STATUS = RESET


TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
Action===>
```

Figure 34. Detailed NCP Information

Using the RMTCMD Command

To control resources that are managed by a remote NetView program from your local NetView program, use the RMTCMD command. This command is especially useful when you want to issue a sequence of commands to one or more remote NetView programs.

Sending Commands

The following example uses the local NetView program and a remote NetView program named CNM02. Complete the following steps to activate an NCP controlled by the VTAM program on CNM02:

1. From your local NetView console, enter the following command:

   ```
   rmtcmd lu=cnm02,act ncp2
   ```

   This command establishes an association with a RMTCMD autotask using the same name as your operator ID running in the remote NetView program CNM02.

2. To ensure the NCP is now active, enter:

   ```
   rmtcmd lu=cnm02,dis ncp2
   ```

   The command response indicates that you activated the NCP successfully.

The first time you issue the RMTCMD command, the NetView program establishes an association between your operator ID and your RMTCMD autotask in the remote NetView program. Subsequent commands are sent using this association. The association remains active until:

- You log off your local NetView program.
- You send a LOGOFF command to your RMTCMD autotask.
- You enter an ENDTASK command from your local NetView console. The NetView program then ends your RMTCMD autotask:

  ```
  endtask lu=cnm02,stop
  ```

- An SNA sense code is received indicating a communication failure with the remote NetView.

Listing the Autotasks You Started

To list the active RMTCMD autotasks which you started, enter the following command from your local NetView console:

```
rmtsess
```

A list of the RMTCMD autotasks which you have started is displayed. An example is shown on Figure 35:

```
NCCF         Tivoli NetView                CNM01 OPER1     04/12/01 11:06:36
C CNM01
BNH060I RMTCMD QUERY INFORMATION
BNH061I ------------------------------------
BNH083I REMOTE             RMTCMD     REMOTE
BNH084I NETVIEW            AUTOTASK   VERSION
BNH061I -----------------  ---------  -------
BNH085I NETA.CNM01         OPER1      V3R1
BNH085I NETA.CNM01         OPER5      V3R1
BNH085I NETB.CNM20         *UNKNOWN*  V2R3









???
RMTSESS
```

Figure 35. Sample Output from the RMTSESS Command

Notice in this example that the operator started two RMTCMD autotasks on NETA.CNM01: OPER1 and OPER5. Also, the operator started a RMTCMD autotask on NETB.CNM20, but the specific details cannot be listed because the NetView version is V2R3. Details are only available from NetView V2R4 and later releases.

Restricting Access before Using the RMTCMD Command

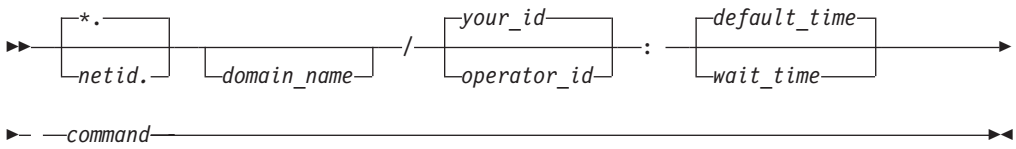
Before using the RMTCMD command, you should consider how to restrict access to cross-domain resources and commands. To restrict access, you can have the NetView program validate an operator's authority to start or stop an autotask through the RMTCMD command.

Using Labels to Route Commands

You can use a label to route a command so it processes under another task, either within your NetView or to a remote NetView. The syntax is shorter than using the NetView RMTCMD or EXCMD commands, and labels provide correlated responses, which is useful to hold responses with commands and in conjunction with a NetView pipe CORRCMD stage.

Syntax

In the simplest case, entering `/: command` allows the label to default to your domain and your operator ID. In this case, the label prefix bypasses RMTCMD or EXCMD processing, and simply correlates the responses with the command.



Where:

netid Specifies the VTAM network ID that should be used for routing the command. If specified, the *netid* value, including an asterisk (*), must be followed by a period (.). If you do not specify a value or an asterisk, the default value is to find the network ID dynamically. See the description of the RMTCMD command in the *IBM Tivoli NetView for z/OS Command Reference Volume 1* for more information.

domain_name
Specifies the application name (such as CNM02) of the NetView program to which the command should be routed. The presence of this value determines that the label is treated like a RMTCMD SEND request.

If the domain name that you specify was defined for IP routing by your system programmer (using a RMTSYN statement in CNMSTYLE or its included members), your command is routed over TCP/IP.

operator_id
Specifies the name of the operator task where the command should process. If you specify an *opid* value, other than your operator ID, the label is treated like an EXCMD command. If you do not specify a value or enter an asterisk (*), the default is to send the command to your operator ID.

wait_time
Specifies the maximum time in seconds that the command running on the target is to collect correlated messages.

If you do not specify *wait_time*, the *default_time* is defined by the CCDEF command specifications, such as the NetView-supplied values in the DSICCDEF profile. If the label specifies a remote domain, the *default_time* of the CCDEF specifications at the remote domain determines the default wait time.

command
Specifies the command, keyword, or values, which are routed and correlated by the label prefix.

Usage Notes

The following list includes usage considerations:

- A label can be used anywhere a regular NetView command can be entered, except on the assembler interface described in *IBM Tivoli NetView for z/OS Programming: Assembler*.
- You must enter a blank before any command, immediately after the colon. No blanks can be used within the label.

- Error conditions and messages, including authority checking, typically apply as if you had entered a RMTCMD or EXCMD command. Unlike RMTCMD or EXCMD, the label syntax causes correlated responses from the command to be returned to the originator. For more information, refer to the description of the NetView RMTCMD and EXCMD commands in the NetView online help.
- If your label addresses a remote NetView program, the command is transmitted by either LU 6.2 or TCP/IP as determined by the RMTSYN definitions in your style member.
- When using labeled commands to send a VTAM command to a remote VTAM, ensure the automation table entries for IST097I match in both the local and remote NetView systems.
- For commands with slower than expected response times (for example MVS ROUTE), you might need to set longer time-out values. The slower response time causes the target task to remain in a wait state, possibly delaying other scheduled commands. For some commands, responses received after the time-out interval is displayed at the target task (but not returned to the labeled command issuer). You can browse the NetView log on the target domain to see the responses. The VTAM VARY and MVS commands are in this category, along with commands that your system programmer has identified with PERSIST in the CCDEF definitions.

Topic:	Reference:
ENDTASK, REFRESH, RMTCMD command	NetView online help
Defining RMTCMD and RMTCMD Security	*IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*
Security Definitions (RMTSEC and RMTSECUR parameters)	*IBM Tivoli NetView for z/OS Administration Reference*

Example

The following example shows how to use the `/AUTO1: QRYGLOBL TASK,VARS=*` command to query the values of a task global variable under another task:

```
* NTV7E    /AUTO1: QRYGLOBL TASK,VARS=*
! NTV7E    QRYGLOBL TASK,VARS=*
' NTV7E
BNH031I NETVIEW GLOBAL VARIABLE INFORMATION
BNH103I COMMAND ISSUED AT: 05/23/01 08:38:25
BNH061I
BNH033I TASK GLOBAL VARIABLES FOR AUTO1
BNH036I GLOBAL VARIABLE NAME:               GLOBAL VARIABLE VALUE:
BNH061I ---------------------               ----------------------
BNH039I GLTIME                              99/05/23 08:37:31
BNH039I LINKOPER                            GEORGE
BNH035I NUMBER OF VARIABLES FOUND: 2
BNH061I
BNH037I NETVIEW GLOBAL VARIABLE INFORMATION COMPLETE
```

Figure 36. Querying the Values of a Task Global Variable

Using the LAN Command List

You can use the LAN command list to communicate with a LAN Network Manager service point to display configuration information for workstations on a

LAN. To use the LAN command list, establish an ownership (SSCP-PU) session between the NetView program and the LAN Network Manager to enable alerts and commands to flow.

Note: Before using the NetView LAN command for a given service point, the service point must be defined to VTAM.

The following steps show how you can use the NetView program with either LAN Network Manager Version 1.1 or LAN Network Manager Entry Version 1.0 to display configuration information.

1. For management purposes, LANs are divided into segments. To display a list of the segments managed by service point LNMSP1, enter:

   ```
   lan qnetwork status lnmsp1
   ```

   Figure 37 is displayed.

```
NCCF                    Tivoli NetView    NTVC0 OPER            04/12/01 16:10:47
T ORIGIN   OPER/JOB
* NTVC0    OPER1    LAN QNETWORK STATUS LNMSP1
C NTVC0    OPER1    CNM377I QNETWORK:INPUT ACCEPTED AND BEING PROCESSED. PLEASE WAIT
C NTVC0    OPER1    SEGMENT NUMBER  SEGMENT TYPE              SEGMENT STATUS
C NTVC0    OPER1    0001            TOKEN-RING 16MBPS         NORMAL
C NTVC0    OPER1    0002            TOKEN-RING 4MBPS          NORMAL
C NTVC0    OPER1    0003            TOKEN-RING 16MBPS         NORMAL
C NTVC0    OPER1    0004            TOKEN-RING 4MBPS          NORMAL
C NTVC0    OPER1    DFI999 OPERATION COMPLETED SUCCESSFULLY.
```

Figure 37. Response from LAN QNETWORK Command

   Notice that this command lists all the segments, the status of each segment, and the type of each segment. For example, segment 0001 has a status of normal and a segment type of token-ring 16 Mbps while segment 0002 has a segment type of token-ring 4 Mbps.

2. To display all the adapters that are known to exist on segment 0002 enter:

   ```
   lan sp=lnmsp1 adp list seg=0002
   ```

   Figure 38 is displayed.

```
NCCF                    Tivoli NetView    NTVC0 OPER1           04/12/01 16:12:12
T ORIGIN   OPER/JOB
* NTVC0    OPER1    LAN ADAPTER LIST 002 LNMSP1
C NTVC0    OPER1    CNM377I ADAPTER:INPUT ACCEPTED AND BEING PROCESSED. PLEASE WAIT
C NTVC0    OPER1    ADAPTER LIST     SEGMENT = 0002    TYPE = TOKEN-RING 4MBPS
C NTVC0    OPER1
C NTVC0    OPER1    ADAPTER ADDR  ADAPTER NAME         ADAPTER ADDR  ADAPTER NAME
C NTVC0    OPER1    10005A258085                       10005A4F35AA
C NTVC0    OPER1    10005AEBD098                       10005AC952C8
C NTVC0    OPER1    10005A8C6F2E                       10005AC3F9B0
C NTVC0    OPER1    10005A8C5EAC                       40001A2A2C08
C NTVC0    OPER1    40001A2A2C07                       10005A8CCD98
C NTVC0    OPER1    10005AF81432                       10005AEBD28B
C NTVC0    OPER1    DFI999 OPERATION COMPLETED SUCCESSFULLY.
```

Figure 38. Response from LAN ADP Command

   Notice that one of the adapters on segment 0002 is adapter 10005A258085.

3. To show the characteristics maintained by LAN Station Manager for the workstation containing this adapter enter:

   ```
   lan sp=lnmsp1 adp query adp=10005a258085 seg=0002 attr=pcinfo
   ```

Figure 39 shows the response.

```
.      STATION PROFILE
ADAPTER ADDRESS/NAME...........: 10005A258085/
LAN SEGMENT NUMBER.............: 002
LAN SEGMENT TYPE...............: TOKEN-RING 4MBPS
.         PERSONAL COMPUTER INFORMATION
USER DEFINED DATA:
LAN STATION MANAGER PROGRAM VERSION.: 1
OPERATING SYSTEM: OS/2 2.1
WORKSTATION LOCATION:
WORKSTATION TYPE:
WORKSTATION SERIAL NUMBER:
DISPLAY TYPE: PS/2 8513 or 8514
DISPLAY SERIAL NUMBER:
PRINTER TYPE:
PRINTER SERIAL NUMBER:
KEYBOARD TYPE:
KEYBOARD SERIAL NUMBER:
DEVICE 1 TYPE:
DEVICE 1 SERIAL NUMBER:
DEVICE 2 TYPE:
DEVICE 2 SERIAL NUMBER:
.       MEMORY
ROM DATE ..........: 10/28/92
BASE MEMORY.........: 16000 KB
EXTENDED MEMORY....: KB
EXPANDED MEMORY....: KB
.           DISK DRIVES
DISK DRIVE ID DRIVE CAPACITY IN MBYTES
------------- ------------------------
DISKETTE DRIVE 1 2.88 MB
FIXED DISK 1 379 MB
.     ADAPTER LIST
MICROCHANNEL ADAPTERS
ADAPTER ID DESCRIPTION
---------- --------------------------------------------------
8FDA   E000
IBM Token-Ring Network Adapter/ADEFF
IBM MultiProtocol Communications Adapter
DFI999 OPERATION COMPLETED SUCCESSFULLY.
```

Figure 39. Response from LAN ADP Command-Workstation Characteristics

Notice that the workstation is running OS/2® 2.1, has 16 MB of memory, and contains not only a token-ring network adapter, but also a multiprotocol communications adapter.

4. To display the attachment data for the same adapter, enter the following command:

   ```
   lan sp=lnmsp1 adp query adp=10005a258085 seg=0002 attr=attach
   ```

   Figure 40 on page 89 shows the response.

```
.        STATION PROFILE
 ADAPTER ADDRESS/NAME.........: 10005A258085
 STATUS.......................:
 LAN SEGMENT NUMBER...........: 002
 LAN SEGMENT TYPE.............: TOKEN-RING 4MBPS
 NAUN ADDRESS/NAME............: 10005A6D16BA
 MICROCODE LEVEL..............: 000002342279A
 UNIVERSAL ADDRESS............:
 GROUP ADDRESS................: 00000000
 FUNCTIONAL ADDRESSES.........: 00000080
 MONITORED....................: NO
 TRACING AUTHORIZED...........: NO
 TIME AUTHORIZED..............: 0000-2400

 DAYS AUTHORIZED..............: SUN-SAT
 COMMENTS.....................:
.     PC NETWORK COUNTER INFORMATION
 CRC ERRORS...................:
 ALIGNMENT ERRORS.............:
 COLLISION NUMBER.............:
 RESOURCE ERROR...............:
 ABORTED TRANSMISSIONS........:

 PACKETS SENT.................:
 PACKETS RECEIVED.............:
```

Figure 40. Response from LAN ADP Command - Attachment Data

Notice that the microcode level of the adapter and the adapter address of the nearest active upstream neighbor (NAUN) are shown.

Using the TOPOSNA Command

To control the collection of SNA subarea and Advanced Peer-to-Peer Networking topology information, use the TOPOSNA command. You can start the SNA topology manager manually using the STARTCNM SNATM command, or you can automatically start it using the NetView automation table with DSIPARM member FLBAUT.

Monitoring Topology Information

Topology information is one of three categories:

Network topology

For Advanced Peer-to-Peer Networking, network topology consists of all the network nodes within a particular subnetwork and the TG circuits connecting them.

For subarea, network topology consists of all CDRMs that are active at the node where the topology is being collected.

Local topology

For Advanced Peer-to-Peer Networking, local topology consists of the node where the topology is being collected and all adjacent nodes, connections to those adjacent nodes, and the local underlying ports and logical links making up those connections.

For subarea, local topology consists of the resources (except LUs) contained in the domain of the node where the topology is being collected.

LU topology

For VTAM agents only, consists of both dependent and independent LUs of various types such as terminals, applications, and CDRSCs.

To collect topology information, use the TOPOSNA MONITOR command. For example, to begin collection of network topology from the agent residing at node A11M, enter:

```
toposna monitor node=a11m network
```

Monitoring Critical LUs

You can monitor critical LUs using the TOPOSNA CRITICAL command. This command causes NetView to discover the LU through VTAM, create an object in RODM, and monitor the status of the LU. A CDRSC must be known in the domain where the LU is monitored before the TOPOSNA CRITICAL command can be issued. For example, to begin monitoring a critical LU named N3111LUC in the node A11M in network NETA, enter:

```
toposna critical startmon=neta.a11m.neta.n3111luc
```

You can create a member in DSIOPEN that contains a list of critical LUs to be monitored. You can then use the REFRESHC command to start or stop monitoring of these LUs. NetView provides a sample list FLBCRLUS (FLBS8002). To start monitoring critical LUs listed in member FLBCRLUS, enter:

```
refreshc startmon member=flbcrlus
```

Displaying the Status of Monitoring Requests

You can display a list of the nodes which are currently being monitored using the TOPOSNA LISTREQS command. This command lists the type of monitoring in effect, the status of the monitor request, and the duration of the monitor request. Use the TOPOSNA CRITICAL command with the LIST keyword to display a list of LUs and CDRSCs that the SNA topology manager is currently monitoring continuously.

Using the Session Monitor (SNA Subarea, SNA Advanced Peer-to-Peer Networking)

The primary tool for solving logical problems dealing with sessions is the NetView session monitor. The session monitor collects and correlates data about SNA (subarea and Advanced Peer-to-Peer Networking) sessions. The session monitor also helps identify network problems and conditions that might cause errors. Some examples of this are failing or unresponsive terminals, lost path information units (PIUs), buffer errors, and resource status errors.

The session monitor collects data about same-domain, cross-domain, and cross-network subarea sessions and SNA Advanced Peer-to-Peer Networking sessions, and maintains the collected data on a session basis. The SNA subarea sessions can involve non-SNA terminals supported by the Network Terminal Option (NTO). These NTO sessions are seen by the host as normal SNA sessions. The session monitor also collects data about data flows for certain non-SNA terminals that are not supported by NTO.

You can use the session monitor to display information about resources in pure SNA subarea, pure SNA Advanced Peer-to-Peer Networking, or mixed networks. This information includes:

- Session parameter data
- Session configuration data
- Session event time stamps
- Session partner identification
- Session response time
- Session trace data

- Session virtual-route data, explicit-route data, and Advanced Peer-to-Peer Networking route data
- Advanced Peer-to-Peer Networking flow control data
- Transmission group information

The data is stored in virtual memory and at session end is written to the VSAM database. See Figure 41 for an overview of the sources of session monitor data.

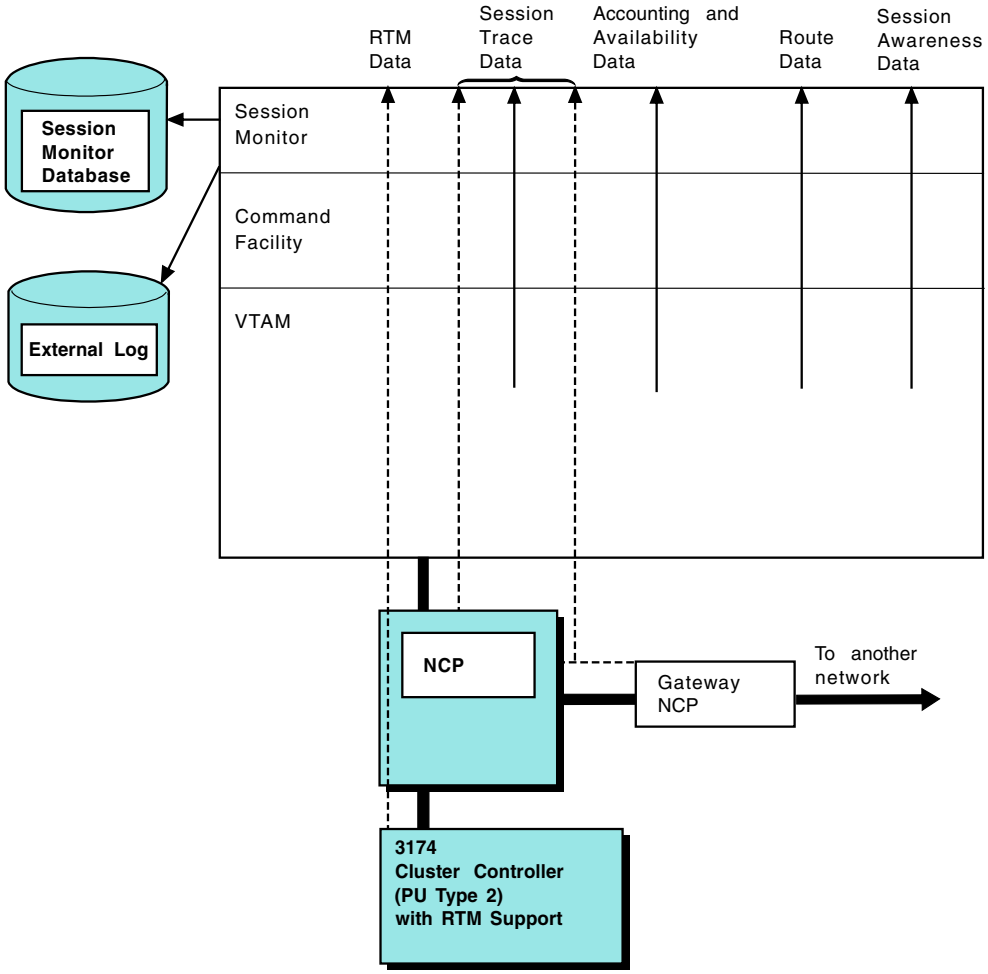


Figure 41. Session Monitor Data Collection

Session Response Time Data

The session monitor collects the response time data on command and when the session ends, and displays the data in various formats. The control units accumulate the measured response times into ranges of time that are specified by the performance class definitions. Sessions are associated with certain performance classes, and each performance class has associated with it a specific response time objective. You can display response-time graphs that show how the actual response time compares to a specified objective.

Response time data is displayed in:
- Response time summary for a terminal LU
- Response time trend for a terminal LU

- Response time for a session by collection period

Response time and configuration data for each session can be written to an external log as the response time data is collected, allowing other programs to process it.

Session Trace Data

Session trace data consists of session activation parameters, VTAM path information unit (PIU) data, and network control program (NCP) data.

Before the session monitor collects session trace data, start a session trace. You can start a trace for a resource before it is activated. After you start a trace for a node, the session monitor remembers to trace the node if it is deactivated and then activated again. NCP gateway trace data does not depend on trace activation status.

You can display the parameters used in session activation. Session activation parameters are those parameters included in the SNA command used to activate the session. BIND, activate physical unit (ACTPU), activate logical unit (ACTLU), and activate cross-domain resource manager (ACTCDRM) are examples of those commands. The session activation parameters can be displayed in hexadecimal or text representation.

You can display two types of NCP trace data for sessions involving NCP-attached resources: boundary function trace data and gateway trace data. Boundary function NCP data consists of the last four PIU sequence numbers (the last two outbound and last two inbound) and selected fields from control blocks passed to the session monitor from the NCP. (These fields are described in *NCP and EP Reference Summary and Data Areas* .) Gateway NCP data consists of the last four PIU sequence numbers (the last two outbound and the last two inbound) to cross the gateway NCP. This data also contains all control blocks sent from the gateway NCP. The NCP control blocks displayed depend on the type of resource in the session.

You can display VTAM PIU data of all sessions for which the session monitor collects session trace data. PIU data includes the transmission header (TH), the request/response header (RH), and the request unit (RU). Truncated PIUs have a maximum of 11 bytes of the RU displayed; otherwise the complete PIU is displayed. PIU data can be displayed in hexadecimal or text representation.

PIUs that are discarded by VTAM are transferred to the session monitor for trace processing. These PIUs fall into two main categories:

- PIUs that are associated with a specific active session and are discarded because of a protocol violation; for example, a data count field (DCF) that is not valid
- PIUs that are discarded because they are not associated with a specific active session; for example, extraneous traffic

In each case, the session monitor retains copies of the discarded PIUs in a *pseudosession* trace buffer. You can access this buffer using the following command:

```
sess *discard
```

Because the PIUs in this area are associated with many different sessions, no session parameters or session configuration data are available. However, selection from the SESS panel displays the trace data. The size of the *DISCARD area is specified by the session monitor KEEPDISC initialization statement. The

*DISCARD data is not saved in the VSAM database when the session monitor is brought down unless the save is set up by a FORCE command. You can use this command with a timer-driven command list.

If associated with a specific session, PIUs discarded by the access method are inserted in the active session's PIU wrap area. You can then examine the discarded PIU in the context of that session's PIU flow. If the PIU is discarded from this area (because of session activity), a copy can still exist in the *DISCARD file.

Network Accounting and Availability Measurement Data

Network accounting and availability data measurement provides you with network availability data and distribution of use of network resources. Start this function when you initialize the session monitor. The measured data is written to an external log by the RECORD command and at session end for offline processing. See the *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components* for your operating system for more information.

Route Data

Active route data is collected whenever a route is first used by a session. The route information includes a list of PUs and transmission groups (TGs) that make up the explicit route. Use the session monitor to view the route data and then proceed into the session hierarchy on a route-by-route basis.

Active route data is displayed in the following ways:

- Active explicit route list
- Active virtual route list
- Active virtual route status
- Explicit route configuration
- Transmission group information
- Advanced Peer-to-Peer Networking route data

Session Awareness Data

Session awareness data is information about session activity within the networks. This data identifies the partners of each session, which can be in the same domain, in different domains, or in different networks.

When the session monitor is active, session awareness data is collected whenever a session begins or ends. Session awareness data consists of information from VTAM, such as:

- Session activation status
- Session type
- Session partner names

  Session partners can be:
  - Logical unit to logical unit (LU-LU)
  - System services control point to logical unit (SSCP-LU)
  - System services control point to physical unit (SSCP-PU)
  - System services control point to system services control point (SSCP-SSCP)
  - Control point to control point (CP-CP)
- LU application states, such as:
  - Active
  - Inactive
  - Recovery pending
  - Recovery in progress

  - Recovery complete
- Session configuration data

Activation status includes BIND failure, UNBIND reason and sense codes, and INIT failure. Session awareness data includes information about the activation status for certain non-SNA terminals not supported by the Network Terminal Option.

Session awareness data is displayed in various forms. Some examples are resource lists, domain lists, session histories for specific resources, and session configuration diagrams. Session awareness data is required for all other types of data collection.

Setting Up the Session Monitor

To view the data described in the previous section, ensure that the session monitor is defined correctly, especially with regard to defining session awareness data, trace data, and so on. For additional information on defining the session monitor, refer to the *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components* . In addition:

- To collect data for cross-domain sessions, a session monitor must be available in each domain.
- To collect data for cross-network sessions, a session monitor must be available in each gateway host on the session path and at the session end points.
- To collect data for SNA Advanced Peer-to-Peer Networking sessions, a session monitor must be available at the Interchange node.

Session Monitor Scenarios

The scenarios in this section show how to navigate through the session monitor panels. A brief description of each panel is provided. You can get general online help for session monitor by entering `help nldm` from the command line. You can obtain specific field level help by entering the following command, where *term* specifies one or more words of the field:

```
help nldm 'term'
```

The scenarios illustrate the following kinds of sessions:

- An LU-LU session for an SNA subarea network
- A CP-CP session for an SNA Advanced Peer-to-Peer Networking network
- An LU-LU session for an SNA Advanced Peer-to-Peer Networking or mixed network
- An SNA session through an Advanced Peer-to-Peer Networking Network (DLUR/DLUS)
- An LU-LU session for an SNA Advanced Peer-to-Peer Networking or mixed network showing Takeover/Giveback data

In addition, the Session and Storage Information panel (obtained with the SESSMDIS command) is explained in detail.

For help on any term on these screens, type:

```
HELP NLDM 'term'
```

Typical LU-LU Session for an SNA Subarea Network

To monitor an LU-LU session for an SNA subarea network:

1. Type **nldm** at the command line to access the session monitor main menu. A panel similar to Figure 42 is displayed.

```
NLDM.MENU                                                          PAGE   1
                                 Tivoli NetView


                                 DOMAIN  CNM09

  SEL#                            DESCRIPTION

  ( 1)   LUNAME LIST     LIST OF ALL ACTIVE LOGICAL UNIT NAMES
  ( 2)   SLUNAME LIST    LIST OF ACTIVE SECONDARY LOGICAL UNIT NAMES
  ( 3)   PLUNAME LIST    LIST OF ACTIVE PRIMARY LOGICAL UNIT NAMES
  ( 4)   PUNAME LIST     LIST OF ACTIVE PHYSICAL UNIT NAMES
  ( 5)   CPNAME LIST     LIST OF ACTIVE CP AND SSCP NAMES
  ( 6)   DOMAIN LIST     LIST OF NLDM DOMAINS
  ( 7)   ER LIST         LIST OF ACTIVE EXPLICIT ROUTES
  ( 8)   VR LIST         LIST OF ACTIVE VIRTUAL ROUTES

         ENTER: H OR HELP FOR INFORMATION ON THE USE OF NLDM
                HELP NLDM COMMANDS FOR NLDM COMMAND LIST

                     NLDM FILE LAST INITIALIZED 04/12/01


ENTER SEL# OR COMMAND
CMD==> 1
```

Figure 42. Session Monitor Main Menu

2. Select *1* to display the list of active LUs. You can also enter **list lu** from the command line to access the list of LUs. A panel similar to Figure 43 is displayed.

```
NLDM.LIST                                                          PAGE    1
                              RESOURCE NAME LIST
LIST TYPE: ACTIVE   LU                                        DOMAIN: CNM09
-------------------------------------------------------------------------------
 SEL#    NAME    STATUS     SEL#    NAME    STATUS     SEL#    NAME    STATUS
 ( 1)  AAUTCNMI  ACTIVE     (16)  BNJHWMON  ACTIVE     (31)  CNM09003  ACTIVE
 ( 2)  A09A701   ACTIVE     (17)  CNM01     ACTIVE     (32)  CNM09004  ACTIVE
 ( 3)  A09A702   ACTIVE     (18)  CNM02     ACTIVE     (33)  CNM09005  ACTIVE
 ( 4)  A09A703   ACTIVE     (19)  CNM02LUC  ACTIVE     (34)  CNM09006  ACTIVE
 ( 5)  A09A704   ACTIVE     (20)  CNM18     ACTIVE     (35)  CNM09007  ACTIVE
 ( 6)  A09A705   ACTIVE     (21)  CNM18LUC  ACTIVE     (36)  CNM09008  ACTIVE
 ( 7)  A09A706   ACTIVE     (22)  CNM20     ACTIVE     (37)  CNM09010  ACTIVE
 ( 8)  A09A740   ACTIVE     (23)  CNM69LUC  ACTIVE     (38)  DSIAMLUT  ACTIVE
 ( 9)  A09A741   ACTIVE     (24)  CNM09     ACTIVE     (39)  DSICRTR   ACTIVE
 (10)  A09A742   ACTIVE     (25)  CNM09LUC  ACTIVE     (40)  DSIGDS    ACTIVE
 (11)  A09A743   ACTIVE     (26)  CNM09PPT  ACTIVE     (41)  ECHOA99   ACTIVE
 (12)  A09A744   ACTIVE     (27)  CNM09SPT  ACTIVE     (42)  ECHOA09   ACTIVE
 (13)  A09A745   ACTIVE     (28)  CNM09000  ACTIVE     (43)  ISTNOP    ACTIVE
 (14)  A09A746   ACTIVE     (29)  CNM09001  ACTIVE     (44)  ISTPDCLU  ACTIVE
 (15)  A09M      ACTIVE     (30)  CNM09002  ACTIVE     (45)  TSOA09    ACTIVE

ENTER TO VIEW MORE DATA OR TYPE FIND NAME TO LOCATE SPECIFIC NAME
ENTER SEL# (SESS LIST), SEL# RTS (RESP TIME SUM) OR SEL# RTT (RESP TIME TREND)
CMD==> 42
```

Figure 43. Resource Name List Panel

In a large network, listing all the LUs can be resource intensive and can result in several panels of information. In such a case, you might consider using the SESS command, as explained in the following step.

3. Locate the specific resource name and select the corresponding number to display a list of sessions for that resource. For example, to list all the sessions for ECHOA09, enter 42 in the **CMD==>** field. You can also enter `sess echoa09` from the command line to get to the session list panel. A panel similar to Figure 44 is displayed.

```
NLDM.SESS                                                          PAGE    1
                                SESSION LIST
NAME: ECHOA99                                                   DOMAIN: CNM09
--------------------------------------------------------------------------------
      ***** PRIMARY *****  **** SECONDARY ****
 SEL#   NAME   TYPE  DOM     NAME   TYPE  DOM     START TIME       END TIME
 ( 1) ECHOA99  LU   CNM99  ECHOA09  LU   CNM09  07/27 09:30:02  *** ACTIVE ***
 ( 2) ECHOA09  LU   CNM09  ECHOA99  LU   CNM99  07/27 09:29:59  *** ACTIVE ***
 ( 3) A09M     SSCP CNM09  ECHOA09  LU   CNM09  07/27 07:27:40  *** ACTIVE ***
 ( 4) ECHOA09  LU   CNM99  ECHOA69  LU   CNM69  07/27 08:08:51  07/27 11:21:45









END OF DATA
ENTER SEL# (CONFIG), SEL# AND CT (CONN. TEST), SEL# AND STR (TERM REASON)
CMD==> 1
```

Figure 44. Session List Panel

This panel lists the active and stopped sessions that are still in the database for a resource. Each entry in the list is one session. Each line shows the session date, start time, session partner, and current status.

4. Select a session number to obtain configuration data for that session (in this case, session 1). A panel similar to Figure 45 on page 97 is displayed.

```
NLDM.CON                  SESSION CONFIGURATION DATA                  PAGE    1
-------------- PRIMARY ---------------+-------------- SECONDARY --------------
NAME ECHOA99   SA 00000063  EL 009D   |   NAME ECHOA09   SA 00000009  EL 00E1
--------------------------------------+---------------------------------------
DOMAIN CNM99       PCID NETA.A99M.CB430D58409E0A79               DOMAIN CNM09
               +-------------+                 +-------------+
A99M           |   CP/SSCP   | ---         --- |   CP/SSCP   | A09M
HOSTA99 (0000) | SUBAREA PU  |                 | SUBAREA PU  | HOSTA09 (0000)
               +------+------+  SUBA TP 00     +------+------+
                      |             VR 00            |
               +------+------+       ER 03     +------+------+
ECHOA99 (009D) |     LU      |      RER 0E     |     LU      | ECHOA09 (00E1)
               +-------------+                 +-------------+


                              LOGMODE INTERACT




SELECT PT, ST (PRI, SEC TRACE), RT (RESP TIME), P, ER, VR, AR
CMD==>
```

Figure 45. Session Configuration Data Panel

This panel shows how each LU is physically connected to its own subarea. Note that even though AR (Advanced Peer-to-Peer Networking Route) is listed as an option, LU-LU sessions across pure SNA subarea networks do not have Advanced Peer-to-Peer Networking route data. If you choose this option, you receive a message stating that Advanced Peer-to-Peer Networking session route data is not available.

5. Enter the option to display trace data. You can enter **pt** to display primary session trace data or **st** to display secondary session trace data. If you enter **st**, a panel similar to Figure 46 on page 98 is displayed:

```
NLDM.PIUT                SESSION TRACE DATA                          PAGE    1
---------- PRIMARY -------------+---------- SECONDARY -------------+- DOM -
NAME ECHOA99  SA 00000063 EL 009D | NAME ECHOA09  SA 00000009 EL 00E1 | CNM99
----------------------------------+-----------------------------------+------
SEL#   TIME   SEQ# DIR   TYPE   ******** REQ/RESP HEADER ******** RULEN SENS N
( 1) 09:30:47 00B6 P-S DATA     ....OC.DR.......BBEB.............    66      T
( 2) 09:30:47 00B6 S-P (+)RSP   ....OC.DR.........................     0
( 3) 09:30:47 00B6 S-P DATA     ....OC.DR.......BBEB.............    66      T
( 4) 09:30:47 00B6 P-S (+)RSP   ....OC.DR.........................     0
( 5) 09:30:47 00B7 P-S DATA     ....OC.DR.......BBEB.............    66      T
( 6) 09:30:47 00B7 S-P (+)RSP   ....OC.DR.........................     0
( 7) 09:30:47 00B7 S-P DATA     ....OC.DR.......BBEB.............    66      T









END OF DATA
ENTER SEL# OR COMMAND
CMD==>
```

Figure 46. Session Trace Data Panel

This panel shows the flow of the most recent PIUs on a session. Also shown is the time, type, and length of the data that was sent, and the direction in which it was sent. Complete PIUs are available for LU-LU session debugging. If the data is truncated, a T marker is displayed in the right margin.

6. If you enter a selection number for a PIU, the PIU is displayed in hexadecimal and EBCDIC representation on the NLDM.PIUD panel.

   If SEL# AND F (FORMATTED RU) is an option, you can enter a selection number followed by a space followed by F to display the formatted PIU, if formatted data is available, on the NLDM.PIUF panel. Formatting is generally available for PIUs with the following characteristics:

   - They contain an SNA request/response header (RH) and a format header (FMH) type 5.
   - They are complete enough to format.
   - They are not compressed.

   The first formatted page shows the FMH. Subsequent pages show the different general data stream (GDS) variable types that are included in the PIU.

   Note: Formatting is limited to approximately the first 1000 bytes.

   From any page in the formatted display, you can enter SET HEX ON to reference the hexadecimal and EBCDIC PIU. The resulting NLDM.PIUF.HEX panel displays the hexadecimal and EBCDIC representation associated with that particular page, as indicated by the matching hex offsets listed on either panel. Enter SET HEX OFF to return to the formatted display.

7. If you use the NetView supplied default PF key values, press PF3 to return to the Session Configuration Data panel. If your PF keys have different values, select the PF key which is set to RETURN.

   To determine your current PF key settings, use the NetView DISPFK command to display the values in effect for the current component.

For more information about how your PF keys are set, refer to the NetView PFKDEF command in the NetView online help, and browse the CNMKEYS sample.

8. Enter **p** to display the Session Parameters panel. If the KEEPPIU count is zero, you have access to the Session Parameters panel, but no other PIUs are kept. You cannot access primary or secondary trace data, the `PT` and `ST` options, from the Session Configuration Data panel. The KEEPPIU count is found in the AAUPRMLP member (used to initialize the session monitor). Depending on the session type, the following information is displayed:

Session type	Information code	Information description
LU-LU, CP-CP	BIND	Bind
SSCP-LU	ACTLU	Logical unit
SSCP-PU	ACTPU	Physical unit
SSCP-SSCP	ACTCDRM	Cross-domain resource manager

For an LU-LU session, a panel similar to Figure 47 is displayed:

```
NLDM.SPRM.BIND              SESSION PARAMETERS                        PAGE   1
----------- PRIMARY --------------+---------- SECONDARY --------------+- DOM -
NAME ECHOA99  SA 00000063 EL 009D | NAME ECHOA09  SA 00000009 EL 00E1 | CNM99
----------------------------------+-----------------------------------+-------
FID TYPE: 4             RU: NON-NEGOTIABLE BIND REQUEST
                     FUNCTION MANAGEMENT (FM) PROFILE:  3
----------- FM USAGE/PLU ------------------------- FM USAGE/SLU -------------
RU CHAINS ALLOWED: MULTIPLE             RU CHAINS ALLOWED: MULTIPLE
REQUEST CONTROL MODE: IMMEDIATE         REQUEST CONTROL MODE: IMMEDIATE
PRI ASKS FOR: DEF OR EXCEPT RESPONSE    SEC ASKS FOR: DEFINITE RESPONSE
2-PHASE COMMIT: NOT APPLICABLE          2-PHASE COMMIT: NOT APPLICABLE
COMPRESSION: WILL NOT BE USED           COMPRESSION: WILL NOT BE USED
PRIMARY: MAY SEND EB                    SECONDARY: WILL NOT SEND EB
----------------------------- FM USAGE/COMMON -------------------------------
PLU RECEIPT OF BIU SEGMENTS: SUPPORTED  BIND QUEUING: NOT ALLOWED
FM HEADERS: NOT ALLOWED                 SEND/RECV MODE: HALF-DUPLEX CONTENTION
BRACKETS ARE USED - RESET STATE: BETB   RECOVERY RESPONSIBILITY: CONTEN. LOSER
BRACKET TERMINATION: CONDITIONAL(R1)    CONTENTION WINNER: SECONDARY
ALTERNATE CODE SET: WILL NOT BE USED    ALTERNATE CODE PROCESSING: NOT APPLIC
SEQUENCE NUMBERS: NOT APPLICABLE        CONTROL VECTORS: YES
BRACKET INITIATION STOP (BIS): N/A      HDX-FF RESET STATE: NOT APPLICABLE
ENTER TO VIEW MORE DATA
ENTER 'R' TO RETURN TO PREVIOUS DISPLAY - OR COMMAND
CMD==>
```

Figure 47. Session Parameters Panel

This panel interprets the BIND request unit for the session displayed. The selected session is identified in the panel heading. The BIND response and the BIND are recorded in the session monitor database.

Several panels of session parameter data are available. For additional information on the information contained in each of the panels, type **help nldm** or **help nldm 'term'** to access the online help for the session monitor.

9. Enter `r` or press the PF key with a value of RETURN (NetView default is PF3) to return to the Session Configuration Data panel.
10. Enter `er` to display the explicit route for the session. A panel similar to Figure 48 on page 100 is displayed.

```
NLDM.ER                  SPECIFIC ER CONFIGURATION                 PAGE    1
-------------------------------------------------------------------------------
SUBAREA1 00000063   SUBAREA2 00000009  ER  03 | NODES (TOTAL/MIGRATION): 02/00
-------------------------------------------------------------------------------


 +-----+ NAME: HOSTA99
 | INN |   SA: 00000063
 +--+--+ SSCP: A99M
    |
1) TG001
    |
 +--+--+ NAME: HOSTA09
 | INN |   SA: 00000009
 +--+--+ SSCP: A09M







END OF DATA
ENTER SEL# (FOR TG DETAIL)
CMD==>
```

Figure 48. Session Parameters Panel

You can use ER data to list the sessions using a specific explicit route, display the network configuration for the explicit route, and display the lines which make up a transmission group. If too many sessions are using the same explicit route, this can result in slow session response.

11. Press the PF key with a value of RETURN (NetView default is PF3) to return to the Session Configuration Data panel.
12. Enter `vr` to display the virtual route for the session. A panel similar to Figure 49 on page 101 is displayed.

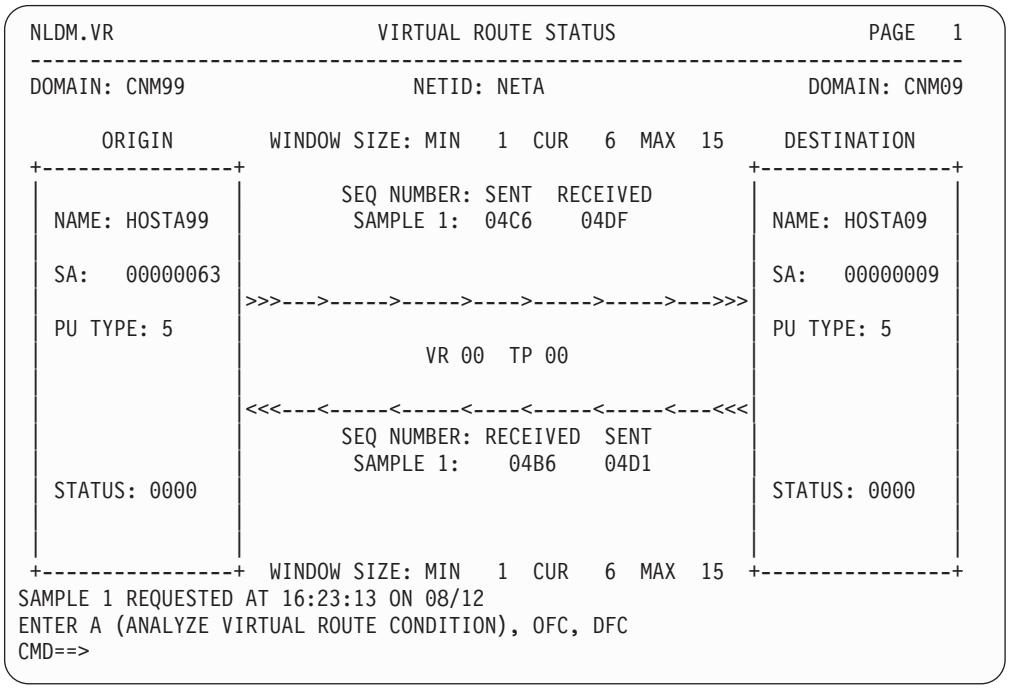


Figure 49. Virtual Route Status Panel

A ***virtual route*** (VR) is a logical data path from one resource to another. Control information flows along the VR to regulate the amount of data flowing at a particular time. The amount of data allowed to flow expands and contracts dynamically based on the capability of intermediate nodes to store and forward data. When you access this panel, the session monitor issues a ROUTE-TEST request. The information in the RSP (ROUTE-TEST) is used to determine the status of the VR.

Use the VR data to list the active virtual routes. From this list, you can display the sessions that use a specific VR, their PUs, and transmission groups. These displays are used to identify users that might have similar problems, especially performance problems that are related to congestion, and to compare which lines are involved in the problem. You can also use VR data to ensure that the route is not being blocked.

13. Enter a at the command line to analyze the virtual route. The session monitor issues another ROUTE-TEST request. The results are then shown in the Virtual Route Status panel (see Figure 50 on page 102).

```
NLDM.VR                      VIRTUAL ROUTE STATUS                      PAGE   1
------------------------------------------------------------------------------
DOMAIN: CNM99                    NETID: NETA                       DOMAIN: CNM09

      ORIGIN        WINDOW SIZE: MIN   1  CUR   6  MAX  15     DESTINATION
+----------------+                                            +----------------+
|                |        SEQ NUMBER: SENT  RECEIVED          |                |
| NAME: HOSTA99  |         SAMPLE 1:  04C6    04DF           | NAME: HOSTA09  |
|                |         SAMPLE 2:  04E7    04FA           |                |
| SA:   00000063 | VR IS NOT BLOCKED                         | SA:   00000009 |
|               >>>--->----->----->---->----->----->--->>>|                |
| PU TYPE: 5     |                                           | PU TYPE: 5     |
|                |                VR 00  TP 00               |                |
|                |                                           |                |
|                |<<<---<-----<-----<----<-----<-----<---<<<|                |
|                |        SEQ NUMBER: RECEIVED  SENT          |                |
|                |         SAMPLE 1:    04B6    04D1          |                |
| STATUS: 0000   |         SAMPLE 2:    04D8    04EE          | STATUS: 0000   |
|                | VR IS NOT BLOCKED                         |                |
|                |                                           |                |
 +----------------+  WINDOW SIZE: MIN   1  CUR   6  MAX  15  +----------------+
SAMPLE 1 REQUESTED AT 16:23:13 ON 04/12 - SAMPLE 2 REQUESTED 11 MIN LATER
ENTER A (ANALYZE VIRTUAL ROUTE CONDITION), OFC, DFC
CMD==>
```

Figure 50. Virtual Route Status Panel with Analysis Data

Based on the two most recent samples taken, status conclusions are displayed on the panel. In this case, the conclusion for both samples is `VR IS NOT BLOCKED`.

Typical CP-CP Session for an SNA Advanced Peer-to-Peer Networking Network

To monitor a CP-CP session for an SNA Advanced Peer-to-Peer Networking network:

1. Type **nldm** at the command line to access the session monitor main menu. A panel similar to Figure 51 on page 103 is displayed:

```
NLDM.MENU                                                          PAGE   1
                                Tivoli NetView


                                DOMAIN  CNM99

  SEL#                           DESCRIPTION

  ( 1)   LUNAME LIST     LIST OF ALL ACTIVE LOGICAL UNIT NAMES
  ( 2)   SLUNAME LIST    LIST OF ACTIVE SECONDARY LOGICAL UNIT NAMES
  ( 3)   PLUNAME LIST    LIST OF ACTIVE PRIMARY LOGICAL UNIT NAMES
  ( 4)   PUNAME LIST     LIST OF ACTIVE PHYSICAL UNIT NAMES
  ( 5)   CPNAME LIST     LIST OF ACTIVE CP AND SSCP NAMES
  ( 6)   DOMAIN LIST     LIST OF NLDM DOMAINS
  ( 7)   ER LIST         LIST OF ACTIVE EXPLICIT ROUTES
  ( 8)   VR LIST         LIST OF ACTIVE VIRTUAL ROUTES

         ENTER: H OR HELP FOR INFORMATION ON THE USE OF NLDM
                HELP NLDM COMMANDS FOR NLDM COMMAND LIST

                     NLDM FILE LAST INITIALIZED 04/12/01


ENTER SEL# OR COMMAND
CMD==> 5
```

Figure 51. Session Monitor Main Menu

2. Select option 5 to display the list of active CP and SSCP names. You can also enter `list cp` or `list sscp` from the command line to access the list of CPs or SSCPs. A panel similar to Figure 52 is displayed.

```
NLDM.LIST                                                          PAGE    1
                              RESOURCE NAME LIST
LIST TYPE: ACTIVE   CP/SSCP                                   DOMAIN: CNM99
--------------------------------------------------------------------------------
 SEL#    NAME    STATUS     SEL#    NAME    STATUS     SEL#    NAME    STATUS
 ( 1)  A69M      ACTIVE
 ( 2)  A99M      ACTIVE
 ( 3)  B18M      ACTIVE
 ( 4)  B20M      ACTIVE
 ( 5)  B52M      ACTIVE
 ( 6)  C01M      ACTIVE
 ( 7)  C02M      ACTIVE









END OF DATA - TYPE FIND NAME TO LOCATE SPECIFIC NAME
ENTER SEL# OR COMMAND
CMD==> 1
```

Figure 52. Resource Name List Panel

3. Locate the specific resource name and select the corresponding option to display a list of sessions for that resource. For example, to list all the sessions for A69M, enter 1 in the `CMD==>` field. You can also enter `sess a69m` from the command line to display the list of sessions. A panel similar to Figure 53 on page 104

page 104 is displayed.

```
NLDM.SESS                                                          PAGE    1
                              SESSION LIST
NAME: A69M                                                      DOMAIN: CNM99
------------------------------------------------------------------------------
      ***** PRIMARY *****  **** SECONDARY ****
 SEL#   NAME   TYPE  DOM     NAME   TYPE  DOM     START TIME       END TIME
 ( 1) A99M     CP   CNM99  A69M     CP   CNM99  07/26 17:09:09  *** ACTIVE ***
 ( 2) A69M     CP   CNM99  A99M     CP   CNM99  07/26 17:09:08  *** ACTIVE ***
 ( 3) A99M     SSCP CNM99  A69M     SSCP CNM09  07/25 08:10:02  07/25 18:46:32









ENTER TO VIEW MORE DATA
ENTER SEL# (CONFIG), SEL# AND CT (CONN. TEST), SEL# AND STR (TERM REASON)
CMD==> 1
```

Figure 53. Session List Panel

This panel lists the active and stopped sessions for a resource. Each entry in the list is one session. Each line shows the session date, start time, session partner, and current status.

4. Select a session number to obtain configuration data for that session (in this case, session 1). A panel similar to Figure 54 is displayed.

```
NLDM.CON                  SESSION CONFIGURATION DATA                  PAGE    1
-------------- PRIMARY ---------------+-------------- SECONDARY --------------
NAME A99M      SA 00000063  EL 0007   |   NAME A69M      SA 00000004  EL 02A7
--------------------------------------+--------------------------------------
DOMAIN CNM99       PCID NETA.A99M.CB430D5840767227               DOMAIN CNM99
               +-------------+                 +-------------+
A99M           |     CP      | ---         --- |     CP      | A69M
               +-------------+  APPN TP 03     +-------------+
                                     VR 00
                                     ER 09
                                    RER 09


                               APPNCOS CPSVCMG

                               LOGMODE CPSVCMG

                               SADJ CP A69M



SELECT PT, ST (PRI, SEC TRACE), RT (RESP TIME), P, ER, VR, AR
CMD==> AR
```

Figure 54. Session Configuration Data Panel

This panel shows how each CP is physically connected. The PT (Primary Trace), ST (Secondary Trace), P (Parameters), ER (Explicit Route), and VR (Virtual Route) options are described in "Typical LU-LU Session for an SNA Subarea Network" on page 94.

5. Enter ar to display the Advanced Peer-to-Peer Networking route configuration panel. A panel similar to Figure 55 is displayed.

```
NLDM.AR              APPN SESSION ROUTE CONFIGURATION               PAGE   1
-- PRIMARY ---+-- SECONDARY --+--------------- PCID ---------------+- DOMAIN -
NAME A99M     | NAME A69M     | NETA.A99M.CB430D5840767227         | CNM99
--------------+---------------+------------------------------------+----------

 +---------+
 |   CP    |
 |A99M     |
 +----+----+
TG021 |
 +----+----+
 |   CP    |
 |A69M     |
 +---------+









END OF DATA
SELECT PAR, SAR
CMD==>
```

Figure 55. Advanced Peer-to-Peer Networking Session Route Configuration Panel

This panel displays Advanced Peer-to-Peer Networking nodes and connecting groups in an Advanced Peer-to-Peer Networking session path.

Typical LU-LU Session for an SNA Advanced Peer-to-Peer Networking Network

Complete the following steps to monitor an LU-LU session for an SNA Advanced Peer-to-Peer Networking or mixed network.

1. Enter **sess echoa29** from the session monitor command line or **nldm sess echoa29** from the NCCF command line to access the session list for resource echoa29. A panel similar to Figure 56 on page 106 is displayed.

```
NLDM.SESS                                                          PAGE    1
                                SESSION LIST
NAME: ECHOA29                                                   DOMAIN: CNM19
--------------------------------------------------------------------------------
      ***** PRIMARY *****  **** SECONDARY ****
 SEL#   NAME   TYPE  DOM     NAME   TYPE  DOM     START TIME       END TIME
 ( 1) ECHOA69  LU   CNM99  ECHOA29  ILU   C-C   08/12 17:54:55  *** ACTIVE ***
 ( 2) ECHOA29  ILU   C-C   ECHOA69  LU   CNM99  08/12 17:54:53  *** ACTIVE ***
 ( 3) ECHOA29  ILU   C-C   ECHOA69  LU   CNM99  08/12 16:05:14  08/12 16:18:20
                                               REASON CODE 0F  SENSE 80030004
 ( 4) ECHOA69  LU   CNM99  ECHOA29  ILU   C-C   08/12 16:05:12  08/12 16:18:20
                                               REASON CODE 0F  SENSE 80030004









END OF DATA
ENTER SEL# (CONFIG), SEL# AND CT (CONN. TEST), SEL# AND STR (TERM REASON)
CMD==> 1
```

Figure 56. Session List Panel

This panel lists the active and stopped sessions for a resource. Each entry in the list is one session. Each line shows the session date, start time, session partner, and current status.

2. Select a session number to obtain configuration data for that session. A panel similar to Figure 57 is displayed.

```
NLDM.CON                 SESSION CONFIGURATION DATA                 PAGE    1
-------------- PRIMARY ---------------+-------------- SECONDARY --------------
NAME ECHOA69   SA 00000004  EL 02B6   |   NAME ECHOA29   SA 00000003  EL 02B8
--------------------------------------+----------------------------------------
DOMAIN CNM99  C-C  PCID NETA.A69M.D2030CADFE6B236A           C-C DOMAIN CNM19
               +-------------+                  +-------------+
               |             | ---         ---  |             |
A04B62  (0000) | SUBAREA PU  |  APPN TP 02      | SUBAREA PU  | A03A62  (0000)
               +------+------+  SUBA TP 00      +------+------+
                      |              VR 00             |
               +------+------+       ER 0F      +------+------+
A04C05         |    LINK     |      RER 06      |    LINK     | A03C02
               +------+------+                  +------+------+
                      |        APPNCOS #INTER          |
               +------+------+                  +------+------+
A04P05A (01C2) |     PU      | LOGMODE INTERACT |     PU      | A03P02A (01C2)
               +------+------+ PADJ CP A69M     +------+------+
                      |        SADJ CP A29M            |
               +------+------+                  +------+------+
ECHOA69 (02B6) |     ILU     |                  |     ILU     | ECHOA29 (02B8)
               +-------------+                  +-------------+

SELECT PT, ST (PRI, SEC TRACE), RT (RESP TIME), P, ER, VR, AR
CMD==> VR
```

Figure 57. Session Configuration Data Panel

See "Typical LU-LU Session for an SNA Subarea Network" on page 94 for descriptions of the PT (Primary Trace), ST (Secondary Trace), P (Parameters), and ER (Explicit Route) options.

3. Enter vr to display the virtual route for the session. A panel similar to Figure 58 is displayed.

```
NLDM.VR                      VIRTUAL ROUTE STATUS                      PAGE   1
-------------------------------------------------------------------------------
DOMAIN: CNM99                    NETID: NETA                       DOMAIN: CNM19

      ORIGIN        WINDOW SIZE: MIN   1  CUR   3  MAX   3     DESTINATION
+-----------------+                                            +-----------------+
|                 |         SEQ NUMBER: SENT  RECEIVED         |                 |
| NAME: A04B62    |          SAMPLE 1:  0DC8    0DD0          | NAME: A03A62    |
|                 |                                            |                 |
| SA:   00000004  |                                            | SA:   00000003  |
|                 |>>>--->----->----->---->----->----->--->>>  |                 |
| PU TYPE: 4      |                                            | PU TYPE: 4      |
|                 |                 VR 00  TP 00               |                 |
| INBND PIU POOL  |                                            | INBND PIU POOL  |
|  CURRENT:    0  |<<<---<-----<-----<----<-----<-----<---<<<  |  CURRENT:    0  |
|  LIMIT:     10  |         SEQ NUMBER: RECEIVED  SENT         |  LIMIT:     10  |
|                 |          SAMPLE 1:    0DC6    0DCE         |                 |
| STATUS: 0000    |                                            | STATUS: 4008    |
|                 |                                            |                 |
|                 |                                            |                 |
+-----------------+  WINDOW SIZE: MIN   1  CUR   3  MAX   3   +-----------------+
SAMPLE 1 REQUESTED AT 17:58:33 ON 04/12
ENTER A (ANALYZE VIRTUAL ROUTE CONDITION), OFC, DFC
CMD==> OFC
```

Figure 58. Virtual Route Status Panel

A virtual route (VR) is a logical data path from one resource to another. For an SNA Advanced Peer-to-Peer Networking network, this panel lets you access flow control data. You can issue flow control requests from this screen: origin flow control (OFC) requests and destination flow control (DFC) requests. DFC requests provide flow control data in the secondary direction at the point where the SNA subarea and SNA Advanced Peer-to-Peer Networking network meet. OFC requests provide flow control data in the primary direction at the point where the SNA subarea and SNA Advanced Peer-to-Peer Networking network meet.

You can enter a at the command line to analyze the virtual route.

4. Enter **ofc** or **dfc** to display flow control data. Enter **ofc** (to display origin flow control data) and a panel similar to Figure 59 on page 108:

```
NLDM.FC                  FLOW CONTROL DATA                          PAGE    1
----------- PRIMARY --------------+----------- SECONDARY -------------+- DOM -
NAME ECHOA69  SA 00000004 EL 02B6 | NAME ECHOA29  SA 00000003 EL 02B8 | CNM99
----------------------------------+-----------------------------------+-------
FULLY QUALIFIED PCID: NETA.A69M.D2030CADFE6B236A

                              PRIMARY SESSION STAGE
MOST RECENT PIUS:
  LAST PIU SENT (TH,RH)       2C00010803C1 0380C0
  LAST PIU RECEIVED (TH,RH)   2C00080103C1 0380C0

PACING DATA:
  LAST IPM SENT               83010000002D
  NEXT SEND WINDOW SIZE          15
  NEXT REC WINDOW SIZE           45
  MSGS IN PACING QUEUE            0

RESIDUAL PACING COUNTS
  SEND WINDOW                     0
  RECEIVE WINDOW                 29

END OF DATA

CMD==>
```

Figure 59. Flow Control Data Panel (Origin)

If you enter **dfc** (to display destination flow control data), a panel similar to Figure 60 is displayed:

```
NLDM.FC                  FLOW CONTROL DATA                          PAGE    1
----------- PRIMARY --------------+----------- SECONDARY -------------+- DOM -
NAME ECHOA69  SA 00000004 EL 02B6 | NAME ECHOA29  SA 00000003 EL 02B8 | CNM19
----------------------------------+-----------------------------------+-------
FULLY QUALIFIED PCID: NETA.A69M.D2030CADFE6B236A

                                                    SECONDARY SESSION STAGE
MOST RECENT PIUS:
  LAST PIU SENT (TH,RH)                             2E000301038F 838000
  LAST PIU RECEIVED (TH,RH)                         2E000103038F 0380C0

PACING DATA:
  LAST IPM SENT                                     830100007FFF
  NEXT SEND WINDOW SIZE                                 7
  NEXT REC WINDOW SIZE                              32767
  MSGS IN PACING QUEUE                                  0

RESIDUAL PACING COUNTS
  SEND WINDOW                                           0
  RECEIVE WINDOW                                     3770

END OF DATA

CMD==>
```

Figure 60. Flow Control Data Panel (Destination)

Flow control data is maintained for low-entry networking (LEN) and Advanced Peer-to-Peer Networking connections where the transmission group (TG) ends in an SNA subarea node. If the TG intersects a virtual route, you can enter `fc`, `ofc`, or `dfc` from the Virtual Route Status panel to access this panel. If the TG

ends in VTAM and no connecting virtual route exists, you can enter `fc` from the Session Configuration Data panel to display this panel.

From this panel, you can:

- Look for missing responses in the flow control which might lead to blocked virtual routes.
- Look for requests to close the VR window. A large number of those requests can indicate an intermediate node running over capacity. The pacing data (specifically the size of the pacing windows) controls the number of PIUs allowed to flow on a virtual route before the SNA subarea node receiving the PIUs authorizes the sending of more data. If the number of messages in the pacing queue is high (indicating a congestion problem), you might need to increase the size of the pacing window sending the PIUs (`SEND WINDOW SIZE`).

5. Press the PF key with a value of RETURN (NetView default is PF3) twice to return to the Session Configuration Data panel.
6. Enter **ar** to display the Advanced Peer-to-Peer Networking route configuration panel. A panel similar to Figure 61 is displayed.

```
NLDM.AR              APPN SESSION ROUTE CONFIGURATION               PAGE   1
-- PRIMARY ---+-- SECONDARY --+--------------- PCID ---------------+- DOMAIN -
NAME ECHOA69  | NAME ECHOA29  | NETA.A69M.D2030CADFE6B236A         | CNM19
--------------+---------------+------------------------------------+----------

 +---------+
 | SUBAREA |
 | NODE(S) |
 +----+----+
IN-TG |
 +----+----+
 | CP(ICN) | PRI-SA: 000E
 |A19M     |
 +----+----+
TG021 | HPR-1234567890123456
 +----+----+
 |   CP    |
 |A29M     |
 +---------+


END OF DATA
SELECT PAR, SAR
CMD==> PAR
```

Figure 61. Advanced Peer-to-Peer Networking Session Route Configuration Panel with Subarea Number from Primary Side

In the SNA Advanced Peer-to-Peer Networking environment, the number of Advanced Peer-to-Peer Networking subnetworks that a session can flow through has no limit. This means that a single session could have more than one Route Selection Control Vector (RSCV). Because of the possibility of multiple RSCVs, this panel only displays local RSCV data. When additional RSCVs are in the session path, the user can scroll in the primary direction (using the PAR option) or in the secondary direction (using the SAR option) to view these RSCVs. SNA subarea nodes existing between the SNA Advanced Peer-to-Peer Networking nodes are shown with a generic subarea node box.

If VTAM is unable to provide part of the route data to the NetView program, a box containing `ROUTE DATA NA` at either the beginning or end of the RSCV display identifies where data is not available for display. If the primary

endpoint node name of the RSCV being displayed is not known, UNKNOWN is displayed. The corresponding PAR and SAR options are not displayed for these situations.

7. Enter par to scroll in the primary direction. A panel similar to Figure 62 is displayed.

```
NLDM.AR              APPN SESSION ROUTE CONFIGURATION               PAGE   1
-- PRIMARY ---+-- SECONDARY --+--------------- PCID ---------------+- DOMAIN -
NAME ECHOA69  | NAME ECHOA29  | NETA.A69M.D2030CADFE6B236A         | CNM99
--------------+---------------+------------------------------------+----------

 +---------+
 |   CP    |
 |A69M     | SEC-SA: 000F
 +----+----+
TG021 | HPR-ABCDEF1234567890
 +----+----+
 | CP(ICN) |
 |A99M     |
 +----+----+
IN-TG |
 +----+----+
 | SUBAREA |
 | NODE(S) |
 +---------+


END OF DATA
SELECT PAR, SAR, OAR
CMD==>
```

Figure 62. Advanced Peer-to-Peer Networking Session Route Configuration Panel with Subarea Number from Secondary Side and OAR Prompt

Note: The following paragraphs explain some of the abbreviations that are displayed on the screen:

The terms PRI-SA (see Figure 61 on page 109) and SEC-SA (Figure 62) indicate the subarea number that is associated with an Advanced Peer-to-Peer Networking node from its primary (above) or secondary (below) side.

HPR indicates a TG that is part of an HPR pipe whose TCID number is shown. VTAM reports path switches and NLDM reflects them in the route.

You might see HPRC, instead of HPR. HPRC indicates a hop that is believed to be part of an HPR pipe; however this NLDM does not know about any path switches.

If you see an OAR prompt at the bottom of the NLDM.CON or the NLDM.AR panel, it means that outboard Advanced Peer-to-Peer Networking route data is present (from a 2210 or 2216 router, for example). If you select the OAR prompt, a panel displays that is similar to Figure 62, but which shows the RSCV that the outboard CP reports.

For details about these terms, see the online help.

SNA Session through an Advanced Peer-to-Peer Networking Network

Complete the following steps to monitor the SSCP-PU session that connects through an Advanced Peer-to-Peer Networking network using an LU 6.2 session pipe. This pipe is established by using the DLUR and DLUS functions. The ability to monitor a session over a pipe was added in NetView V3R1.

1. Enter **sess ps2dl2pa** from the session monitor command line from the NCCF command line to access the session list for resource ps2dl2pa. A panel similar to Figure 63 is displayed.

```
NLDM.SESS                                                          PAGE    1
                                SESSION LIST
NAME: PS2DL2PA                                                  DOMAIN: CNM09
-------------------------------------------------------------------------------
      ***** PRIMARY *****  **** SECONDARY ****
 SEL#   NAME   TYPE  DOM     NAME   TYPE  DOM     START TIME       END TIME
 ( 1) A09M     SSCP CNM09  PS2DL2PA PU   CNM09  01/07 12:09:45  *** ACTIVE ***
                                                                 DLUS-DLUR PIPE
 ( 2) A09M     SSCP CNM09  PS2DL2PA PU   CNM09  01/05 13:27:51  01/05 14:04:26
                                                                 DLUS-DLUR PIPE
 ( 3) A09M     SSCP CNM09  PS2DL2PA PU   CNM09  01/05 12:38:19  01/05 13:27:47
                                                                 DLUS-DLUR PIPE









END OF DATA
ENTER SEL# (CONFIG), SEL# AND CT (CONN. TEST), SEL# AND STR (TERM REASON)
CMD==>
```

Figure 63. Session List Panel

This panel lists the active and stopped sessions for a resource. Each entry in the list is one session. Each line shows the session date, start time, session partner, and current status. These sessions also have DLUS-DLUR PIPE displayed below the current status. This designation indicates that the sessions contain an Advanced Peer-to-Peer Networking network that is crossed using a LU 6.2 session pipe. The pipe is established and controlled by the dependent LU server (DLUS) and dependent LU requestor (DLUR) functions.

2. Session 1 is the only active session. Select session 1 to obtain configuration data for that session. A panel similar to Figure 64 on page 112 is displayed.

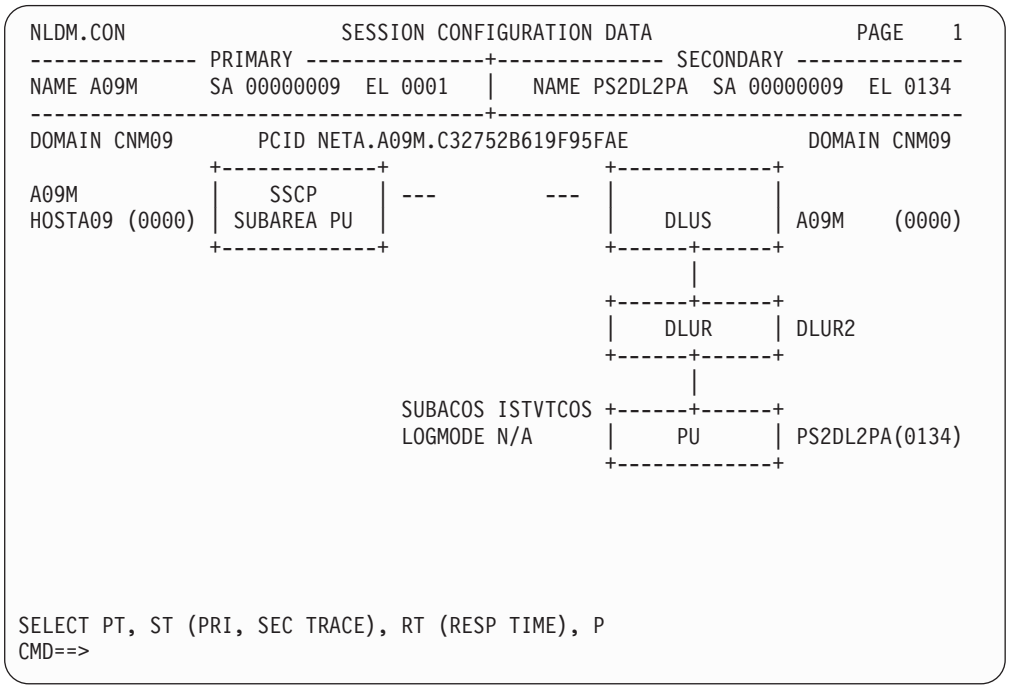


Figure 64. Session Configuration Data Panel

This panel displays the resource (ps2dl2pa) and session path that connects it to the host (hosta09). The DLUR and DLUS ends of the LU 6.2 pipe that travels through the Advanced Peer-to-Peer Networking network are also shown. The DLUR function for this session is located in resource dlur2, and the DLUS function is located in resource a09m. Note that the Advanced Peer-to-Peer Networking network itself is not displayed. Similar data is also available for the SSCP-LU sessions. To display more information about the resources that the pipe crosses, view the Advanced Peer-to-Peer Networking Route Data displays (AR) for the DLUR-DLUS sessions.

Typical Takeover/Giveback Session

To monitor an LU-LU session in a takeover/giveback scenario for either an SNA subarea or SNA Advanced Peer-to-Peer Networking network, enter `sess echoa29` from the session monitor command line or `nldm sess echoa29` to access the session list for resource echoa29. A panel similar to Figure 65 on page 113 is displayed.

```
NLDM.SESS                                                          PAGE    2
                                SESSION LIST
NAME: ECHOA69                                                   DOMAIN: CNM09
------------------------------------------------------------------------------
      ***** PRIMARY *****  **** SECONDARY ****
 SEL#   NAME   TYPE  DOM     NAME   TYPE  DOM     START TIME       END TIME
 ( 1) ECHOA29  LU    C-C   ECHOA69  LU   CNM19  05/07 08:46:02  05/07 08:47:40
      TOV                                                       ** TAKEOVER **
                                                 REASON CODE OF  SENSE 087D000A
 ( 2) ECHOA69  LU   CNM19  ECHOA29  LU    C-C   05/07 08:46:02  05/07 08:47:40
                           TOV                                  ** TAKEOVER **
                                                 REASON CODE OF  SENSE 087D000A
 ( 3) ECHOA69  ILU   C-C   ECHOA19  LU   CNM09  05/07 08:41:24  05/07 08:41:48
      TGV                                                       ** GIVEBACK **
 ( 4) ECHOA19  LU   CNM09  ECHOA69  ILU   C-C   05/07 08:41:24  05/07 08:41:48
                           TGV                                  ** GIVEBACK **
 ( 5) ECHOA69  LU    C-C   ECHOA09  LU   CNM09  05/07 08:40:24  05/07 08:52:30
      GTK                                                       ** TAKEOVER **
                                                 REASON CODE OF  SENSE 80030004


ENTER TO VIEW MORE DATA
ENTER SEL# (CONFIG), SEL# AND CT (CONN. TEST), SEL# AND STR (TERM REASON)
CMD==>
```

Figure 65. Session List Panel for an SNA Advanced Peer-to-Peer Networking or Mixed Network

VTAM can take over or give back control of the NCP providing boundary function for some sessions. When takeovers and givebacks exist, the Session List panel can display Takeover/Giveback statuses (as shown here) and the active and stopped status (as shown in "Typical LU-LU Session for an SNA Subarea Network" on page 94).The following takeover/giveback notifications are possible:

**** TAKEOVER ****
: Indicates that the local VTAM has taken over the NCP boundary function connection to one of the session endpoints. One of the following values is displayed under the name of the resource which has been taken over:

  TOV To indicate that the resource has been taken over

  GTK To indicate that the resource was previously given back and has been taken over.

**** GIVEBACK ****
: Indicates that the local VTAM has given up the NCP boundary function connection to one of the session endpoints. One of the following values is displayed under the name of the resource which has been given up:

  GBK To indicate that the resource has been given back

  TGV To indicate that the resource was previously taken over and has now been given back.

For additional information about this and other session monitor panels, see "Typical LU-LU Session for an SNA Subarea Network" on page 94, "Typical CP-CP Session for an SNA Advanced Peer-to-Peer Networking Network" on page 102, and "Typical LU-LU Session for an SNA Advanced Peer-to-Peer Networking Network" on page 105.

Because of the limited data received in the takeover notification, some session PD route functions might be limited.

SESSMDIS Command

You can display session and storage information by entering the NetView SESSMDIS command from the command line. A panel similar to Figure 66 is displayed.

```
SESSMDIS  Session Monitor Session and Storage Information   Page 1 of 1

Options in Effect   SAW: YES  LU Trace: YES  CP/SSCP Trace: YES SESSTATS: YES

Session Counts        CP-CP   SSCP-SSCP   SSCP-PU   SSCP-LU     LU-LU  Filtered
       Current:           2           1         5        35        26         0
       Maximum:           2           1         5        35        28         0

Session Monitor Storage Usage
     Resources:         16K        Sessions:      28K   Session Parms:      10K
     PIU Trace:         28K        SESSTATS:       4K             RTM:       0K
          RSCV:          4K           Other:    1754K
         Total:       1846K

VSAM Record Queue
       Current:           0         Maximum:           3

Session Monitor Workload since 04/12/01 07:25:11
                  SAW       Session   Session     PIU          PIUs    Sessions
                  Buffers    Starts      Ends     Buffers              Recorded
     4 seconds:         0         0         0           2       168           0
         Total:        70        83        13        1172     84894          13

ENTER= Refresh             PF2= End  PF3= Return
```

Figure 66. Session and Storage Information Panel

Check the following information:

- The session count. If the session count is 0, no sessions are active between the given resource types. On Figure 66, two CP-CP sessions are active, one active SSCP-SSCP session, and so on.
- The amount of session and trace storage used. If, for example, the session storage amount is too high, you might want to filter certain session types (CP-CP, LU-LU, and so on), or to decrease trace storage, limit tracing functions.

Topic:	**Reference:**
Description of the output displayed from the SESSMDIS command	Additional information about the SESSMDIS command can be found in the *IBM Tivoli NetView for z/OS Tuning Guide*
NLDM panel help	NetView Online Help
NLDM panel Field Level Help	NetView Online Field Level Help `help nldm '`*`term`*`'`
Configuration examples	Appendix C, “Interpreting Session Data,” on page 357
Setting up the session monitor	*IBM Tivoli NetView for z/OS Installation: Configuring Additional Components* and “Using Session Monitor Filters” on page 213

Using the Status Monitor (SNA Subarea)

The status monitor dynamically collects information about SNA resources in the network and summarizes this information into a full screen display. You can also

use the status monitor to automatically reactivate specified failing resources. You can use the status monitor in a 3270 environment, where the NetView management console is not available.

The status monitor, like VTAM, groups resources into major and minor nodes. Figure 67 shows an example of the hierarchy that the status monitor uses.

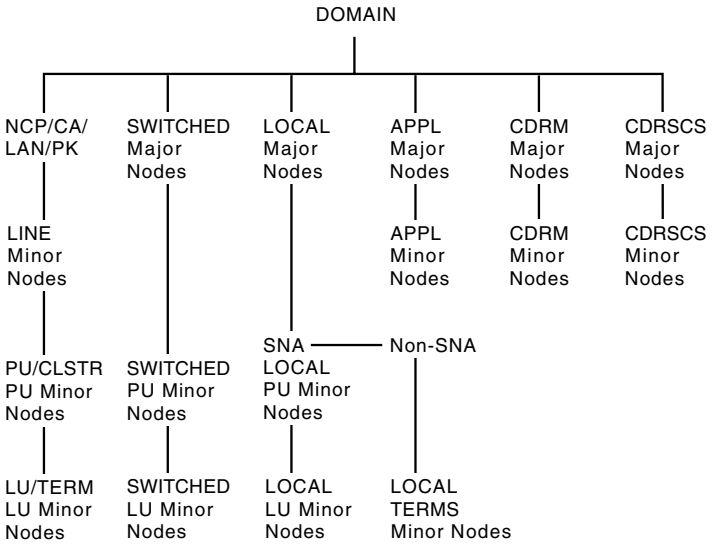


Figure 67. Status Monitor Hierarchy

The term ***higher node*** refers to the next node up in the hierarchy. For example, in Figure 67, the switched major nodes are the next higher node in relation to the switched PU minor nodes. The term ***lower node*** refers to the next node down in the hierarchy. ***Domain*** represents the highest level in the status monitor hierarchy. Resources of the same type are considered to be at the same level. For example, all PUs are on the same level in the hierarchy.

Understanding the Status Monitor Panel Colors

The status monitor uses colors on color terminals or high and normal intensity on monochrome terminals to display information about different resource states. The following states are used:

ACTIVE
: Nodes that are active (shown in green or normal intensity)

PENDING
: Nodes that are waiting to become active or inactive (shown in white or normal intensity)

INACT
: Nodes that have been inactivated (shown in red or high intensity)

MONIT
: Nodes that are inactive, but that the status monitor is automatically trying to reactivate (shown in turquoise or normal intensity)

NEVACT
: Nodes that have never been in an active state (shown in turquoise or normal intensity)

OTHER
All other possible states (shown in turquoise or normal intensity)

When you first enter the status monitor, the status of the resources shown in the status monitor panels is refreshed automatically.

Understanding Status Mapping

Table 11 shows how the VTAM states are generally mapped to the status monitor states:

Table 11. Mapping VTAM States to Status Monitor States

VTAM Status Code	VTAM Status	Status Monitor Status	Notes
00*xx*	Inactive	Inactive (INACT)	The following exceptions are used: • 0000 (Reset) is mapped to OTHER. This is a substate of the VTAM Inactive status and is handled differently because of multiple ownership considerations. • 0002 (Released) is mapped to OTHER. This is a substate of the VTAM Inactive status and is handled differently because of multiple ownership considerations. • If the resource has been selected for re-activation by using the STATOPT statement, it is mapped to MONIT. • If the resource never reaches the active state since the resource has been known to VTAM, it is mapped to NEVACT. If the resource is released or reset, all the information associated with the resource is lost. Inactivating a major node causes all of the resources under it to be reset.
01*xx*	Pending Inactive	Pending (PENDING)	
02*xx*	Connectable	Other (OTHER)	
03*xx*	Reactivate		This VTAM status is changed to a VTAM Active or Inactive status after the resource it reactivated. Until then, this VTAM status is not mapped to a status monitor status.
04*xx*	Pending Active	Pending (PENDING)	
05*xx*	Active	Active (ACTIVE)	
06*xx*	Routable	Other (OTHER)	

Setting Up the Status Monitor

If the status monitor does not work as described in the previous section, check for the following actions:

- Resources and relationships are defined between resources. You can define these relationships using STATOPT statements in VTAMLST. In the following example, resource LINE01 is assigned the description `LINE020` and is excluded from automatic reactivation (`NOMONIT`):

```
LINE01    LINE    ADDR=(001,FULL),
                  SPEED=56000
                  STATOPT=('LINE020',NOMONIT)
```

- The preprocessor, CNMNDEF, which reads the VTAMLST members and creates a member DSINDEF in DSIPARM, has run. DSINDEF is used by the status monitor initialization process.
- The status monitor is defined. This can be done in the status monitor initialization member sample DSICNM. In this sample, you can specify the following items:
  - Command lists available for processing through the status monitor
  - The automatic reactivation function
  - A secondary status monitor
  - The message alert settings
  - The message filter parameters

Navigating Status Monitor Panels

Complete the following steps to use the status monitor panels:

1. Enter **statmon** at the command line. A panel similar to Figure 68 is displayed.

```
STATMON.DSS                    DOMAIN STATUS SUMMARY   (REFRESH=ON)    08:35
HOST: HOST009           *1*   *2*   *3*   *4*
                        ACTIVE  PENDING   INACT    MONIT    NEVACT   OTHER
 .....9 NCP/CA/LAN/PK  .....2   ......   ......   ......   .....6   .....1
 ...559  LINES         .....2   ......   .....1   ......   ...343   ...213
 ...859  PUS/CLUSTERS  .....2   ......   ......   ......   ...844   ....13
 ..3260  LUS/TERMS     ......   ......   ......   ......   ..3232   ....28
 .....1 SWITCHED/XCA   .....1   ......   ......   ......   ......   ......
 .....2  PU/XCA LINE   ......   ......   ......   ......   ......   .....2
 .....2  LU/XCA PU     ......   ......   ......   ......   ......   .....2
 .....4 LOCAL MAJ NDS  .....2   ......   ......   ......   .....2   ......
 .....3  PUS           ......   ......   ......   ......   .....3   ......
 ....11  LUS/TERMS     ....11   ......   ......   ......   ......   ......
 .....2 APPL MAJ NDS   .....2   ......   ......   ......   ......   ......
 ...260  APPLICATIONS  ....19   ......   ......   ......   ......   ...241
 .....1 CDRM MAJ NDS   .....1   ......   ......   ......   ......   ......
 ....13  CDRMS         .....4   .....9   ......   ......   ......   ......
 .....1 CDRSC MAJ NDS  .....1   ......   ......   ......   ......   ......
 ....65  CDRSCS        ....65   ......   ......   ......   ......   ......
 ------ -------------  ------   ------   ------   ------   ------   ------
 ..5052 TOTAL NODES    ...112   .....9   .....1   ......   ..4430   ...500

 CMD==>
 TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
```

Figure 68. Domain Status Summary Panel

This panel summarizes the status for all the resource types within the domain's hierarchy. The status monitor uses two types of panels:

Summary
: Provides information on the status for all resource types under any resource

Detail
: Provides a list of resources (by name) one level immediately below the resource for which the detail panel was selected

For more information on the hierarchy of the status monitor panels, see Appendix B, "NetView Component Hierarchies," on page 343.

You can then use the NetView SREFRESH command or press a PF key set to that command (NetView default for status monitor is PF9) to switch the status monitor Domain Status Summary panel between dynamic and static states.

In the current setting of the panel, the REFRESH=ON state, changes to the displayed resources are reflected dynamically on the panel as they occur. If you are using the NetView-supplied default PF key setting for the status monitor component, pressing PF9 or entering SREFRESH switches the panel to the REFRESH=OFF state. In this state the panel is static, so resource status changes are not refreshed automatically on the panel.

2. To determine your current PF key settings, use the NetView DISPFK command to display the values in effect for the current component. For example, if you enter DISPFK while in the status monitor component, you see one or more screens similar to the one shown here:

```
CNMKWIND OUTPUT FROM  DISPFK                                LINE 1    OF 29
DISPLAY OF PF/PA KEY SETTINGS FOR STATMON
KEY   ----TYPE----   -----------COMMAND------------  SET-APPL
PA1   IMMED,IGNORE   RESET                          NETVIEW
PA2   IMMED,IGNORE   AUTOWRAP TOGGLE                NETVIEW
PA3   IMMED,IGNORE   RETRIEVE AND EXECUTE           NETVIEW
PF1   IMMED,APPEND   HELP                           NETVIEW
PF2   IMMED,IGNORE   END                            NETVIEW
PF3   IMMED,IGNORE   RETURN                         NETVIEW
PF4   IMMED,APPEND   DISPFK                         NETVIEW
PF5   IMMED,IGNORE   BROWSE NETLOGA                 NETVIEW
PF6   IMMED,IGNORE   ROLL                           NETVIEW
PF7   IMMED,IGNORE   BACK                           STATMON
PF8   IMMED,IGNORE   FORWARD                        STATMON
PF9   IMMED,IGNORE   SREFRESH                       STATMON
PF10  IMMED,IGNORE   SVTAM                          STATMON
PF11  IMMED,IGNORE   SCLIST                         STATMON
PF12  IMMED,IGNORE   RETRIEVE                       NETVIEW
PF13  IMMED,APPEND   CMD HELP                       NETVIEW
PF14  IMMED,APPEND   STATIONS                       NETVIEW
PF15  IMMED,IGNORE   LINES                          NETVIEW
PF16  IMMED,IGNORE   PFKDEF CNMKEYS2                NETVIEW
PF17  IMMED,IGNORE   BROWSE NETLOGI                 NETVIEW
PF18  IMMED,APPEND   NCCF                           NETVIEW
PF19  IMMED,IGNORE   BACK                           STATMON
PF20  IMMED,IGNORE   FORWARD                        STATMON
PF21  IMMED,IGNORE   SREFRESH                       STATMON
PF22  IMMED,APPEND   MAPCL                          NETVIEW
PF23  IMMED,APPEND   NPDA                           NETVIEW
PF24  IMMED,IGNORE   SMENU                          STATMON
TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
CMD==>
```

Figure 69. List of NetView-Supplied Default Status Monitor PF Keys

For more information about how your PF keys are set, refer to the NetView PFKDEF command in the NetView online help, and browse the CNMKEYS sample. Press **PF3** to return to the Domain Status Summary screen.

3. To select detailed information about specific resources:
   a. Press the **Tab** key to position the cursor in front of the resource type for which you want more information. To display detailed information for applications, position the cursor in the following way:

      ```
      _...260  APPLICATIONS  ....19   ......   ......   ......   ......   ...241
      ```

   b. Type any character except a blank in the space immediately before the field you just located. For example:

```
    x...260  APPLICATIONS  ....19   ......   ......   ......   ......   ...241
```

c. Press **Enter**.

A panel similar to Figure 70 is displayed.

```
STATMON.DSD(DESC)              DOMAIN STATUS DETAIL (DESCRIPTION)      09:02
HOST: HOST009          *1*   *2*   *3*   *4*
                       ACTIVE  PENDING   INACT    MONIT    NEVACT   OTHER
?...260  APPLICATIONS ?....19  ?......  ?......  ?......  ?......  ?...241
-------------------------------------------------------------------------------
? DISPLAY       |   NODE ID.  DESCRIPTION           NODE ID.  DESCRIPTION
 ? APPLS        |
 ? LINES        | ? CNM09     APPLICATION         ? A010      APPLICATION
 ? PUS/CLSTRS   | ? CNM09PPT  APPLICATION         ? A011      APPLICATION
 ? LUS/TERMS    | ? A         APPLICATION         ? A012      APPLICATION
 ? CDRMS        | ? APPT      APPLICATION         ? A013      APPLICATION
 ? CDRSCS       | ? A000      APPLICATION         ? A014      APPLICATION
  ? ACT         | ? A001      APPLICATION         ? A015      APPLICATION
  ? EVERY       | ? A002      APPLICATION         ? CNM09000  APPLICATION
  ? INACT       | ? A003      APPLICATION         ? CNM09001  APPLICATION
 ? PENDING      | ? A004      APPLICATION         ? CNM09002  APPLICATION
 ? BFRUSE       | ? A005      APPLICATION         ? CNM09003  APPLICATION
? VARY INACT    | ? A006      APPLICATION         ? CNM09004  APPLICATION
 ? I     ? F    | ? A007      APPLICATION         ? CNM09005  APPLICATION
? VARY ACT      | ? A008      APPLICATION         ? CNM09006  APPLICATION
 ? ONLY  ? ALL  | ? A009      APPLICATION         ? CNM09007  APPLICATION

CMD==>
TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
```

Figure 70. Domain Status Detail (Description) Panel Showing the VTAM Commands You Can Run against the Resources

This panel displays the name and description for each resource in the resource group you selected to access this panel. You can use any of the VTAM commands listed on this panel to display, activate, or inactivate any of the resources shown in the panel. To make a selection on the VTAM command menu, type any character except a blank or a question mark (?) over the ? field next to the command you want to use and next to the resource for which you want the command performed, then press Enter.

4. Enter the NetView SCLIST command to display the command lists that you can run from this panel, or press a PF key set to that command, such as the NetView default STATMON setting of PF11. A panel similar to Figure 71 on page 120 is displayed.

```
STATMON.DSD(DESC)              DOMAIN STATUS DETAIL (DESCRIPTION)      09:03
HOST: HOST009          *1*   *2*   *3*   *4*
                       ACTIVE  PENDING   INACT    MONIT    NEVACT   OTHER
?...260  APPLICATIONS ?....19  ?......  ?......  ?......  ?......  ?...241
-------------------------------------------------------------------------------
? AUTOTR         |   NODE ID.  DESCRIPTION           NODE ID.  DESCRIPTION
? NODE           |
? EVENTS         | ? CNM09     APPLICATION         ? A010      APPLICATION
? INACTF         | ? CNM09PPT  APPLICATION         ? A011      APPLICATION
? MONOFF         | ? A         APPLICATION         ? A012      APPLICATION
? MONON          | ? APPT      APPLICATION         ? A013      APPLICATION
? RECYCLE        | ? A000      APPLICATION         ? A014      APPLICATION
? REDIAL         | ? A001      APPLICATION         ? A015      APPLICATION
? SESS           | ? A002      APPLICATION         ? CNM09000  APPLICATION
? STATIONS       | ? A003      APPLICATION         ? CNM09001  APPLICATION
? STATS          | ? A004      APPLICATION         ? CNM09002  APPLICATION
                 | ? A005      APPLICATION         ? CNM09003  APPLICATION
                 | ? A006      APPLICATION         ? CNM09004  APPLICATION
                 | ? A007      APPLICATION         ? CNM09005  APPLICATION
                 | ? A008      APPLICATION         ? CNM09006  APPLICATION
                 | ? A009      APPLICATION         ? CNM09007  APPLICATION

CMD==>
TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
```

Figure 71. Domain Status Detail (Description) Panel Showing the Command Lists You Can Run against the Resources

This panel displays the command lists that you can run against one or more of the resources listed. To return to the original panel, enter the SVTAM command or press the NetView default STATMON PF10 key to display the VTAM commands that you can run from that panel.

To issue a command for a resource, type any character over the ? field next to the command you want to use and next to the resource for which you want the command performed, then press Enter.

5. Enter the NetView SMENU command, or press a PF key set to that command (the NetView status monitor default is PF24) to display activity and analysis information for the selected resources. A panel similar to Figure 72 on page 121 is displayed.

```
STATMON.DSD(DESC)              DOMAIN STATUS DETAIL (DESCRIPTION)      09:03
HOST: HOST009          *1*   *2*   *3*   *4*
                       ACTIVE  PENDING   INACT    MONIT    NEVACT   OTHER
?...260  APPLICATIONS ?....19  ?......  ?......  ?......  ?......  ?...241
-------------------------------------------------------------------------------
DISPLAY:          |   NODE ID.  DESCRIPTION           NODE ID.  DESCRIPTION
 HIGHER NODE      |
  ? SUMMARY       | ? CNM09     APPLICATION         ? A010      APPLICATION
  ? DETAIL        | ? CNM09PPT  APPLICATION         ? A011      APPLICATION
 THIS NODE        | ? A         APPLICATION         ? A012      APPLICATION
  ? SUMMARY       | ? APPT      APPLICATION         ? A013      APPLICATION
  ? DETAIL        | ? A000      APPLICATION         ? A014      APPLICATION
                  | ? A001      APPLICATION         ? A015      APPLICATION
                  | ? A002      APPLICATION         ? CNM09000  APPLICATION
----------------  | ? A003      APPLICATION         ? CNM09001  APPLICATION
DETAIL FORMAT:    | ? A004      APPLICATION         ? CNM09002  APPLICATION
                  | ? A005      APPLICATION         ? CNM09003  APPLICATION
  ? ANALYSIS      | ? A006      APPLICATION         ? CNM09004  APPLICATION
  ? ACTIVITY      | ? A007      APPLICATION         ? CNM09005  APPLICATION
                  | ? A008      APPLICATION         ? CNM09006  APPLICATION
                  | ? A009      APPLICATION         ? CNM09007  APPLICATION

CMD==>
TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
```

Figure 72. Domain Status Detail (Description) Panel Containing Activity and Analysis Information

You can use the status indicators (ACTIVE, PENDING, and so on) displayed in the heading to view information about a portion of the resources displayed on this panel. For example, to view information about only the ACTIVE applications, type any character over the ? field below ACTIVE and press Enter. The status monitor displays a new Description panel with information about only the active applications, as shown in Figure 73:

```
STATMON.DSD(DESC)              DOMAIN STATUS DETAIL (DESCRIPTION)      09:48
HOST: HOST009          *1*   *2*   *3*   *4*
                       ACTIVE  PENDING   INACT    MONIT    NEVACT   OTHER
?...260  APPLICATIONS ?....19  ?......  ?......  ?......  ?......  ?...241
-------------------------------------------------------------------------------
DISPLAY:          |   NODE ID.  DESCRIPTION           NODE ID.  DESCRIPTION
 HIGHER NODE      |
  ? SUMMARY       | ? CNM09     APPLICATION         ? BNJHWMON  APPLICATION
  ? DETAIL        | ? CNM09PPT  APPLICATION         ? DSIGDS    APPLICATION
 THIS NODE        | ? CNM09000  APPLICATION         ? CNM09VPD  APPLICATION
  ? SUMMARY       | ? CNM09001  APPLICATION         ? TSOA09    APPLICATION
  ? DETAIL        | ? CNM09002  APPLICATION         ? ECHOA09   APPLICATION
                  | ? CNM09003  APPLICATION
                  | ? CNM09004  APPLICATION
----------------  | ? CNM09005  APPLICATION
DETAIL FORMAT:    | ? CNM09006  APPLICATION
                  | ? AAUTCNMI  APPLICATION
  ? ANALYSIS      | ? DSIAMLUT  APPLICATION
  ? ACTIVITY      | ? CNM09LUC  APPLICATION
                  | ? CNM09SPT  APPLICATION
                  | ? DSICRTR   APPLICATION

CMD==>
TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
```

Figure 73. Domain Status Detail (Description) Panel Showing only Active Applications

Use the **DISPLAY** menu on the upper left side of the panel to ask for summary information or more details about the resources displayed on this panel (THIS NODE) or about the next HIGHER NODE above THIS NODE in the network configuration. To make your selection, type any character over the ? field next to your choice on the DISPLAY menu and next to the resource for which to display the information, then press Enter.

Use the **DETAIL FORMAT** menu on the lower left side of the panel to ask for more status information about the resources listed on this panel. You can view an analysis of the status of the resources by replacing the question mark in front of ANALYSIS with any character and pressing Enter. For resource types of APPLICATIONS and APPL MAJ NDS , an ACTIVITY option displays application message traffic information. You can view information about the activity of the applications with their current session partners by replacing the question mark in front of ACTIVITY with any character and pressing Enter.

6. Replace the question mark in front of ACTIVITY with any character and press Enter to view activity information. A panel similar to Figure 74 is displayed.

```
STATMON.DSD(ACT)                DOMAIN STATUS DETAIL (ACTIVITY)         09:09
HOST: HOST009          *1*   *2*   *3*   *4*
                       ACTIVE  PENDING   INACT    MONIT    NEVACT   OTHER
?...260  APPLICATIONS ?....19  ?......  ?......  ?......  ?......  ?...241
-------------------------------------------------------------------------------
DISPLAY:          |
 HIGHER NODE      |      NODE ID.  DESCRIPTION      SENDS CHANGE |   RECVS CHANGE
  ? SUMMARY       |    ? CNM09     APPLICATION          0      0 |        0      0
  ? DETAIL        |    ? CNM09PPT  APPLICATION          0      0 |        0      0
 THIS NODE        |    ? CNM09000  APPLICATION          0      0 |        0      0
  ? SUMMARY       |    ? CNM09001  APPLICATION          0      0 |        0      0
  ? DETAIL        |    ? CNM09002  APPLICATION          0      0 |        0      0
                  |    ? CNM09003  APPLICATION          0      0 |        0      0
                  |    ? CNM09004  APPLICATION          0      0 |        0      0
----------------  |    ? CNM09005  APPLICATION          0      0 |        0      0
DETAIL FORMAT:    |    ? CNM09006  APPLICATION         84      0 |       75      0
  ? DESCRIPT      |    ? AAUTCNMI  APPLICATION          0      0 |        0      0
  ? ANALYSIS      |    ? DSIAMLUT  APPLICATION          0      0 |        0      0
  ? ACTIVITY      |    ? CNM09LUC  APPLICATION        148      0 |       55      0
                  |    ? CNM09SPT  APPLICATION          0      0 |        0      0
                  |    ? DSICRTR   APPLICATION          0      0 |        0      0

CMD==>
TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
```

Figure 74. Domain Status Detail (Activity) Panel

This panel displays information about the activity between applications and the terminals and LUs in session with them. For the application you choose, the panel shows the number of messages sent to and received from the session partners of each application. You can use this information to monitor how frequently a particular application is accessed and how heavily it is used at any given time of day.

7. Replace the question mark in front of ANALYSIS with any character and press Enter to view analysis information. A panel similar to Figure 75 on page 123 is displayed.

```
STATMON.DSD(ANALYSIS)           DOMAIN STATUS DETAIL (ANALYSIS)         09:15
HOST: HOST009          *1*   *2*   *3*   *4*               ELAPSED TIME   1:22
                      ACTIVE  PENDING   INACT    MONIT    NEVACT   OTHER
?...260  APPLICATIONS ?....19  ?......  ?......  ?......  ?......  ?...241
-------------------------------------------------------------------------------
DISPLAY:        |             STATUS    |    ACTIVE   PENDING   INACTIVE   OTHER
 HIGHER NODE    |   NODE ID.   SINCE    |  COUNT  %  COUNT  %  COUNT  %  COUNT  %
  ? SUMMARY     | ? CNM09    A  8:11    |     3 100     0   0     0   0     1   0
  ? DETAIL      | ? CNM09PPT A  7:53    |     1 100     0   0     0   0     1   0
 THIS NODE      | ? CNM09000 A  7:53    |     1 100     0   0     0   0     1   0
  ? SUMMARY     | ? CNM09001 A  7:53    |     1 100     0   0     0   0     1   0
  ? DETAIL      | ? CNM09002 A  7:53    |     1 100     0   0     0   0     1   0
                | ? CNM09003 A  7:53    |     1 100     0   0     0   0     1   0
                | ? CNM09004 A  7:53    |     1 100     0   0     0   0     1   0
---------------| ? CNM09005 A  7:53    |     1 100     0   0     0   0     1   0
DETAIL FORMAT:  | ? CNM09006 A  8:11    |     2  77     1   0     0   0     2  23
  ? DESCRIPT    | ? AAUTCNMI A  7:53    |     1 100     0   0     0   0     1   0
                | ? DSIAMLUT A  7:53    |     1 100     0   0     0   0     1   0
  ? ACTIVITY    | ? CNM09LUC A  7:53    |     1 100     0   0     0   0     1   0
                | ? CNM09SPT A  7:53    |     1 100     0   0     0   0     1   0
                | ? DSICRTR  A  7:53    |     1 100     0   0     0   0     1   0

CMD==>
TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
```

Figure 75. Domain Status Detail (Analysis) Panel

This panel displays statistics about changes in the status of network resources. For the major resource you selected to display this panel, the status monitor presents the following information about that major resource and the minor resources grouped under it.

- The current status of each resource
- The time of day each resource went into its current state
- The number of times each resource has been in the ACTIVE, PENDING, INACTIVE, or OTHER state
- The percentage of time each resource has been in the ACTIVE, PENDING, INACTIVE, or OTHER state

The status monitor begins collecting statistics about network resources when it is initialized. These statistics are updated each time the status of a resource changes. You can use the NetView CLRSTATS command to clear these statistics from the status monitor database. This resets all counts to zero and begins accumulating new data (as though it had been reinitialized).

The amount of time the status monitor has been collecting statistics since its last initialization or since the CLRSTATS command was issued is displayed in the heading under the ELAPSED TIME field.

To browse the active network log from any of the status monitor panels, take one of the following actions:

- Enter **BROWSE NETLOGA**
- Press a PF key set to BROWSE NETLOGA (such as the NetView default PF setting of PF5)
- Select one of the message indicators at the top of the panel

Tab to select one of the message indicators, type a character to the left of the indicator (for example, *1*) and press Enter. A figure similar to Figure 76 on page 124 is displayed.

```
STATMON.BROWSE     ACTP  NETWORK LOG FOR 04/12/01 (93221) COLS 017 094  09:17
HOST: HOST009          *1*   *2*   *3*   *4*                  SCROLL ==> CSR
 ---2----+----3----+----4----+----5----+----6----+----7----+----8----+----9----
 CNM09    08:49:42   CNME1087  CNM35 DSILCRTR CNM09LUC *     00000050
 CNM09    08:49:43   CNME1087  CNM43 DSILCRTR CNM09LUC *     00000051
 CNM09    08:49:43   CNME1087  CNM54 DSILCRTR CNM09LUC *     00000052
 CNM09    08:49:43   CNME1087  CNM72 DSILCRTR CNM09LUC *     00000053
 CNM09    08:49:44   CNME1087  CNM83 DSILCRTR CNM09LUC *     00000054
 CNM09    08:56:30   CNM154I HOURLY OPERATOR MESSAGE INDICATOR STATISTICS
 CNM09    08:56:30   CNM155I    MI #1   MI #2    MI #3    MI #4  LOGTOTAL
 CNM09    08:56:30   CNM156I    00000   00000    00000    00000    000000
 CNM09    08:59:41   CNME1087  CNM69 DSILCRTR CNM09LUC *     00000055
 CNM09  % 08:59:41   DSI781I CNM09LUC : UNABLE TO ALLOCATE SESSION FOR 'CNMD9LU
 CNM09    08:59:42   CNME1087  CNM52 DSILCRTR CNM09LUC *     00000056
 CNM09    08:59:42   CNME1087  CNM24 DSILCRTR CNM09LUC *     00000057
 CNM09    08:59:42   CNME1087  CNM11 DSILCRTR CNM09LUC *     00000058
 CNM09    08:59:42   CNME1087  CNM35 DSILCRTR CNM09LUC *     00000059
 CNM09    08:59:43   CNME1087  CNM43 DSILCRTR CNM09LUC *     0000005A
 CNM09    08:59:43   CNME1087  CNM54 DSILCRTR CNM09LUC *     0000005B
 CNM09    08:59:43   CNME1087  CNM72 DSILCRTR CNM09LUC *     0000005C
 CNM09    08:59:44   CNME1087  CNM83 DSILCRTR CNM09LUC *     0000005D

CMD==>
TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
```

Figure 76. Browse Network Log Panel

Topic:	Reference:
Network log message format	Appendix A, “Message Format,” on page 341
STATMON, CLRSTATS command	NetView online help
STATOPT statement syntax	*IBM Tivoli NetView for z/OS Administration Reference*
Defining the status monitor	*IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*

Using the Status Monitor for Automatic Reactivation of Resources

The status monitor MONIT statement enables automatic reactivation of failing resources.To set up automatic reactivation, the O MONIT statement must be coded in the status monitor initialization member DSICNM.

Major nodes, applications, cross domain resources, and resources past the local NCP cannot be reactivated automatically with the MONIT function. Other resources can be excluded from automatic reactivation by coding NOMONIT on the STATOPT statement in the VTAMLST definition for the resource.

When a resource that is eligible for automatic reactivation becomes INACTIVE, and the status of its higher node is ACTIVE or CONNECTABLE, the status monitor attempts to reactivate the resource every minute until the resource status is no longer INACTIVE. The resource is placed in the MONIT column on the status monitor screen during this time.

If a resource is inactivated in a solicited manner (for example, a VARY NET,INACT command was issued), the status monitor does not attempt to reactivate the resource unless a `MONIT START,ID=resname` command is issued for that resource after it has been inactivated.

You can use the MONIT command to start or stop global monitoring, or to start or stop monitoring for one or more resources. When global monitoring is set off, status monitor does not attempt to reactivate any resources. For more information, refer to the MONIT command in the NetView online help and the O MONIT statement in the *IBM Tivoli NetView for z/OS Administration Reference*.

Using Service Points

A service point can be used to collect data not normally collected by VTAM or the NetView program, such as data for devices on a token ring or on non-VTAM devices. Commands can also be initiated through a service point to interrogate and control non-VTAM devices. You can collect data from and control devices using Service Point Command Services, or Common Operations Service such as RUNCMD, LINKDATA, LINKPD, or LINKTEST, where the Service Point application supports them.

Topic:	Reference:
Unknown service point resources	HELPDESK 6

Issuing Commands to a Service Point Application Using the RUNCMD Command

Although you can issue the RUNCMD command directly from the command line, it is designed to be coded inside a REXX or NetView command list language command list and used with the `CLISTVAR=YES` option, which saves replies in command list variables. You can use the RUNCMD from the NetView command line to test the results of a specific RUNCMD command. Note that, in such cases, the `CLISTVAR=YES` option is not valid.

The RUNCMD command routes commands to service points for processing by one of the service point applications. The following example shows using the RUNCMD command to send the `SWITCH_LINES OLD=LINE1,NEW=LINE2` command to the service point application APPL07 located on NET01:

```
runcmd sp=nmws1,appl=appl07,switch_lines old=line1,new=line2
```

In this example, NMWS1 is the name of the service point that processes the command. The service point name is the PU name for nodes connected for management by an SSCP-PU session or a Control Point (CP) name for nodes connected and managed through an LU 6.2 MultiDomain Router session.

Topic:	Reference:
RUNCMD command	NetView online help

Setting Up Service Points

Two types of transport can be specified to deliver network management data between the NetView host and the Service Point: SSCP-PU transport and APPC LU 6.2 (MS) transport.

SSCP-PU Transport: The following examples show the host definitions needed for SSCP-PU transport between the NetView host and the service point. The following example is of an NCP configuration definition:

```
NVPCLINE LINE ADDRESS=(025),
              CLOCKNG=EXT,
              DUPLEX=HALF,
              NRZI=YES,
```

```
              RETRIES=(7,4,4),
              SPEED=9600,
              MAXPU=1

NVPCORD SERVICE ORDER=(NVIXCP),MAXLIST=1

NVIXCP PU  ADDR=C1,
           IRETRY=NO,
           MAXDATA=512,
           MAXOUT=7,
           PASSLIM=7,
           PUTYPE=2,
           ISTATUS=ACTIVE
```

To transfer files between the NetView program and a workstation, add a host definition similar to the following definition for the CICS/DDM program (the following definitions are specifically for the host side of NetView/PC and an AIX service point).

```
NVIXL621 LU  LOCADDR=1,
             ISTATUS=ACTIVE,
             PACING=1,
             MODETAB=NVPCTAB,
             DLOGMOD=NVPCMODE
```

The following example is of a VTAM logmode definition:

```
NVPCTAB MODETAB

LABEL MODEENT LOGMODE=NVPCMODE,
              FMPROF=X'13',
              TSPROF=X'07',
              PRIPROT=X'B0',
              SECPROT=X'B0',
              COMPROT=X'D0B1',
              RUSIZES=X'8686',
              PSERVIC=X'060200000000000000002F00',
              TYPE=X'00'
       MODEEND
       END
```

Multidomain Services (MDS) LU 6.2 Transport: The host definitions for multidomain services LU 6.2 transport are similar to the definitions for SSCP-PU transport, with the exception that you need to specify the logical units and DLOGMOD=M3SDLCQ logmode at the Group level. The following example is of an NCP configuration:

```
NTSDLC Group DIAL=NO,
             LNCTL=SDLC,
             REPLYTO=3,
             RNRLIMT=3,
             TESTTO=1,
             TYPE=NCP,
             VIRTUAL=NO,
             ISTATUS=INACTIVE
             DLOGMOD=M3SDLCQ,
             MODETAB=AMODETAB,
             USSTAB=AUSSTAB,
             VPACING=0

NTLN04 LINE ADDRESS=(004)
            CLOCKNG=EXT,
            DUPLEX=FULL,
            SPEED=9600,
            NRZI=NO,
            RETRIES=(7,4,4),
```

```
            MAXPU=9,
            ETRATIO=1

NVPCORD SERVICE ORDER=(NTPU04),MAXLST=17

NTPU04 PU ADDR=C1,
          IRETRY=YES
          MAXDATA=2048,
          MAXOUT=7,
          ANS=CONT,
          PASSLIM=12,
          PUTYPE=2,
          PUDR=YES,
          XID=YES

NTLU41 LU LOCADDR=0
NTLU42 LU LOCADDR=0
NTLU43 LU LOCADDR=0
NTLU44 LU LOCADDR=0
NTLU45 LU LOCADDR=1
NTLU46 LU LOCADDR=2
NTLU47 LU LOCADDR=3
```

In addition, specify the MDSRTR application to VTAM. This is the actual component used for communication between the service point and the host system. The following example is of the VTAM definition:

```
MDSRTR APPL AUTH=ACQ,
   EAS=6,
   APPC=YES,
   MODETAB=NVPCMODE,
   DLOGMOD=NVPCMODE,
   PARSESS=YES

NVPCMODE MODEENT LOGMODE=NVPCMODE,
   FMPROF=X'13',
   TSPROF=X'07',
   PRIPROT=X'B0',
   SECPROT=X'B0',
   COMPROT=X'50B5',
   RUSIZES=X'8686',
   PSERVIC=X'060200000000000000002F00',
   TYPE=X'00'
```

For the service point to establish the MS sessions with the NetView program, both primary and secondary LUs must be active. To accomplish this, ensure that your line is activated with the SCOPE=ALL parameter. For example:

```
v net,act,id=linename,scope=all
```

The SCOPE=ALL parameter ensures that the PU and LUs associated with that line become active.

Configuring Communications Manager for LU 6.2 Commands: To configure Communications Manager for LU 6.2 commands, define the configuration parameters for the SNA communication services in the Node Definition Files (NDF). The following example supports a Communications Manager/2 end node directly connected to the NetView program:

```
DEFINE_LOCAL_CP  FQ_CP_NAME(USIBMTH.THX141G0)
                 CP_ALIAS(THX141G0)
                 NAU_ADDRESS(INDEPENDENT_LU)
                 NODE_TYPE(EN)
                 NODE_ID(X'05D00141')
                 HOST_FP_SUPPORT(YES);
```

Figure 77. Configuring Communications Manager/2 for the LAN NetView Tie Program (Part 1 of 3)

```
DEFINE_LOGICAL_LINK  LINK_NAME(HOST0001)
                     ADJACENT_NODE_TYPE(LEARN)
                     DLC_NAME(IBMTRNET)
                     ADAPTER_NUMBER(0)
                     DESTINATION_ADDRESS(X'400010000307')
                     CP_CP_SESSION_SUPPORT(YES)
                     ACTIVATE_AT_STARTUP(NO)
                     LIMITED_RESOURCE(USE_ADAPTER_DEFINITION)
                     LINK_STATION_ROLE(USE_ADAPTER_DEFINITION)
                     SOLICIT_SSCP_SESSION(YES)
                     NODE_ID(X'05D00141')
                     EFFECTIVE_CAPACITY(USE_ADAPTER_DEFINITION)
                     COST_PER_CONNECT_TIME(USE_ADAPTER_DEFINITION)
                     COST_PER_BYTE(USE_ADAPTER_DEFINITION)
                     SECURITY(USE_ADAPTER_DEFINITION)
                     PROPAGATION_DELAY(USE_ADAPTER_DEFINITION)
                     USER_DEFINED_1(USE_ADAPTER_DEFINITION)
                     USER_DEFINED_2(USE_ADAPTER_DEFINITION)
                     USER_DEFINED_3(USE_ADAPTER_DEFINITION);
```

Figure 77. Configuring Communications Manager/2 for the LAN NetView Tie Program (Part 2 of 3)

```
DEFINE_DEFAULTS  IMPLICIT_INBOUND_PLU_SUPPORT(YES)
                 DEFAULT_MODE_NAME(BLANK)
                 MAX_MC_LL_SEND_SIZE(32767)
                 DIRECTORY_FOR_INBOUND_ATTACHES(*)
                 DEFAULT_TP_OPERATION(NONQUEUED_AM_STARTED)
                 DEFAULT_TP_PROGRAM_TYPE(BACKGROUND)
                 DEFAULT_TP_CONV_SECURITY_RQD(NO)
                 MAX_HELD_ALERTS(10);
                 START_ATTACH_MANAGER;
```

Figure 77. Configuring Communications Manager/2 for the LAN NetView Tie Program (Part 3 of 3)

Attaching to a LAN Network Manager Service Point: You can use the LAN command list to access additional functions supported by the IBM LAN Network Manager. To access all supported IBM LAN Network Manager commands, enter:

```
lan sp=spname,cmd help
```

Note: Use the command list with IBM LAN Network Manager Version 1.1 or later releases. The LAN command list is not valid for IBM LAN Network Manager Version 1.0 or LAN Manager Version 2. (The LAN command is a shell that issues the RUNCMD command.)

Attaching to the IBM LAN NetView Tie Program: With the IBM LAN NetView Tie program, you can receive notifications from network resources managed by the LAN Network Manager program. The LAN NetView Tie program receives alarm and non-alarm events from the LAN Network Manager program and converts

them into alerts which are sent to the NetView program (using Communications Manager). The IBM LAN NetView Tie program converts the LAN Network Manager program into a service point for the NetView program.

Starting and Stopping the Tie program: To start the Tie program from the NetView command line, enter:

```
runcmd sp=puname,appl=remoteop,op=operatorid; start tie [tiebase] op=operatorid
```

Where *puname* is the physical unit name of the workstation on which you are starting the Tie program and `tiebase` tells the Tie program to start, using the TIEBASE.INI file.

If the NetView program is recycled or Communications Manager is restarted, issue the following command:

```
focalpt change target=cpname, fpcat=alert
```

Where *cpname* is the independent LU name of the LAN Tie node, depending on the configuration of the NetView program.

To stop the Tie program from the NetView command line, enter:

```
runcmd sp=puname,appl=tie,op=operatorid; stop_normal
```

Where `stop_normal` is the command to stop the Tie program in a normal manner.

To stop the Tie program immediately, enter:

```
runcmd sp=puname,appl=tie,op=operatorid; stop_immediate
```

Topic:	Reference:
Installing and configuring the Tie Program	*IBM LAN NetView Tie Administration Guide*
Tie Program commands	*IBM LAN NetView Tie Getting Started*
Managing hardware and software resources on a LAN using the IBM LAN NetView Manage program	*IBM LAN NetView Manage Administration Guide*

Attaching to a Communications Manager/2 Remote Operations Service Point: You can use the Command Facility of the NetView program to issue commands through the Service Point Application Router (SPA Router) to Remote Operation Services (ROP Services).

Note: Before you can process commands, enable ROPS and then start SPAR and ROPS.

Topic:	Reference:
Developing REXX executable files and command lists to use SPA Router and ROP Services and setting up a SPA Router and ROP Services	*Communications Manager/2 Service Point Application Router and Remote Operations Service Guide*

Using a REXX Command List to Issue Commands to a Service Point Application

You can customize the NetView program for use with service points through REXX executable files and command lists. REXX executable files and command lists allow service point commands to be issued automatically, that is, without the need to manually enter each command. In addition, REXX executable files and command lists provide a wide range of capabilities; they can perform functions on all LANs in the enterprise. Plus, REXX executable files can be placed within other REXX executable files or other high level programs to provide more complex functions. This is also true for command lists.

You can issue the RUNCMD in a command list, and use the CLISTVAR keyword to have the RUNCMD responses returned in command list variables. You can then process these responses in the command list, or present them to the operator as a full-screen display using the VIEW command processor.

Note: Using a service point (LAN Network Manager, LAN NetView Tie) with ROPS involves care in installing.

Topic:	Reference:
RUNCMD command syntax	NetView online help
Writing command lists	*IBM Tivoli NetView for z/OS Programming: REXX and the NetView Command List Language*

Using the Automation Table to Control Resources Attached through Service Points

MultiSystem Manager (MSM), the LAN Network Manager program, and other programs and components create alerts which are forwarded to NetView, where an automation table segment can extract information from the alert and automatically react.

In the following example, an automation table segment detects alerts prompted by the receipt of a link-down trap from IP address 9.67.5.120. The command list, FNDROUTE, is run 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('FNROUTE ')) ;
  END;
```

The REXX command list looks like this:

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

The command list retrieves the name of the service point program and the service point application name from the alert to create a RUNCMD command.

Topic:	Reference:
RUNCMD command	NetView online help
Controlling TCP/IP resources	*Tivoli NetView for AIX Host Connection*

Using CICS Automation Feature

You can use the CICS Automation Feature (CICSAO) to check the status of multiple subsystems, start and stop CICS subsystems individually or in groups, and check the status of interregion and intersystem connections.

Obtaining Detailed Status Information for a CICS Subsystem

Complete the following steps to obtain information for a CICS subsystem.

1. Enter `cics` from any NetView command line to access the CICSAO main menu. The panel shown in Figure 78 is displayed.

```
EVEK0000       CICS Automation: Main Menu                    Page:   1 OF   1
           (C) 5695-064 Copyright IBM Corp 2000              Date: 04/12/01
Subsystem, Group or Domain   ________ (? for list)           Time: 11:26

Select an Option . . . . .   __

   1. Inquire                Display detailed status of CICS subsystems
   2. Start                  Start a CICS subsystem, group or domain
   3. Shutdown               Shutdown a CICS subsystem, group or domain
   4. Triggers               Display start and shutdown trigger condition
   5. Service Periods        Perform service periods functions
   6. Master Terminal        Perform master terminal functions
   7. Monitoring             Perform monitoring functions
   8. Broadcast              Send message to specific CICS subsystem(s)
   9. Support                Provide support functions
  99. Local functions        Provide access to user defined local functions









Command ===>
F1=Help      F2=End       F3=Return                          F6=Roll
```

Figure 78. CICS Automation Main Menu

2. Enter the name of the CICS subsystem, group, or domain for which you want to display information in the `Subsystem, group or domain` field and select option 1. A panel similar to Figure 79 on page 132 is displayed.

```
EVEKQ400      CICS Automation: Subsystem Information          Page:   1 of   1
                                                              Date: 04/12/01
Subsystem  . . . . . .   CICS10AA   (? for list)             Time: 13:49

Subsystem status . . :  STOPPED         Job name . . . . . . :  CICS10AA
Since  . . . . . . . :  04/12/01 18:16  NetView domain . . . :  ACO10

VTAM information
  Specific appl. name:  CICS10AA        ACB status  . . :   CLOSED
  Generic appl. name :  CICS10A         XRF status  . . :   ACTIVE
  Active sessions    :  0
  Pending sessions   :  0

Last start                            Last shutdown
  Initiated : 04/12/01  15:17:49        Initiated . . : 04/12/01 18:15:31
  Completed : 04/12/01  15:18:45        Completed . . : 04/12/01 18:16:29
  Start type: EMERGENCY                 Warm keypoint : TAKEN
                                        Abend msgid   : ----------
                                        Abend code    : ------
Next start  : 04/15/01  07:30         Next shutdown   : 04/14/01 17:30


Command ===>
F1=Help      F2=End        F3=Return        F4=CICS Menu          F6=Roll
```

Figure 79. CICS Subsystem Information Panel

This panel contains detailed subsystem information, including the status of the subsystem, how the subsystem is defined to VTAM, and the last and next start and shutdown dates.

Using IMS Automation Feature

You can use the IMS Automation Feature (IMSAO) to check the status of all IMS subsystems and start or stop IMS subsystems individually or in groups.

Obtaining Detailed Status Information for an IMS Subsystem

Complete the following steps to obtain information for an IMS subsystem.

1. Enter **ims** from any NetView command line to access the IMS Automation main menu. The panel shown in Figure 80 on page 133 is displayed.

```
EVIK0000           IMS Automation: Main Menu                  Page: 1 of 1
           (C) 5695-063 Copyright IBM Corp 2000               Date: 04/12/01
Subsystem, Group or Domain   ________ (? for list)            Time: 16:27
                                                             Domain: CNM01
Select an option.
        __  1  Display detailed status of an IMS subsystem
            2  Start an IMS subsystem, group or domain
            3  Shutdown an IMS subsystem, group or domain
            4  Display start and shutdown trigger conditions
            5  Perform service periods functions
            6  Perform Master Terminal Operator functions
            7  Display critical messages
            8  Send message to specific IMS subsystem
            9  Provide support functions
           99  Provide access to user defined local functions




Command ===>
F1=Help      F2=End       F3=Return                                F6=Roll
```

Figure 80. IMS Automation Main Menu

2. Type the name of the IMS subsystem, group, or domain for which you want to display the status in the **Subsystem, Group or Domain** field and select option **1**. A panel similar to Figure 81 is displayed.

```
EVIKQ100         IMS Automation: Inquire Subsystem Components   Page:   1 of 1
                                                                Date: 04/12/01
Subsystem  . . . . . .   IMS10AA  (? for list)                 Time: 17:06
                                                              Domain: CNM01
Select an option . . . . .  _ 1  Detailed Subsystem status
                              2  Defined dependent regions
                              3  Active dependent regions
                              4  Shutdown status of active terminals
                              5  Explanation of Takeover reason code
```

Figure 81. IMSAO Inquire Subsystem Components Panel

From this screen, you can select the type of display that you want. For example, to view detailed subsystem information, select option **1**. A panel similar to Figure 82 on page 134 is displayed.

```
EVIKI00          IMS Automation: Subsystem Information         Page:   1 of 1

                                                               Date: 04/12/01
Subsystem  . . . . . .   IMS10A1_ (? for list)                 Time: 10:34

Subsystem status . . : UP               Since . . . . . : 16:42    04/10/01
Job  . . . . . . . . : IMS10AA          Job number  . . : 9843
NetView domain . . . : AOF10

VTAM Information
  Specific appl. name: IMS10AA          DC status   . . : UP
  Generic appl. name : IMSESA1          XRF . . . . . : YES
  Active sessions    : 1                XRF status  . . : ACTIVE
  Pending sessions   : 0

Last start                              Last shutdown
  Initiated : 16:40:28    04/10/01        Initiated . . : 17:06:00    04/05/01
  Completed : 16:42:35    04/10/01        Completed . . : 17:07:56    04/05/01
  Start type: AUTO                        Abend code    :

Next start  :          none             Next shutdown   :          none

Command ===>
F1=Help      F2=End       F3=Return    F4=IMS Menu  F5=Refresh   F6=Roll
```

Figure 82. IMSAO Detailed Subsystem Information Panel

You can also display defined regions (option 2), active regions (option 3), a list of terminal shutdowns and types of shutdowns (option 4), and reason code and explanation for a takeover (option 5).

Chapter 6. Managing Network and System Status

To manage the status of your network from a workstation, use the NetView management console or the System Automation for z/OS graphical interface to collect status data and display it in real time. From a 3270 terminal, use the following products to monitor the status of your network and to provide performance measurements:

- Tivoli Workload Scheduler for z/OS
- Tivoli Decision Support for z/OS
- NTune
- System Automation for z/OS

Note: These products are not shipped with NetView.

Using Tivoli Workload Scheduler for z/OS

Using Tivoli Workload Scheduler for z/OS to plan and control your production workload according to your business schedules, you can perform the following tasks:

- Define the deadlines, order of processing, and resource requirements of your production batch jobs and started tasks. This information is used by Tivoli Workload Scheduler for z/OS to automatically start your processing in the correct order. When conflicts arise, such as when more processing needs to be started than the available resources can accommodate, Tivoli Workload Scheduler for z/OS gives priority to processing that is closest to the defined deadline.
- Schedule communication with the NetView program when a NetView process is dependent on the business processing schedules.
- Generate alerts to the NetView program when problems are detected in the production workload, such as under the following conditions:
  - An operations ends in error
  - A batch job has been queued by JES for a long time
  - A batch job or started task has been running longer than expected
  - Processing is getting late and deadlines are in jeopardy
  - A Tivoli Workload Scheduler for z/OS subtask fails
  - A defined threshold has been reached on the Tivoli Workload Scheduler for z/OS queue
- Provide a hot standby facility to maximize the availability of the controlling functions in a z/OS sysplex.
- Automatically recover failures in batch jobs and started tasks, including cleaning up the catalog.
- Automatically restart or reroute the processing of controlled destinations to alternate destinations when the primary destination is not available, such as when a z/OS failure or a communications outage occurs.

Using Performance Reporter

The Performance Reporter for MVS accepts the output of the session monitor to create a logical view of the layout of your network. For example, groups of lines are grouped with the communication controllers and PUs which they connect. NCPs are also linked with the communication controllers on which they run and

with the VTAM programs to which they connect so that users can perform availability, response time, throughput, and exception reporting on a higher level.

For example, line utilization on an aggregate or unit basis can be queried for a given geographical location. Performance Reporter resolves individual network component names (in this case, line names) to geographical sites that have meaning to the enterprise. This is particularly valuable when enterprises are trying to quantify end-user availability site by site, application by application, or NCP by NCP.

These statistics are provided by Performance Reporter through the NetView RECORD SESSTATS command and the NetView program's ability to write System Management Facilities (SMF) Record Type 39.

Setup Prior to Using the Performance Reporter

The Performance Reporter is dependent on data obtained by the session monitor. Therefore, define the session monitor to pass the required information (SMF Record Type 39) to the NetView Log Task.

Topic:	Reference:
Installing and customizing Network Reporter	*Performance Reporter for MVS: Installation/Customization*
Setting up the Session Monitor to log data to the external log (SMF)	*IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*

Using NetView Performance Monitor

You can use the NetView Performance Monitor to collect performance data to determine if performance objectives are being met. If these objectives are not being met, you can send alerts to the NetView program. The alerts can either trigger an automated response or be sent to an operator for action.

With the NetView Performance Monitor, you can:
- Collect performance data from various network sources
- Monitor defined thresholds
- Alert operators about performance degradation
- Identify bottlenecks in the network
- Provide information on response time
- Send alerts to NetView

Topic:	Reference:
NetView Performance Monitor	*NetView Performance Monitor User's Guide*
Using the NetView Performance Monitor and the NetView program to solve network problems	"Sluggish Network Performance (NetView Performance Monitor)" on page 322

Using NTune

You can use NTune to monitor and tune your NCP while your communication network is running. NTune provides a detailed view of the NCP and you can alter key fields without having to interrupt operations.

NTune is composed of NTuneMON and its feature, NTuneNCP.

NTuneMON runs on NetView and monitors NCPs that were activated by VTAM on the host where NTuneMON is running. You can use NTuneMON to display detailed information about NCPs covering a wide variety of areas from frame relay to control block pools. NTuneMON queries NCP storage for information regarding:

- Virtual routes
- Transmission groups
- SNA Network Interconnect
- Network Name Table
- Token-ring resources
- Ethernet subsystem and Internet Protocol
- NCP buffers and pool utilization
- IBM 3746 Model 900

NTuneNCP is used with NTuneMON to interactively tune the NCP without the need to regenerate or reload. NTuneNCP is responsible for receiving change requests, altering key NCP fields, and logging changes to the trace table.

Topic:	**Reference:**
Using NTune	*NTune User's Guide*
Using NTuneNCP	*NTuneNCP Reference*

Chapter 7. Monitoring Hardware and Software Problems

Hardware problems are associated with the physical structure of a network. The physical network consists of the hardware and software that connect network resources, allowing them to communicate with each other. The physical network includes the following connections:

- Hosts
- Communication controllers
- Cluster controllers
- Cable, telephone lines, or satellites
- Various devices such as printers and terminals

Associated with each connection is the network problem determination application (NPDA) responsible for performing link tests and diagnosing problems.

You can use the NetView management console or the hardware monitor to detect hardware problems. The sections that follow describe how to use the hardware monitor; to obtain additional information about using the NetView management console to monitor hardware problems, see Chapter 3, "Monitoring and Controlling Your Network from a Workstation," on page 45.

Using the Hardware Monitor

Many hardware resources in a network send information records and error records to the host system. The hardware monitor collects this information and arranges and displays the data to help you with problem determination and prevention.

You can use the hardware monitor to display the most recent events and statistics recorded for a network resource. The hardware monitor analyzes error data for probable causes and lists actions that can be taken to correct the problem. You can use filters to keep extraneous information from complicating your problem-solving efforts (for additional information on setting filters, see "Using Hardware Monitor Filters" on page 208). An alert function informs you quickly of high-priority problems. You can also record problems directly into the Information/Management System from the hardware monitor. Use the NetView management console to display the GMFALERT records, which represent resources monitored by the NetView management console.

Data Collection

The hardware monitor collects data from many different sources in various formats and gives a common structure to this information. This data can be classified as solicited or unsolicited data.

Solicited Data

Solicited data is received as the result of a specific request for information or as the result of an action that you have taken. Certain SNA control units keep counters of different types of communication errors they detect and transmit the counters to the host only as solicited data.

Unsolicited Data

Unsolicited data can be recorded as a statistic, an event, or as a GMFALERT record. Unsolicited data is received without any action on your part. You can receive unsolicited data when an error or performance problem is detected in the network. Unsolicited data can also be received when a problem in the network is resolved or a resource is deactivated.

Statistics are records of traffic volumes and temporary errors. *Events* can be records of permanent errors, or of other unusual occurrences, and can come from statistics that qualify for event status because of a high ratio of temporary errors to traffic. Hardware alerts are events that require attention. *GMFALERT records* represent events that pertain to resources monitored by the NetView management console.

When the hardware monitor receives unsolicited data, it creates a record containing information about the data and stores it as an event, statistical record, or GMFALERT in the database. If the data qualifies as an alert, an alert record is also created. Unsolicited alerts can also be received when forwarded from distributed NetView programs or entry point nodes.

Figure 83 on page 141 provides an illustration of hardware monitor data collection.

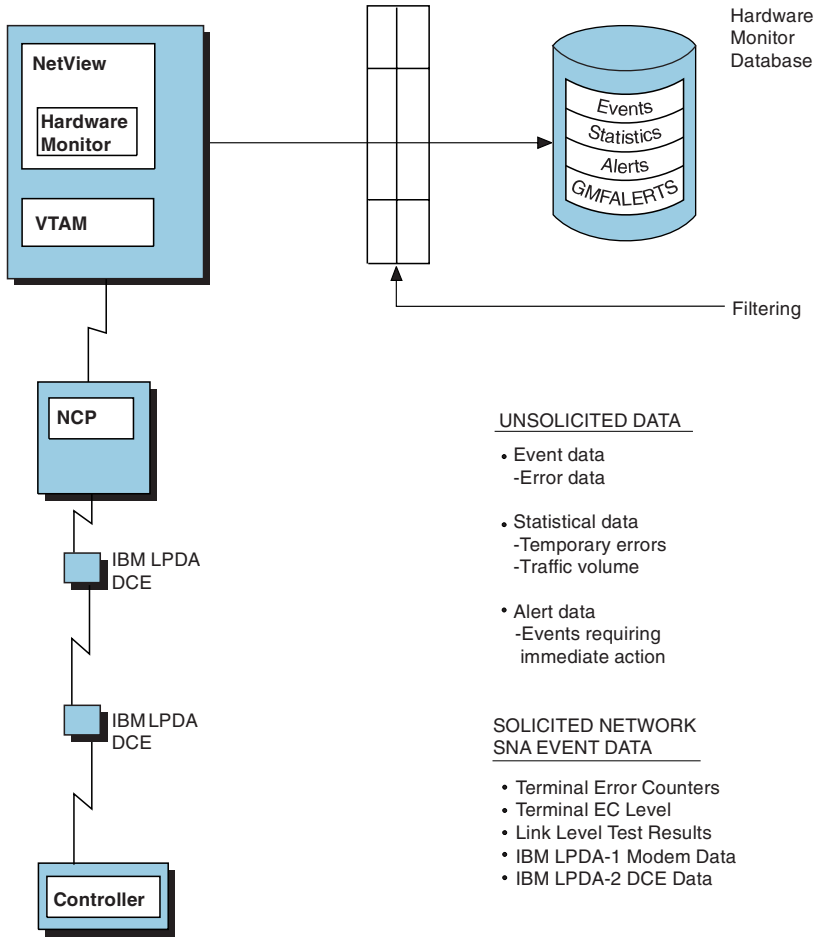


Figure 83. Data Collected by the Hardware Monitor

Record Types

The hardware monitor creates a database made up of several record types: statistics, events, GMFALERTs, and alerts.

Statistics

Statistics are records of traffic and recoverable error counts that have been collected at certain resources and reported to the host system. Statistical data generated by resources is sent to the host, and the hardware monitor stores these records in its database. For certain resources, the hardware monitor analyzes each statistical record to determine whether to create a performance event record, which can become an alert.

A statistic can become an event when it exceeds the limits that you have set as a threshold. A threshold is a ratio of temporary errors compared to the traffic associated with the resource and is expressed as a percentage. A threshold

indicates the least acceptable percentage of temporary errors. If the threshold is exceeded, the hardware monitor creates an event record to record this condition. The original record is also recorded as a statistic.

Events

Events are unexpected occurrences in network operation. An event can be created when the attempted activation of a resource fails. This failure can be because of a physical error in the network. Event data detected and generated by resources is sent to the host system for the hardware monitor to store in its database and to determine whether to issue and record an alert. Resolution major vectors (X'0002'), which inform you that an alert was resolved, are also stored on the database as events.

GMFALERTs

GMFALERT records represent events that pertain to resources monitored by the NetView management console. If the NetView management console is not installed, the GMFALERT records, which are a subset of NetView management console event report records, are recorded in the hardware monitor database. The alert history window of NetView management console is one place where GMFALERT records are displayed. Prior to NetView V3R2, the GMFALERT records were recorded to the GMFHS VSAM database along with the other event report records. See the *IBM Tivoli NetView for z/OS Customization Guide* for more information.

Alerts

Alerts are events (including resolutions) that require attention. If the records pass the event filters, the hardware monitor checks the current state of its recording filters to see if this event qualifies for alert status. If it does, several things occur:

- An alert record about the event is written to the hardware monitor database.
- A line item is created for presentation to the hardware monitor users on the Alerts-Dynamic panel if their viewing filters are set to pass an alert of this type from this resource. These users' panels are automatically updated to reflect the occurrence of this special event. They can then take immediate action as called for by the nature of the event and any pertinent local procedures.
- An alert can also be forwarded to the NetView alert focal point. The following methods are used to forward alerts:
  - The primary method uses the ROUTE filter. This filter controls the selection of alert records that are routed.
  - The secondary method uses the OPER filter and NetView automation. With this method, the alert is converted to a message and sent to the focal point. The message is converted back to an alert at the focal point.

    Note: The message might not contain all the important data stored at the sending NetView program. Use the ROUTE filter for forwarding alerts to the focal point. See "Network Management for Multiple Domains" on page 163 for more information.

An alert is displayed on your Alerts-Dynamic panel as a one-line summary of the event that shows the error description and probable cause. The alert summary also shows the NetView domain where the alert originated. The hardware monitor also issues a message about the alert to an authorized operator, if filters are set up to provide this function. For a description of the different alert types, refer to *SNA Formats*.

Events are classified by type. Table 12 provides a list of event types and their corresponding abbreviations and codes.

Table 12. Event Types with Abbreviations and Codes

Abbr.	Event Type	Description	Code
AVAL	Availability	The availability status of the reported resource has changed.	09
BYPS	Alert bypass	A loss of availability was circumvented to allow the resource or an alternative resource to be used. The original problem still exists and you might not notice recovery. The recovery can be accomplished by intervention, either internal or external to the reporting product.	14
CUST	Customer application generated	A program that does not have an IBM order number generated the problem record.	05
DLRC	Delayed recovery	The sender is reporting a previously detected alertable condition that prevented reporting when detected, or the sender is reporting recovery from a condition that occurred earlier.	0F
ENV	Environment	A physical environmental problem has occurred.	0B
HELD	Held alert flag	An error condition was detected earlier, but the record was not sent at the time because no session is available to send it. In filtering, the hardware monitor treats the HELD flag as if it was a second alert or event type. This means a HELD flag is always associated with another event type. The HELD event type has the same filter priority as all other event types.	--
IMPD	Impending problem	Availability to the user is about to be lost.	11
IMR	Intensive Mode Recording	An error record resulted from the user calling intensive mode recording, a feature of the NCP. When IMR is called, an error record is generated each time the NCP goes through an error retry.	08
INST	Installation	A system definition or an incompatibility between components was reported.	0C
INTV	Intervention required	Intervention of a human operator is needed for corrective action.	04
NTFY	Notification of status change	Availability to the user is about to be lost. An important change of component, system, or network status requiring operator notification is required.	0A
PAFF	Permanently affected resource	The originator of this alert has determined that the target resource is lost because of a persistent error in a resource other than the target.	10

Table 12. Event Types with Abbreviations and Codes (continued)

Abbr.	Event Type	Description	Code
PERF	Performance	A recognized measurement of performance, such as response time, has exceeded a determined threshold.	03
PERM	Permanent error	Availability to the user is lost unless external intervention to the reporting product is provided.	01
PROC	Operation or procedure	A requested function cannot be performed because of an operational or procedural error.	0D
REDL	Redundancy lost	Redundant hardware or software is provided to ensure continued operation in the event of a failure or malfunction. As a result, failure of the remaining operational hardware or software results in a loss of corresponding services.	15
RSLV	Resolve major vector	The resolve major vector provides notification of the resolution of a previously reported problem. It contains an identification of the type of problem resolution and an identification of the failing resource.	--
RSNT	Resent alert flag	The alert was resent, providing additional information about the original problem. In filtering, the hardware monitor treats the resent flag as if it were a second alert or event type.	--
SCUR	Security	A report of an incident that can indicate a possible security violation was detected.	0E
SNA	SNA summary	A record containing SNA summary error counters. The record is typically the result of a NetView hardware monitor solicitation.	07
TEMP	Temporary or recoverable error	A momentary loss of availability is noticeable by the user, but is recovered from without intervention external to the reporting product.	02
USER	End user generated	A problem record initiated by a terminal operator.	06
UNKN	Unknown	The severity of the alert cannot be assessed.	12
Note: BYPS, IMPD, PAFF, PERF, PERM, REDL, and TEMP are supported as part of the generic alert architecture. In certain instances, the definitions of alert or event types used by non-generic alert records differ from the current architected generic definitions.			

You can use event types in filter-setting commands to control the types of data recorded in the hardware monitor's database or viewed by a NetView operator.

Secondary Recording of Event Records

In certain cases, the hardware monitor analyzes event data and determines that the resource causing the failure is not the resource that was specified in the event data. In this situation, the resource specified in the event data was affected by the failure but is not the cause. When this occurs, the hardware monitor records events for the actual failing resource and the resource reported in the event data. The default recording filters create alerts only for events against failing resources.

By recording two event records in this situation, you can display the information about this event condition using either the name of the actual failing resource, or the name of the resource affected by this event condition.

With LUC alert forwarding, hardware monitor secondary recording is prevented from occurring at the focal point. So, even if two alerts are logged at the entry point (one for the primary alert and one for the secondary alert), only one primary alert is logged at the focal point.

However, with SNA-MDS/LU 6.2 alert forwarding, secondary recording of SNA-MDS/LU 6.2 forwarded alerts can occur at the focal point. Thus, two alerts can be logged at the focal point for a single SNA-MDS/LU 6.2 (NetView or non-NetView) forwarded alert. Zero alerts can also be logged if the ESREC and AREC recording filters of the focal point are blocked. For NetView-forwarded alerts, this requires using the automation table SRF action, because the normal recording filter settings, using the SRFILTER command to specify filter settings from the hardware monitor, are not supported for this type of alert. For information on using the SRF action, refer to *IBM Tivoli NetView for z/OS Automation Guide*.

ALERT-NETOP, an architected alert focal point introduced in NetView V2R2, supports secondary recording of SNA-MDS/LU 6.2 non-NetView-forwarded alerts, and local (non-forwarded) alerts. As of V3, the NetView program also supports secondary recording of SNA-MDS/LU 6.2-forwarded alerts from entry point NetView hosts.

Monitoring the Network Using the Hardware Monitor Panels

You can use the hardware monitor panels to monitor your system and react to problem situations. To obtain help for any of the fields found in any hardware monitor panel, type `help`, then one or more field names within single quotation marks. For example, to obtain help for the field `RESNAME` in the Alerts-Static panel, type:

```
help 'resname'
```

A hardware monitor glossary panel is displayed which contains the definition for `RESNAME`.

You can also enter `help` from any hardware monitor panel to access the main help menu. For additional information on getting help, see NetView Online Help.

The following section gives typical scenarios that walk you through the major hardware monitor panels. Each option from the hardware monitor main menu is covered by one or more scenarios, with the exception of option 5, `SNA CONTROLLERS (CTRL)`. For additional information on using this option, see "Determining Controller Status (Hardware Monitor)" on page 293. For additional information on

how to use the hardware monitor panels to solve specific network problems, see Part 3, “Controlling the NetView Environment,” on page 191.

Investigating Non-Network Management Vector Transport Alerts

The following scenario shows how to investigate the cause of a non-network management vector transport (non-NMVT) alert.

1. Enter **npda** from the main menu panel. A panel similar to Figure 84 is displayed.

```
Tivoli NetView           SESSION DOMAIN: CNM01  OPER1   04/12/01 16:41:00
NPDA-01A                        * MENU *               HOST DOMAIN: CNM09



SEL#   PRODUCES:
( 1)    ALERTS-DYNAMIC DISPLAY
( 2)    TOTAL EVENTS DISPLAY
( 3)    TOTAL STATISTICAL DATA DISPLAY
( 4)    HELP MENU DISPLAY


       REQUEST DATA FROM NETWORK RESOURCES:
( 5)    SNA CONTROLLERS (CTRL)
( 6)    MODEMS AND ASSOCIATED LINKS (TEST)


                        DATA TYPES INITIALIZED/PURGED
AL.. (8/18/01)   EV.. (8/18/01)   ST.. (8/18/01)   GMFALERT.. (8/18/01)


ENTER SEL#

???
CMD==>
```

Figure 84. Hardware Monitor Main Menu

2. Select option **1** to monitor the alerts. A panel similar to Figure 85 on page 147 is displayed.

```
Tivoli NetView       SESSION DOMAIN: CNM01    OPER1     04/12/01 16:42:54
NPDA-30B                     * ALERTS-DYNAMIC *

    DOMAIN RESNAME  TYPE TIME  ALERT DESCRIPTION:PROBABLE CAUSE
     CNM01 D11CCL48 CTRL 16:32 TIMEOUT:DEVICE OFF/REMOTE MODEM OFF/COMM
     CNM01 LDEV0009 LDEV 16:31 INCORRECT LENGTH:HOST PROGRAM
     CNM01 LDEV0009 LDEV 14:52 INCORRECT LENGTH:HOST PROGRAM
     CNM01 GENACTRL CTRL 13:22 NO DATA RECEIVED:DEVICE OFF/MODEM OFF/COMM
     CNM01 GENACTRL CTRL 13:22 BAD FCS IN LPDA RESPONSE:LINE
     CNM01 LDEV0009 LDEV 13:18 INCORRECT LENGTH:HOST PROGRAM
     CNM01 LDEV0009 LDEV 13:18 INCORRECT LENGTH:HOST PROGRAM
     CNM01 LDEV0009 LDEV 13:17 INCORRECT LENGTH:HOST PROGRAM
     CNM01 LDEV0009 LDEV 13:14 INCORRECT LENGTH:HOST PROGRAM
     CNM01 LDEV0009 LDEV 13:13 INCORRECT LENGTH:HOST PROGRAM
     CNM01 LDEV0009 LDEV 00:05 INCORRECT LENGTH:HOST PROGRAM
     CNM01 LDEV0009 LDEV 00:03 INCORRECT LENGTH:HOST PROGRAM
     CNM01 LDEV0009 LDEV 00:00 INCORRECT LENGTH:HOST PROGRAM
     CNM01 LDEV0009 LDEV 23:59 INCORRECT LENGTH:HOST PROGRAM
     CNM01 LDEV0009 LDEV 23:07 INCORRECT LENGTH:HOST PROGRAM

 DEPRESS ENTER KEY TO VIEW ALERTS-STATIC

 ???
CMD==>
```

Figure 85. Alerts-Dynamic Panel

This is the Alerts-Dynamic panel, a single-page display designed to continuously show local alerts and alerts forwarded from entry points. As failures occur, each alert is displayed at the top of the display, and the alert at the bottom of the display is removed.

For each alert the following information can be displayed:

DOMAIN
The name of the domain from which the alert originated

RESNAME
The name of the device or other resource which is the one most affected by the event that originated the alert

TYPE An abbreviation of the resource type

TIME The time the alert was recorded on the database

ALERT DESCRIPTION:PROBABLE CAUSE
An abbreviated message describing the error that occurred and the probable cause

Note: Other formats are available for displaying alerts. You can code the ALT_ALERT statement in the member specified by the MEM keyword of the BNJDSERV TASK statement to select a specific format for the Alerts-Dynamic, Alerts-Static, and Alerts-History panels.

3. Press **Enter** to display the Alerts-Static panel. A panel similar to Figure 86 on page 148 is displayed.

```
Tivoli NetView      ESSION DOMAIN: CNM01    OPER1     04/12/01 16:42:59
NPDA-30B                     * ALERTS-STATIC *

SEL# DOMAIN RESNAME TYPE TIME  ALERT DESCRIPTION:PROBABLE CAUSE
( 1) CNM01 D11CCL48 CTRL 16:32 TIMEOUT:DEVICE OFF/REMOTE MODEM OFF/COMM
( 2) CNM01 LDEV0009 LDEV 16:31 INCORRECT LENGTH:HOST PROGRAM
( 3) CNM01 LDEV0009 LDEV 14:52 INCORRECT LENGTH:HOST PROGRAM
( 4) CNM01 GENACTRL CTRL 13:22 NO DATA RECEIVED:DEVICE OFF/MODEM OFF/COMM
( 5) CNM01 GENACTRL CTRL 13:22 BAD FCS IN LPDA RESPONSE:LINE
( 6) CNM01 LDEV0009 LDEV 13:18 INCORRECT LENGTH:HOST PROGRAM
( 7) CNM01 LDEV0009 LDEV 13:18 INCORRECT LENGTH:HOST PROGRAM
( 8) CNM01 LDEV0009 LDEV 13:17 INCORRECT LENGTH:HOST PROGRAM
( 9) CNM01 LDEV0009 LDEV 13:14 INCORRECT LENGTH:HOST PROGRAM
(10) CNM01 LDEV0009 LDEV 13:13 INCORRECT LENGTH:HOST PROGRAM
(11) CNM01 LDEV0009 LDEV 00:05 INCORRECT LENGTH:HOST PROGRAM
(12) CNM01 LDEV0009 LDEV 00:03 INCORRECT LENGTH:HOST PROGRAM
(13) CNM01 LDEV0009 LDEV 00:00 INCORRECT LENGTH:HOST PROGRAM
(14) CNM01 LDEV0009 LDEV 23:59 INCORRECT LENGTH:HOST PROGRAM
(15) CNM01 LDEV0009 LDEV 23:07 INCORRECT LENGTH:HOST PROGRAM
 DEPRESS ENTER KEY TO VIEW ALERTS-DYNAMIC OR ENTER A TO VIEW ALERTS-HISTORY
 ENTER SEL# (ACTION),OR SEL# PLUS M (MOST RECENT), P (PROBLEM), DEL (DELETE)

 ???
CMD==>
```

Figure 86. Alerts-Static Panel

The Alerts-Static panel freezes the current contents of the Alerts-Dynamic panel. It does not allow new alerts to be displayed on the panel, because a dynamic display can show alerts so quickly that it might be difficult to view. The alerts are listed in reverse chronological order.

The following options are listed at the bottom of the panel:

A Use this option to display all the alerts recorded in the database. You can then press the Enter key to page forward through the alerts.

SEL# This option is used to view the recommended actions for a specific alert.

SEL# M
Use this option to view the most recent events recorded for a specific resource (such as a controller). You can enter the number of one of the alerts generated by that resource followed by **m**. For example, to view the most recent events for CTRL D11CCL48, enter **1 m**.

SEL# P
Use this option to create a problem report for a specific alert. For example, to create a problem report for the first alert shown on the panel, enter **1 p**.

SEL# DEL
Use this option to delete a specific alert from the hardware monitor database. For example, to delete the first alert shown on the panel, enter **1 del**.

Not all of the available options are shown at the bottom of the panel. For a list of all the available options, enter **help** and then select **PROMPTS** from the help menu.

You can also scroll through panels using PF keys. The NetView supplied hardware monitor default PF key setting for FORWARD is PF8. To determine your current hardware monitor PF key settings, use the NetView DISPFK command.

You can also display current PF key settings for other components, such as command facility or status monitor. For a list of default settings for those components, see Figure 14 on page 37 and Figure 69 on page 118.

4. Enter the alert number in the command area to obtain the recommended actions for the alert. For the first alert, a panel similar to Figure 87 is displayed.

```
 Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/01 16:43:16
 NPDA-BNIFFD3F      * RECOMMENDED ACTION FOR SELECTED EVENT *       PAGE 1 OF 1
  CNM01       D11B54C    D11B54C    D11CCL48
             +--------+            +--------+
  DOMAIN     |  COMC  |----LINE----|  CTRL  |
             +--------+            +--------+
 USER    CAUSED - REMOTE DEVICE POWER OFF/NOT INITIALIZED OR COMMUNICATION
                  LINE SWITCH IN WRONG POSITION OR REMOTE MODEM POWER OFF
        ACTIONS - D001 - CORRECT THEN RETRY
 INSTALL CAUSED - REMOTE DEVICE ADDRESS OR SPEED SELECTION INCORRECT
                  LINE GEN PARAMETER INCORRECT (OSC, SPEED, NRZI, ADDRESS, ETC.)
                  COMMUNICATION LINE NOT INSTALLED
                  TWO REMOTE DEVICES WITH SAME ADDRESS
        ACTIONS - D006 - CORRECT GENERATION PROBLEM
 FAILURE CAUSED - REMOTE DEVICE OR LINE OR LOCAL/REMOTE MODEM
                  COMMUNICATION CONTROLLER HARDWARE
        ACTIONS - D003 - RUN LINE TESTS
                  D004 - RUN REMOTE DEVICE TESTS
                  D002 - RUN MODEM TESTS
                  D005 - CONTACT APPROPRIATE SERVICE REPRESENTATIVE
 ENTER ST TO VIEW MOST RECENT STATISTICS, OR D TO VIEW DETAIL DISPLAY

  ???
CMD==>
```

Figure 87. Recommended Action for Selected Event Panel

The Recommended Action panel lists the probable causes of a problem and displays a pictorial hierarchy of the problem. The pictorial hierarchy consists of a diagram showing the configurations through which the resources associated with the problem are attached. The probable causes are listed from three perspectives: user caused, install caused, and failure caused. This type of panel is available for any error the hardware monitor has listed, whether the error is a permanent or temporary problem.

The action numbers (D*nnn*, E*nnn*, I*nnn*, or R*nnn*) indicate actions that you can take to investigate the error. If you want to display an explanation of these recommended actions first, you can enter `action` followed by the action number. While D*nnn* actions have associated NetView-supplied panels, E*nnn*, I*nnn*, and R*nnn* actions do not have NetView-supplied panels. However, with the NetView program, you can overlay I-numbers and E-numbers with action numbers to create panels that are specific to the sending product. For additional information on creating your own action panels, refer to the *IBM Tivoli NetView for z/OS Customization Guide*.

5. Enter **d** to display event detail information for the alert. A panel similar to Figure 88 on page 150 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/01 16:43:22
NPDA-43B             * EVENT DETAIL FOR BSC/SS STATION *          PAGE 1 OF 1

 CNM01       D11B54C    D11B54C    D11CCL48
            +--------+            +--------+
 DOMAIN     |  COMC  |----LINE----|  CTRL  |
            +--------+            +--------+
DATE/TIME: 04/12 16:32
OPERATION - UNDEFINED


PROBABLE CAUSE - COMMUNICATIONS/REMOTE DEVICE FAILURE
ERROR DESCRIPTION - TIMEOUT - NOTHING RECEIVED




RECMS:     010381 83250400 00000001 80423000 000002BF 00028000 0016001F
002052D1 0007CCCC 00C10000 00040000 01D30016 019A0016 00000000 1E00FC00
00000000 00000000 00000000 00000000 00000000 00000000 00000000 F108C4F1
ENTER A TO VIEW ACTION DISPLAY

 ???
CMD==>
```

Figure 88. Event Detail Menu, First Panel

The Event Detail panel displays additional information about the event that generated the alert. Event detail data has several distinct formats. These formats are tailored to the type of resource for which the data is being displayed. In general, this panel can contain the following information collected at the time of the error:

- The resource ID
- The name of the application that was running
- The channel identifier
- The operation with which the resource was involved
- The channel status
- The unit status
- Sense data

6. Enter **a** to return to the Recommended Action panel.
7. If one of the recommended actions is to view the most recent statistics, you can enter **st** to display the Most Recent Statistical Data panel. This panel provides statistics about the most recent data transmissions sent over the line between the resources shown in the pictorial hierarchy. Starting with the most recent transmission, the panel shows for each transmission the amount of traffic that has traveled over the line, the number of temporary errors that have occurred, and the percentage of the total transmissions that contained temporary errors. The panel also displays a configuration diagram for the resources you specified and other related resources. The purpose of the display is to look for temporary errors which might be causing problems a lack of symptoms, which show a problem must be elsewhere. To see total statistical data for the hardware monitor, see "Displaying Total Statistical Data" on page 157.

Investigating Network Management Vector Transport (NMVT) Alerts

The following scenario shows how to investigate network management vector transport (NMVT) alerts. These alerts can also flow in MDS-MU, CP-MSU, or NMVT headers.

1. Enter **npda** from the main menu panel. A panel similar to Figure 89 is displayed.

```
 Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/01 16:43:00
 NPDA-01A                          * MENU *               HOST DOMAIN: CNM09



 SEL#   PRODUCES:
 ( 1)    ALERTS-DYNAMIC DISPLAY
 ( 2)    TOTAL EVENTS DISPLAY
 ( 3)    TOTAL STATISTICAL DATA DISPLAY
 ( 4)    HELP MENU DISPLAY


        REQUEST DATA FROM NETWORK RESOURCES:
 ( 5)    SNA CONTROLLERS (CTRL)
 ( 6)    MODEMS AND ASSOCIATED LINKS (TEST)


                        DATA TYPES INITIALIZED/PURGED
        AL..... (03/12/01)     EV..... (03/12/01)     ST..... (03/12/01)

 ENTER SEL#

 ???
CMD==>
```

Figure 89. Hardware Monitor Main Menu

2. Select option **1** to monitor the alerts. A panel similar to Figure 90 is displayed.

```
 Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/01 16:43:30
 NPDA-30B                      * ALERTS-DYNAMIC *

     DOMAIN RESNAME  TYPE TIME  ALERT DESCRIPTION:PROBABLE CAUSE
      CNM01 D11CCL48 CTRL 16:32 TIMEOUT:DEVICE OFF/REMOTE MODEM OFF/COMM
      CNM01 LDEV0009 LDEV 16:31 INCORRECT LENGTH:HOST PROGRAM
      CNM01 LDEV0009 LDEV 14:52 INCORRECT LENGTH:HOST PROGRAM
      CNM01 GENACTRL CTRL 13:22 NO DATA RECEIVED:DEVICE OFF/MODEM OFF/COMM     &
      CNM01 GENACTRL CTRL 13:22 BAD FCS IN LPDA RESPONSE:LINE                  &
      CNM01 LDEV0009 LDEV 13:18 INCORRECT LENGTH:HOST PROGRAM
      CNM01 LDEV0009 LDEV 13:18 INCORRECT LENGTH:HOST PROGRAM
      CNM01 LDEV0009 LDEV 13:17 INCORRECT LENGTH:HOST PROGRAM
      CNM01 LDEV0009 LDEV 13:14 INCORRECT LENGTH:HOST PROGRAM
      CNM01 LDEV0009 LDEV 13:13 INCORRECT LENGTH:HOST PROGRAM
      CNM01 LDEV0009 LDEV 00:05 INCORRECT LENGTH:HOST PROGRAM
      CNM01 LDEV0009 LDEV 00:03 INCORRECT LENGTH:HOST PROGRAM
      CNM01 LDEV0009 LDEV 00:00 INCORRECT LENGTH:HOST PROGRAM
      CNM01 LDEV0009 LDEV 23:59 INCORRECT LENGTH:HOST PROGRAM
      CNM01 LDEV0009 LDEV 23:07 INCORRECT LENGTH:HOST PROGRAM
  DEPRESS ENTER KEY TO VIEW ALERTS-DYNAMIC OR ENTER A TO VIEW ALERTS-HISTORY
  ENTER SEL# (ACTION),OR SEL# PLUS M (MOST RECENT), P (PROBLEM), DEL (DELETE)

 ???
CMD==> 5
```

Figure 90. Alerts-Dynamic Panel

For a complete description of this panel, see "Investigating Non-Network Management Vector Transport Alerts" on page 146.

3. Press **Enter** to display the Alerts-Static panel. A panel similar to Figure 91 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/01 16:42:54
NPDA-30B                     * ALERTS-STATIC *

SEL# DOMAIN RESNAME TYPE TIME  ALERT DESCRIPTION:PROBABLE CAUSE
( 1) CNM01 D11CCL48 CTRL 16:32 TIMEOUT:DEVICE OFF/REMOTE MODEM OFF/COMM
( 2) CNM01 LDEV0009 LDEV 16:31 INCORRECT LENGTH:HOST PROGRAM
( 3) CNM01 LDEV0009 LDEV 14:52 INCORRECT LENGTH:HOST PROGRAM
( 4) CNM01 GENACTRL CTRL 13:22 NO DATA RECEIVED:DEVICE OFF/MODEM OFF/COMM     &
( 5) CNM01 GENACTRL CTRL 13:22 BAD FCS IN LPDA RESPONSE:LINE                  &
( 6) CNM01 LDEV0009 LDEV 13:18 INCORRECT LENGTH:HOST PROGRAM
( 7) CNM01 LDEV0009 LDEV 13:18 INCORRECT LENGTH:HOST PROGRAM
( 8) CNM01 LDEV0009 LDEV 13:17 INCORRECT LENGTH:HOST PROGRAM
( 9) CNM01 LDEV0009 LDEV 13:14 INCORRECT LENGTH:HOST PROGRAM
(10) CNM01 LDEV0009 LDEV 13:13 INCORRECT LENGTH:HOST PROGRAM
(11) CNM01 LDEV0009 LDEV 00:05 INCORRECT LENGTH:HOST PROGRAM
(12) CNM01 LDEV0009 LDEV 00:03 INCORRECT LENGTH:HOST PROGRAM
(13) CNM01 LDEV0009 LDEV 00:00 INCORRECT LENGTH:HOST PROGRAM
(14) CNM01 LDEV0009 LDEV 23:59 INCORRECT LENGTH:HOST PROGRAM
(15) CNM01 LDEV0009 LDEV 23:07 INCORRECT LENGTH:HOST PROGRAM
 DEPRESS ENTER KEY TO VIEW ALERTS-DYNAMIC OR ENTER A TO VIEW ALERTS-HISTORY
 ENTER SEL# (ACTION),OR SEL# PLUS M (MOST RECENT), P (PROBLEM), DEL (DELETE)

 ???
CMD==>
```

Figure 91. Alerts-Static Panel

For a complete description of this panel, see "Investigating Non-Network Management Vector Transport Alerts" on page 146.

4. Enter the alert number in the command area to obtain the recommended actions for the alert. For example, if you enter 4, a panel similar to Figure 92 on page 153 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/01 16:43:43
NPDA-45A           * RECOMMENDED ACTION FOR SELECTED EVENT *     PAGE  1 OF  1
 CNM01       GENALERT   GENALINE   GENACTRL
            +---------+           +---------+
 DOMAIN     |  COMC   |----LINE----|  CTRL   |
            +---------+           +---------+

 USER    CAUSED - NONE

 INSTALL CAUSED - NONE

 FAILURE CAUSED - LSL 1 INBOUND LINE
                  LSL 1 REMOTE MODEM
        ACTIONS - D087 - REVIEW MOST RECENT TRAFFIC STATISTICS
                  D219 - RUN LINE ANALYSIS TEST
                  D227 - CHANGE TO BACKUP SPEED
                  D000 - IF PROBLEM PERSISTS THEN DO THE FOLLOWING
                  D228 - ACTIVATE SNBU, IF AVAILABLE
                  D005 - CONTACT APPROPRIATE SERVICE REPRESENTATIVE

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

 ???
CMD==>
```

Figure 92. Recommended Action for Selected Event Panel

5. Enter **d** to display event detail information for the alert. A panel similar to Figure 93.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/01 16:43:50
NPDA-43S                       * EVENT DETAIL *                 PAGE  1 OF  2

 CNM01       GENALERT     GENALINE               C1  GENACTRL
            +---------+--+         +-+ +-+        +-+ +---------+
 DOMAIN     |  COMC   |IM|===LINE==|M|-|X|--LINE--|X|-|  CTRL   |
            +---------+--+         +-+ +-+        +-+ +---------+

 DATE/TIME: RECORDED - 04/12 13:22

 EVENT TYPE: PERMANENT

 DESCRIPTION: BAD FCS IN LPDA RESPONSE

 PROBABLE CAUSES:
    LINE
    REMOTE MODEM



 ENTER A (ACTION) OR DM (DETAIL MENU)

 ???
CMD==>
```

Figure 93. Event Detail Panel

6. Enter the NetView FORWARD command, or a PF key set to that command, to display the second event detail panel. The NetView default PF key for FORWARD is PF8. A panel similar to Figure 94 on page 154 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/01 16:43:55
NPDA-43S                      * EVENT DETAIL *                 PAGE  2 OF  2

 CNM01       GENALERT     GENALINE                C1  GENACTRL
            +--------+--+         +-+ +-+        +-+ +--------+
 DOMAIN     |  COMC  |IM|===LINE==|M|-|X|--LINE--|X|-|  CTRL  |
            +--------+--+         +-+ +-+        +-+ +--------+

 QUALIFIERS:
    1)  1ST PROBABLE CAUSE IS ON LSL1
    2)  2ND PROBABLE CAUSE IS ON LSL1

 APPLICATION PROGRAM TEXT:
    RESPONSE WITH BAD FCS RECEIVED FROM REMOTE MODEM-LSL1




 UNIQUE ALERT IDENTIFIER: PRODUCT ID - 5685111    ALERT ID - 3C411B2B

 ENTER A (ACTION) OR DM (DETAIL MENU)

 ???
CMD==>
```

Figure 94. Event Detail, Continued

Note that, for an NMVT alert, an additional DM option exists. With this option, you can display more detail on the failure.

7. Enter **dm** to display the Event Detail Menu. A panel similar to Figure 95 is displayed.

```
Tivoli NetView        SESSION DOMAIN: CNM01    OPER1     04/12/01 16:43:59
NPDA-43R                    * EVENT DETAIL MENU *              PAGE 1 OF 1

 CNM01       GENALERT     GENALINE                C1  GENACTRL
            +--------+--+         +-+ +-+        +-+ +--------+
 DOMAIN     |  COMC  |IM|===LINE==|M|-|X|--LINE--|X|-|  CTRL  |
            +--------+--+         +-+ +-+        +-+ +--------+

 DATE/TIME: 04/12 13:22

 SEL#  PRODUCES:
 ( 1)   EVENT DETAIL DISPLAY
 ( 2)   PRODUCT SET IDENTIFICATION DISPLAY
 ( 3)   HEXADECIMAL DISPLAY OF DATA RECORD
 ( 4)   LINK CONFIGURATION DISPLAY
 ( 5)   MODEM AND LINE STATUS DISPLAY - LINK SEGMENT LEVEL 1




 ENTER SEL# OR A (ACTION)

 ???
CMD==>
```

Figure 95. Event Detail Menu, DM Option

This panel lists available detailed information about the problem. In this example, five options are provided. Depending on the problem, the panel can contain up to six options:

Event Detail Display
This option provides detailed information about the problem associated with the alert. You can also access this panel by using the `D` option from the Recommended Action panel (see step 5 on page 153).

Product Set Identification Display
This option provides information about the origin of the alert. It identifies the software or hardware components (such as NCPs) from which the alert was sent. This can help you isolate problems by directing you to the appropriate documentation.

Hexadecimal Display of Data Record
This option provides the complete alert data record or dump of the data record. This can be useful in isolating unrecognized vectors, for example, when you are running an older version of the NetView program. For additional description of all the major vectors, refer to *SNA Network Product Formats.*

Link Configuration Display
This option describes the attributes associated with the link or connection between two nodes.

Modem (or DSU/CSU) and Line Status Display - Link Segment Level 1
This option displays the result of associated link tests for the appropriate modems and CSUs. For additional information about running modem and link tests, see "Running Modem and Link Tests" on page 159.

Note: Option 6, if applicable, is similar to option 5, with the exception that it displays the results of associated link tests for level 2 instead of level 1.

8. Enter **a** to return to the Recommended Action for Selected Event panel.

Displaying Total Events

The `TOTAL EVENTS DISPLAY` option in the hardware monitor main menu gives summary totals of event data about specified resources.

The Total Events display for a particular resource level identifies the higher level resource to which the requested resource level is attached. The pictorial representation always includes an empty box. As you select lower and lower resource level displays, the pictorial representation shows the current level hardware connections.

When you select option 2, a panel similar to Figure 96 on page 156 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/01 14:07:38
NPDA-40A                      * TOTAL EVENTS *               PAGE   1 OF   6

 CNM01
           +--------+
 DOMAIN    |        |
           +--------+
     ************** RESOURCE EVENTS **************      ATTACHED RESOURCES EV
 SEL# TYPE RESNAME  TOTAL      FROM         TO             TOTAL      TO
 ( 1) COMC NTFFC       25  04/01 13:59  04/12 13:59          949  04/12 12:01
 ( 2) CP   NTADPU05     0  00/00 00:00  00/00 00:00            2  04/03 07:19
 ( 3) CP   NTA0PU       0  00/00 00:00  00/00 00:00            2  04/12 08:57
 ( 4) CP   NTA1I013     6  04/06 10:40  04/06 12:39           12  04/07 16:42
 ( 5) CP   NTA1PU       0  00/00 00:00  00/00 00:00            1  03/12 13:37
 ( 6) CP   NTA1PU02     0  00/00 00:00  00/00 00:00            1  03/12 13:37
 ( 7) CP   NTA1PU03     0  00/00 00:00  00/00 00:00            4  04/12 08:40
 ( 8) CP   NTA1PU06     0  00/00 00:00  00/00 00:00            3  04/06 01:30
 ( 9) CP   NTA2I001     0  00/00 00:00  00/00 00:00            1  04/08 14:51
 (10) CP   NTA7I001     0  00/00 00:00  00/00 00:00           42  04/12 10:44
 (11) CP   NTB4I001     0  00/00 00:00  00/00 00:00           70  04/12 09:14
 ENTER ST (STAT), OR SEL# (ATTACHED), OR SEL# PLUS M (MOST RECENT)

 ???
CMD==>
```

Figure 96. Total Events Panel

This panel shows the total counts for first-level resource types. It provides the highest-level view of all attached events recorded for the domain. From this panel, you can select the total display for the next lower resource level. For example, if you select event 1, a panel similar to Figure 97 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/01 14:08:27
NPDA-40A                      * TOTAL EVENTS *               PAGE   1 OF  10

 CNM01       NTFFC
           +--------+   +--------+
 DOMAIN    |  COMC  |-- |        |
           +--------+   +--------+
     ************** RESOURCE EVENTS **************      ATTACHED RESOURCES EV
 SEL# TYPE RESNAME  TOTAL      FROM         TO             TOTAL      TO
 ( 1) CHAN NTCH06       0  00/00 00:00  00/00 00:00            5  04/12 07:43
 ( 2) CHAN NTCH07       0  00/00 00:00  00/00 00:00            9  04/06 02:17
 ( 3) CHAN NTCH08       0  00/00 00:00  00/00 00:00            3  04/06 10:33
 ( 4) LAN  NTFFTRLN     7  03/12 12:46  04/07 10:38            0  00/00 00:00
 ( 5) LINE J007V0D3     0  00/00 00:00  00/00 00:00            1  04/06 13:26
 ( 6) LINE J007V0ED     0  00/00 00:00  00/00 00:00            1  04/08 19:53
 ( 7) LINE J007V001     0  00/00 00:00  00/00 00:00            1  04/06 13:26
 ( 8) LINE J007V003     0  00/00 00:00  00/00 00:00            1  04/06 13:26
 ( 9) LINE J007V03F     0  00/00 00:00  00/00 00:00            1  04/06 13:26
 (10) LINE J007V05B     0  00/00 00:00  00/00 00:00            1  04/06 13:26
 (11) LINE J007V089     0  00/00 00:00  00/00 00:00            1  04/06 12:47
 ENTER ST (STAT), OR SEL# (ATTACHED), OR SEL# PLUS M (MOST RECENT)

 ???
CMD==>
```

Figure 97. Total Events Panel, Next Level

As you can see, this panel displays the event totals for the communication controller NTFFC. To continue to display event totals for lower resource levels,

select a resource from this panel. During event tracking you can choose total event displays for the next lower resource until you reach the resource level suspected of causing the problem.

Displaying Total Statistical Data

Statistical data is generated by resources and stored in the hardware monitor database. For certain resources, the hardware monitor analyzes each statistical record to determine whether to create a performance event record which can become an alert. This analysis consists of a comparison of current error-to-traffic (E/T) ratios to pre-established E/T thresholds for those resources that can provide the error and traffic statistics. For information on how to set the E/T threshold values using the NetView SRATIO command, refer to the NetView online help.

When you select option 3 from the hardware monitor main menu, a panel similar to Figure 98 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/01 14:09:09
NPDA-50A                 * TOTAL STATISTICAL DATA  *           PAGE   1 OF   1

 CNM01
            +--------+
 DOMAIN     |        |
            +--------+
                   ********************* TOTALS ********************  DAILY
SEL# TYPE RESNAME     TRAFFIC      TEMPS  E/T     FROM         TO       E/T
( 1) COMC NTFFC           N/A        N/A  N/A   N/A   N/A 04/12 13:52   N/A
( 2) CPU  CPU72068        N/A        N/A  N/A   N/A   N/A   N/A   N/A   N/A









 ENTER EV (EVENT), OR SEL# (ATTACHED)

 ???
CMD==>
```

Figure 98. Total Statistical Data Panel

This panel displays the statistical record totals for first-level resources. To navigate these panels in the same manner as the total events panels and display record totals for lower resource levels, select the appropriate resource. For example, if you select resource 1, a panel similar to Figure 99 on page 158 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/01 14:09:50
NPDA-50A                 * TOTAL STATISTICAL DATA  *           PAGE   1 OF  11

 CNM01       NTFFC
            +--------+   +--------+
 DOMAIN     |  COMC  |-- |        |
            +--------+   +--------+
                    ********************* TOTALS *********************  DAILY
 SEL# TYPE RESNAME     TRAFFIC      TEMPS  E/T     FROM         TO       E/T MR
 ( 1) CHAN NTCH05          N/A          0  N/A 00/00 00:00 00/00 00:00   N/A
 ( 2) CHAN NTCH06          N/A          0  N/A 00/00 00:00 00/00 00:00   N/A
 ( 3) CHAN NTCH07          N/A          0  N/A 00/00 00:00 00/00 00:00   N/A
 ( 4) CHAN NTCH08          N/A          0  N/A 00/00 00:00 00/00 00:00   N/A
 ( 5) LAN  NTFFTRLN          0          0  N/A 03/12 12:32 03/12 13:07   N/A Y
 ( 6) LINE J007V0D3         24          0  N/A   N/A   N/A 04/06 13:26   N/A
 ( 7) LINE J007V0ED      28816          0  N/A   N/A   N/A 04/08 19:53   N/A
 ( 8) LINE J007V001         20          0  N/A   N/A   N/A 04/06 13:26   N/A
 ( 9) LINE J007V003         37          0  N/A   N/A   N/A 04/06 13:26   N/A
 (10) LINE J007V03F         24          0  N/A   N/A   N/A 04/06 13:26   N/A
 (11) LINE J007V05B         20          0  N/A   N/A   N/A 04/06 13:26   N/A
 ENTER EV (EVENT), OR SEL# (ATTACHED), OR SEL# PLUS M (MOST RECENT)

 ???
CMD==>
```

Figure 99. Total Statistical Data Panel, Level 2

This panel displays statistical record counts for the resources attached to the communication controller NTFFC.

To display statistical record counts for the resource attached to line J007V0ED, enter **7**. A panel similar to Figure 100 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/01 14:10:20
NPDA-50A                 * TOTAL STATISTICAL DATA  *           PAGE   1 OF   1

 CNM01       NTFFC      J007V0ED
            +--------+            +--------+
 DOMAIN     |  COMC  |----LINE--- |        |
            +--------+            +--------+
                    ********************* TOTALS *********************  DAILY
 SEL# TYPE RESNAME     TRAFFIC      TEMPS  E/T     FROM         TO       E/T MR
 ( 1) CTRL NTC9PU        28816          0  0.0 04/08 19:53 04/08 19:53   0.0 Y









 ENTER EV (EVENT), OR SEL# (ATTACHED), OR SEL# PLUS M (MOST RECENT)

 ???
CMD==>
```

Figure 100. Total Statistical Data Panel, Level 3

Running Modem and Link Tests

Link Problem Determination Aid (LPDA®) is a series of testing programs that reside in the modems attached to communication controllers and cluster controllers. LPDA is used by the NCP to determine the status of modems and attached devices and to test the transmission quality of communication links.

Two sets of LPDA programs exist. LPDA-1 software is used to test IBM 386X modems, including IBM 3863, 3864, and 3868 modems. LPDA-1 can also be used to test IBM586X modems. LPDA-2 is used to test only IBM 586X modems, including IBM 5865, 5866, and 5868 modems.

The LPDA-1 and LPDA-2 programs run independently of the NetView program product. However, you can use the NetView hardware monitor to request that the following LPDA-1 or LPDA-2 tests be run on the modems in your network.

LPDA-1	**LPDA-2**
Remote data terminal equipment interface test (DTE)	Line analysis test (LA)
Link status test (LS)	Modem and line status test (MLS)
Remote modem self-test (RST)	Transmit receive test (TRT)

Complete the following steps to perform modem and link tests:

1. Select option **6** from the hardware monitor main menu. A panel similar to Figure 101 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/01 14:52:00
NPDA-02D               * TEST INFORMATION DISPLAY *               PAGE 1 OF 1
DOMAIN: CNM01

  THE HARDWARE MONITOR SUPPORTS TWO SETS OF TEST COMMANDS (LPDA-1 AND LPDA-2).
  IF YOU ENTER TWO RESOURCE NAMES, THE HARDWARE MONITOR WILL DETERMINE THE
  PROPER COMMAND SET.

  THE RESOURCE NAMES ARE DEFINED BELOW AS THE VARIABLES RESNAME1 AND
  RESNAME2.  ACTUAL RESOURCE NAMES MAY BE FOUND ON THE LINE ABOVE THE NETWORK
  FIGURE ON DISPLAYS SUCH AS RECOMMENDED ACTIONS AND MOST RECENT EVENTS.

  RESNAME1 = THE NETWORK NAME OF A COMMUNICATION OR NETWORK CONTROLLER
             (COMC OR CTRL, RESPECTIVELY) AT THE CONTROL END OF THE LINK.
  RESNAME2 = THE NETWORK NAME OF THE CONTROLLER (CTRL) AT THE REMOTE END
             OF THE LINK.

NOTE:  NON-HARDWARE MONITOR COMMANDS (EXCEPT 'NCCF') ARE TAKEN AS RESOURCE
       NAMES.

ENTER RESNAME1 RESNAME2

???
CMD==>
```

Figure 101. Test Information Display Panel

   This panels prompts you for the IDs of the devices that you want to test.

2. On the command line, enter the IDs for the devices that you want to test. The NetView program determines which set of test commands (LPDA-1 or LPDA-2) is appropriate for testing the line between the two devices and brings up the appropriate panels. For example, if you enter **ntffc ntffpu37** and the NetView

program determines that the line between the two specified resources supports LPDA-2, a panel similar to Figure 102 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/01 14:55:45
NPDA-LPDA2               * LPDA-2 COMMAND MENU *                  PAGE 1 OF 1

DOMAIN: CNM01      RESNAME1: NTFFC      RESNAME2: NTFFPU37   LINK SEG LVL: 1

 SEL#      TEST                           DESCRIPTION

 (1)    MLS-MODEM AND   RETRIEVES A COMPREHENSIVE SET OF DCE (MODEM, DSU/CSU,
            LINE        OR CNMA) AND LINE DATA AND PRESENTS THE RESULTS ON
            STATUS      DISPLAY NPDA-22B/C.

 (2 XX) TRT-TRANSMIT    CAUSES A DCE (MODEM, DSU/CSU, OR CNMA) PAIR TO EXCHANGE
            RECEIVE     ONE OR MORE SEQUENCES OF PREDEFINED BIT PATTERNS OVER
            TEST        THE LINE AND REPORT THE RESULTS ON DISPLAY NPDA-25B. XX
                        IS A NUMBER FROM 1 TO 10 INDICATING THE NUMBER OF TEST
                        SEQUENCES. THE DEFAULT IS 1 IF XX IS NOT SPECIFIED

 (3)    LA-LINE         RETRIEVES LINE PARAMETERS SUCH AS SIGNAL TO NOISE
           ANALYSIS     RATIO AND PRESENTS RESULTS ON DISPLAY NPDA-24B
                        (FOR ANALOG LINES ONLY).
ENTER SEL#

 ???
CMD==>
```

Figure 102. LPDA-2 Command Menu Panel

3. Select option **1** to review the modem and line status information. A panel similar to Figure 103 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/01 15:07:12
NPDA-22B                  * MODEM AND LINE STATUS *               PAGE 1 OF 3
             * MODEM AND LINE PARAMETERS-LINK SEGMENT LEVEL 1 *
 CNM01       NTFFC        NTFFLN37 C1  NTFFPU37
            +--------+ +-+        +-+ +--------+
 DOMAIN     |  COMC  | |M|--LINE--|M| |  CTRL  |
            +--------+ +-+        +-+ +--------+
 DESCRIPTION,PROBABLE CAUSE: NO CRITICAL ERROR:NO PROBABLE CAUSE IDENTIFIED

                             LOCAL MODEM        REMOTE MODEM        EXPECTED
 RECEIVE LEVEL, LEAST:      -14 DBM, -14 DBM  -17 DBM, -17 DBM    -16 +/- 7 DBM
 REC LVL THRESH EXCEEDED:   NO                NO                   NO
 RLSD LOSSES, AGE:          0                 0                    0
 LINE QUALITY, WORST:       GOOD/0, GOOD/0    BAD/10, BAD/12       GOOD/0-4
 IMPULSE HITS, AGE:         0                 0                    0-15/15 MIN
 POWER-OFF TONE, AGE:       NO                NO                   NO
 REINITIALIZATION, AGE:     NO                NO                   NO
 FAILURE TONE, AGE:         NO                NO                   NO
 BASE MODEM IN ERROR:       NO                NO                   NO
 FEATURE(S) IN ERROR:       NONE              NONE                 NONE
 SEE NEXT PAGE FOR REMOTE DTE INTERFACE SUMMARY

 ???
CMD==>
```

Figure 103. Modem and Line Status, Panel 1

The information on this panel gives you detailed modem information and line status for the:

- Local modem

- Remote modem
- Expected modem and line status

You can press the Enter key, use the NetView FORWARD command, or press a PF key set to that command, to page through the modem and line status panels. The NetView default PF key for FORWARD is PF8. The second modem and line status panel is similar to Figure 104.
The third modem and line status panel is similar to Figure 105.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/01 15:08:10
NPDA-22B                  * MODEM AND LINE STATUS *               PAGE 2 OF 3
     * REMOTE MODEM INTERFACE-REMOTE DEVICE STATUS-LINK SEGMENT LEVEL 1 *
 CNM01       NTFFC        NTFFLN37 C1  NTFFPU37
            +--------+ +-+        +-+ +--------+
 DOMAIN     |  COMC  | |M|--LINE--|M| |  CTRL  |
            +--------+ +-+        +-+ +--------+
                              STATUS AT COMMAND        ACTIVITY DURING TWO
                              EXECUTION TIME           MINUTES BEFORE COMMAND
  REQUEST TO SEND:                 OFF                        YES
  CLEAR TO SEND:                   OFF                        YES
  TRANSMIT DATA:                   OFF                        YES
  RECEIVE DATA:                    OFF                        YES
  RECEIVE LINE SIGNAL DETECT:      N/A                        NO
  DATA SIGNALLING RATE SELECTOR:   ON                         NO
  DATA TERMINAL READY:             ON                         NO
  DTE POWER LOSS DETECTED:         OFF                        NO
  TEST CONTROL:                    N/A                        NO
                             REMOTE DEVICE
                       STREAMING DETECTED: NO DATA
 SEE NEXT PAGE FOR LINK AND MODEM CONFIGURATIONS

 ???
CMD==>
```

Figure 104. Modem and Line Status, Panel 2

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/01 15:09:30
NPDA-22B                  * MODEM AND LINE STATUS *               PAGE 3 OF 3
               * CONFIGURATION SUMMARY-LINK SEGMENT LEVEL 1 *
 CNM01       NTFFC        NTFFLN37 C1  NTFFPU37
            +--------+ +-+        +-+ +--------+
 DOMAIN     |  COMC  | |M|--LINE--|M| |  CTRL  |
            +--------+ +-+        +-+ +--------+
    LINK CONFIGURATION: LEASED, POINT-TO-POINT

                                    LOCAL MODEM            REMOTE MODEM
    TYPE-MODEL, TEST MODE:       5866-02(C), SOLICITED   5866-02(C), SOLICITED
    CMD RETRIED, OPERATING MODE: NO,  X6                 NO,  X6
    SPEED, RLSD STATE:           9.6 KBPS(FULL), ON      9.6 KBPS(FULL), N/A
    NETWORK FUNCTION:            PRIMARY                 PRIMARY
    CUSTOMER CONFIG DATA LOST:   NO                      NO
    LPDA MICROCODE LEVEL:        2                       2
    SNBU, TYPE OF CONNECTION:    NO                      NO
    MODEM ADDRESS:               N/A                     01
    DTE INTERFACE CONNECTION:    DTE                     DTE
    FEATURE(S) INSTALLED:        NONE                    NONE
    CONFIGURATION MISMATCH:      N/AV                    N/AV

 ???
CMD==>
```

Figure 105. Modem and Line Status, Panel 3

4. Use the NetView RETURN command, or press a PF key set to that command, to return to the LPDA-2 or LPDA-1 Command Menu panel. The NetView default PF key for RETURN is PF3.
5. To request that the NetView program run a series of tests on the transmit and receive paths for the line between the local and remote modems, enter **2** followed by the number of tests (1–10) to run. For example, to run 10 tests, enter **2 10** at the command line. A panel similar to Figure 106 is displayed:

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/01 15:03:35
NPDA-25B1       * TRANSMIT RECEIVE TEST-LINK SEGMENT LEVEL 1 *     PAGE 1 OF 1

 CNM01       NTFFC        NTFFLN37 C1  NTFFPU37
            +--------+ +-+        +-+ +--------+
 DOMAIN     |  COMC  | |M|--LINE--|M| |  CTRL  |
            +--------+ +-+        +-+ +--------+

                                       LOCAL MODEM        REMOTE MODEM

   TYPE-MODEL:                         5866-02            5866-02
   MODEM ADDRESS:                      01                 01
   CURRENT TRANSMIT SPEED:             9.6 KBPS           9.6 KBPS
   SPEED IN USE:                       FULL               FULL
   RLSD LOST:                          NO                 NO
   LINE QUALITY:                       GOOD/0             BAD/12
   IMPULSE HITS DURING TEST:           0                  0
   NUMBER OF BLOCKS:
    RECEIVED                           160                160
    RECEIVED WITH ONE OR MORE ERRORS   0                  57


 ???
CMD==>
```

Figure 106. Transmit-Receive Test Panel

This panel displays the results of a transmit-receive test. When you request this test, a command is sent to the local and remote modems directing them to exchange one or more sequences of predefined bit patterns over the line and report the results. The results include information about the line quality and the number of data blocks received in error.

6. Enter RETURN or press the PF3 (using NetView PF key defaults) to return to the LPDA-2 or LPDA-1 Command Menu screen.
7. Select option 3 to conduct a line analysis test. The line analysis test compares the quality of the data transmissions being sent across a line. A panel similar to Figure 107 on page 163 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/01 15:06:56
NPDA-24B           * LINE ANALYSIS-LINK SEGMENT LEVEL 1 *         PAGE 1 OF 1

 CNM01       NTFFC        NTFFLN37 C1  NTFFPU37
            +--------+ +-+        +-+ +--------+
 DOMAIN     |  COMC  | |M|--LINE--|M| |  CTRL  |
            +--------+ +-+        +-+ +--------+
 ROUND TRIP DELAY: 0 MSEC
                            LOCAL             REMOTE             ACCEPTABLE
                            MODEM             MODEM              LIMITS
 TYPE-MODEL, MODEM ADDRESS: 5866-02           5866-02
 FREQUENCY SHIFT:            0 HZ             -3 HZ              MAX  6 HZ
 2ND HARMONIC DISTORTION:   40 DB             39 DB              MIN 27 DB
 3RD HARMONIC DISTORTION:   40 DB             37 DB              MIN 32 DB
 SIGNAL TO NOISE RATIO:     40 DB             18 DB              MIN 22 DB
 PHASE JITTER:               0 DEG PP          9 DEG PP          MAX 15 DEG PP
 RECEIVE LEVEL, LEAST:     -14, -14 DBM      -18, -18 DBM        MIN-32 DBM
 IMPULSE HITS:               0                 0                 15 IN 15 MIN
 RLSD LOSSES:                0                 0
 TRANSMIT LEVEL:             0 DBM             0 DBM
 SPEED:                     9.6 KBPS(FULL)    9.6 KBPS(FULL), 01

 ???
CMD==>
```

Figure 107. Line Analysis Panel

This panel shows the type and model for the local and remote modems. The panel also presents the acceptable limits for message transmission quality. You can compare the test values for the two modems to the acceptable limits to find the source of transmission problems.

Topic:	Reference:
Using the ALT_ALERT statement to customize hardware monitor panels	*IBM Tivoli NetView for z/OS Administration Reference*, "Using Hardware Monitor Filters" on page 208

Network Management for Multiple Domains

Using the hardware monitor, an operator at a single central host domain can monitor the alert activity for one or more entry point host domains. This ability simplifies the task of network management for multiple domains.

The central host domain is known as the *focal point domain*, or the *focal point*, and the entry point host domains are called *distributed hosts*. The sphere of control for a focal point is the set of distributed hosts that forwards alerts to a particular focal point. A distributed host can forward alerts to only one focal point. Thus, a host can reside within the sphere of control of only one focal point. Note in Figure 108 on page 164 that distributed hosts CNM03 through CNM15 reside in the sphere of control of focal point CNM01, while distributed hosts CNM17 and CNM22 reside in the sphere–of–control of focal point CNM02. Planning decisions determine the number of focal points and the number of distributed hosts that reside in the sphere-of-control for each focal point.

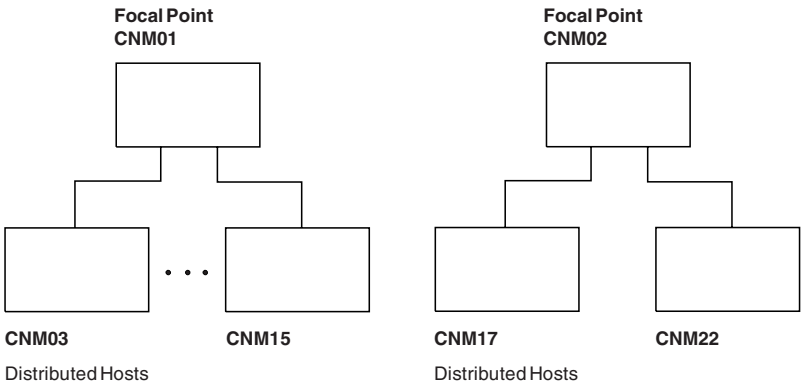


Figure 108. Distributed Hosts

Alert Forwarding

Any operators logged on to the focal point can view these forwarded and local alerts on the Alerts-Dynamic, Alerts-Static panel, or Alerts-History panels. See Figure 109 for an example of an Alerts-Static panel.

```
Tivoli NetView     SESSION DOMAIN: CNM01    OPER1     04/12/01 10:20:00
NPDA-30B                  * ALERTS-STATIC *

SEL# DOMAIN RESNAME  TYPE TIME  ALERT DESCRIPTION:PROBABLE CAUSE
 (1) CNM01 RAL01     COMC 09:16 MOSS OFFLINE:MAINTENANCE MODE
 (2) CNM04@L24350    LINE 09:13 MODEM ERROR:LOCAL MODEM
 (3) CNM01 RVS22     COMC 08:59 HARDWARE ERROR:CHANNEL ADAPTOR
 (4) CNM15 L25025    LINE 08:31 CONFIGURATION ERROR:LOCAL MODEM-LSL1
 (5) CNM15 RRV32     CTRL 08:27 SNA DATA STREAM ERROR:HOST PROGRAM
 (6) CNM01@RAL02     COMC 08:23 HARDWARE ERROR:LINE ADAPTOR
 (7) CNM04 RVR850    CTRL 08:16 DELAYED ALERT:HOST LINK COMMUNICATIONS
 (8) CNM15 LRV02     LDEV 08:12 BIPHASE CODE VIOLATIONS:COMMUNICATIONS









DEPRESS ENTER KEY TO VIEW ALERTS-DYNAMIC OR ENTER A TO VIEW ALERTS-HISTORY
ENTER SEL# (ACTION),OR SEL# PLUS M (MOST RECENT), P (PROBLEM), DEL (DELETE)
CMD==> 1
```

Figure 109. Alerts-Static Panel for LU 6.2

The *session* domain of CNM01 is presented on the first line of the Alerts-Static panel. The session domain is the domain with which the operator is currently in session. More specifically, it is the domain associated with the hardware monitor database being accessed. The domain names shown under the DOMAIN column heading are owning domains. The owning domain is the domain that originally received the alert. For example, the alert corresponding to selection 2 originated in distributed host (and owning) domain CNM04 and was forwarded to the focal point (and session) domain CNM01.

The session domain is always on the first line of all hardware monitor panels. The owning domain is presented on all hardware monitor panels that have a pictorial

hierarchy, and on the Alerts-Dynamic/Static/History panels. For those panels with a pictorial hierarchy, the owning domain is the value above the constant DOMAIN, the leftmost entry of the pictorial hierarchy. The session and owning domains match, except when the session domain is also a focal point. Only focal points have alerts forwarded to them from other domains, such as distributed NetView programs or entry points.

Using the DOMAIN operand of the SVFILTER command, the focal point operator can prevent alerts from specified entry point host domains from displaying on the Alerts-Dynamic, Alerts-Static, and Alerts-History panels.

With the ROUTE option of the SRFILTER command, the distributed host operator can control which alerts are forwarded to the alert focal point. For more information about these commands and operands, refer to the NetView online help.

NetView supports two alert forwarding methods:
- SNA-MDS/LU 6.2
- NV-UNIQ/LUC

Alerts forwarded over SNA-MDS (using LU 6.2) have an @indicator following the owning domain name, as shown by the alerts corresponding to selections 2 and 6 in Figure 109 on page 164. When the owning domain and the session domain for an SNA-MDS forwarded alert are the same, as they are in the alert for selection 6, this indicates that the alert was forwarded from a non-NetView entry point such as an AS/400®. When the owning domain is not the same as the session domain, as in the section 2 alert, this indicates that the alert was forwarded over SNA-MDS from a NetView entry point. You can display the entry point name for SNA-MDS forwarded alerts by entering the selection number followed by "Q". For example, entering `2 q` causes the following message to be displayed in the message line:

```
BNH092I ALERT WAS FORWARDED FROM NODE NETA.CNM04 VIA SNA-MDS.
```

The selection 4 alert was forwarded over LUC. You can determine this because the owning domain and session domain are different and no `@` indicator exists.

The selection 1 alert is a local alert as indicated by the absence of an `@` indicator and the fact that the owning domain is the same as the session domain.

Topic:	**Reference:**
Alert forwarding	*IBM Tivoli NetView for z/OS Automation Guide*

Distributed Database Retrieval

From the Alerts-Static or Alerts-History panels, the focal point operator can enter a selection number to display Recommended Action data or a selection number followed by M to display Most Recent Events data. If the operator requests data for an alert forwarded from an entry point NetView (if the owning domain does not match the session domain), the hardware monitor sends the request for data to the owning domain (distributed host) rather than the session domain (focal point). This allows data to be retrieved from a domain other than the session domain without having to change session domains by using the SDOMAIN command. Automatic retrieval of data from a domain other than the session domain is known as *distributed database retrieval*. Distributed database retrieval is possible only when the session domain is a focal point.

Distributed database retrieval begins when an operator makes a selection for data for an alert forwarded from an entry point NetView from the Alerts-Static or Alerts-History panels, and continues as long as the prompts at the bottom of each panel are taken to traverse displays (unless you select a prompt which processes an explicit command, such as ST or EV). Distributed database retrieval ends whenever an explicit command is issued, such as when an explicit MENU command is entered, or when the RETURN command is repeatedly entered until the Alerts-Static panel or Alerts-History panel is redisplayed. Distributed database retrieval has occurred when the owning domain in the pictorial hierarchy does not match the session domain on the first line.

Notes: Additional information about distributed database retrieval follows:

- When logging to Information/Management (MVS only) is requested with selection P, the logging is done at the domain of the NetView program where the operator is logged on. This domain is referred to as the *host* domain, and it can differ from the session and owning domains.
- Whenever the set recording filter (SRFILTER) command is requested with the SRF selection, the command is processed at the owning (distributed host) domain, not the focal point. A focal point operator who wishes to clear the filters that were set at the owning domain must set up a cross-domain session with the distributed host using the SDOMAIN command, and then issue the CLEAR command.
- Whenever the selection DEL command is entered from the Alerts-Static or Alerts-History panel, the alert is deleted from the session (focal point) domain database, not the owning (distributed host) domain database.
- Refer to the NPDA SDOMAIN command description in the NetView online help for restrictions that apply when distributed database retrieval is called in a cross-domain session.
- If an operator at the focal point attempts to retrieve hardware monitor data from an entry point using distributed database retrieval, and one or more intermediate nodes separate the focal point and entry point, the focal point might not be able to establish a cross-domain session (using LU 6.2 or LUC) with the entry point. If this happens, the focal point operator cannot retrieve the requested data using distributed database retrieval. An operator can use the NPDA SDOMAIN command to try to establish a session to retrieve the data.
- When an operator enters "**SEL# M**" from the Alerts Static panel for an alert forwarded from a remote entry point NetView, the transport used to forward the alert is the same transport that is used to retrieve the requested event data from the entry points database.

  For example, if an alert is forwarded using LU 6.2, the LU 6.2 transport is used to retrieve the event data from the entry point database. As another example, if an alert is forwarded using LUC, the LUC transport is used.

  To summarize, the transport used to forward the alert from the entry point to the focal point is the same transport that is used to retrieve the data.
- Distributed database retrieval is performed even though the data might be present in the focal point database.

  When SNA-MDS/LU 6.2 forwarded alerts are received from an entry point NetView, the default is to log these only as alerts (not as event or statistical data) in the database. However, using the automation table SRF action, you can override this default and cause event and statistical data

to be logged. But this data is logged against the local focal point domain name, not against the sending NetView entry point domain name. Therefore, if an operator enters SEL# M from the Alerts Static panel the event data might already be present on the focal point database. However, distributed database retrieval is still performed (just as it is with LUC forwarded alerts), and the event data is retrieved from the entry point database rather than the focal point database.

Topic:	Reference:
Using filters	"Using Hardware Monitor Filters" on page 208
Implementing filtering decisions using the XITCI exit	*IBM Tivoli NetView for z/OS Automation Guide*

Event/Automation Service

The Event/Automation Service (E/AS) integrates the management of events from the Tivoli Management Region platform and SNMP managers with events from the IBM Tivoli NetView for z/OS platform. By acting as a gateway between these platforms, the E/AS enables centralized network management from any platform.

The E/AS is composed of 5 services. The Alert Adapter service converts IBM Tivoli NetView for z/OS alerts into Tivoli Enterprise Console events, and then forwards the events on to a Tivoli Enterprise Console. The Message Adapter service converts IBM Tivoli NetView for z/OS messages that originate from the automation table into console events, and then forwards the events on to a Tivoli Enterprise Console. The Event Receiver service converts events into IBM Tivoli NetView for z/OS alerts and forwards the alerts to the alert receiver PPI mailbox. The Alert to Trap service converts IBM Tivoli NetView for z/OS alerts into SNMP traps, and then forwards the events on to an SNMP manager using an SNMP agent. The Trap to Alert service converts SNMP traps into IBM Tivoli NetView for z/OS alerts and forwards the alerts to the alert receiver PPI mailbox.

The alert adapter service converts alert data into a console event through a conversion rules file that can be customized. The E/AS is shipped with a default conversion rules file; see the IHSAACDS file for a look at these conversion rules. The conversion rules file is more commonly referred to as the Class Definition Statement (CDS) file.

The message adapter service converts message data into event data through a conversion rules file that can be customized. This customization enables you to specify how various pieces of information from the message are encoded into the slot/value pairs that compose an event. The E/AS is shipped with a default conversion rules file; see the IHSAMFMT file for a look at these conversion rules. The conversion rules file is more commonly referred to as the Message Format (FMT) file.

The event receiver service converts Tivoli Enterprise Console events into NetView alerts using a conversion rules file that can be customized. The E/AS is shipped with a default conversion rules file; see the IHSAECDS file for a look at these conversion rules. The conversion rules file is more commonly referred to as the class definition statement (CDS) file. The conversion rules file is a CDS file.

The alert to trap service converts alert data into an SNMP trap through a conversion rules file that can be customized. The E/AS is shipped with a default conversion rules file; see the IHSATCDS file for a look at these conversion rules. The conversion rules file is a CDS file.

The trap to alert service converts SNMP traps into NetView alerts using a conversion rules file that can be customized. The E/AS is shipped with a default conversion rules file; see the IHSALCDS file for a look at these conversion rules. The conversion rules file is a CDS file.

Topic:	**Reference:**
IBM Tivoli NetView for z/OS adapters	*Tivoli Enterprise Console User's Guide*

Common Event Infrastructure Service

You can use representations of system events to monitor status changes and problem reports by using Common Base Events. These Common Base Events are generated by NetView from messages and Message Service Units (MSUs) and are passed to the Common Event Infrastructure, an IBM component technology, to store and distributed as you specify.

You can create Common Base Events either by automating a message or a Management Services Unit or by setting hardware monitor filters which capture messages and alerts.

Topic:	**Reference:**
Common Base Event overview	Autonomic Computing Toolkit Developer's Guide, SC30-4083
Common Base Event format	*IBM Tivoli NetView for z/OS Customization Guide*
Automation involving Common Base Events	*IBM Tivoli NetView for z/OS Automation Guide*

Chapter 8. Managing Network Inventory

To effectively manage the various parts of your Information System, from your central computers to your most remote terminal, stay informed of all its components. An effective configuration management process with maintaining a centralized, up-to-date inventory of system components and their relationships to one another, and with the ability to gather, organize, and locate information about your Information System (IS) installation.

You can create records about your system and store them in a database. You can then extract facts about your system, update the records as changes occur, create reports and diagrams, and search for records with specific information. You can also maintain financial information specific to one component or to a group of components, and you can establish relationships to these configuration components with the problem and change management information. With this information at your fingertips, you can react more quickly to a potential failure. You can help your network group more easily detect failing components, swap or bypass components, and institute recovery procedures.

Using Vital Product Data

Vital Product Data (VPD), also known as Network Asset Management (NAM), is a feature of many IBM and Tivoli products that provides the following information:

- Product details
- DCE details
- Answering node configuration data
- Attached device configuration data
- User details and device location

Any device that supports the REQUEST/REPLY product set identification (PSID) or link problem determination aid-2 (LPDA-2) architecture can report VPD. Use this data to control the terminal inventory of remote locations from a central site. Without this function, you have to check all the terminal serial numbers using visual verification upon visiting all the locations or by calling terminal users and asking them to check the numbers. This can be a major task in large, geographically distributed networks.

VPD can be collected centrally at the host site by the NetView program. This information is collected online either through operator commands or by using a command list. In a multi-domain network, VPD can also be collected at each domain and then forwarded to a focal point host. After it is collected at the host, the data can be logged and management reports can be generated.

To request VPD from the NetView program, use VPD commands. With these commands, you can retrieve data from supported devices within your network. You can solicit data from the NetView program for:

- A specific LU
- A specific PU and its ports
- DCEs between an NCP and a PU

Collecting Vital Product Data

Use the following commands to collect VPD: VPDALL and VPDCMD.

Use the VPDALL command to create commands to collect VPD and write it to the external log for PUs and link segments defined in the user's VTAM configuration definitions. The VPDALL command can either run these VPD commands as they are generated or create a command list containing the VPD command that can be processed later.

To create a command list (named VPDACT) to collect VPD for all VTAM major node definitions listed in the configuration member ATCCON01, enter:

```
vpdall config(atccon01),create,clist(vpdact),add
```

An example of the command list generated is shown in Figure 110:

```
BROWSE -- SYS1.COMMON.CLISTS(VPDACT)------------ LINE 0
COMMAND===>
******************************** TOP OF DATA ************
VPDTEST CLIST
&CONTROL ERR
VPDLOGC START
* RABQ48
VPDPU ALL RABP48   NOERROR
* RABP48
VPDPU ALL RABP48   NOERROR
* SW3174
VPDPU ALL P3174SW  NOERROR
* SW45A4XX
VPDPU ALL P45A451C NOERROR
* SWRAJ
VPDPU ALL PCRAJ    NOERROR
* SWPC
VPDPU ALL PCSW     NOERROR
* SWPSPC
VPDLOGC END
&EXIT
******************************** BOTTOM OF DATA *******************
```

Figure 110. VPDACT Command List

Use the VPDCMD command to retrieve VPD data from the following devices:
- A specific LU
- A specific PU and its ports
- Data circuit-terminating equipment (DCE) between and NCP and a PU

The solicited VPD is displayed on your terminal and is not saved in storage. However, you can use a command list to automate the collection of VPD, and to write it to an external log.

For example, to request VPD from all modems that exist between NCP N139F47 and PU P13008A, beginning at link segment level 2, enter:

```
vpdcmd dce n139f47 p13008a 2
```

To request VPD from PU H040PU and all devices attached to the PU, enter:

```
vpdcmd all h040pu
```

Setup for Configuring VPD to Work with the NetView Program

Complete the following steps to configure the NetView program to support VPD:

1. Define the following ACBNAME parameter in your APPL statements:

```
CNM01VPD  APPL  AUTH=CNM,ACBNAME=VPDACB,PRTCT=CNM01
                STATOPT='VPD TASK'
```

2. Define the following statements in DSIVPARM. DSIVPARM contains the initialization parameter for the VPD task:

```
VPDINIT ACBNAME=VPDACB,PASSWORD=CNM01,VPDREQ=001
VPDINIT VPDWAIT=030,SNAPRQ=OFF,VPDSTOR=02
```

Topic:	**Reference:**
Defining VPD to the NetView program	Refer to *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.
VPDALL and VPDCMD commands	NetView online help

Chapter 9. Controlling Remote Processors

NetView for z/OS provides the ability to control remote processors. In typical operation, NetView communicates with a peer NetView program on the remote z/OS processor to issue commands and receive responses and unsolicited messages. When not available with distributed NetView programs, the NetView program uses the facilities provided by Processor Operations to directly communicate with the remote processor to perform tasks such as IPL and system or subsystem initialization. In this case, the goal is to initialize the environment including the remote NetView so that typical NetView-to-NetView communication can take over.

The NetView program can also control remote non-z/OS processors that support the host command facility (HCF) interface. Additionally, you can use the Distributed Console Access Facility (DCAF) from a workstation to control a remote workstation.

For information about setting NetView timer commands for remote systems and processors, see Chapter 17, "Scheduling Commands," on page 249.

Using the Target System Control Facility

You can use the Target System Control Facility (TSCF) status panel to monitor the overall status of the components in your TSCF configuration. You can also view the current settings of variables that are relevant to the operation of the system, how the TSCF application is defined, which components are in use for which target system, and so on.

In addition, TSCF provides commands that extend the automation capabilities of the NetView program to provide for the operation of target systems. These commands let you:

- Perform a power-on reset of the target processor.
- Initialize the target system (IPL).
- Shut down the target system.
- Specify commands to the target system.

Note: For information about issuing NetView timer commands to remote targets, see Chapter 17, "Scheduling Commands," on page 249

Using the Status Panels

Complete the following steps to display detailed information for a specific target system:

1. Type **isqxdst** from a NetView command line. A panel similar to Figure 111 on page 174 is displayed.

```
ISQESUM                TSCF Status Summary         Updates: Dynamic

  Place cursor on desired system and press PF key for more details

  Target System Name   Status

       SYSTEM01        IPL COMPLETE
       SYSTEM02        IPL COMPLETE
       SYSTEM03        IPL COMPLETE
       SYSTEM04        IPL FAILED
       SYSTEM05        LOAD FAILED
       SYSTEM06        INITIALIZED
       SYSTEM07        WAITING FOR IEA101A MESSAGE
       SYSTEM08        WAITING FOR IEA347A MESSAGE
       SYSTEM09        WAITING FOR VM START MESSAGE
       SYSTEM10        CLOSED
       SYSTEM11        UNKNOWN
       SYSTEM12        UNKNOWN
       SYSTEM13        UNKNOWN
       SYSTEM14        UNKNOWN


Enter=Static  PF1=Help PF3=Exit PF4=Target System Summary PF5=Resource
PF6=Roll      PF7=Up   PF8=Down PF9=Target Hardware Summary  PF12=Quit
```

Figure 111. TSCF Status Summary Panel

Notice that in this example, the panel is being updated dynamically (the update status is displayed on the upper right corner of the panel, in the `Updates:` field). To toggle between a dynamic and a static display, press the **Enter** key. This applies to this panel and to any other TSCF status panels. If update are very frequent, you might want to place the panel in a static condition.

2. Move the cursor to the name of the target system you want to monitor and press **PF4**. A panel similar to Figure 112 on page 175 is displayed.

```
ISQETARG            Target System Summary         Updates: Dynamic

Target System Name: SYSTEM01      Group: CHICAGO  Subgroup: ACCTG
Target System Description: This is the executive payroll system
Status                   : INITIALIZED
Target Hardware          : LPAR DEFINITION PROBLEM
Attention                : DCCF


Target Hardware: BANKER        O.S.     : MVS
Mode           : LPAR          LPAR name: EXECPAY
Channel Status Summary: OPTIONAL CHANNELS UNAVAILABLE

Console Summary:        PS/2 Name  Port Status

Active System Console   PS2A       S
Active Operator Console PS2A       M
Backup System Console   PS2B       T
Backup Operator Console PS2B       N

Last Error Message: 03/18/01 11:05:03
ISQ800I SYSTEM1 Channel status has changed

Enter=Static  PF1=Help PF3=Exit  PF5=Resource   PF6=Roll PF7=Oper List
PF9=Target Hardware    PF10=Port Detail PF11=PS/2 Detail PF12=Quit
```

Figure 112. TSCF Target System Summary Panel

3. Review the information in this panel. Some of the information provided is:
   - The group and subgroup to which the target system was assigned.
   - The current value of the TSCF internal variable *tstat* (displayed in the `Status` field). This variable indicates the status of the target system (if the system was initialized successfully, if a communication link with the target system has failed, and so on). This value is displayed in green to indicate a normal condition, yellow to indicate a situation that requires attention by an operator or a transient state, and red to indicate an unsatisfactory state that requires action.
   - The type of operating system on the target system.
   - The status of the active and backup system or operator console.

   Note: For the purpose of this explanation, this panel is used as the starting point in accessing the other status panels. Many of the other panels can be accessed from other locations and directly by issuing a command from the NetView command line.
4. To view the status of the resources available to the target system, press **PF5**. If the target system is running on hardware that is in LPAR mode, a panel similar to Figure 113 on page 176 is displayed.

```
ISQETSR          Target System LPAR Resource       Updates: Dynamic

Target Hardware Name: BANKER          Target System Name: SYSTEM01
Description: This is the executive payroll system
Channel Status: OK                                  Mode: ESA

Central Storage (desired/actual)              : 16/16
Expanded Storage (desired/actual)             : 128/128
Number of Central Processors (desired/actual) : 2/2
Number of Vector Processors (desired/actual)  : 1/1
LPAR name: EXECPAY    Favored LPAR: Y            LPAR automatic IPL: N

CHPID map (desired)   CHIPD map (actual)
 x=0123456789ABCDEF    x=0123456789ABCDEF
0x ...O......M.....   0x ***R******R***** Legend
1x ................   1x ****************
2x MMM...OOO.......   2x RRR***RRR******* M - Mandatory (required)
3x ................   3x **************** O - Optional
4x ................   4x **************** . - Not specified
5x ................   5x **************** R - Reconfigurable
6x ................   6x **************** * - Not defined


Enter=Static  PF1=Help  PF3=Exit  PF6=Roll  PF12=Quit
```

Figure 113. Target System LPAR Resource Status Panel

If the target system is running on hardware that is not in LPAR mode, a panel similar to Figure 114 is displayed.

```
ISQETHR                    Target Resources       Updates: Dynamic

Target Hardware Name: BANKER                        Mode: ESA
Description: This is the executive payroll system

Central Storage              : 16
Expanded Storage             : 128
Number of Central Processors : 2
Number of Vector Processors  : 1

CHPID map (desired)
 x=0123456789ABCDEF                     Legend
0x ...O......M.....                     M - Mandatory (required)
1x ................                     O - Optional
2x MMM...OOO.......
3x ................
4x ................
5x ................
6x ................


Enter=Static  PF1=Help  PF3=Exit  PF6=Roll  PF12=Quit
```

Figure 114. Target System Resource Status Panel

Depending on the type of hardware on which the target is running (for example, a 9021 can have up to 256 CHPIDs), these panels might be split into two panels (with the CHPID map information on a different panel and accessible by pressing the **PF2** key).

When you review the information, press **PF3** to return to the Target System Summary panel.

5. To view detailed status information about the target hardware on which the target system is defined, press **PF9**. A panel similar to Figure 115 is displayed.

```
ISQEHARD            Target Hardware Summary        Updates: Dynamic


Target Hardware Name: BANK01      Type: 9121        Mode: LPAR
Target Hardware Description: Executive 9121 System


Initialized Target Systems: SYSTEM01    SYSTEM02



Channel Summary Status: UNKNOWN


  Console Summary             PS/2 Name  Port  Status

  Active System Console       PS2A       S
  Backup System Console       PS2B       T




Enter=Static   PF1=Help  PF3=Exit  PF5=Resource      PF6=Roll
PF7=Oper List  PF10=Port Detail    PF11=PS/2 Detail  PF12=Quit
```

Figure 115. Target System Hardware Summary Status Panel

When you have reviewed the information, press **PF3** to return to the Target System Summary panel.

6. To view detailed status information about a specific workstation, move the cursor to the name of the workstation you want to monitor and press **PF11**. A panel similar to Figure 116 on page 178 is displayed.

```
ISQEPS2                 PS/2 Detail              Updates: Dynamic

Name: PS2NAM01         LU Name: LU62AAB       WWV Installed: No
PS/2 Description: This is the executive payroll PS/2 system
Focal Point Port Letter: F
Control Port Letter    : P

PS/2 Status: CLEAR TO SEND

Port Letter        Status
-----------        --------------------

    M              ACTIVE
    N              CLOSED
    O              LINK ERROR
    T              UNKNOWN

Last Error Message: 03/18/01 11:05:03
ISQ522I PS/2: TEST@PS2 allocation failed primary RC=1 secondary RC=2


Enter=Static           PF1=Help          PF3=Exit          PF6=Roll
PF7=Oper List          PF10=Port Detail                    PF12=Quit
```

Figure 116. PS/2® Detail Status Panel

When you have reviewed the information, press **PF3** to return to the Target System Summary panel.

7. To view detailed status information about a specific workstation port, move the cursor to the name of the workstation and port letter you want to monitor and press **PF10**. A panel similar to Figure 117 is displayed.

```
ISQEPORT                PS/2 Port Detail          Updates: Dynamic

PS/2 Name        : PS2NAM01
LU Name          : LU62AAB
Port             : O



Status           : ACTIVE
Port Name        : CUT1
Port Type        : ACTIVE SYSTEM CONSOLE
Screen Handler   : SYS3090
Protocol         : 3270    (3270 or ASCII)
System Name      : BANKER  (system name)
Lock Holder      : OPER1


Last Error Message: 03/18/01 11:05:03
ISQ522I PS/2: TEST@PS2 allocation failed primary RC=1 secondary RC=2


Enter=Static  PF1=Help  PF3=Exit  PF6=Roll  PF7=Oper List  PF12=Quit
```

Figure 117. PS/2 Port Detail Status Panel

When you have reviewed the information, press PF3 to return to the Target System Summary panel.

8. To view detailed status information about the operators that receive messages from the console connected to a specified port and workstation, move the cursor to the name of the workstation and port letter you wish to monitor and

press **PF7**. A panel similar to Figure 118 is displayed.

```
ISQEIOL            Interested Operator List       Updates: Dynamic

PS/2 Name: PS2NAM01
Port Id  : S

             PS2NAM01                      DEVLAB
             S                             SC

             FRANK                         ALICE
             JOHNNIE                       RHONDA
                                           WILEY
                                           FRANK









Enter=Static  PF1=Help  PF3=Exit  PF6=Roll  PF8=Next   PF12=Quit
```

Figure 118. Interested Operator List Status Panel

If more data exists than can fit on this panel, press **PF8** to scroll through the data.

When you have reviewed the information, press **PF3** to return to the Target System Summary panel. From this panel, press **PF3** again to return to the TSCF Status Summary panel and to select a different target system.

Using the Commands

You can use TSCF commands to perform an IPL or to shutdown target systems. In addition, you can send commands directly to the operator console or to the system console of a target system.

Performing an IPL of a Target System

To IPL a target system, initialize the target system and load and start the operating system software. You can use the Activate common command to initialize a target system. This initialization extends from a power-on reset to performing the initial program load process. For example, to initialize the target system SYS2, enter:

```
isqccmd sys2 activate
```

Use the Load common command to load and start a target system's operating system, without initializing the system. This can happen if, for example, the target system is reinitialized after a disabled wait state. For example, to load and start the target system SYS2, enter:

```
isqccmd sys2 load
```

Use the ISQXIII command to initialize a target system (without starting and loading the operating system software). Initializing a target system associates the target system with the target hardware and with the PS/2 computers and PS/2

ports that provide the communication path between the focal point system and the target system. For example, to initialize the active and backup operator and system console for SYS2, enter:

```
isqxiii sys2
```

Shutting Down a Target System

Use the Deactivate common command to shut down a target system. This command causes the target system to end normal operation and also closes the system console and operator console ports. For example, to shut down the target system SYS2, enter:

```
isqccmd sys2 deactivate
```

Specifying Commands at the Target System

Use TSCF to interact with a single console in a simple and efficient manner. You can use the ISQSEND command to send commands to an operator console (OC) or to a system console (SC) at a specified target system. You can also use the ISQTCC command to establish a pass-through session between the current operator station task (OST) and a specific target system. Use the passthrough session to enter commands as if you were at the console of the target system and to immediately see the results of each command without any messages from other systems cluttering up the screen.

Topic:	**Reference:**
Monitoring the status of the components in your TSCF configuration.	*Target System Control Facility Operations and Commands*

Using Tivoli Remote Control

The Tivoli Remote Control component provides a remote console function that allows one programmable workstation, called a controlling workstation, to control the keyboard input and monitor the display output of another programmable workstation, called the target workstation.

When the remote control session is in the monitoring state, you can see the screen image of the target workstation's display from the controlling workstation. When the remote control session is in the active state, you can use the controlling workstation to operate and control the target workstation. Any keystrokes that you type at the controlling workstation are relayed to the target workstation and acted upon as if they were typed by the target workstation user. The remote control component provides the following network management and maintenance functions:

- Remote help desk assistance for applications, online education, and maintenance of application programs
- Remote problem determination for trace and dump analysis, including the transfer of data
- Remote control of unattended workstations (for example, LAN servers)
- Remote management of personal computers, and accessibility to data and programs stored on it (for example, a system running in the home or in the office)
- Remote access to system consoles when they are implemented on personal computers
- Remote monitoring of work in progress on target workstations (for example, between teachers and students)

As an example of using the remote control component, suppose a target workstation user is having difficulty understanding the company's new accounting program. The target workstation user contacts you, and you open a session with that particular workstation. With the accounting program on the screen, you can switch to the active state and type the correct keystrokes to run the accounting program. The user at the target workstation observes the process and learns how to use the new accounting program. You then switch to monitoring the state and return control to the user at the target workstation.

Topic:	**Reference:**
Using the Distributed Console Access Facility	*IBM Distributed Console Access Facility User's Guide*

Chapter 10. Controlling Operating System Resources

You can manage operating system resources through the NetView program, System Automation for z/OS, and Tivoli Workload Scheduler for z/OS. In addition, you can use the NetView program and the Programmable Operator Facility of VM to control VM systems and the Operator Communication Control Facility of VSE to control VSE systems.

Using the NetView Program

Use the NetView program as a control point to manage operating system resources and to perform some of the tasks that operators have traditionally performed, including:

- Processing messages
- Running regularly scheduled procedures
- Recovering and restarting the system and network in the event of a failure

Issuing MVS System Commands

To issue commands to MVS, use the NetView MVS command to control MVS system operations without using a separate screen for multiple console support (MCS).

To issue a command from the NetView command facility, enter MVS followed by a valid MVS command. For example, to display a list of active MVS tasks, enter the following command:

```
mvs d a,l
```

The NetView command facility displays the response from MVS.

Setup Required to Issue Commands to MVS

If extended MCS consoles are used, no setup is required.

If standard MCS consoles are used:

- Start the NetView subsystem.
- Start the NetView subsystem router to issue MVS commands.

To issue commands to MVS, the NetView subsystem and the NetView subsystem router, must be started. Refer to *IBM Tivoli NetView for z/OS Installation: Getting Started* for more information.

Automating MVS Commands

You can automate MVS and subsystem commands entered from any MVS console or console interface. To do this, you must install a load module as an MVS command exit, add a CMD statement in one of the `MPFLSTxx` members, and issue a `SET MPF=`*xx* command to activate the exit. Refer to *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components* for more information.

When MVS Commands Fail

You can receive the following messages:

CNM560I

The NetView subsystem router is not active. To start the NetView subsystem router, enter the following command:

```
start task=taskname
```

From the NetView command facility where *taskname* is the name of the task associated with load module CNMCSSIR.

CNM564I
You had a syntax error in your MVS command. Correct the error and issue the command again.

CNM566I
The NetView console ID table is not available. This is probably because the NetView subsystem is not active. To start the NetView subsystem, enter the following command:

```
s procname
```

From the MVS console, where *procname* is the name of the procedure defined by your system programmer to start the NetView subsystem.

If the subsystem is already started, your system programmer can check the startup parameters for the NetView subsystem interface. Refer to the *IBM Tivoli NetView for z/OS Installation: Getting Started*.

Hint: You do not need to start the subsystem to send MVS commands from the NetView operator if you are using extended MCS consoles.

CNM567I
No MVS console is available. You can either ask your system programmer to define additional MVS consoles or you can enter the following command:

```
disconid
```

To determine which other operators have consoles assigned to them and ask one of them to release their console. An operator can release a console by entering the following command:

```
relconid
```

CNM568I
You do not have command authorization to issue the keyword. Contact your system programmer to give your operator task access.

DWO338I
The console you requested is already in use. To request a different console, enter the following command, where *name* is a different console than you first requested, and the default console name is the same as your operator ID:

```
getconid console=name
```

Topic:	**Reference:**
MVS, GETCONID, RELCONID, DISCONID, SETCONID commands	NetView online help
Consoles	*IBM Tivoli NetView for z/OS Automation Guide*
MVS System Commands	*MVS/ESA System Commands Reference*
Defining consoles	*MVS/ESA Initialization and Tuning Reference*

Issuing JES2 Commands

To issue a JES2 command, enter MVS from the NetView command facility, followed by a valid JES2 command. For example, you can issue commands to accomplish the following tasks:

1. Determine the current job printing on prt15
2. Keep JES2 from printing any other jobs on prt15
3. Allow the current job on prt15 to finish printing on another printer

Perform the following steps:

1. To display the status of prt15, enter the following command:

   ```
   mvs $du,prt15
   ```

2. To drain prt15, enter the following command:

   ```
   mvs $pprt15
   ```

3. To interrupt the job printing on prt15, enter the following command:

   ```
   mvs $iprt15
   ```

Issuing JES3 commands

You can issue commands to JES3 from the NetView program. Figure 119 shows how to issue the JES3 *I S command to display the status of JES3 system resources.

```
NCCF                    Tivoli NetView    VABNV AHNJE    04/12/01 11:12:36 A
* VABNV    MVS *I S
E VABNV    IAT5619 ALLOCATION QUEUE    = 00001  BREAKDOWN QUEUE = 00000
E VABNV    IAT5619 SYSTEM SELECT QUEUE = 00001  ERROR QUEUE     = 00000
E VABNV    IAT5619 SYSTEM VERIFY QUEUE = 00000  FETCH QUEUE     = 00000
E VABNV    IAT5619 UNAVAILABLE QUEUE   = 00001  RESTART QUEUE   = 00000
E VABNV    IAT5619 WAIT VOLUME QUEUE   = 00000  VERIFY QUEUE    = 00001
E VABNV    IAT5619 ALLOCATION TYPE = AUTO
E VABNV    IAT5619 CURRENT SETUP DEPTH - ALL PROCESSORS = 00004
E VABNV    IAT5619 MAIN NAME    STATUS          SETUP DEPTH       DASD
           TAPE
E VABNV    IAT5619 SYSA      ONLINE    IPLD SMAX=255 SCUR=00001 3056,0000
           0072,0023
E VABNV    IAT5619 SYSB      ONLINE    IPLD SMAX=255 SCUR=00000 3056,0000
           0072,0023
E VABNV    IAT5619 SYSC     OFFLINE NOTIPLD SMAX=255 SCUR=00000 3056,0756
           0072,0000
E VABNV    IAT5619 SYSD      ONLINE    IPLD SMAX=255 SCUR=00003 3120,0000
           0072,0023



???
```

Figure 119. Issuing a JES3 Command from the NetView Program

Topic:	Reference:
Issuing JES3 commands from the NetView program	*IBM Tivoli NetView for z/OS Automation Guide*

Issuing an MVS DISPLAY Command

Use the @D command to issue the MVS system command DISPLAY. You can page through the resulting full-screen response.

You can use this command to display information about the operating system, the jobs and applications that are running, the processor, devices that are online or offline, real and extended storage, and the time of day. For example, to display unit status information for 40 devices of type DASD that are online, enter the following command:

```
@d u,dasd,online,,40
```

A full-screen panel similar to Figure 120 is displayed.

```
AOFK3GEN             COMMAND RESPONSE DISPLAY
Command:  MVS D U,DASD,ONLINE,,40
  IEE450I 11.50.52 UNIT STATUS 111
  UNIT TYPE STATUS  VOLSER VOLSTATE   UNIT TYPE STATUS  VOLSER VOLSTATE
  3A0  3390 A       RACF01 PRIV/RSDNT 3A1  3390 A       PROD01 PRIV/RSDNT
  3A2  3390 A-SPD   IPOCAT PRIV/RSDNT 3A3  3390 S       IPORES PRIV/RSDNT
  3A5  3390 A       IMS002 PRIV/RSDNT 3A6  3390 A       IPOSMP PRIV/RSDNT
  3A7  3390 O       IPODL1  PUB/RSDNT 3C0  3390 A-SPD   3C0DSK PRIV/RSDNT
  3C1  3390 A       3C1DSK STRG/RSDNT 3C2  3390 A       3C2DSK PRIV/RSDNT
  3C3  3390 A    -R 3C3DSK STRG/RSDNT 3D0  3390 O       ASC000 PRIV/RSDNT
  3D1  3390 O       ASC001 PRIV/RSDNT 3D2  3390 O       ASCRES PRIV/RSDNT
  3D3  3390 O       ASCCAT PRIV/RSDNT 3D6  3390 O       ASCSMP PRIV/RSDNT
  3D7  3390 O       ASCDL1 PRIV/RSDNT
  IEE452I UNIT STATUS NUMBER OF UNITS REQUESTED EXCEEDS NUMBER AVAILABLE









ACTION===>
         PF1=Help    PF2=End        PF3=Return
         PF6=Roll                                  PF9=Refresh   PF12=Retrieve
```

Figure 120. Displaying Unit Status Information

Note: If the selected MVS DISPLAY command @D DASD is issued, the resulting display is the same.

To display overview information about system activity and detailed information about all active units of work, enter the following command:

```
@d a,all
```

A full-screen panel similar to Figure 121 on page 187 is displayed.

```
AOFK3GEN             COMMAND RESPONSE DISPLAY
Command:  MVS D A,ALL                                        Page 1    of 6
  IEE450I 11.53.03 96.078 ACTIVITY 115
   JOBS      M/S      TS USERS      SYSAS      INITS     ACTIVE/MAX VTAM
00000     00012      00011        00009      00006      00011/00025
 *MASTER* *MASTER*          NSW  *   A=0001   PER=NO   SMC=000
                                     PGN=000  DMN=000  AFF=NONE
                                     CT=013.943S  ET=02.41.37
PCAUTH    PCAUTH             NSW  *   A=0002   PER=NO   SMC=000
                                     PGN=001  DMN=001  AFF=NONE
                                     CT=000.074S  ET=02.41.37
RASP      RASP               NSW  *   A=0003   PER=NO   SMC=000
                                     PGN=001  DMN=001  AFF=NONE
                                     CT=000.015S  ET=00218.26
TRACE     TRACE              NSW  *   A=0004   PER=NO   SMC=000
                                     PGN=001  DMN=001  AFF=NONE
                                     CT=000.067S  ET=02.41.37
XCFAS     XCFAS   IEFPROC    NSW  *   A=0005   PER=NO   SMC=000
                                     PGN=000  DMN=000  AFF=NONE
                                     CT=000.184S  ET=02.41.37

ACTION===>
          PF1=Help    PF2=End        PF3=Return
          PF6=Roll                                PF9=Refresh   PF12=Retrieve
```

Figure 121. Displaying Information about System Activity and Active Units of Work

As a result of the primary operand (A), the system displays overview information about system activity such as the number of active batch jobs, the number of started tasks, the number of logged-on time-sharing users, and the number of active system address spaces. The ALL operand provides detailed information about all active units of work. You can use the PF8 key to scroll forward through the six pages of information and PF7 to scroll backward. Note that these PF key values are hardcoded on these product panels and in these product settings. These PF keys cannot be displayed and changed in the same way as the NetView PF keys.

Issuing JES2 Commands

Use the JES2 command to issue JES2 subsystem commands. You can page through the full-screen response. For example, to display the status of all or specified local JES2 controlled non-direct access devices, enter the following command:

```
jes2 du,all
```

A full-screen panel similar to Figure 122 on page 188 is displayed.

```
AOFK3GEN            COMMAND RESPONSE DISPLAY
Command:  MVS $DU,ALL                                      Page 1    of 1
$HASP882 OFFLOAD1 DSN=,STATUS=DRAINED
$HASP880 LINE1    UNIT=AA0,STATUS=DRAINED
$HASP880 LINE2    UNIT=A01,STATUS=DRAINED
$HASP880 LINE3    UNIT=A02,STATUS=DRAINED
$HASP603 PRT1     UNIT=,STATUS=DRAINED
$HASP603 PRT2     UNIT=,STATUS=DRAINED
$HASP603 PRT3     UNIT=,STATUS=DRAINED
$HASP603 PRT4     UNIT=,STATUS=DRAINED
$HASP603 PRT5     UNIT=,STATUS=DRAINED
$HASP603 PUN1     UNIT=,STATUS=DRAINED
$HASP603 PUN2     UNIT=00B,STATUS=DRAINED
$HASP603 RDR1     UNIT=00C,STATUS=INACTIVE









ACTION===>
         PF1=Help    PF2=End        PF3=Return
         PF6=Roll                                 PF9=Refresh   PF12=Retrieve
```

Figure 122. Displaying the Status of JES2 Access Devices

The ALL operand displays detailed information about all local JES2 controlled devices, active remote devices, and internal readers.

Topic:	Reference:
MVS command	NetView online help
Setting up, displaying, and changing the System Automation for z/OS automation control file	*System Automation for z/OS Customization and Programming* and *System Automation for z/OS User's Guide*
Assigning automation operators for System Automation for z/OS messages	*System Automation for z/OS User's Guide*
Managing the status of MVS resources	*System Automation for z/OS User's Guide*
Issuing MVS and JES2 commands from System Automation for z/OS	*System Automation for z/OS User's Guide*

Controlling Resources Utilization Using OPC/ESA

Your data center has resources, both physical and logical, that must be shared between the batch jobs and started tasks that run to satisfy the business processing needs of your enterprise. Optimum utilization of resources not only maximizes the throughput of processing but is also critical to your ability to meet the increasingly high service demands of your customers.

OPC/ESA defines three resources types to represent the various resources in your environment. The availability indicators of each resource type can be changed dynamically by the NetView program to reflect the actual resource status. The different resource types are shown in the following list:

Parallel servers
Define the total number of operations that can be started at a workstation simultaneously. On computer batch workstations, parallel servers represent JES initiators.

Workstation resources
Two workstation resources are recognized per workstation. You decide what these resources represent. They are most commonly used to represent tape or cartridge drives. They represent a pool of resources that are shared by the operations.

Special resources
Any other resource which cannot be described as a parallel server or workstation resource. They describe a situation that for scheduling purposes is important. For example, batch jobs which cannot process while an online transaction processor is active. A special resource can be allocated by an operation for shared or exclusive use. Availability of the resource can be used as a trigger to start an operation or to include some processing in the schedule that cannot be planned.

Parallel Servers and Workstation Resources

OPC/ESA is not aware of the actual status of resources in your environment. Instead, it schedules the work according to what it believes to be the case, that is, the number and status of resources you have previously defined. This can lead to over-scheduling or under-scheduling of the resources if the status or number of resources is changed by an operator or automatically by the system.

The impacts of over-scheduling resources such as JES initiators or a pool of tape drives might not be immediately obvious. When a queue for JES initiators exists, queuing is handled on a first-in-first-out basis. Additionally, JES automatically increases the priority of a queued job if it has been queued for a long time. This queuing mechanism is efficient for many purposes, but it does not reflect the relative priority of the jobs nor does it consider your deadlines.

Over-scheduling a tape or cartridge pool can create many problems. MVS tries to give all requestors what it considers an equal share of the devices. This means that volumes are dismounted at step end if outstanding device requests exist. Valuable time is lost rewinding, dismounting, remounting, and repositioning the volume. Further, the volume is unlikely to be remounted on the same device from which it was dismounted, this means your operators wage a never-ending battle chasing volumes from device to device.

When the NetView program is used to adjust the status of resources defined to OPC/ESA as a result of events occurring in the operating environment, resource utilization can always be maximized and over-scheduling of critical resources can be avoided.

Modifying Resource Ceilings from the NetView Program

The OPC/ESA sample library member EQQPIFWI contains a program which can be used to modify the number of parallel servers and workstation resources in the current plan. You can tailor this program to your installation requirements and call the program from the NetView program to modify resource ceilings in response to events initiated, or detected, by the NetView program.

Part 3. Controlling the NetView Environment

Chapter 11. Maintaining the NetView Program

Controlling the NetView program is the continual adjustment of the NetView environment to achieve the goals of monitoring, investigating, analyzing, and controlling network and system components.

For information about how to protect commands and resources, define operators to the NetView program, and restrict access to data sets, refer to the *IBM Tivoli NetView for z/OS Administration Reference*.

Defining a NetView Command

Use the CMDDEF statements (located in CNMCMD) to define commands to the NetView program. For example, the LIST command is defined by the following statement:

```
CMDDEF.LIST.MOD=DSISHP
```

Where DSISHP is the name of the module that contains the code to run the command. If you are defining your own command processor, be sure to specify a unique module name on the MOD operand. Do not use a name that the system might recognize as a NetView-supplied command, because the NetView program attempts to process the NetView command instead of your command processor. Use the following conventions when defining commands:

- Start the name with an alphabetical character.
- Do not use NetView prefixes.
- Avoid special characters such as commas and colons.
- Avoid NetView command names, both internal commands and those shipped in CNMCMD.

For more information about NetView prefixes and internal command names, refer to the *IBM Tivoli NetView for z/OS Customization Guide*

You can also include CMDDEF statements for a command list for which you want to provide a synonym. For example, to define a command list named MYSTATUS and a synonym of MYSTAT, include the following statements in DSIPARM member CNMCMDU:

```
CMDDEF.MYSTATUS.MOD=DSICCP
CMDDEF.MYSTATUS.CMDSYN=MYSTAT
```

You can define command security using the NetView command authorization table, or a system authorization facility (SAF) security product such as Resource Access Control Facility (RACF). When you make changes to command security using the NetView command authorization table or SAF product, you do not need to recycle the NetView program for these changes to take effect.

For more information, refer to the *IBM Tivoli NetView for z/OS Security Reference*.

Defining Resources in the Network

A *resource* is an element of a network to which a name can be assigned. Resources can also be called *nodes*. Subarea nodes are defined to VTAM using the VTAMLST data set. Advanced Peer-to-Peer Networking nodes are dynamically defined to VTAM. Nodes are grouped together into an aggregation called a *major node*. An example of a major node is a cluster controller and its subordinate logical units (LUs). A major node is represented in VTAMLST by a single member. Individual nodes within a major node are called ***minor nodes***. An example of a minor node is an LU.

The NetView program uses the VTAMLST data set to define the network that is monitored by the status monitor. If the SNA topology manager is not being used, and if the MONIT function is required, when changes are made to the VTAMLST data set, the status monitor preprocessor (CNMNDEF) must be run to update the tables used by the status monitor.

Topic:	Reference:
Status Monitor Preprocessor	*IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*

Maintaining Objects and Relationships in RODM

The Resource Object Data Manager (RODM) is an in-memory data cache that stores, retrieves, and manages operational resource information needed for network and systems management.

For the NetView management console to manage non-SNA resources in your system and network, the resources and relationships between them must exist in the RODM data cache. Several facilities can be used for creating, updating and deleting objects and relationships in RODM:

- NetView Network Planner/2
- NetView MultiSystem Manager
- NetView SNA topology manager
- Remote Operations Manager
- NetView RODM load utility
- RODMView

The NetView Network Planner/2 program manages inventoried resources, their operational characteristics, and their operational relationships. This program can generate a load file for use with the NetView RODM load utility program for maintaining objects and relationships in RODM.

The NetView MultiSystem Manager program collects topology information about local LAN resources managed by LAN Network Manager and Novell servers, and internet protocol (IP) resources. This program stores this information in RODM for the NetView management console to use.

The SNA Topology Manager collects topology information for SNA subarea and Advanced Peer-to-Peer Networking resources, and stores the topology information in RODM for use with the NetView management console.

The NetView Remote Operations Manager creates, updates, and deletes objects and relationships in RODM that represent NetView Remote Operations Agent/400s.

The NetView RODM load utility reads control statements that specify the creation, update, or deletion of objects and relationships in the RODM data cache.

The NetView RODMView function can be used directly, from a command line as EKGV commands, or from a series of NetView panels. Using RODMView simplifies the task of defining classes, objects, and fields to the NetView GMFHS data model.

Using the NetView MultiSystem Manager

You can use NetView MultiSystem Manager to manage your LAN, IP, Tivoli management region, and Open Topology Interface resources. MultiSystem Manager dynamically collects resource and configuration information from LAN topology agents, Tivoli management region agents, and IP agents in the network, and places this information in RODM. As the topology changes, MultiSystem Manager updates this configuration information in RODM. You can also use REXX calls to MultiSystem Manager Access to load objects into RODM. As in the case of other agents in the network, status information is kept in RODM for the NetView management console to use.

Topic:	Reference:
Novell networks	*MultiSystem Manager MVS/ESA for Novell Netware Networks*
LAN Network Manager (LNM) networks	*MultiSystem Manager MVS/ESA for Internet Protocol (IP) networks and MultiSystem Manager: Internet Protocol Networks*
Other resources	*MultiSystem Manager: Open Topology Interface*

Using the NetView SNA Topology Manager

Use the NetView SNA topology manager to gather and record data about SNA subarea and Advanced Peer-to-Peer Networking topology. The SNA topology manager collects topology data from a VTAM agent. The topology data collected is stored in RODM for use by the NetView management console.

Topic:	Reference:
SNA topology manager usage	*IBM Tivoli NetView for z/OS SNA Topology Manager Implementation Guide*

Using the NetView RODM Load Utility

Use the NetView RODM load utility to load object class definitions, objects, and relationships into the RODM data cache using a previously generated load file. A load file can be generated by NetView Network Planner/2, a user-written utility, or an editor.

Topic:	Reference:
NetView RODM load utility usage	*IBM Tivoli NetView for z/OS Resource Object Data Manager and GMFHS Programmer's Guide*

Using the RODMVIEW Command

The RODMView panel interface is a series of menu-driven, full-screen panels with context and PF key help. You can use the RODMView panels to create or modify objects such as SNA subarea and Advanced Peer-to-Peer Networking objects, domains, gateways, non-SNA objects, and SNA shadow objects and their connectivity and containment relationships.

The RODMView panels simplify the display, addition, updating, and deletion of objects and relationships in the RODM data cache. The panels perform one operation at a time directly on the RODM data cache. Also, refer to the NetView online help for information about the RODMView EKGV commands.

Changing the Value of a RODM Object Attribute Using RODMView

You can use the NetView RODMView command to trigger a RODM method, and to add, change, and delete the values of RODM classes, objects, and fields.

You can trigger a RODM method either as an object-independent or object-specific (named) method. To trigger a RODM method, perform the following steps:

1. Type **rodmview** on the NetView command facility command line and press Enter. The RODMView main menu is displayed as shown in Figure 123:

```
EKGVMMNI                R O D M V i e w  A01NV OPER2    03/20/99 12:34

Select one of the following, press Enter.

                          __ 1.  Access and Control
                             2.  Simple Query
                             3.  Compound Query
                             4.  Locate Objects
                             5.  Link/Unlink
                             6.  Change Field
                             7.  Subfield Actions
                             8.  Create Actions
                             9.  Delete Actions
                             10. Method Actions









CMD==>
F1= Help   F2= End    F3= Return                          F6= Roll  F12=PrevCmd
```

Figure 123. RODMView Program Main Menu

2. Select option **1** (Access and control). The Access and Control panel is displayed as shown in Figure 124 on page 197. Enter your RODM name, your user ID and password, and specify **connect**. When the connection is successful, press the Return key to return to the RODMView main menu.

```
EKGVACTI              Access and Control  A01NV OPER2    03/20/99 12:34

RODM name . . rodmname
User ID . . . rodmuser

User password

RODM function connect (COnnect, Disconnect, CHeckpoint, Stop, Upd

Query pattern matching character *
Checkpoint before stop Y (Y, N)  For Stop function only









CMD==>
F1= Help   F2= End    F3= Return                          F6= Roll  F12=PrevCmd
```

Figure 124. RODMView Access and Control Panel

3. Select option **10** (Method actions). The Method Actions panel is displayed as shown in Figure 125.

```
EKGVMETI                  Method Actions  A01NV OPER2    03/20/99 12:34

RODM name   RODMNAME
User ID . . RODMUSER

Method name _________
Method type _________  (Named, Object independent)

Action  . . TRIGGER   (Trigger, Install, Delete, Replace)

Additional information for Named Methods only:
  Class name ____________________________________________________________
  Class ID   __________

  Object name ___________________________________________________________
  Object ID   ________________ (Hexadecimal value)

  Field name ____________________________________________________________
  Field ID   __________


CMD==>
F1= Help   F2= End    F3= Return                          F6= Roll  F12=PrevCmd
```

Figure 125. RODMView Methods Actions Panel - EKGVMETI

4. Enter the appropriate values in the corresponding fields. For example, if you have a field called MethodSpecField of type MethodSpec defined on the class UsefulClass, and MethodSpecField has a value that includes a method called USFLMETH, you can call it by entering the information as shown in Figure 126 on page 198:

```
EKGVMETI                  Method Actions  A01NV OPER2    03/20/99 12:34

RODM name   RODMNAME
User ID . . RODMUSER

Method name usflmeth
Method type named  (Named, Object independent)

Action  . . TRIGGER   (Trigger, Install, Delete, Replace)

Additional information for Named Methods only:
  Class name  UsefulClass
  Class ID    __________

  Object name ____________________________________________________
  Object ID   _______________ (Hexadecimal value)

  Field name  MethodSpecField
  Field ID    __________


CMD==>
F1= Help   F2= End    F3= Return                          F6= Roll  F12=PrevCmd
```

Figure 126. Triggering a Named Method

Topic:	Reference:
Introduction to RODMView	"Changing the Value of a RODM Object Attribute Using RODMView" on page 196
RODMView panel flow	"Using the RODMView Panels" on page 355
RODMView panels and usage	*IBM Tivoli NetView for z/OS Resource Object Data Manager and GMFHS Programmer's Guide* .

Displaying Data Sets Used by the NetView Program

If you are authorized, you can BROWSE members of NetView data sets including:
- Parameter data set (DSIPARM)
- Help source data sets (CNMPNL1, BNJPNL1, and BNJPNL2)
- Command list data sets (DSICLD)
- Operator profile data set (DSIPRF)
- Network definitions and span information (DSIVTAM)
- Automation table listings and usage reports data set (DSILIST)
- Unprotected definitions, such as PF keys (DSIOPEN)
- Message members (DSIMSG)
- Automation testing reports (DSIARPT) and source files (DSIASRC)

For example, to view the DISPFK command list, enter:

```
browse dispfk
```

You can display members of data sets on a remote NetView system. For example, to view the CNMKEYS settings for PF keys on the remote NetView system NETV2, enter:

```
browse lu=netv2 cnmkeys
```

Use the following BROWSE command to view the contents of an active network `netv2` log:

```
browse netloga
```

If your command security is appropriately configured and allows remote system access, you can use the BROWSE command to view the contents of a remote network log or remote member on *netv2* as shown in the following examples:

```
browse lu=netv2 netloga
```

Topic:	Reference:
BROWSE command	NetView online help
Protecting data sets	*IBM Tivoli NetView for z/OS Administration Reference*

Chapter 12. Controlling NetView Operation

Generally, NetView tasks are started automatically when the NetView program starts and remains active. You can use the STARTCNM and STOPCNM command lists to start or stop groups of DST or OPT tasks by function or all tasks. For example, to start all tasks for the NetView management console program, enter the following command:

```
startcnm graphics
```

There might also be tasks, which are not frequently used, that you might need to start or stop. Here are the steps to follow:

1. To start a task named MYTASK that has been predefined in CNMSTYLE or its included members, enter:

   ```
   start task=mytask
   ```

   If the task has not been predefined in CNMSTYLE, you can still start the task and specify its characteristics using additional parameters on the START command.
2. To stop a task named MYTASK that is active, enter:

   ```
   stop task=mytask
   ```

Each NetView task is assigned a dispatching priority from 1 to 9, where 9 is the lowest and 1 is the highest. The initial priority of a task can be defined in CNMSTYLE or its included members or when the task is started. You can display the priority of all tasks with the LIST command. For example, to list the priorities of all active tasks, enter:

```
list priority
```

You can also specify the priority of a task on the START command. For example, to change the priority of task MYTASK to 8, first stop and then restart the task:

```
stop task=mytask
start task=mytask,pri=8
```

Note: Changing the priority of a task can affect the performance of other tasks running on your system.

Topic:	Reference:
Additional task definitions	*IBM Tivoli NetView for z/OS Administration Reference*
AUTOTASK, START, STOP, STARTCNM, and STOPCNM commands	NetView online help
For a list of tasks	*IBM Tivoli NetView for z/OS Installation: Getting Started*

Controlling Resource Utilization

Use the NetView resource utilization function to prioritize, monitor, and limit the resource usage for various tasks in the NetView program. Resource limits are set and monitored using the TASKMON, TASKURPT, LOGTSTAT, DEFAULTS, and OVERRIDE commands. You can obtain information to help you plan and tune your network and to adjust tasks according to

- The amount of storage and processor consumed

- Based on the rate of I/O activity
- The message-queuing traffic to and from NetView tasks

Topic:	Reference:
TASKMON, LOGTSTAT, DEFAULTS, and OVERRIDE commands	*IBM Tivoli NetView for z/OS Command Reference Volume 1*
TASKURPT	*IBM Tivoli NetView for z/OS Troubleshooting Guide*

Defining and Deleting NetView Operators

You can dynamically add or delete NetView operators while the NetView program is running. You can define new operator profiles in the NetView product or in an SAF security product, such as Resource Access Control Facility (RACF).

For information about adding new NetView operators, when operators are defined to an SAF product or when operators are defined using DSIOPF NetView definitions, refer to the *IBM Tivoli NetView for z/OS Administration Reference*.

Defining NetView Operators

Here are the steps to follow:

1. If defining operators using the NetView product rather than an SAF product, verify that enough application (APPL) statements are defined in your APPL major node for each additional operator you want to add. The samples use member A01APPLS (CNMS0013).
2. If not enough APPL statements are defined for new NetView operators, create a new APPL major node similar to your existing APPL major node. In this new member, define an APPL statement for each new operator you want to add. Be sure to either transfer the new APPL statements to a major node defined in VTAM sample ATCCON*xx* (CNMS0003), or add the new major node to ATCCON*xx*.
3. Activate the new APPL major node.
4. Define the new operator. If using NetView for operator definitions, you can assign an existing profile to the operator. You can define new operator definitions in the NetView product or in an SAF product, such as RACF. Using NetView to define operators, specify the profile for the new operator in a DSIPRF data set member, such as DSIPROFA. Using an SAF product, define the operator in the NETVIEW segment.
5. If the operator definitions are in a NetView DSIPRF data set member, issue the REFRESH OPERS command to dynamically refresh the operator definitions in DSIOPF. Message DWO831I is displayed for each operator successfully added, then message DSI633I is displayed to indicate that the refresh command completed successfully.

   If the operator definitions are in an SAF product, the operator definition is dynamic, taking effect as soon as the operator is defined to the SAF product and permitted to the resource representing NetView in the APPL class.
6. Log onto NetView using the new operator ID.

Deleting NetView Operators

To dynamically delete NetView operators while the NetView program is running, follow these steps:

1. If defining operators using the NetView product, update DSIOPF to delete statements for operators you no longer want or need.

   If you delete a statement in DSIOPF for an operator that was already logged on, the operator session continues until the operator logs off. However, the operator can no longer issue the DISPLAY, MODIFY, or VARY commands for any resource that is defined in any span of control. If you do not want a deleted operator to remain logged on after issuing the REFRESH OPERS command, issue the STOP FORCE command to stop the operator session.

   If the operator is not logged on when you issue the REFRESH OPERS command, the operator can no longer log on.

   If defining operators using an SAF product, delete the operator from the SAF product.
2. Issue the REFRESH OPERS command to dynamically refresh the operator statements in DSIOPF. Message DWO830I is displayed on your screen for each operator successfully deleted, then message DSI633I is displayed to indicate that the refresh command completed successfully.

Topic:	Reference:
APPL statements	Refer to *IBM Tivoli NetView for z/OS Installation: Getting Started*
Operator definitions in DSIPRF and DSIOPF, or in an SAF product	*IBM Tivoli NetView for z/OS Administration Reference*
REFRESH and STOP commands	NetView online help

Controlling the NetView Screen Contents and Format

You can control the format and the amount of information presented on the NetView screen. You can also control the setting of your program function keys, the date and time format, and the way you enter data.

Setting Date and Time Formats

The date and time can be entered freeform and presented in the format you specify. The format is specified using the DEFAULTS or OVERRIDE commands. When sending commands with dates or times to other tasks or other NetView programs, use the receiver's format.

Topic:	Reference:
The DEFAULTS command	The *IBM Tivoli NetView for z/OS Command Reference Volume 1*
Help information	The online help facility

Defining Program Function Keys

You can use PF and PA keys to send commands to the system. You can modify the NetView-supplied CNMKEYS member in DSIOPEN to change the commands sent by the PF and PA keys for various components, then use the NetView PFKDEF command to use those settings. To view the current settings of the PF keys, use the NetView DISPFK command.

You can set and display PF keys by component, determine whether a PF key sends a command immediately or delays, and whether it uses information entered by the operator on the command line or it ignores input.

Use the NetView SET command to change individual PF keys from the command line. For example, to interactively set PF9 in the current component to display the status of the lines and channel links in your part of the network, and to have the command sent immediately to the system, enter:

```
set pf9,immed,lines
```

If instead, you want to define the PF key for just the command facility component, and add text to a command before sending it to the system, enter:

```
set nccf pf9 append dis
```

When the command facility is active and you press PF9, anything typed from the input area is placed directly following the DIS command before processing it. You can enter a resource name without having to enter the DIS command and press the Enter key.

You can specify different PF keys for each component. For example, in addition to specifying `nccf` as the component name, you can specify any of the following keywords:

Keyword	Component Name
NETVIEW	The default setting, unless otherwise specified
LBROWSE	Log browse
MAINMENU	The NetView main menu panel
MBROWSE	Member browse
NCCF	Command facility
NLDM	Session monitor
NPDA	Hardware monitor
STATMON	Status monitor
TARA	4700 support facility
VIEW	View applications, such as the NetView WINDOW command
WINDOW	The NetView WINDOW command
PFKDEF	The PFKDEF display

If an operator data set is defined for you, an OVERRIDE DSIOPEN=*datasetname* command may have already been issued in your logon profile. You can check this by issuing LIST OVERRIDE. If a data set name is shown next to DSIOPEN: under OVERRIDES, you can use the SAVE function of DISPFK to save your key settings across logons or NetView restarts. Settings are saved in that data set in member CNMKEYSV, and picked up by the PFKDEF command.

Topic:	Reference:
Setting PF keys	PFKDEF and NCCF SET in the NetView online help
PF key definitions	Browse member CNMKEYS or enter DISPFK ALL
Saving PF Keys	DISPFK and PFKDEF in the NetView online help. For additional information, refer to operator data set references in the online help for OVERRIDE and in the *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

Repeating Commands

The RETRIEVE command tells the system to place the last command you entered on the command line. If necessary, you can alter the command on the command line, or leave it as it is, then press Enter to send the command to the system.

You can repeat the RETRIEVE command several times to display the last few commands that you sent to the system. The easiest way to use the RETRIEVE command is by assigning it to a PF key. The NetView-supplied default for the RETRIEVE command is PF12.

Entering Mixed–Case Commands

When you enter a command, NetView converts lowercase characters to uppercase prior to processing. Use NETVASIS to prevent this conversion.

NETVASIS is valid only from the command line of the following panels:

- Command facility
- WINDOW
- NetView Management Console

Use NETVASIS in either of the following ways:

- Prefix commands with NETVASIS
- Use the OVERRIDE command with NETVASIS

Many commands do not recognize mixed–case for certain values, for example, START DOMAIN. When you use NETVASIS or OVERRIDE NETVASIS in these cases, enter the values in uppercase. For commands that do not support synonyms, use uppercase for keywords and values. If you are not using DSIEBCDC, your command name must be in uppercase.

Prefixing Commands with NETVASIS

You can use the prefix NETVASIS with a command to prevent NetView from converting lowercase characters in the command to uppercase. For example, RODM class names are case-sensitive; to call your command list RODMINST that displays a list of network management gateways defined in RODM, enter the following command:

```
netvasis rodminst NMG_Class
```

Note that NETVASIS is recognized only when it is followed by a command.

Using the OVERRIDE Command with NETVASIS

You can use the OVERRIDE command with NETVASIS to prevent NetView from converting lowercase characters in commands to uppercase. For example, RODM class names are case-sensitive; to call your command list RODMINST that displays a list of network management gateways defined in RODM, enter the following command:

```
OVERRIDE NETVASIS=YES
rodminst NMG_Class
```

Note that when `OVERRIDE NETVASIS=YES` is entered, the ??? at the bottom of the panel is replaced by >>>. `OVERRIDE NETVASIS=YES` remains in effect until `OVERRIDE NETVASIS=NO` is entered.

Suppressing Commands

You might want to keep certain information, such as a password, from being echoed to your screen, being recorded in the NetView log, or being retrieved. You can use a suppression character to do this. A question mark (?) is the default suppression character.

To suppress a command, enter the suppression character immediately before the command name (if you are also using NETVASIS, NETVASIS must precede the suppression character). For example, to dynamically allocate a data set with a password, enter the following command:

```
?allocate dsn(user.init),shr,password(xyz)
```

If the text of one command is embedded in another command, for example with EXCMD, you must enter the suppression character as the first character on the command line or the command buffer, as shown in the following example:

```
?excmd oper1,allocate dsn(user.init),shr,password(xyz)
```

Note: The suppression character must precede the EXCMD command; do not enter the suppression character with the queued command.

The suppression character is defined by the SUPPCHAR statement in CNMSTYLE. To automatically suppress the command echo for a command, you can include ECHO=N on the CMDDEF statement for the command in DSIPARM member CNMCMDU. Command echo suppression works only in the command facility and is not supported in full-screen data mode.

Controlling Message Wrapping

The AUTOWRAP command controls how your terminal displays new messages. You can have the system wait for you to request new messages manually, or you can control how often new messages are displayed on your screen automatically.

To have the system wait for you to request new messages, enter:

```
autowrap no
```

In the response area (next to ???), the following message is displayed:

```
DSI083I AUTOWRAP STOPPED
```

Your screen locks when the message area is full. When you see the asterisks (***) at the bottom of the screen, press either the Clear or Enter key, or enter a command to receive more messages.

To have the system automatically update messages every 5 seconds, enter the following command:

```
autowrap 5
```

In the response area (next to ???), the following message is displayed:

```
DSI082I AUTOWRAP STARTED
```

The `A` in the upper right corner of the screen indicates that AUTOWRAP is being used.

Changing the NetView Screen Layout

You can customize how the following items are presented on the NetView screen:
- Message prefixes
- How much of the screen is to be used for action and held messages
- Default colors for the different classes of messages
- Colors for the command area
- Colors for the different fields on the screen

To define a screen layout, use the system editor to create the DSIPARM member that contains your screen definitions. The NetView program provides a sample member CNMSCNFT that you can use as a model.

To specify a customized screen layout described by DSIPARM member SHIFT01, enter:

```
override scrnfmt=shift01
```

To reset the screen format to the system defaults, enter:

```
override scrnfmt=*
```

To display the screen format currently in effect, enter:

```
list override
```

You can also control message colors and attributes using the NetView automation table.

Topic:	Reference:
Setting up your screen definitions	*IBM Tivoli NetView for z/OS Customization Guide*
Syntax of screen definition statements	*IBM Tivoli NetView for z/OS Administration Reference*
OVERRIDE and LIST commands	NetView online help

Defining Receivers for Alerts and Other MDS-MUs

The NetView product enables a focal point to manage unattended remote sites. The hardware monitor at the focal point processes alerts and other major vectors that it receives in various formats, including:
- Multiple-domain support message units (MDS-MUs)
- Control point management services units (CP-MSUs)
- Network Management Vector Transports (NMVTs)

The generic automation receiver and the hardware monitor submit received MDS-MUs to the NetView automation table for processing.

To enable the generic automation receiver function, follow these steps:

1. If you expect your use of the generic automation receiver to be heavy, change the `RES` specification for the DSINVGRP command definition from `N` to `Y` by adding the following statement to CNMCMDU:

   ```
   CMDDEF.DSINVGRP.RES=Y
   ```
2. If you define operators using an SAF product, define operator DSINVGR.
3. If you define operators in an SAF product, such as RACF, define the IC, MSGRECVR, CTL and other values in the NETVIEW segment of the SAF product as defined in DSIPRF member DSIPRFGR.

4. Define and start the alert receiver autotask, DSINVGR, in CNMSTYLE or its included members.

Refer to the *IBM Tivoli NetView for z/OS Administration Reference* for examples of various operator and autotask definitions.

Deleting Alerts

After NetView alerts have been resolved or are no longer useful, you can use the hardware monitor to remove the alerts from the hardware monitor database and therefore from hardware monitor screens. You can do this from the command facility screen and from the hardware monitor alerts display screens.

To delete a specific alert from the hardware monitor database while viewing the Alerts Static panel, enter the selection number from the hardware monitor screen followed by the DEL function.

To delete all alerts recorded in the hardware monitor database using the command facility screen, follow these steps:

1. Delete all the alerts by resetting the wrap count for alerts:

   ```
   npda sw al 0
   ```

2. Reset the wrap count to its default setting:

   ```
   npda sw al 100
   ```

Topic:	Reference:
SWRAP Command	NetView online help

Using Hardware Monitor Filters

A filter is a method of controlling what data is processed by the hardware monitor. Filters process data that has not been previously suppressed by the NetView automation table.

Overview of Filter Types

The NetView program provides viewing filters and recording filters.

Viewing filters provides a way to see only a subset of alerts while you are using the hardware monitor. Use the SVFILTER command to define the criteria for displaying different alerts on different terminals.

Recording filters control what data is written on the hardware monitor database or forwarded to a hardware monitor focal point. Use the SRFILTER command to define the criteria for recording event and alert data in the database. Recording filters are similar to viewing filters; however, recording filters control all the data (events, statistics, and alerts) while viewing filters affect one operator. When statistics and event records are received by the hardware monitor, the ESREC recording filters determine whether the records are stored in the database. AREC recording filters then determine whether an event record also qualifies as an alert, and is stored in the alert portion of the database. When an alert record is recorded, OPER recording filters determine if messages are issued to a NetView operator task. ROUTE recording filters determine which data is forwarded to a hardware monitor focal point. TECROUTE recording filters determine which data is forwarded to a Tivoli event server.

You can also use the SRF action in the NetView automation table. The advantage of this is that you can be even more specific regarding the conditions under which the recording filter is set.

Strategy for Implementing Filters

The goal of filtering is to prevent alerts that are repetitive or which do not require operator action. You want to provide information an operator can effectively use to identify and resolve system problems.

Use the following steps to implement filters:

1. Disable all filter settings to create and display alerts for all events recorded. One way to do this is with a NetView or REXX command list. For example, issue the **npda dfilter arec** command to list alerts that are written to the hardware monitor database and displayed on the Alerts panels. A panel similar to Figure 127 is displayed:

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/99 11:06:36
NPDA-20A                  * CURRENT FILTER STATUS *          REC 1 TO 15
                          FILTER TYPE: AL RECORDING

SEL# ACTION DATA   ETYPE FTYPE   -------- RESNAME, TYPE, OR ADAPTADR ---
( 1) BLOCK  .....  HELD  TREF    CTRL
( 2) BLOCK  .....  HELD  TREF    LCTL
( 3) PASS   .....  PERM  TREF    CTRL
( 4) PASS   .....  PERF  TREF    CTRL
( 5) PASS   .....  PERM  TREF    LCTL
( 6) PASS   .....  PERF  TREF    LCTL
( 7) BLOCK  .....  ....  TREF    CPU
( 8) BLOCK  .....  HELD
( 9) PASS   .....  PERM
(10) PASS   .....  USER
(11) PASS   .....  NTFY
(12) PASS   .....  INST
(13) PASS   .....  SCUR
(14) PASS   .....  UNKN
(15) PASS   .....  PERF
ENTER SEL# FOLLOWED BY DEL (DELETE)

 ???
CMD==>
```

Figure 127. Alerts Defaults

You can then use the sample REXX command list shown in Figure 128 on page 210 to delete the alert filters listed:

```
/* REXX command list to delete default alert filter settings */
'NPDA SRF AREC DELETE E HELD TREF CTRL'
'NPDA SRF AREC DELETE E HELD TREF LCTL'
'NPDA SRF AREC DELETE E PERM TREF CTRL'
'NPDA SRF AREC DELETE E PERF TREF CTRL'
'NPDA SRF AREC DELETE E PERM TREF LCTL'
'NPDA SRF AREC DELETE E PERF TREF LCTL'
'NPDA SRF AREC DELETE        TREF CPU'
'NPDA SRF AREC DELETE E HELD'
'NPDA SRF AREC DELETE E PERM'
'NPDA SRF AREC DELETE E USER'
'NPDA SRF AREC DELETE E NTFY'
'NPDA SRF AREC DELETE E INST'
'NPDA SRF AREC DELETE E SCUR'
'NPDA SRF AREC DELETE E UNKN'
'NPDA SRF AREC DELETE E PERF'
'NPDA SRF AREC PASS DEFAULT'
EXIT
```

Figure 128. Command List to Delete Alert Filters

Note: The last statement in the command list allows all alerts to flow as a default.

2. Determine which alerts are unnecessary. You have to run your system with the defaults disabled for a period of time before you can gather the data necessary to make your filtering decisions. Ask the following questions for each alert:
   - Does the event need to be recorded or deleted?
   - Does the event need to be made an alert: does it require operator intervention or attention?
   - Can the response be automated?

   Based on these answers, you can:
   - Record the event and create an alert
   - Not record the event
   - Record the event and not make it an alert
   - Add automation to handle the event
   - Forward the event or alert to the hardware monitor focal point

   Note: Each time you create a new filter, review the other filters to ensure that no conflicts with other filter settings exist.
3. Add alerts that are critical. Specific events or alerts that cannot be handled by automation, such as critical network resources or important applications, probably need to be recorded and displayed by the hardware monitor.

Setting Viewing Filters

You can use the hardware monitor SVFILTER command to define your viewing filters for the Alerts panels. The valid filter options are CLEAR, PASS, BLOCK, and DELETE. The CLEAR option is used to remove filters you have set and returns the filter settings to the NetView-supplied defaults.The PASS option is used to display alerts. The BLOCK option is used to block alerts from being displayed. The DELETE option is used to remove filters. For example, to block all alerts for resource T66PLN17 from being displayed, enter:

```
npda svf block n t66pln17
```

Table 13 shows examples of how to set specific viewing filters.

Table 13. Examples of Viewing Filters

To:	Example:
Not display alerts for event type IMR.	`NPDA SVF BLOCK E IMR`
Not display alerts for event type IMR from resource GRETL.	`NPDA SVF BLOCK E IMR N GRETL`
Not display alerts for event type IMR from resource type COMC.	`NPDA SVF BLOCK E IMR T COMC`
Not display alerts for event 04C10.	`NPDA SVF BLOCK C 04C10`
Display alerts for event 04C10 from resource GRETL.	`NPDA SVF PASS C 04C10 N GRETL`
Not display alerts for product ID 5601227 with an alert ID of 6D3EF9A1 from resource GRETL.	`NPDA SVF BLOCK P 5601227 6D3EF9A1 N GRETL`
Start displaying alerts for domain CNM01.	`NPDA SVF CLEAR D CNM01`

Setting Recording Filters

You can use the hardware monitor SRFILTER command to define recording filters. Include the type of action to take on the data. The valid types are CLEAR, PASS, BLOCK, and DELETE. The CLEAR option is used to remove filters you have set and returns the filter settings to the NetView-supplied defaults.The PASS option is used to generate alerts or record events.The BLOCK option is used to block alerts or stop the recording of events. The DELETE option is used to remove filters.

The hardware monitor SRFILTER command can be issued from the command facility screen, and the BLOCK option of the SRFILTER command can be called from either the Alerts Dynamic or Alerts Static panel.

For example, for a given alert displayed on the Alerts Static panel, you can block future creation of alerts for the specific alert code and resource by entering the selection number followed by SRF. To block future creation of alerts for the specific alert code for all resources, enter the selection number followed by SRF ALL.

From the command facility screen, all options of the SRFILTER command are available. For example, to block alert 04C10 for device T66PLN17, enter:

```
npda srf arec block c 04c10 n t66pln17
```

Table 14 shows examples of how to set specific recording filters.

Table 14. Examples of Recording Filters

To:	Example:
Block specific events (identified by the unique codes 04C10 and 05823) from being recorded on the hardware monitor database. Remember that if you block an event, an alert cannot be created.	`NPDA SRF ESREC BLOCK C 04C10` `NPDA SRF ESREC BLOCK C 05823`
Prevent alerts from being recorded as a result of events identified by the unique codes 04C10 and 05823.	`NPDA SRF AREC BLOCK C 04C10` `NPDA SRF AREC BLOCK C 05823`

Table 14. Examples of Recording Filters (continued)

To:	Example:
Block event 04C10 for device T66PLN17.	`NPDA SRF ESREC BLOCK C 04C10 N T66PLN17`
Block alert 04C10 for device T66PLN17.	`NPDA SRF AREC BLOCK C 04C10 N T66PLN17`
Block information-only events (identified by the unique code FFD4C). This filter applies to all devices that send in this event.	`NPDA SRF ESREC BLOCK C FFD4C`
Block all alerts with a specific product ID (5601227) and alert ID (6D3EF9A1) regardless of which device (of the same type) caused the event to occur.	`NPDA SRF AREC BLOCK P 5601227 6D3EF9A1`
Block alerts that contain resources of type COMC, LINE, CTRL, LAN, or CP in the hierarchy resource list.	`NPDA SRF AREC BLOCK T COMC LINE CTRL LAN CP`
Create alerts for the event type IMR for the NCP resource GRETL.	`NPDA SRF AREC PASS E IMR N GRETL`
Generate alerts for the event type of IMPD for a device with adapter address 400047140419.	`NPDA SRF AREC PASS E IMPD A 400047140419`
Block temporary alerts for the NCP called GRETL and for all its attached devices.	`NPDA SRF AREC BLOCK E TEMP NREF GRETL`

Resetting a Filter

Use the CLEAR option to remove filters you have set and return the filter settings to the NetView-supplied defaults. To remove a filter that blocks a specific event (whose unique character code is 04C10), use the following command:

```
npda srf esrec clear c 04c10
```

Diagnosing Filter Performance

The most likely reason a filter is not working as expected is that it might have been negated by another filter. Check your search order and priority. Filter statements are processed in priority order. Priority is determined by how specific a filter is. If two filters of equal priority are encountered, they are processed in the order in which they were entered. You can display the filter statements to see the order that the hardware monitor has established by entering `df arec` from the hardware monitor. This display shows you if the hardware monitor is processing filters in a different order than you expected.

Be sure to check the actions taken in your automation table for possible SRF settings. You can view the automation table using the BROWSE command.

Topic:	Reference:
SVFILTER, SRFILTER, and DFILTER commands	NetView online help
Automation table	*IBM Tivoli NetView for z/OS Automation Guide*
SRF action in the automation table	*IBM Tivoli NetView for z/OS Automation Guide*

Using Session Monitor Filters

A filter is a method of controlling what data is passed to and processed by the session monitor.

Overview of Filter Types

The two basic filter types are filters that control the session awareness data processed by the session monitor and filters that control the data stored on the session monitor database.

Strategy for Implementing Filters

One goal of filtering is to suppress unwanted session awareness data. Ideally this is done as close to the source as possible. You can suppress unwanted session awareness data in VTAM and prevent it from being sent to the session monitor, and you can suppress the processing of the unwanted session awareness data in the session monitor. In either case, you control the suppression on a session-by-session basis.

Another goal of filtering is to prevent storage of session-related data that you are not going to use. You can suppress the storage of session monitor data on the database.

Setting Session Awareness Data Filters in VTAM

VTAM filtering of session awareness data is performed by the ISTMGC10 VTAM filter table. The two statements that define the filtering rules are KCLASS and MAPSESS. In the VTAM table, KCLASS specifies whether or not to pass session awareness data to the session monitor, and MAPSESS specifies which sessions relate to a given KCLASS.

For example, if you want to filter out session awareness data for all LU-LU sessions with terminals whose names begin with T3277, unless those terminals are in session with IMS. In the following example, the VTAM SSCP name is SSCP1:

1. Create the following source statements for VTAM table ISTMGC10:

```
ISTMGS10 KEEPMEM START
NOSAW    KCLASS  SAW=NO
SAW      KCLASS  SAW=YES
M1       MAPSESS KCLASS=SAW,PRI=SSCP1,SEC=*
M2       MAPSESS KCLASS=SAW,PRI=IMS,SEC=*
M3       MAPSESS KCLASS=NOSAW,PRI=*,SEC=T3277*
         KEEPMEM STOP
         END
```

   VTAM examines the session partner names for session awareness data against each of the MAPSESS statements. The first MAPSESS statement that matches determines the KCLASS and therefore the action taken on the data. If no MAPSESS statement matches the session partner names, VTAM defaults to SAW=YES for that data.
2. Assemble and link edit IGCMGC10 into SYS1.VTAMLIB.
3. You can dynamically load or reload session awareness filter table IGCMGC10 from the NetView console by entering:

```
mvs f net,table,type=filter,option=load,newtab=istmgc10
```

Setting Session Awareness Data Filters in the Session Monitor

Using session awareness data filters in the session monitor, you can control both the session awareness data that is processed and the amount of session awareness data that is stored on the session monitor database. You can only filter SSCP-LU and LU-LU sessions. The session monitor filter statements are stored in a DSIPARM member whose name is specified in DSIPARM member AAUPRMLP. The two statements that define the filtering rules are KCLASS and MAPSESS. KCLASS specifies how to process session awareness data, and MAPSESS specifies which sessions relate to a given KCLASS. Using the KCLASS statement, you can control:

- Whether to filter the session awareness data
- Whether to record the session awareness data as session history
- The number of sessions kept on the session monitor database
- The amount of trace data collected

Table 15 shows examples of how to define KCLASS statements and Table 16 shows examples of MAPSESS statements.

Table 15. Examples of KCLASS Statements

To:	Example:
Keep session awareness data and store it on the database, keeping 42 PIUs per session.	`DASDK42 KCLASS SAW=YES,DASD=YES,KEEPPIU=42`
Keep session awareness data in storage only, keeping 10 PIUs per session.	`STORK10 KCLASS SAW=YES,DASD=NO,KEEPPIU=10`
Keep session awareness data and store it on the database if trace or RTM data for the session exists, or if a BIND failure, INIT failure, or abnormal UNBIND occurs, keeping 14 PIUs per session.	`FAILK14 KCLASS SAW=YES,DASD=(DATA,FAILURES),KEEPPIU=14`
Keep session awareness data and store it on the database for a maximum of 500 sessions, keeping 30 PIUs per session.	`DASDK30 KCLASS SAW=YES,DASD=YES,KEEPPIU=30,KEEPSESS=500`

Table 16. Examples of MAPSESS Statements

To:	Example:
Control session awareness data using KCLASS DASDK42 for sessions whose primary session partner is SSCP1 and whose secondary session partner name begins with CDRM.	`M1 MAPSESS KCLASS=DASDK42,PRI=SSCP1,SEC=CDRM*`
Control session awareness data using KCLASS STORK10 for sessions whose primary session partner is SSCP1 and whose secondary session partner name has the characters LU in the fourth and fifth positions.	`M2 MAPSESS KCLASS=STORK10,PRI=SSCP1,SEC=???LU*`
Control session awareness data using KCLASS FAILK14 for sessions whose primary session partner is SSCP1 and whose secondary session partner name begins with CICS.	`M3 MAPSESS KCLASS=FAILK14,PRI=SSCP1,SEC=CICS*`

Table 16. Examples of MAPSESS Statements (continued)

To:	Example:
Control session awareness data using KCLASS DASDK30 for any session that did not match a prior MAPSESS statement.	`M4 MAPSESS KCLASS=DASDK30,PRI=*,SEC=*`

To define the session monitor filters:

1. Specify a valid value for NLDM.KEEPMEM in CNMSTYLE or its included members, for example `FILTER1`.
2. Create DSIPARM member FILTER1, including appropriate KCLASS and MAPSESS statements to define filtering conditions and session awareness data processing policy. Keep in mind that the session monitor searches the MAPSESS statements when a session begins, and determines the session awareness data processing based on the first MAPSESS statement that matches the session partner names. Session awareness can also be filtered by Exit 20, which requires assembler code but allows more flexibility than KCLASS and MAPSESS statements.

Topic:	Reference:
VTAM filter table ISTMGC10	Refer to the *VTAM Library.*

Chapter 13. Managing NetView Data

Focal points are the designated receivers of management data. *Entry points* are the designated senders of management data. The NetView program can act as a focal point or an entry point for the following items:

- Alerts
- Link services
- Operations management data
- Service point command services
- User defined categories

The roles of focal point and entry point can be set from the NetView program. Generally the roles are defined by the sphere of control manager (SOC-MGR) at the focal point through its use of a sphere of control configuration file (DSIPARM member DSI6SCF). The focal point *sphere-of-control* is defined as the set of entry points that have an established relationship with the focal point.

Setting the Primary Focal Point

Use the FOCALPT CHANGE command to establish your system as the focal point for problem management data sent from an entry point. To do this, complete the following steps at the NetView console of the new focal point:

1. To set your system as the focal point to receive operations management data from the entry point CNM02, enter the following command:

   ```
   focalpt change fpcat=ops_mgmt,target=cnm02
   ```

2. To set your system as the focal point to receive alerts from the entry point CNM02, enter the following command:

   ```
   focalpt change fpcat=alert,target=cnm02
   ```

Also use the FOCALPT CHANGE command to establish a backup focal point for problem management data sent from an entry point. To do this, complete the following steps at the NetView console of the primary focal point:

1. To retain your system as the focal point to receive operations management data from the entry point CNM02 and to establish CNM88 as the backup focal point, enter the following command:

   ```
   focalpt change fpcat=ops_mgmt,target=cnm02,backup=cnm88
   ```

2. To retain your system as the focal point to receive alerts from the entry point CNM02, and to establish CNM88 as the backup focal point, enter the following command:

   ```
   focalpt change fpcat=alert,target=cnm02,backup=cnm88
   ```

Changing the Primary Focal Point from an Entry Point

To use the FOCALPT ACQUIRE command to allow the primary focal point to be acquired at the entry point, complete the following steps at the NetView console of the entry point:

1. To name CNM99 as the new primary focal point for operations management data, enter the following command:

   ```
   focalpt acquire fpcat=ops_mgmt,backup=cnm99
   ```

   All existing backup focal points are dropped and the existing primary focal point remains unchanged.

2. To name CNM99 as the new primary focal point for alerts, enter the following command:

   ```
   focalpt acquire fpcat=alert,backup=cnm99
   ```

   All existing backup focal points are dropped and the existing primary focal point remains unchanged.

Changing the Backup Focal Point from an Entry Point

To use the FOCALPT ACQUIRE command to acquire the backup focal point at the entry point, complete the following steps at the NetView console of the entry point:

1. To name CNM99 as the new backup focal point for operations management data, enter the following command:

   ```
   focalpt acquire fpcat=ops_mgmt,backup=cnm99
   ```

   Existing backup focal points are dropped and the existing primary focal point remains unchanged.
2. To name CNM99 as the new backup focal point for alerts, enter the following command:

   ```
   focalpt acquire fpcat=alert,backup=cnm99
   ```

   Existing backup focal points are dropped and the existing primary focal point remains unchanged.

Displaying the Primary and Backup Focal Points

You can use the FOCALPT QUERY command to display the primary and backup focal points for an entry point. To do this, at the NetView console of the entry point, enter the following command:

```
focalpt query fpcat=ops_mgmt
```

This command displays the primary focal point and the list of backup focal points for this entry point.

Displaying the Sphere of Control for a Focal Point

You can use the FOCALPT DISPSOC command to display all the entry points in the sphere of control for a focal point. To do this, at the NetView console of the focal point, enter the following command:

```
focalpt dispsoc fpcat=alert,target=*,active
```

This command displays active entry points that are to forward alerts to this focal point.

Removing an Entry Point from the Focal Point Sphere of Control

You can use the FOCALPT DELETE command to remove an entry point from the sphere of control of the focal point. To do this, at the NetView console of the focal point, enter the following command:

```
focalpt delete fpcat=alert,target=cnm03
```

This command removes CNM03 from the sphere of control of the focal point.

Note: The entry point is not actually removed until either the session with the entry point ends or the entry point issues a FOCALPT DROP command.

Refreshing the Focal Point Sphere of Control

You can use the FOCALPT REFRESH command to refresh the sphere of control of the focal point to the state defined in the sphere of control configuration file. To do this, at the NetView console of the focal point, enter the following command:

```
focalpt refresh
```

This command reads the sphere of control configuration file and issues FOCALPT CHANGE commands to each entry point to establish a sphere of control as specified.

Topic:	Reference:
FOCALPT commands	NetView online help
Setting up focal points	*IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*

Controlling the Processing of Problem Management Data

NetView receives problem management data in the form of SNA alerts or other forms such as RECFMS. These alerts originate in the network or in the same host as the NetView program. Alerts that originate in the network are forwarded to NetView through the communications network management interface (CNMI), or other interfaces such as LU 6.2. Alerts that originate in the same host as the NetView program arrive through the program-to-program interface (PPI) or other interfaces such as the GENALERT command. Regardless of the source of the alert, it passes through several filters that decide which alerts are presented to the operator, which alerts are saved in the hardware monitor database, and which are discarded.

Generating Alerts Using GENALERT

You can use the GENALERT command to specify the information contained in an alert which is then processed by the NetView program. The alert sent by the GENALERT command can be one of the following types:

- Generic
- Nongeneric
- RECFMS

The default format is a generic alert format.

Generating Alerts Using the PPI

You can use the PPI to send an alert from any address space on the same host as the NetView program. For example, a program encounters an out of storage condition and needs to notify an operator to initiate a recovery procedure. To do this, the program needs to take the following actions:

1. Generate an NMVT that contains alert information such as software alert, out-of-storage condition, and initiate recovery procedure.
2. Build a data transport request buffer which references the NMVT.
3. Query the status of the PPI to ensure that it is active.
4. Start the PPI to send the NMVT to the NetView program.

An example of this scenario is in CNMSAMP member CNMS4227 (PL/I).

Setting Error Thresholds for Alerts

Whenever statistics are reported to the hardware monitor, the error counters and traffic counters are compared to determine the current error-to-traffic ratio. If this ratio exceeds the threshold set by your system programmer, the statistic becomes an alert, unless blocked by an alert recording filter.

For a specified resource, you can use the SRATIO command to change the threshold value that generates an alert. For example, to change the threshold value for PU08 to 2.0 per cent, enter the following command:

```
sratio 020 n pu08
```

Topic:	Reference:
GENALERT command	NetView online help
SRATIO command	NetView online help
Filtering	"Overview of Filter Types" on page 208
Alert types	"Chapter 9" in *SNA Formats*
Sending alerts using the PPI	*IBM Tivoli NetView for z/OS Application Programmer's Guide*

Using and Maintaining the Network Log

The network log is the record of the terminal activity that has occurred on the system. You can send commands, responses, and messages to the network log. Each message contains the time and date it was sent and the names of the operator and system it came from.

You can filter the information on an operator's screen using the network log browse installation exit DSIEX18. Note that with TME 10™ NetView release 1 and later, the BLOG command is available to accomplish this without requiring DSIEX18.

You can print the inactive network log file in batch mode, while the system is using the active file as the log.

Displaying the Network Log

You can use the BROWSE command to display a particular network log data set. You can select the active or inactive log, or you can name the specific log (primary or secondary) to browse. For example, to display the active log, enter the following command:

```
browse netloga
```

You can also specify a time and date range to limit the amount of network log information displayed. For example, to display the primary network log from 1:00 p.m. on 4/07/99 to 8:30 a.m. on 4/08/99, enter the following command:

```
browse netlogp from 4/07/99 13:00 to 4/08/99 8:30
```

Note: If you specify a time range for browsing the network log, the first and the last record of the specified time range remains the first and the last record during the entire browse.

You can use the FIND or ALL commands to locate specific information while you are browsing the network log. For example, to find the words INVALID COMMAND, enter the following command:

```
f 'invalid command'
```

Log Browse Filtering

The BLOG command activates the network log browse facility based on filters. You can select which records to display using any combination of the following filters:

- Select a local or remote NetView. The default is the local NetView system. Changing the NetView domain, netid, or operid fields can result in browsing a remote NetView log.
- Select the NETLOGA, NETLOGI, NETLOGS, or NETLOGP log.
- Select the starting display column.
- Select the operator ID for which records were logged.
- Select the origin domain of records that were logged.
- Select the message identifier of messages that were logged.
- Select the starting time and date for records that were logged.
- Select the ending time and date for records that were logged.
- Select a character string to be matched with the text of a message that was logged.

For example, you might decide to browse all records on a remote NetView NTVF1 logged by operator AUTO1 between noon and midnight on August 5, 1999.

Figure 129 is an example of the log browse interface:

```
CNMKBLIP               NetView Log Browse                     08/10/99

Display NetView log records for:

 NetView Domain  ===> NTVF1         ( NetView Netid ===> *     )
                                    ( RMTCMD Operid ===> *     )

 NetView Log     ===> NETLOGA

Selection Criteria:

 Display Column  ===> 017

 From:  Time     ===> 12:00         ( Date ===>  08/05/99 )
 To:    Time     ===> 24:00         ( Date ===>  08/05/99 )

 Operator ID     ===> AUTO1         ( The * and ? wildcards can be used )
 Domain id       ===>               ( anywhere in this group of fields. )
 Message id      ===>
 Message text    ===>



TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
CMD==>
```

Figure 129. Example of a BLOG Input Panel

The following list describes BLOG input fields:

NetView Domain
Specifies the NetView domain where the network log to be browsed resides. The default value is the local NetView domain; you can change this value to another NetView domain to activate remote netlog browse.

The value of this field is used on the LU parameter of the BROWSE command when a remote browse is necessary.

NetView Netid
Specifies the NetView netid name where the network log to be browsed resides. The default value is an asterisk. The value of this field is used on the NETID parameter of the BROWSE command when remote browse is necessary.

RMTCMD Operid
Specifies the RMTCMD autotask used for a remote browse display. The value of this field is used on the OPERID parameter of the BROWSE command when a remote browse is necessary.

NetView Log
Indicates one of the following logs:

NETLOGA The active network log

NETLOGI The inactive network log

NETLOGP The primary network log

NETLOGS The secondary network log

Display column
Indicates the starting display column for the browse display. This value is used on the STARTCOL parameter of the OVERRIDE command to set the display column when entering browse.

From Time
Indicates the starting time for the netlog display. This value corresponds to the FROM parameter of the BROWSE command for specifying time. The format for entering the time follows the format set in your environment.

From Date
Indicates the starting date for the netlog display. This value corresponds to the FROM parameter of the BROWSE command for specifying date. The format for entering the date follows the format set in your environment.

To Time
Indicates the ending time for the netlog display. This value corresponds to the TO parameter of the BROWSE command for specifying time. The format for entering the time follows the format set in your environment.

To Date
Indicates the ending date for the netlog display. This value corresponds to the TO parameter of the BROWSE command for specifying date. The format for entering the date follows the format set in your environment.

Operator ID
Indicates the operator ID that is to be matched with log records for display. This value corresponds to the *oper_id* parameter of the BLOG command. You can use the * and ? characters as wildcard characters anywhere in this specification. The * matches zero or more characters and the ? matches exactly one character.

Domain id
Indicates the domain ID that is to be matched with log records for display. This value corresponds to the *domain_id* parameter of the BLOG command. You can use the * and ? characters as wildcard characters anywhere in this specification. The * matches zero or more characters and the ? matches exactly one character.

Message id
Indicates the message ID that is to be matched with log records for display. This value corresponds to the *msg_id* parameter of the BLOG command. You can use the * and ? characters as wildcard characters anywhere in this specification. The * matches zero or more characters and the ? matches exactly one character.

Message text
Indicates the message text that is to be matched with log records for display. This value corresponds to the *msg_id* parameter of the BLOG command. You can use the * and ? characters as wildcard characters anywhere in this specification. The * matches zero or more characters and the ? matches exactly one character.

Note that browse filters are not case-sensitive.

Switching the Network Log

You can use the LIST command to determine which network log is active, then use the SWITCH command to change the active network log. Typically, NetView automatically switches to the inactive log when the active log fills up.

To display which network log is active, enter the following command:

```
list dsilog
```

To switch to the secondary network log, enter the following command:

```
switch dsilog,s
```

Using Browse

If the BROWSE screen defaults are set to display a scroll field, as shown in the following example, entering a number on the command line before pressing a PF key for BACK or FORWARD has an effect only the next time a PF key is pressed.

```
 NETVIEW.BRWS ------ BROWSE CNMKEYS  (DSIOPEN ) --- LINE 00000 TO 00036 OF 00165
                                                          SCROLL ==> CSR
----+----1----+----2----+----3----+----4----+----5----+----6----+----7----+----
```

You can enter a new value for the SCROLL field to change the effect of the BACK and FORWARD PF keys.

If your SCROLL field is not displayed on the BROWSE screens, entering a value on the command line changes the number of lines scrolled by the BACK and FORWARD PF keys. You can change whether the BROWSE screens have a SCROLL field using `OVERRIDE SCROLL=OFF`. For more information about the effects of the OVERRIDE command, refer to the NetView online help.

Topic:	Reference:
Setting up the network log	*IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*
Filtering the log display using the log browse installation exit DSIEX18	*IBM Tivoli NetView for z/OS Programming: Assembler*
Printing the network log (DSIPRT)	*IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*
Message formats	Appendix A, “Message Format,” on page 341
BROWSE and FIND commands	NetView online help

Creating and Displaying NetView Trace Data

The NetView program provides facilities for tracing internal events which you can use for solving problems. The command facility can create trace records in storage, on an external data set, or to be handled by the MVS Generalized Trace Facility (GTF). The session monitor can trace session awareness data (SAW) and path information unit data (PIU). The program-to-program interface (PPI) can create trace records in storage or to be handled by MVS GTF.

Creating and Displaying Command Facility Trace Data

The command facility trace can record dispatching, queuing of buffers, presentation services, module entry and exit, getting and freeing of storage, and installation exit calls for one or more types of tasks. For example, to start tracing module entry and exit including installation exits for operator station tasks (OSTs) and record the trace information on an external data set, perform the following steps:

1. Start the DSITRACE task:
   ```
   nccf start task=dsitrace
   ```
2. Start the command facility trace:
   ```
   nccf trace on,option=(mod,uexit),mode=ext,task=ost
   ```
3. Verify trace settings:
   ```
   nccf list trace
   ```
4. To stop the trace, enter the following command:
   ```
   nccf trace end
   ```
5. Stop the DSITRACE task:
   ```
   stop task=dsitrace
   ```
6. To print the trace data, use the command facility utility program DSIPRT. An example of the job to start this utility is located in member CNMPRT of the CNMSAMP data set.

Topic:	Reference:
Setting up the command facility trace log	*IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*
Command facility LIST, START, STOP, and TRACE commands	NetView online help
Reading the command facility trace data	"Diagnostic Tools for the NetView Program" in *IBM Tivoli NetView for z/OS Troubleshooting Guide*

Creating and Displaying Session Monitor Trace Data

The session monitor trace can record SAW or PIU data. For example, to trace complete PIUs for logical unit (LU) TERM1 in domain CNM01, network NETA, perform the following steps:

1. To start the session monitor trace from the command facility, enter the following command:
   ```
   nldm trace start cpiu term1
   ```
2. To stop the trace, enter the following command:
   ```
   nldm trace stop cpiu term1
   ```
3. To display, see "Typical LU-LU Session for an SNA Subarea Network" on page 94.

Topic:	Reference:
Session monitor TRACE command	NetView online help

Creating and Displaying PPI Trace Data

The PPI can record buffers destined for one or all receivers. For example, to trace buffers destined for receiver TASK1, and send the data to MVS GTF, perform the following steps:

1. Start the MVS GTF task from the command facility. Set GTF up to trace to an external data set, and to trace USR events of class X'5EF'. To start GTF from the command facility, enter the following command:

   ```
   mvs s gtf.gtf
   ```

2. Start the PPI trace for SSI task NETVSSI from the command facility. Enter the following command:

   ```
   mvs f netvssi,traceppi on rcvrid=task1
   ```

3. To stop the trace, enter the following command:

   ```
   mvs f netvssi,traceppi end
   ```

4. Stop the MVS GTF task from the command facility:

   ```
   mvs p gtf
   ```

5. To display the trace data, use IPCS and the NetView sample CNMS4501 to format the PPI trace records.

Topic:	Reference:
Using GTF to collect PPI trace data	*IBM Tivoli NetView for z/OS Application Programmer's Guide*
MVS START and STOP commands	*MVS/ESA System Commands*
TRACEPPI command	NetView online help
Displaying the trace data	*MVS/ESA Diagnosis: Using Dumps and Traces*

Maintaining the Hardware Monitor Database

The hardware monitor database contains history records which summarize cumulative information regarding a specific device, and detail records which contain detail information regarding one error incident. The database also contains cross-reference records which correlate specific resources with specific configuration hierarchies in the network.

While only one physical hardware monitor database exists, it is divided into four logical databases containing history and detail records:

- Alerts
- Events
- Statistics
- GMFALERTs

Switching Primary and Secondary Databases

If the active database is either near full as determined by the LISTCAT command or full as noted by message BNJ022I, you can use the DBAUTO command to switch from the active to the inactive hardware monitor database. For example, enter the following command:

```
dbauto npda,switch
```

Controlling the Amount of Data Retained in the Hardware Monitor Database

You can control the number of event or statistical records to be retained for a specific resource or the total number of alert records to be retained on the hardware monitor database.

For example, to retain a maximum of 500 alerts for all resources, enter the following from the command facility:

```
npda swrap al 500
```

Also, to retain a maximum of 100 events for resource RES1, enter the following from the command facility:

```
npda swrap ev 100 n res1
```

Removing Unwanted Data from the Hardware Monitor Database

When you no longer need certain data in the database (for example, older than a certain date), you can remove this data using the DBAUTO command. For example, to remove data older than 60 days, enter the following command:

```
dbauto npda,purge,60
```

To reclaim the space used by the purged records, reorganize the database. To do this, enter the following command:

```
dbauto npda,reorg
```

Note: If the default is not what you want, you can also specify primary and secondary space allocation.

To delete all data in the database, enter the following command:

```
dbauto npda,clear
```

If you use the CLEAR option, it is not necessary to reorganize the database.

You can automate the process of maintaining the database by using the automation table.

Collecting Hardware Monitor Data in an SMF Data Set

You can enter the REPORTS command from the NetView console to start data collection to the system management facilities (SMF) log. However, when you use this command all the hardware monitor alerts is recorded. You cannot select which alerts are logged.

To start alert recording, enter the following command:

```
npda reports on
```

Topic:	Reference:
Setting up the hardware monitor database	*IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*

Topic:	Reference:
Maintaining the hardware monitor database through automation	Refer to *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*
Using SMF logs	Refer to *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.
REPORTS and SWRAP commands	NetView online help
Processing SMF data	*Service Level Reporter Version 3 Release 3 Command and Macro Reference*

Using and Maintaining the 4700 Support Facility Database

The 4700 Support Facility database contains data specific to the 4700 Finance Communication System. This data consists of:

- Performance data for the 4700 controllers
- Operational status of loops attached to the 4700 controllers

The database includes master records that contain cumulative summary information, detail records that contain statistical information, and cross-reference records that correlate controller names with the loops attached to them.

Switching Primary and Secondary Databases

If the active database is either near full as determined by the LISTCAT command or full as noted by message BNJ022I, you can use the DBAUTO command to switch to the inactive 4700 support facility database. For example, enter the following command:

```
dbauto tara,switch
```

Removing Unwanted Data from the 4700 Support Facility Database

If you need to clear the 4700 support facility database, you can use the DBAUTO command. The database must be inactive before it can be cleared. For example, to clear the inactive database, enter the following command:

```
dbauto tara,clear
```

You can automate the process of maintaining the database by using the automation table.

Reorganizing the 4700 Support Facility Database

When you have determined using the LISTCAT command that the index level is higher than 3, you can reorganize the database to reclaim the space or improve performance of the database respectively. To do this, enter the following command:

```
dbauto tara,reorg
```

Note: Specify primary and secondary space allocation if the default is not appropriate.

Topic:	Reference:
Setting up the 4700 support facility database	*IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*

Topic:	Reference:
Maintaining the 4700 support facility database through automation	Refer to *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*
DBAUTO and LISTCAT commands	NetView online help

Using and Maintaining the Session Monitor Database

The session monitor collects data about same-domain, cross-domain, and cross-network SNA (subarea and Advanced Peer-to-Peer Networking) sessions, and maintains the collected data on a session basis. To collect data for cross-domain sessions, a session monitor must be available in each domain. To collect data for cross-network sessions, a session monitor must be available in each gateway host on the session path and at the session end points.

The session monitor collects the following types of data:
- Session awareness data
- Session trace data
- Session response time data
- Route data
- Network accounting and availability measurement data

The data is stored in memory and at session end is written to the VSAM database.

Switching Primary and Secondary Logs

If the active log is either near full as determined by the LISTCAT command or full as noted by messages AAU022I and AAU272I, you can use the DBAUTO command list to switch to the inactive session monitor database. For example, enter the following command:

```
dbauto nldm,switch
```

Removing Unwanted Data from the Session Monitor Log

When you no longer need certain data in the log (for example older than a certain date), you can remove this data using the DBAUTO command. For example to remove data older than 60 days, enter the following command:

```
dbauto nldm,purge,60
```

To reclaim the space used by the purged records, reorganize the log. To do this, enter the following command:

```
dbauto nldm,reorg
```

To delete all data in the log, enter the following command:

```
dbauto nldm,clear
```

If you use the CLEAR option, it is not necessary to reorganize the log.

You can automate the process of maintaining the database by using the automation table.

Collecting Session Monitor Data in an SMF Data Set

You can enter the RECORD command from the NetView console to write accounting and resource statistics or storage and processor utilization data to the SMF data set.

To write accounting and resource statistics to the external log for sessions between primary session partner PRIMLU1 and secondary session partner SECLU2 enter the following command:

```
nldm record sesstats primlu1 seclu2
```

To write storage and processor utilization data to the external log enter the following command:

```
nldm record strgdata
```

Topic:	Reference:
Setting up the session monitor log	*IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*
Maintaining the session monitor log through automation	Refer to *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*
DBAUTO, LISTCAT, and RECORD commands	NetView online help
Using Session Monitor filters	"Using Session Monitor Filters" on page 213

Maintaining the Save/Restore Database

The save/restore databases are two VSAM databases used to save and restore global variables and timed events. The primary database is defined by DSISVRTP and the secondary database is defined by DSISVRTS.

Switching Primary and Secondary Databases

If the active database is full as determined by the LISTCAT command, you can use the DBAUTO command to switch to the inactive database. For example, enter the following command:

```
dbauto save,switch
```

Removing Unwanted Data from the Save/Restore Database

To clear the Save/Restore database, you can use the DBAUTO command. The database must be inactive before it can be cleared. For example, enter the following command:

```
dbauto save,clear
```

Reorganizing the Save/Restore Database

When you have determined using the LISTCAT command that the index level is higher than 3, you can reorganize the inactive database to reclaim the space or improve performance of the database respectively. To do this, enter the following command:

```
dbauto save,reorg
```

Note: You might also want to specify primary and secondary space allocation if the default is not what you want.

Topic:	Reference:
Setting up the save/restore data set	*IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*
DBAUTO and LISTCAT commands	NetView online help

Using the MVS System Log (SYSLOG)

MVS maintains a log of messages, commands, and responses. This includes commands sent by NetView using the MVS subsystem interface (SSI) and MVS extended consoles. MVS/JES makes the contents of the log available for printing either when the size of the log reaches its defined maximum size or the operator issues the MVS WRITELOG command.

You can use the NetView automation table to log messages to the MVS system log.

Using and Maintaining the RODM Log

The RODM log contains log types 0–10. You can use the data contained in these logs to assist in problem determination and diagnosis. For example, you can use log record types 9 and 10 for method debugging.

User-supplied information can be written to the RODM log through the Output to Log method application program interface (MAPI) function. You can customize member EKGCUST to specify which log records to write to the RODM log, or you can start a MAPI call from a RODM method to write records to the RODM log.

Switching the Primary and Secondary RODM Logs

You can switch the primary log to the secondary log. You might want to do this if you need to format the active log to review the information contained on the log. To do this, complete the following steps:

1. From the NetView console, issue the MVS modify command to write any existing internal buffers to the active log:

   ```
   f ekgxrodm,logf
   ```

   Where EKGXRODM is the RODM startup procedure.
2. Determine which RODM log is active (primary or secondary)

   ```
   f ekgxrodm,logq
   ```
3. Make the inactive log the active log:

   ```
   f ekgxrodm,logs
   ```

   Where LOGS is the name of the newly active log.

Formatting the RODM log

You can use the RODM log formatter to format the inactive RODM log. You can start the RODM log formatter using a submit JCL, EKGRLOG. A sample job is found in member EKGRLOG of the CNMSAMP data set. The SYSPRINT data set contains the formatted log.

Topic:	Reference:
Setting up the RODM log	*IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*

Topic:	Reference:
Calling a MAPI call from a RODM method to write records to the RODM log	*IBM Tivoli NetView for z/OS Resource Object Data Manager and GMFHS Programmer's Guide*
Customizing member EKGCUST	*IBM Tivoli NetView for z/OS Administration Reference*
Using the RODM log formatter for problem diagnosis	*IBM Tivoli NetView for z/OS Troubleshooting Guide*

Copying the Contents of RODM to a Checkpoint Data Set

The RODM data cache resides in memory. This means that in the event of a system failure, the data in the cache is lost. For this reason, RODM provides a checkpoint capability that you can use to copy the contents of the RODM data cache to a checkpoint data set. You can also load the data cache during RODM initialization from a checkpoint data set. Therefore, you need to checkpoint the contents of the RODM data cache either periodically or when you make a significant update to the data in the cache.

To copy the contents of RODM to a checkpoint data set, perform the following steps:

From the NetView console, enter the following command:

```
mvs f ekgxrodm,chkpt
```

This command causes RODM to checkpoint to the next available checkpoint data set. EKGXRODM is the RODM startup procedure. Message EKG1303I is displayed when the checkpoint is complete.

Note: Before starting RODM, specify one or more checkpoint data sets in the RODM procedure.

Topic:	Reference:
Setting up the RODM checkpoint data set	*IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*
MVS command	NetView online help

Part 4. Automating the Network or System

Chapter 14. Using the NetView Automation Table

Automating the network and system consists of developing procedures which respond to specific events. Development of an automated procedure requires you to understand how to detect the condition to which you want to respond automatically, and what action the automatic response includes. You can then use a combination of the NetView automation table and RODM to correlate events and their automated responses. You have the flexibility of using the automation table and RODM together or each can be used separately. These automated responses can include the calling of a command list or command processor using an automation task.

You can also schedule commands at periodic intervals or specific times. This is helpful for maintaining status information about your environment for automation. You can also perform routine operations automatically.

The NetView automation table provides a way to examine and separate data, and then take actions in response. It enables the following actions:

- Processing system, subsystem, application, and network messages
- Scanning for any errors or indicators of significant events in the network
- Collecting status information by analyzing messages
- Examining network management service units (MSUs) for errors or significant events in the network. An *MSU* is a data structure, such as an alert major vector X'0000' contained within a Network management vector transport (NMVT) that carries management services data that the NetView program uses to manage the system or network. Many IBM and non-IBM products send data to the NetView program in the form of MSUs. You can also create your own MSUs.

  NetView automation processes the following MSU types:

  – Network management vector transports (NMVT), including alerts, resolutions, link configuration data, link events, and problem determination statistics
  – Control point management services units (CP-MSU)
  – Multiple domain support message units (MDS-MU), which usually contains a CP-MSU
  – Record maintenance statistics (RECMS)
  – Record formatted maintenance statistics (RECFMS)

Use the generic automation receiver function of the NetView program to send data from your application to the NetView program without having to provide your own receiving application. The data must be in the form of a multiple domain support message unit (MDS-MU). The generic automation receiver presents the received data to the NetView automation table. For more information about the generic automation receiver, refer to the *IBM Tivoli NetView for z/OS Customization Guide*.

Automation Table and Alerts

You can use the SRFILTER and PDFILTER commands to change recording filters. The PDFILTER command list is called from a statement in the sample NetView automation table (DSITBL01) when the NetView BNJDSERV task completes initialization. You can customize the PDFILTER command list by using NPDA.PDFILTER statements in sample CNMSTYLE.

Usually, you set the AREC (alert recording) filters to cause the hardware monitor to send alerts for any high-priority problem records that require immediate attention. The following types of data can become hardware monitor alerts:

- Alert major vectors carried to the hardware monitor in MSUs
- System-format alert records, such as OBR, MCH, CWR, and SLH records, received from local MVS or VM devices

Many of the records that the hardware monitor receives go to the automation table during the course of typical processing. There, you can have the automation table change filtering and highlighting attributes or issue automatic responses. The hardware monitor sends only the following major vectors:

- Alerts, key X'0000'
- Link events, key X'0001'
- Resolutions, key X'0002'
- Problem determination statistics, key X'0025'
- Record maintenance statistics (RECMS), key X'1044'
- Record formatter maintenance statistics (RECFMS), key X'1045'
- Link configuration data, key X'1332'

Automate most messages and MSUs so that only the few situations requiring operator action are forwarded to an operator.

Setting Network and System Security

If you are using a system authorization facility security product (SAF) , such as Resource Access Control Facility (RACF), work with your security administrator to determine appropriate command and data set security so network and system programmers can work with the automation table:

- Restrict unauthorized viewing or altering of automation table statements.
- Enable modification of automation table statements.
- Enable creation of usage reports using the AUTOCNT command.
- Restrict access to use of the LISTING keyword of the AUTOTBL command.

Your security administrator can define data set security and protect the AUTOTBL and AUTOCNT commands and their keywords using command security.

Topic:	**Reference:**
Using the AUTOTBL and AUTOCNT commands	NetView online help
Protecting data sets	*IBM Tivoli NetView for z/OS Security Reference*
Protecting commands and keywords	*IBM Tivoli NetView for z/OS Security Reference*
Planning security for automation	*IBM Tivoli NetView for z/OS Security Reference*

Planning Message or MSU Automation

This comparison of automating messages and MSUs shows the steps necessary before updating an automation table. For information about adding statements to the automation table, see the *IBM Tivoli NetView for z/OS Automation Guide*.

Table 17. Planning Message and MSU Automation

If you are automating a message:	If you are automating an MSU:
Obtain a copy of the actual message (using network or system logs).	Look at the contents of the MSU (using the hardware monitor).
Obtain the ID of the message.	Get the major vector of the MSU.
Identify any specific message instances that you wish to automate (such as from a particular domain, network device, or application).	Identify any specific MSU instances that you want to automate (such as from a particular domain, network device, or application).
If the message is issued for several purposes, specify the purpose for which the message is to be automated. Specify the particular message text position or message token that contains the information, such as the message number or message text.	If the MSU is issued for several purposes, specify the purpose for which the MSU is to be automated. Each MSU can be identified using some part of the MSU, such as a particular subvector or subfield.
Identify what actions need to be performed when the message is processed by NetView automation. You might want to suppress the message from display, change the coloring or other highlight attributes, suppress it from logging, process a command or command list, or route it to a particular operator or group of operators.	Identify the actions to be performed when the MSU is processed by NetView automation. You might want to block the MSU from recording and being displayed, change the coloring or other highlight attributes, or process a command or command list.

Browsing the Automation Tables

You can browse your automation tables using the NetView BROWSE command. For example, if your automation table is named AUTOTAB2, enter the following command:

```
browse autotab2
```

Notice that all the automation table statements are displayed, including those which are in embedded members.

The automation tables are located in the DSIPARM library.

You can analyze the existing statements in the automation table with the NetView AUTOCNT command, as described in"Analyzing Automation Table Usage" on page 239.

You can create a listing of an automation table using the NetView AUTOTBL command. This listing is placed in a member of the first data set defined by the DSILIST DD statement. You might want to do this before you design your changes to the automation table. For example, if your automation table is named AUTOTAB2, enter:

```
autotbl autotab2,listing=autolist,test
```

This places a listing of this automation table including all embedded members in the AUTOLIST member of the DSILIST data set. If the AUTOLIST member already exists, the existing list is not replaced unless you use the REPLACE parameter on AUTOTBL.

Testing an Automation Table

To test the automation table:

1. Use the AUTOTBL command with the TEST and MEMBER keywords, to verify that the syntax of the statements is correct. For example, to test DSIPARM member DSITBL01 without activating it and to generate an automation table listing to EXLIST, enter:

   ```
   autotbl member=dsitbl01 test listing=exlist
   ```

2. Use the TRACE action on an IF-THEN statement to trace the processing of a message or MSU through the automation table. Detailed trace information is displayed by message BNH370I for each part of the automation table statement that analyzes the AIFR. The following example shows an automation statement with a TRACE action:

   ```
   IF (LABEL: STATEMENT1) TEXT = 'WAC' . THEN
    TRACE('TRCTAG01');
   ```

   When a message whose text begins with the characters WAC is processed by the automation table statement, message BNH370 is generated and includes the trace results.

3. Use the AUTOTEST command to test the automation table. Specify the LISTING keyword, to generate an automation table listing, and the REPORT keyword, to generate a listing of the commands that have been run. For example, to test the DSIPARM member DSITBL01, generating an automation table listing to EXLIST and a report to TESTRPT, enter the following command:

   ```
   autotest member=dsitbl01 listing=exlist report=testrpt source=parallel
   ```

   This command tests the automation table DSITBL01 in parallel with the active automation table.

4. Use the following AUTOTEST command with the STATUS keyword to verify that testing is still active:

   ```
   autotest status
   ```

5. Use one of the following AUTOTEST commands to end the test:

   ```
   autotest off
   autotest source=off
   ```

6. Browse the report by entering the following command:

   ```
   browse testrpt
   ```

Activating an Automation Table

To activate the automation table:

1. Verify that the syntax of the automation table statements is correct by using the AUTOTBL command with the TEST and MEMBER keywords. For example, to test DSIPARM member DSITBL01 without activating it and to generate an automation table listing to EXLIST, enter:

   ```
   autotbl member=dsitbl01 test listing=exlist
   ```

   The following example shows how a syntax error is displayed in the listing:

   ```
   0011 001 IF BADFUNC = 'INFO' THEN DISPLAY(N);
   ERROR    CNM505E INVALID FUNCTION NAME "BADFUNC" SPECIFIED IN
               CONDITIONAL
   ```

2. Activate the automation table by using the AUTOTBL command without the TEST keyword. Specify the LISTING keyword to generate an automation table listing. For example, to activate the DSIPARM member DSITBL01 and to generate an automation table listing to EXLIST, enter:

   ```
   autotbl member=dsitbl01 listing=exlist replace
   ```

   When activated successfully, two messages are displayed: message DWO044 indicating that the listing was successfully generated, and message DSI410 indicating that the table is active.
3. To add another DSIPARM member to the list of active automation tables, specify where in the list the new member is to be inserted. For example, to insert member DSITBL99 as the second member in the list of active automation table members, enter:

   ```
   autotbl member=dsitbl99 at=2
   ```
4. To ensure that a specific DSIPARM member is always the first or last table within the list of automation tables, you can use the FIRST or LAST keyword on the AUTOTBL command. For example, to ensure that DSITBL99 is always the last table, enter:

   ```
   autotbl member=dsitbl99 insert last
   ```
5. To verify the automation table is still active, use the AUTOTBL command with the STATUS keyword.

   ```
   autotbl status
   ```

Enabling and Disabling Sections of an Automation Table

You can enable or disable sections of the automation table using the AUTOTBL command. These sections can be selected statements or groups of statements.

If a block of automation table statements in member DSITBL01 are identified by LABEL=VTAM and ENDLABEL=VTAM, you can enter the following statements:

```
IF LABEL:VTAM MSGID = 'IST051A"
   THEN EXEC (CMD('CLISTA') ROUTE (ONE * OPER1));
IF MSGID = 'IST052A"
   THEN EXEC (CMD('CLISTB') ROUTE (ONE * OPER1));
IF ENDLABEL:VTAM MSGID = 'IST053A"
   THEN EXEC (CMD('CLISTC') ROUTE (ONE * OPER1));
```

To disable this block of automation table statements, enter the following command:

```
autotbl member=dsitbl01 disable block=vtam
```

If, instead, you want to enable the single automation table statement identified by LABEL=VTAM (and not the entire block of statements), enter the following command:

```
autotbl member=dsitbl01 enable label=vtam
```

You can also enable or disable automation table statements with the AUTOMAN command. See the *IBM Tivoli NetView for z/OS Automated Operations Network User's Guide* for more information.

Analyzing Automation Table Usage

You can use an automation table report to analyze how your automation table is functioning in the following ways:

- To determine whether any statements need to be moved to improve performance
- To assess the automation workload

- To compare historical statistics for capacity planning and system stress analysis
- To locate statements that are not supposed to match messages or MSUs but do match
- To recognize statements that are supposed match but do not match
- To verify new condition items before adding corresponding actions
- To determine the impact of changes made to the system or network automation table

Use the AUTOCNT command to generate usage reports, which can be summary, detailed, or both. Each type of report can include message statements, MSU statements, or both. Because the output can be lengthy, especially for detailed reports, you can use the FILE option to send the output to a file. You can also generate the report from a command list and process the information automatically.

Automation Table Detail Usage Report

To generate a detailed usage report, enter the following command:

```
autocnt stats=detail report=both file=report
```

| See Figure 130 and Figure 131.

```
- DWO800I AUTOMATION TABLE MSG DETAIL REPORT BY OPER1

DWO803I ------------( AUTOSEG1 MESSAGE DETAILS  04/12/99 14:32:42 )------------
DWO805I                                                    |-- PERCENTAGES --|
DWO806I STMT   SEQ      MEMBER    COMPARE    MATCH  E  C  A MATCH/ COMP/ MATCH/
DWO807I NUMBER NUMBER   NAME      COUNT      COUNT  C  I  I COMP   TOTAL TOTAL
DWO808I ---------------------------------------------------------------------
DWO809I 00001  00000800 AUTOSEG1     2304      798          34.6  100.0  34.6
DWO809I 00002  00001000 AUTOSEG1      798      177          22.2   34.6   7.7
DWO809I 00003  00001400 AUTOSEG1      621        9  1         1.4   27.0   0.4
DWO809I 00004  00001600 AUTOSEG1      612        0  1         0.0   26.6   0.0
DWO809I 00005  00002000 AUTOSEG1      612      612        X 100.0   26.6  26.6
DWO809I 00007  00002700 AUTOSEG1     1506      160          10.6   65.4   6.9
DWO809I 00008  00002900 AUTOSEG1      160       52          32.5    6.9   2.3
DWO809I 00009  00003400 AUTOSEG1      108        1           0.9    4.7   0.0
DWO809I 00010  00003700 AUTOSEG1      107      107        X 100.0    4.6   4.6
DWO808I ---------------------------------------------------------------------
```

Figure 130. MSG Detail Report

```
- DWO800I AUTOMATION TABLE MSU DETAIL REPORT BY OPER1

DWO804I -------------( AUTOSEG1 MSU DETAILS  04/12/99 14:32:42 )-------------
DWO805I                                                    |-- PERCENTAGES --|
DWO806I STMT   SEQ      MEMBER    COMPARE    MATCH  E  C  A MATCH/ COMP/ MATCH/
DWO807I NUMBER NUMBER   NAME      COUNT      COUNT  C  I  I COMP   TOTAL TOTAL
DWO808I ---------------------------------------------------------------------
DWO809I 00012  00004400 AUTOSEG1     3363     3233          96.1  100.0  96.1
DWO809I 00013  00004700 AUTOSEG1     3233        5           0.2   96.1   0.1
DWO809I 00014  00005200 AUTOSEG1     3228       17           0.5   96.0   0.5
DWO809I 00015  00005600 AUTOSEG1     3211     3211        X 100.0   95.5  95.5
DWO808I ---------------------------------------------------------------------
```

Figure 131. MSU Detail Report

To analyze a detail report, associate specific automation statements with the actual statements in the source member or the automation table listing; the actual text of the statement is not shown in the report. For each statement, the detail report provides:

- The member name and sequence number of the source statement. Note that these values might not be current if the source automation table member has been changed since the automation table was activated.
- The sequential statement number as stored in an automation table list. Note that this is only current if the list was generated when the automation table was loaded and not replaced after the table was activated.

If an automation table list is generated when the automation table is activated, and no AUTOCNT RESET command is issued between the automation table activation and the usage report generation, the date and time in the listing match the STATISTICS STARTED date and time in the summary usage report. Comparing the dates and times is one way you can verify that you have correlation between the detailed usage report statements and the actual automation statements.

Automation Table Summary Usage Report

To generate a summary usage report, issue the AUTOCNT command with STATS=SUMMARY. See Figure 132 and Figure 133.

```
- DWO801I AUTOMATION TABLE MSG SUMMARY REPORT BY OPER1

 DWO810I ------------( AUTOSEG1 MESSAGE SUMMARY  04/12/96 14:32:42 )------------
 DWO812I STATISTICS STARTED          = 04/12/99  13:32
 DWO813I TOTAL MSGS PROCESSED        =     2304
 DWO814I MSGS MATCHED                =      958
 DWO815I MSGS RESULTING IN COMMANDS  =        9
 DWO816I TOTAL COMMANDS EXECUTED     =        9
 DWO817I TOTAL ROUTES EXECUTED       =        1
 DWO818I AVERAGE COMPARES/MSG        =        2.58
 DWO819I TOTAL MSGS/MINUTE           =       38
 DWO820I MINUTES ELAPSED             =       60
 DWO808I
```

Figure 132. MSG Summary Report for Message Automation

```
 - DWO801I AUTOMATION TABLE MSU SUMMARY REPORT BY OPER1

 DWO811I --------------( AUTOSEG1 MSU SUMMARY  04/12/99 14:32:42 )--------------
 DWO812I STATISTICS STARTED          = 04/12/96  13:32
 DWO821I TOTAL MSUS PROCESSED        =     3363
 DWO822I MSUS MATCHED                =     3233
 DWO823I MSUS RESULTING IN COMMANDS  =        0
 DWO816I TOTAL COMMANDS EXECUTED     =        0
 DWO824I AVERAGE COMPARES/MSU        =        2.92
 DWO825I TOTAL MSUS/MINUTE           =       56
 DWO820I MINUTES ELAPSED             =       60
 DWO808I ------------------------------------------------------------------------
```

Figure 133. MSU Summary Report for MSU Automation

Storing Summary Usage Reports

Store summary data for comparison purposes so that you can see the impact of automation when changes are made to the environment, such as the following kinds of changes:

- Adding more devices to the network (possibly more MSUs to process)
- Adding more software to the system (possibly more messages to process)
- Changing the automation table (adding new statements, adding BEGIN/END sections
- Effect of shift changes, different days of the week, or holidays on your automation processing, and so on

Summary reports can be stored using the FILE keyword on the AUTOCNT command, or the information can be processed and stored in a custom format by processing the report in a REXX command list and storing to a file using the TSO/E EXECIO function.

Hint: Because the AUTOCNT command FILE option does not support adding information to the end of an existing file, use EXECIO if you want to store the data from multiple summary reports in the same file.

Reviewing Summary Usage Reports

To track the amount of work that automation is accomplishing, the summary report contains:

- The number of messages or MSUs processed and messages or MSUs per minute indicate the traffic levels in the system for those messages or MSUs processed by the system.
- The number of messages or MSUs matched and commands processed indicate how much work the automation table is handling, so operators do not have to react to the messages or MSUs.
- The number of routes processed indicate how many messages were automatically routed to the correct operator to handle the message.
- The number of comparisons and the number of messages and MSUs processed is indicative of the performance load of processing the automation table.
- The number of messages or MSUs processed minus the number of messages or MSUs matched indicates the number of messages or MSUs that were processed but not automated. Reduce this as much as possible for messages by suppressing system messages in the operating system message facility that are not required.

  If a particular message, class of messages, or MSU type is not automated, but is frequently received, you can add a statement near the top of the automation table to indicate that no further processing of this message is to be performed. For example, the following statement indicates that automation processing is to stop for any message with a message identifier that begins with XYZ:

  ```
  IF MSGID = 'XYZ'. THEN;
  ```

  The next example indicates that automation processing is to stop for all problem determination statistics major vectors (key X'0025'):

  ```
  IF MSUSEG(0025) ¬= ' THEN;
  ```

  Note: When an ALWAYS statement is processed for a message or MSU, the message or MSU is then counted as being matched. Therefore, the number of messages or MSU matches can be misleading if you use ALWAYS statements.

Analyzing the Detail Usage Report

The following table shows some of the ways to analyze the data from a detailed usage report:

Table 18. Analyzing Detail Usage and Summary Reports

Indicators	Possible Error Source
COMPARE COUNT = MATCH COUNT MATCH COUNT > 0 A I (Always Indicator) = blank	The automation table statement might have a logic error causing it to always match a message or MSU when it is compared
COMPARE COUNT = 0 MINUTES ELAPSED = substantial	A prior statement might be preventing this statement from being compared when it needs to be compared
MATCH COUNT = 0 MINUTES ELAPSED = substantial	This statement might no longer be needed because the message or MSU the statement is trying to match is no longer generated, or a coding error on the condition might be preventing the message or MSU from matching.

Where possible (without changing the automation logic), order the automation table in the following way:

- Place BEGIN/END sections with the highest MATCH COUNT at the top of the table and those with the lowest MATCH COUNT at the bottom.
- Within BEGIN/END sections, place statements with the highest MATCH COUNT at the top and those with the lowest MATCH COUNT at the bottom.

Ordering your automation table in this way optimizes the performance of your automation processing so that the automation table requires less time to process messages and MSUs.

Maintaining the Automation Table

After you add statements to the automation table, the statements need to be maintained because products add, change, and delete messages. When installing or upgrading system products, notice messages that are added, changed, or deleted. Most IBM product documentation lists this information.

Topic:	Reference:
AUTOTBL and AUTOCNT commands	NetView online help
Automation table language, automation table listings, and automation table usage reports	*IBM Tivoli NetView for z/OS Automation Guide*
Planning for automation	*IBM Tivoli NetView for z/OS Automation Guide*
MSUs in NetView	*IBM Tivoli NetView for z/OS Automation Guide*
MSUs in SNA	*SNA Management Services Reference* and *SNA Formats*

Chapter 15. Controlling Message Routing Using the ASSIGN Command

You can use the NetView ASSIGN command to route solicited and unsolicited messages and to assign operators to groups. The ASSIGN command is useful for preliminary routing of messages to autotasks to get messages to the automation table faster, and for assigning operators to groups.

If operators in a group are not yet defined when the ASSIGN command is issued, the assignment takes effect after the operator is defined and logs on to NetView.

If the ASSIGN command defines message routing to a single operator, and that operator is not yet defined, the assignment fails.

To activate changes to operators defined by NetView profiles, modify the definition in DSIOPF, then issue the NetView REFRESH OPERS command.

If the operators are defined in a system authorization facility (SAF) security product (SAF) product such as RACF, changes to the NETVIEW segment definitions take effect immediately.

Topic:	Reference:
ASSIGN and REFRESH commands	NetView online help

Assigning Operators to Groups

You can use the ASSIGN command with the GROUP option to assign a list of operators to a particular group. You can then use the operator group with other assign commands, with the MSGROUTE command in a command list, or with the EXEC(ROUTE) action in the automation table. For example, to assign operators OPER1 and OPER2 to group +GROUP1, enter:

```
assign group=+group1,op=(oper1,oper2)
```

All group names must begin with a plus sign (+).

Working with Unsolicited Messages

An ***unsolicited message*** is a message that was not expected in response to an operator action. If an unsolicited message has not been suppressed, you might want to direct it to an operator or autotask to handle the situation. The ASSIGN command is particularly useful when you want to route messages or groups of messages by message ID. The messages are routed in specific-to-general order. For example, if you enter:

```
assign msg=*,pri=oper1,sec=oper2
assign msg=ist*,pri=(vtamoper,auto1)
assign msg=ist5*,pri=(vtamoper,auto2)
```

Messages beginning with IST5 are routed to VTAMOPER or AUTO2, and all other IST messages are routed to VTAMOPER or AUTO1. All remaining messages are routed to OPER1 and if OPER1 is available, they are also routed to OPER2.

Working with Solicited Messages

A ***solicited message*** is a message which is sent in response to an operator command, and which has a specific destination, such as a NetView operator, an autotask, or a NetView-to-NetView task.

You can use the ASSIGN command with the COPY option to send a copy of a solicited message to all operators. For example, if you want OPER2, OPER3, and OPER4 to be notified whenever anyone uses the STOP command to stop a NetView task, enter:

```
assign msg=dsi660i,copy=(oper2,oper3,oper4)
```

Chapter 16. Starting an Autotask to Handle Automation

Creating and using NetView automated operator station tasks (autotasks) enables work to be performed automatically. Autotasks can do work usually performed by operators, thus providing more time for operators to perform less repetitive tasks. Autotasks can perform the following tasks:

- Perform a wide range of tasks, such as running command lists in response to messages and MSUs, sending messages to other operator tasks, scheduling commands to run using NetView timer commands, and so on.
- Respond quickly to system or network failures.
- Facilitate cross domain communication, thus reducing the required number of NetView programs to which an operator must be logged on.
- Ensure consistent responses to system and network problems.

For information about defining autotasks, see the *IBM Tivoli NetView for z/OS Automation Guide*.

You can start autotasks by using the NetView AUTOTASK or RMTCMD command. Table 19 shows how each command implements an autotask:

Table 19. Starting an Autotask Using AUTOTASK and RMTCMD

Autotasks started with the AUTOTASK command:	**Autotasks started with the RMTCMD command:**
• Perform tasks usually reserved for NetView operators. • Can be started before the VTAM program is started so the NetView program can be used to monitor VTAM program failures and recover them automatically. • Can be associated with MVS consoles when started, and NetView commands can be entered at the MVS console which are then processed under the NetView autotask associated with that MVS console.	• Are used to provide cross domain communication using LU 6.2. • Can be used to provide an operation path into another NetView program on the same host or on a different host. Commands can be processed on different NetView systems, and the results can be viewed.

For example, to start an autotask AUTO3 using the AUTOTASK command, enter:

```
autotask opid=auto3
```

To start an autotask named OPER2 on the remote NetView CNM02 and display the name of the alert focal point, enter:

```
rmtcmd lu=cnm02,operid=oper2,list focpt=alert
```

Topic:	**Reference:**
AUTOTASK and RMTCMD commands	NetView online help
Defining operators using a security application	*IBM Tivoli NetView for z/OS Administration Reference*.

Chapter 17. Scheduling Commands

A command issued by a timer command is a *timed command*. Any command that you can issue from the NetView program can be a timed command. For example, command lists and NetView, VTAM, and MVS commands can be timed commands.

Like other NetView commands, timed commands can be issued from the following places:
- An operator console
- An autotask
- Within a command list or command processor
- Any active task

NetView timer commands include AT, AFTER, CHRON, and EVERY. You can use timer commands to issue commands whenever you choose and to conveniently issue commands repeatedly.

Note: A timed command is subject to any restrictions of the task under which it runs.

You can schedule a command to automatically perform tasks that operators traditionally perform, such as the following tasks:
- Periodically reviewing the status of a critical resource
- Starting a process at a scheduled time
- Verifying, after a designated period of time, whether or not a process completed successfully

You can issue timed commands in either of the following two ways:
- Using NetView commands at the command line
- Using NetView Timer Management Panels

Preparing to Issue NetView Timer Commands

Before you establish a NetView timer, follow these steps:

1. Determine a timer ID naming convention.

   Having a naming convention simplifies the creation and maintenance of timer commands. For example, to delete a timer command, knowing the timer ID saves time by not having to list all the timer commands.
2. Determine the tasks that should issue timer commands.

   You need to determine if you are going to use the PPT for running the timed commands, a particular autotask, or different operator tasks.
3. Enable command authorization for PPT timer commands.

   Command security cannot protect commands issued by the PPT task. You can enable command authorization for PPT timer commands in either of the following two ways:
   - By checking the authorization of the originating task
   - By protecting the PPT operand for the timer commands

   If you are using SECOPTS.CMDAUTH=TABLE or SECOPTS.CMDAUTH=SAF, you can specify SECOPTS.AUTHCHK = SOURCEID in CNMSTYLE or its

included members, or AUTHCHK = SOURCEID on the REFRESH command to have command security check the authorization of the original issuer of the command.

Restricting access to the PPT keyword prevents operators from routing commands to the PPT task. Refer to *IBM Tivoli NetView for z/OS Security Reference* for a description of how to protect AFTER, AT, CHRON, and EVERY commands and keywords.

4. If you are using the Save/Restore capability, redefine the VSAM database, which was originally defined during NetView installation.

   For more information, refer to the *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*.

Using NetView Commands at the Command Line

You can issue NetView timer commands by typing the commands at the command line at the lower left side of the screen.

Issuing Timer Commands for a Specified Date or Time

To issue commands at a specific date and time, use the NetView AT or CHRON command.

If PPT is not specified, the timed command attempts to process on the task that issued the timer. This can cause the following problems:

- If the operator is not logged on at the specified time the timed command is scheduled to run, the command is not processed.
- If the operator is in the middle of an important task when the command starts processing, the task is interrupted when the timed command runs.

Note: You can customize date and time formats through the DEFAULTS and OVERRIDE commands. For more detailed information on the DEFAULTS and OVERRIDE commands refer to the NetView online help.

By specifying PPT, timer commands process under the primary program operator interface task (PPT). This is convenient because the PPT is always active when the NetView program is active. Another option is to issue timer commands from one or more NetView autotasks, because autotasks are typically active when NetView is active.

It is better to issue timer commands from autotasks rather than the PPT, because the PPT should be available to perform critical work.

For example, to schedule the STATREP timed command for 09/24 at 9:00 a.m., enter the following command:

```
at 09/24 09:00:00,id=statrep,statrep
```

Issuing Commands at Regular Intervals

To issue commands at regular intervals, use the NetView EVERY or CHRON command with a time interval.

For example, to process a TASKUTIL every hour from the NetView Primary POI Task (PPT), enter the following command:

```
every 1:00:00,ppt,taskutil
```

Issuing Commands After a Specified Time Period

To issue commands after a specified delay in time, use the NetView AFTER or CHRON command.

For example, to process the CHKVTAM command an hour from now, enter the following command:

```
after 1:00:00,id=statvtam,chkvtam
```

Displaying Timers That Are Waiting to Process

The LIST TIMER command lists the following information:

- The type of timer command
- When the timer is scheduled to run
- What timed command is to be issued
- Whether the PPT operand was specified
- Whether the timer was saved in the VSAM database

To display the active timer commands for all the NetView operators, enter the following command:

```
list timer=all,op=all
```

To display a specific timer command with an ID, specify an ID with the `TIMER` parameter. For example, to display a timer command with an ID of SHOWLINK on the task of the calling operator, enter the following command:

```
list timer=showlink
```

To display all timers for a specific operator, add OP= followed by the operator ID. For example, to display all timers issued by operator OPER1, enter the following command:

```
list timer=all,op=oper1
```

Note: To facilitate viewing timer information, preface the LIST command with the WINDOW command. This displays the list timer output in a scrollable window.

Deleting Timer Commands

You can use The NetView PURGE command to delete timer commands that you no longer require.

For example, you might have issued an EVERY command to periodically check something that is now fixed, or you might have made an error when entering the timer command, and you want to remove the timer in error.

To delete the timed command previously issued by OPER1 with an ID of STATUS1, enter the following command:

```
purge op=oper1,timer=status1
```

If the SAVE parameter was used on the timer command, purging the timer also deletes it from the Save/Restore database.

Saving a Timer

To restore a TIMER command so that it can be processed when the NetView program is recycled, use the SAVE parameter. This parameter saves the TIMER command in the Save/Restore VSAM database.

For example, to schedule the TASKUTIL timed command for 09/24 at 9 a.m. and to have the timed command saved in case NetView is recycled, enter the following command:

```
at 09/24 09:00:00,id=taskstat,save,taskutil
```

Restoring Timers

The NetView RESTORE command can be used to restore timers that have been saved to the VSAM database.

To restore all saved timers, enter the following command:

```
restore timer
```

To erase all saved timer records from the database, add the DELETE option:

```
restore timer delete
```

Topic:	Reference:
AT, AFTER, CHRON, EVERY, LIST, PURGE, and RESTORE commands	NetView online help
Timed commands	*IBM Tivoli NetView for z/OS Automation Guide*
Using System Automation for z/OS to set timers	*IBM Tivoli System Automation for z/OS User's Guide*

Using NetView Timer Management Panels

Timers issue commands and command lists at specified time intervals. The types of timers are EVERY, AT, AFTER, and CHRON.

You can schedule a timer setting for a specific date and time, after a certain date and time, or repetitively at defined intervals. You can use the Timer Management panel (and its subordinate panels) to add, change, delete, and purge timers of various types.

Timers can be scheduled several ways. For example, with NetView, you can issue the AT, EVERY, AFTER, and CHRON command in the following ways:

- From a command list
- On the command line
- From the Timer Management panel

To display the Timer Management panel, type **TIMER** on any command line; or, if using AON, type **AON 1.6** at the command line.

The Timer Management panel is displayed, as shown in Figure 134 on page 253.

Note: Although **D** for Delete is not an option on the Timer Management panel, it is supported.

```
EZLK6000              TIMER MANAGEMENT    NTV6D OPER2    07/19/01 19:18:40
                                                            1 TO    5 OF    5
 Target: NTV6D    Target Network ID:          Operid: OPER2     Selected:    5
IP Addr:                                                       Purged:    0
   Port:          Remote Target Date and Time:

Filter criteria:
Type one action code. Then press enter.
  1|A=Add  2|C=Display/Change  3|P=Purge  4=Add CHRON timer
    Timer ID  Scheduled           Type   Interval   Task      Save   Catchup
 _  IDLEOFF   07/19/01 19:22:19   EVERY  00:10:00   AUTO1
              IDLEOFF 10000
 _  EZLRSET   07/20/01 00:01:00   AT                PPT
              EXCMD AUTO1 EZLEASTM
 _  PSTS      07/23/01 02:00:00   EVERY  MONDAY     AONMSG1
              DBMAINT EZLSTS 7
 _  PNPDA     07/23/01 04:00:00   EVERY  MONDAY     AONMSG1
              DBMAINT NPDA 7
 _  PNLDM     07/23/01 06:00:00   EVERY  MONDAY     AONMSG1
              DBMAINT NLDM 7

Command ===>
F1=Help      F2=End         F3=Return                F5=Refresh    F6=Roll
F7=Backward  F8=Forward                          F11=Reset Target  F12=Cancel
```

Figure 134. Timer Management Panel

The Timer Management panel displays the following data fields:

Target Specifies the ID of the remote system whose timers you want to display.

Target Network ID
Specifies the ID of the remote domain whose timers you want to display. If you do specify Target Network ID, the Target field is used as a domain name.

Operid
Specifies the operator ID on the remote domain whose timers you want to display. This field is only displayed when COMMON.EZLRMTTIMER = NETV is specified in CNMSTYLE or its included members.

IP Addr
Specifies the IP address or host name of the remote domain whose timers you want to display. This field is displayed only when COMMON.EZLRMTTIMER = NETV is specified in CNMSTYLE or its included members.

Port Specifies the port number on the remote domain whose timers you want to display. This field is only displayed when COMMON.EZLRMTTIMER = NETV is specified in CNMSTYLE or its included members.

Timer ID
Specifies the IDs of the active timers. The IDs are supplied by the operators that create the timers.

Scheduled
Specifies the date and time when the command is to be issued.

Type Specifies the type of timer:
- EVERY
- AT
- AFTER
- CHRON

Interval
Specifies how often timers repeat.

Task Specifies which task is to issue the command.

If task=PPT, a specific task is not required for the command to be issued.

Save Indicates to NetView whether this timer event is saved to the NetView SAVE/RESTORE database.

If SAVE=YES, the timer is stored in the NetView SAVE/RESTORE database. If SAVE is set to NO or is left blank, the timer is not saved. If SAVE is set to YES, the timer is restored after a NetView outage. If CATCHUP=YES is specified in the AON control files, SAVE=YES is required.

Catchup
Indicates that a timer that was saved is to be caught up after a system outage (if the timer was defined in an AON control file).

You can use the Timer Management panel to add, change, and purge timers. The following sections explain how to perform these actions:
- Selecting Remote Targets
- Setting Timers for a Specific Date and Time
- Adding a Timer

Selecting Remote Targets

To display the Remote Target Selection panel, type **?** in one of the following fields on the Timer Management panel:
- Target Network ID
- Target
- Operid
- IP Addr
- Port

For example, type a question mark in the Target field, as shown in Figure 135 on page 255, and press Enter.

```
EZLK6000              TIMER MANAGEMENT    NTV6D OPER2    07/19/01 19:33:32
                                                          1 TO    2 OF    2
 Target: ?TV6D    Target Network ID:          Operid: OPER2     Selected:    2
IP Addr:                                                       Purged:    0
   Port:          Remote Target Date and Time:

Filter criteria:
Type one action code. Then press enter.
  1|A=Add  2|C=Display/Change  3|P=Purge  4=Add CHRON timer
    Timer ID  Scheduled           Type   Interval   Task      Save   Catchup
 _  IDLEOFF   07/19/01 19:42:19   EVERY  00:10:00   AUTO1
              IDLEOFF 10000
 _  EZLRSET   07/20/01 00:01:00   AT                PPT
              EXCMD AUTO1 EZLEASTM
 _  PSTS      07/23/01 02:00:00   EVERY  MONDAY     AONMSG1
              DBMAINT EZLSTS 7
 _  PNPDA     07/23/01 04:00:00   EVERY  MONDAY     AONMSG1
              DBMAINT NPDA 7
 _  PNLDM     07/23/01 06:00:00   EVERY  MONDAY     AONMSG1
              DBMAINT NLDM 7


Command ===>
F1=Help      F2=End         F3=Return                 F5=Refresh    F6=Roll
F7=Backward  F8=Forward                           F11=Reset Target  F12=Cancel
```

Figure 135. Timer Management Panel with Target Specified

If you are using the NetView RMTCMD interface (COMMON.EZLRMTTIMER = NETV set in CNMSTYLE or its included members), the Remote Target Selection panel is displayed, as shown in Figure 136.

```
EZLK5500               REMOTE TARGET SELECTION            1 to    2 of  2

Filter:
Type one action code and press enter.

    DOMAIN    SYSTEM    SYSPLEX   COMM      NETID     OPERID    PORT   VERSION
 _  NTV70                         SNA       USIBMNT   OPER2             V5R2

 /  NTV6D                         TCP/IP    USIBMNT   OPER4     4022    V5R2
         IP Addr: 9.67.50.34




Command ===>
F1=Help                   F3=Return                   F5=Refresh   F6=Roll
F7=Backward  F8=Forward                                          F12=Cancel
```

Figure 136. Remote Target Selection Panel (COMMON.EZLRMTTIMER = NETV)

The Remote Target Selection Panel displays the following columns of data:

Filter Used for specifying a DOMAIN, SYSTEM, SYSPLEX, or COMM method to display.

DOMAIN Specifies the IDs of the domains that you can select as a target.

SYSTEM Specifies the IDs of systems that you can select as a target.

SYSPLEX Specifies the IDs of sysplexes that you can select as a target.

COMM Specifies the communications facility over which the data is transferred between remote domains.

NETID Specifies the network ID of the remote domain whose timers you want to display.

OPERID Specifies the autotask to be used on the remote domain for processing the command. The default is your operator ID.

PORT Specifies the port number to be used for TCP/IP communications.

VERSION Specifies the version of the remote NetView program.

If you are using the System Automation for z/OS interface (COMMON.EZLRMTTIMER = SA set in CNMSTYLE or its included members), NetView displays the Remote Target Selection panel, as shown in Figure 137.

```
EZLK5500               REMOTE TARGET SELECTION            1 to    2 of  2

Filter:
Type one action code and press enter.

    DOMAIN    SYSTEM    SYSPLEX   COMM
 _  IPUFB     AOCB      AOCPLEX   XCF
 _  IPUFC     AOCC      AOCPLEX   XCF
 _  IPUFA     AOCA      AOCPLEX   XCF
 _  IPUFM     AOC7      AOC7PLEX  GATEWAY
 _  IPUFO     KEY3      KEY1PLEX  GATEWAY
 _  IPUFD     AOCD      AOCPLEX   LOCAL



Command ===>
F1=Help                   F3=Return                   F5=Refresh   F6=Roll
F7=Backward  F8=Forward                                           F12=Cancel
```

Figure 137. Remote Target Selection Panel (COMMON.EZLRMTTIMER = SA)

Type any character to select a target system, as shown in Figure 136 on page 255 and press Enter.

The NetView program displays the active timers for the Target that you selected.

```
EZLK6000              TIMER MANAGEMENT    NTV6D          07/19/01 19:38:38
                                                            1 TO    5 OF    5
 Target: NTV6D    Target Network ID: USIBMNT  Operid: OPER4     Selected:    5
IP Addr: 9.67.50.34                                           Purged:    0
   Port: 4022     Remote Target Date and Time: 07/19/01 19:38

Filter criteria:
Type one action code. Then press enter.
  1|A=Add  2|C=Display/Change  3|P=Purge  4=Add CHRON timer
    Timer ID  Scheduled           Type   Interval   Task      Save   Catchup
 _  ADOIV     07/19/01 19:38:53   EVERY  00:03:00   AUTOIV1
              EZLEOIVT
 _  EZLRSET   07/20/01 00:01:00   AT                PPT
              EXCMD AONBASE EZLEASTM
 _  PSTS      07/23/01 02:00:00   EVERY  MONDAY     AONMSG1
              DBMAINT EZLSTS 7
 _  PNPDA     07/23/01 04:00:00   EVERY  MONDAY     AONMSG1
              DBMAINT NPDA 7
 _  PNLDM     07/23/01 06:00:00   EVERY  MONDAY     AONMSG1
              DBMAINT NLDM 7


Command ===>
F1=Help      F2=End         F3=Return                 F5=Refresh    F6=Roll
F7=Backward  F8=Forward                           F11=Reset Target  F12=Cancel
```

Figure 138. Timer Management Panel for the Selected Target

Setting Timers for a Specific Date and Time

To add an EVERY, AT or AFTER timer:

1. Display the Timer Management panel.

   To display the Timer Management panel, see "Using NetView Timer Management Panels" on page 252.

2. Type **1** or **A** in the entry field either next to an existing timer or on the command line.

3. Press **Enter**.

   A Timer Set panel is displayed, as shown in Figure 139 on page 258 in which an EVERY timer was selected:

```
EZLK6110              Set EVERY timer     NTV6D OPER2    07/19/01 19:40:50
 Target: NTV6D    Target Network ID: USIBMNT  Operid: OPER2
IP Addr:
   Port:             Remote Target Date and Time:
                                    .....................................
Timer Type   1 1 EVERY              :               EVERY                 :
               2 AT                 : Interval format (HH:MM:SS)          :
               3 AFTER              : Interval  00 :   00 :   00          :
               4 CHRON              :                                     :
                                    : Select    1 SUNDAY      6 FRIDAY    :
TIMEFMSG. .     1 No 2 Yes          :           2 MONDAY      7 SATURDAY  :
Timerid . .                         :           3 TUESDAY     8 DAY       :
Task  . . .                         :           4 WEDNESDAY   9 000 DAYS  :
Save  . . .    1 No 2 Yes           :           5 THURSDAY                :
                                    : EVERYCON     1 No 2 Yes             :
Scheduled .                         :.....................................:

Timer Command

Command ===>
F1=Help      F2=End         F3=Return                              F6=Roll
                                                                 F12=Cancel
```

Figure 139. Timer Set Panel for a Type of EVERY

The pop-up window that displays on the panel depends on the type of the timer whose entry field you used to make the add request on the Timer Management panel. The timers are one of the following types:

EVERY
The timer times out at recurring intervals each time the interval passes. The timer is rescheduled for the next interval automatically after it goes off.

AT The timer goes off at the specified date and time.

AFTER
The timer goes off after the specified interval passes.

CHRON
The timer can have any of the properties described above with additional functions available. See the CHRON command in the *IBM Tivoli NetView for z/OS Command Reference Volume 1* for more information.

The following sections explain how to set each type of timer.

Adding a Timer

EVERY Timer

To add a timer that pops at recurring intervals and is not deleted:

1. Display the Timer Management panel.

   To display the Timer Management panel, see "Using NetView Timer Management Panels" on page 252.
2. Display the Timer Set panel.

   To display the Timer Set panel, see "Setting Timers for a Specific Date and Time" on page 257.
3. If the EVERY pop-up window is not already displayed on the Timer Set panel, type **1** in the Timer Type field and press **Enter**.

The Timer Set panel, shown in Figure 140, is displayed with the EVERY pop-up window.

```
EZLK6110              Set EVERY timer     NTV6D OPER2    07/19/01 19:44:12
 Target: NTV6D    Target Network ID: USIBMNT  Operid: OPER2
IP Addr:
   Port:             Remote Target Date and Time:
                                    .....................................
Timer Type   1 1 EVERY              :               EVERY                 :
               2 AT                 : Interval format (HH:MM:SS)          :
               3 AFTER              : Interval  00 :   00 :   00          :
               4 CHRON              :                                     :
                                    : Select    1 SUNDAY      6 FRIDAY    :
TIMEFMSG. .     1 No 2 Yes          :           2 MONDAY      7 SATURDAY  :
Timerid . .                         :           3 TUESDAY     8 DAY       :
Task  . . .                         :           4 WEDNESDAY   9 000 DAYS  :
Save  . . .    1 No 2 Yes           :           5 THURSDAY                :
                                    : EVERYCON     1 No 2 Yes             :
Scheduled .                         :.....................................:

Timer Command


Command ===>
F1=Help      F2=End         F3=Return                              F6=Roll
                                                                 F12=Cancel
```

Figure 140. Timer Set Panel for a Timer Type of EVERY

Note: To set the timer for a different domain or system, see "Selecting Remote Targets" on page 254.

4. Define whether you want messages generated if the requested timer fails. Specify TIMEFMSG in the following way:
   - Type **1** if you do not want messages generated.
   - Type **2** if you want messages generated.
5. In the Interval and Select fields, choose one of these options:

   To specify a timer that goes off more than once every day, type the time of day in the Interval field, type **9** in the Select field, but leave **000** in the DAYS field.

   For example, to set the timer for every 15 minutes everyday, type:

   ```
   Interval  00 : 15 : 00
   Select  9
             9 000 DAYS
   ```

   To specify a time of day and a day of the week, type the time in the Interval fields, and in the **Select** field, type the number that corresponds to the day. The time is shown in military time or the *hh:mm:ss* format.

   For example, to set the timer for Sunday at 2 p.m., type:

   ```
   Interval  14 : 00 : 00
   Select  1
   ```

   To specify a timer that goes off at a certain time of day every *x* number of days, type the time of day in the Interval fields, and type **9** in the Select field. Then, specify a number of days in the **DAYS** field.

   For example, to set the timer for noon every 5 days, type:

   ```
   Interval  12 : 00 : 00
   Select  9
             9 005 DAYS
   ```
6. Specify an ID for the timer in the Timerid field (Optional).

7. Specify a task in the task field (Optional).
8. Define whether you want EVERY timers to continue to be scheduled if one fails.

   Specify EVERYCON in the following way:

   - Enter **1** if you do not want EVERY timers to continue to be scheduled.
   - Enter **2** if you want EVERY timers to be scheduled.
9. Specify **1** if you do not want to save the timer, or **2** to save the timer in the Save field.
10. Type the command that you want to be issued in the Timer Command field.
11. Press **Enter**.

    The following message is displayed to confirm the timer you set:

    `EZL973I REQUESTED TIMER timer ADDED`

AT Timer

To add a timer that pops on a specific date and time:

1. Display the Timer Management panel.

   To display the Timer Management panel, see "Using NetView Timer Management Panels" on page 252.
2. Display the Timer Set panel.

   To display the Timer Set panel, see "Setting Timers for a Specific Date and Time" on page 257.
3. If the Timer Set panel does not already display the AT pop-up window, type **2** in the Timer Type field and press **Enter**.

   The Timer Set panel shown is displayed with the AT pop-up window, as shown in Figure 141.

```
EZLK6120              Set AT timer        NTV6D OPER2    07/19/01 19:45:48
 Target: NTV6D    Target Network ID: USIBMNT  Operid: OPER2
IP Addr:
   Port:             Remote Target Date and Time:

Timer Type   2 1 EVERY              ..........................
               2 AT                 :           AT             :
               3 AFTER              :                          :
               4 CHRON              : Time Format (HH:MM:SS)   :
                                    :                          :
TIMEFMSG ..     1 No 2 Yes          : Time .  19 :   44 :   12 :
Timerid . .                         :                          :
Task  . . .                         : Date Format (MM/DD/YY)   :
Save  . . .    1 No 2 Yes           :                          :
                                    : Date .  07/19/01         :
Scheduled .                         :..........................:

Timer Command


Command ===>
F1=Help      F2=End         F3=Return                              F6=Roll
                                                                 F12=Cancel
```

Figure 141. Timer Set Panel with Timer Type of AT

Note: To set the timer for a different domain or system, see "Selecting Remote Targets" on page 254.

4. Define whether or not you want messages generated if the requested timer fails.

   Specify TIMEFMSG in the following way:

   - Type **1** if you do not want messages generated.
   - Type **2** if you want messages generated.

5. In the Time field of the pop-up window, type the time of day when you want the command to run. The time is shown in the *hh:mm:ss* format; for example, specify 2:43:58 p.m. in the following format:

   ```
   14 : 43 : 58
   ```

6. In the Date field of the pop-up window, type the date when you want the command to run. The date follows the *mm/dd/yy* format; for example, specify August 3, 2006 in the following way:

   ```
   08/03/06
   ```

7. Type an ID for the timer in the `Timerid` field (Optional).
8. Specify a task in the Task field (Optional).
9. Type **1** if you do not want to save the timer or type **2** to save the timer in the Save field.
10. Type the command that you want to be issued in the Timer Command field.
11. Press **Enter**.

    The following message is displayed to confirm the timer you set:

    ```
    EZL973I REQUESTED TIMER timer ADDED
    ```

AFTER Timer

To add a timer that goes off after a specified period of time:

1. Display the Timer Management panel.

   To display the Timer Management panel, see "Using NetView Timer Management Panels" on page 252.

2. Display the Timer Set panel.

   To display the Timer Set panel, see "Setting Timers for a Specific Date and Time" on page 257.

3. If the Timer Set panel does not already display the AFTER pop-up window, type **3** in the Timer Type field and press **Enter**.

   The AFTER pop-up window, shown in Figure 142 on page 262, is displayed.

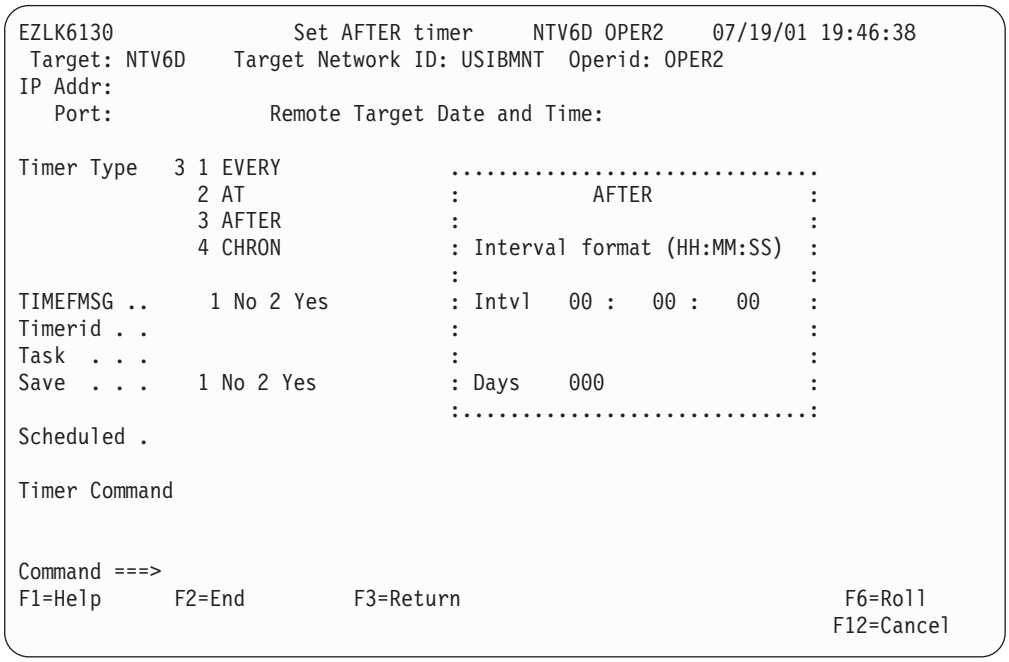


Figure 142. Timer Set Panel with Timer Type of AFTER

The AFTER timer type works differently from the EVERY and AT types.

When you use the AFTER type, do not specify a time of day or a date setting for the timer. Instead, specify a number of days, hours, minutes, and seconds after which you want the timer to expire. An interval is set that begins the moment you set the timer and ends after the specified number of days, hours, minutes, and seconds have passed.

Note: To set the timer for a different domain or system, see "Selecting Remote Targets" on page 254.

4. Use the Intvl and Days fields of the pop-up window together to specify the timer setting.

   For example, to set the timer for 14 hours from now, type:

   ```
   Intvl  14 : 00 : 00
   Days   000
   ```

   When you set the number of days to 000, the day the timer goes off is today. If you specify a number other than 000, the timer goes off after the specified number of days from the current day.

   For example, to set the timer for 5 days, 12 hours, 10 minutes, and 15 seconds from now, type:

   ```
   Intvl  12 : 10 : 15
   Days   005
   ```

   To set the timer for the current time 5 days from now, type:

   ```
   Intvl  00 : 00 : 00
   Days   005
   ```

5. Define whether or not you want messages generated if the requested timer fails.

   Specify TIMEFMSG in the following way:
   - Type **1** if you do not want messages generated.
   - Type **2** if you want messages generated.

6. Specify a timer ID in the **Timerid** field (Optional).
7. Specify a task in the Task field (Optional).

8. Specify **1** if you do not want to save the timer or **2** to save the timer in the Save field.
9. Type the command that you want to be issued in the Timer Command field.
10. Press **Enter**.

    The following message is displayed to confirm the timer you set:

    ```
    EZL973I REQUESTED TIMER timer ADDED
    ```

CHRON Timer

To add a CHRON timer that pops on regular intervals, perform the following steps:

1. Display the Timer Management panel. To display the Timer Management panel, see "Using NetView Timer Management Panels" on page 252.
2. Display the Timer Set panel. To display the Timer Set panel, see "Setting Timers for a Specific Date and Time" on page 257.
3. If the Timer Set panel does not already display the CHRON pop-up window, type **4** in the **Timer Type** field and press **Enter**. The pop-up window matching the CHRON timer type is displayed, as shown in Figure 143.

```
EZLK6210            Set CHRON EVERY Timer  NTV6D OPER2    07/19/01 19:49:45
 Target: NTV6D    Target Network ID: USIBMNT  Operid: OPER2
IP Addr:
   Port:             Remote Target Date and Time:
CHRON Type 1 1 EVERY         ..............................................
             2 AT            :                   EVERY                      :
             3 AFTER         :                                              :
                             : Interval 3 1  00 :   00 :   00     (HH:MM:SS) :
Save . . . 2 1 Yes   2 No    :            2                                 :
Clock. . . 1 1 Local 2 GMT   :              (yyyy-mm-dd-hh.mm.ss.micros)    :
Timerid. .                   :            3 Daily                           :
Route. . .                   :..............................................:

Scheduled.                                                  Refresh 2 1 Yes 2 No
Recovery . 1 1 Ignore  2 Autolgn  3 Purge                   Test. . 2 1 Yes 2 No
                                                            Debug . 2 1 Yes 2 No
Remark
Command


Command ===>
F1=Help  F2=Display Results F3=Return      F4=Options  F5=Intervals  F6=Roll
                           F9=Set Timer  F10=Notify  F11=Preview   F12=Cancel
```

Figure 143. Set Panel with CHRON Timer Type of EVERY

Note: To set the timer for a different domain or system, see "Selecting Remote Targets" on page 254.

- In the Interval pop-up window, specify how often you want your command to be issued in one of the following ways:
  - Type **1** to specify how often the command is to be issued in your local time format.
  - Type **2** to specify how often the command is to be issued in programmer format, which specifies intervals greater than 24 hours.
  - Type **3** to specify that the command is to be issued every 24 hours.

Note: The pop-up windows for CHRON AT and CHRON AFTER timers contain slightly different information.

- Type **1** in the **Save** field to save the timer or type **2** if you do not want to save the timer.
- Type **2** in the **Clock** field for Greenwich Mean Time, or type **1** if you want local time.
- Specify a timer ID in the **Timerid** field (optional).
- Type the operator ID that is to issue the command in the Route field (optional).
- Type **1** in the **Recovery** field to ignore the command if the task on which it is to run is not active, type **2** to automatically have the task started to issue the command, or type **3** to purge the timer if the task is not active.
- Type **1** in the **Refresh** field for Yes, to refresh the command; or type **2** for No, do not Refresh.
- Type **1** for Yes, in the **Test** field to test the command, or type **2** for No, do not Test.
- Type **1** in the **Debug** field for Yes, to debug the command or type **2** for No, do not Debug.
- Type a comment to be included in the CHRON command in the **Remark** field, for example: `This timer periodically displays a list of active operators.`
- Type the command that you want to be issued in the **Command** field, for example: `list status=ops`

The following list describes the function keys for the CHRON TIMER panels:

F1 Displays brief help for the current panel.

F2 Displays the results of the CHRON command that was issued when **F9** was pressed.

F3 Displays the previous panel. No data is saved.

F4 Displays the options panel.

F5 This function key is available only for a CHRON EVERY timer; use it to specify more detailed interval options.

F6 Rolls you to another component.

F9 Sets the CHRON timer.

F10 Displays the Notify panel.

F11 Displays a preview of the CHRON command that is to be issued when you press **F9**.

F12 Displays the previous panel. No data is saved.

4. When you press **F10** in the timer set panels, the panel shown in Figure 144 on page 265 is displayed.

```
EZLK6202            CHRON Notify panel    NTV6D OPER2    07/19/01 19:49:45
.....................................................................
: Enter the operator IDs to be notified and press enter.            :
:                                                                   :
: Ignore                                                            :
:                                                                   :
: Purge                                                             :
:                                                                   :
: Remove                                                            :
:                                                                   :
: Run                                                               :
:                                                                   :
: F1=Help F2=Display result                                F6=Roll  :
:                                              F11=Preview  F12=Cancel :
:...................................................................:
                                                    Debug . 2 1 Yes 2 No
Remark  This timer periodically displays a list of active operators.
Command list status=ops


Command ===>
F1=Help  F2=Display result  F3=Return                          F6=Roll
                            F9=Set Timer  F10=Notify  F11=Preview   F12=Cancel
```

Figure 144. Timer Notify Panel

- Type one or more operator IDs in the **Ignore** field to specify which operators to notify when the command does not run because the specified task is not active.
- Type one or more operator IDs in the **Purge** field to specify which operators to notify when the command does not run because it was purged.
- Type one or more operator IDs in the **Remove** field to specify which operators to notify when the command does not run because it was removed.
- Type one or more operator IDs in the **Run** field to specify which operators to notify when the command runs.

5. Press **Enter** to return to the EZLK6210 panel.
6. If you press **F5** in the EZLK6210 panel, for more detailed interval options, the panel shown in Figure 145 on page 266 is displayed:

```
EZLK6211            Set CHRON EVERY Timer  NTV6D OPER2    07/19/01 19:57:07
 Target: NTV6D    Target Network ID:          Operid: OPER2
IP Addr:
   Port:             Remote Target Date and Time:
CHRON Type 1 1 EVERY         .......... ............................... ....
            2 AT             :          : Select all options desired   :    :
            3 AFTER          :          : and press ENTER              :    :
                             : Interval  :                             :    :
Save . . . 2 1 Yes   2 No    :          :  /  Start timer AT  ( OR )   :    :
Clock. . . 1 1 Local 2 GMT   :          :     Start timer AFTER        :    :
Timerid. .                   :          :                              : ...:
Route. . .                   :.......... :     Repeat options           :
                                        :     Remove                   :
Scheduled.                              :     Days of the week         : 2 No
Recovery . 1 1 Ignore  2 Autolgn  3 Purg :     Days of the month        : 2 No
                                        :     Calendar entries         : 2 No
Remark  This timer periodically displays :                              :
Command list status=ops                 : F1=Help           F12=Cancel :
                                        :..............................:



Command ===>
F1=Help  F2=Display Results F3=Return      F4=Options  F5=Intervals  F6=Roll
                            F9=Set Timer  F10=Notify  F11=Preview   F12=Cancel
```

Figure 145. Timer Interval Panel

- **Start timer AT** displays a panel where you can specify the time when the EVERY is to start.
- **Start timer AFTER** displays a panel where you can specify a delay interval after which the EVERY is to start.
- **Repeat options** displays a panel where you can specify how often a command is issued.
- **Remove** displays a panel where you can specify when the command is to be deleted.
- **Days of the week** displays a panel where you can specify the days of the week the command is or is not to be issued.
- **Days of the month** displays a panel where you can specify the days of the month the command is or is not to be issued.
- **Calendar entries** displays a panel where you can specify key names (that are defined in DSISCHED) on which the command is or is not to be issued.

7. Select the options you want, in this case, **Start timer AT**, and press **Enter**. A panel similar to the panel shown in Figure 146 on page 267 is displayed.

```
EZLK6212            Set CHRON EVERY Timer  NTV6D OPER2    07/19/01 20:10:48
 Target: NTV6D    Target Network ID:          Operid: OPER2
IP Addr:
   Port:             Remote Target Date and Time:
CHRON Type 1 1 EVERY         ..........................................  .
             2 AT            :  :              Start AT Time             : :
             3 AFTER         :  :                                        : :
                             :  :  3   1  00 :   00 :   00   (HH:MM:SS)    : :
Save . . . 2 1 Yes   2 No    :  :         07/19/01           (MM/DD/YY)    : :
Clock. . . 1 1 Local 2 GMT   :  :      2                                  : :
Timerid. .                   :  :        (yyyy-mm-dd-hh.mm.ss.micros)     : :
Route. . .                   :. :      3  Now                             : :
                             :  :                                         :
Scheduled.                   : F1=Help F2=Display Results     F3=Return : o
Recovery . 1 1 Ignore  2 Autolg : F6=Roll                     F12=Cancel : o
                             :.....................................: o
Remark  This timer periodically displays a list of active operators.
Command list status=ops

Command ===>
F1=Help  F2=Display Results F3=Return      F4=Options  F5=Intervals  F6=Roll
                            F9=Set Timer  F10=Notify  F11=Preview   F12=Cancel
```

Figure 146. CHRON EVERY Timer Example

8. To return to the EZLK6210 panel, press **Enter**. A panel similar to the panel shown in Figure 147 is displayed.

```
EZLK6210            Set CHRON EVERY Timer  NTV6D OPER2    07/19/01 20:12:40
 Target: NTV6D    Target Network ID:          Operid: OPER2
IP Addr:
   Port:             Remote Target Date and Time:
CHRON Type 1 1 EVERY         ..............................................
             2 AT            :                   EVERY                     :
             3 AFTER         :                                             :
                             : Interval 3 1  00 :   00 :   00     (HH:MM:SS) :
Save . . . 2 1 Yes   2 No    :            2                                :
Clock. . . 1 1 Local 2 GMT   :              (yyyy-mm-dd-hh.mm.ss.micros)   :
Timerid. .                   :            3 Daily                          :
Route. . .                   :.............................................:

Scheduled.                                                 Refresh 2 1 Yes 2 No
Recovery . 1 1 Ignore  2 Autolgn  3 Purge                  Test. . 2 1 Yes 2 No
                                                           Debug . 2 1 Yes 2 No
Remark  This timer periodically displays a list of active operators.
Command list status=ops

 Command ===>
F1=Help  F2=Display Results F3=Return      F4=Options  F5=Intervals  F6=Roll
                            F9=Set Timer  F10=Notify  F11=Preview   F12=Cancel
```

Figure 147. CHRON EVERY Timer Example

9. To see the options that are set in the CHRON command, press **F11**. A panel similar to the panel shown in Figure 148 on page 268 is displayed.

```
CNMKWIND OUTPUT FROM  EVERY COMMAND PREVIEW                  LINE 0 OF 3
*------------------------------ Top of Data -------------------------------*
 CHRON AT=(),EVERY=(INTERVAL=(),REMOVE=MANUALLY,DAYSWEEK=ALL,DAYSMON=ALL,CALEN
 DAR=ALL),RECOVERY=IGNORE,NOSAVE,LOCAL,ROUTE=OPER2,REM='This timer periodicall
 y displays a list of active operators.',COMMAND='list status=ops'
*----------------------------- Bottom of Data -----------------------------*



TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
CMD==>
```

Figure 148. CHRON EVERY Timer Preview

10. After previewing the timer, press **F3** to return to the EZLK6210 panel.
11. To set the timer, press **F9**. A message saying the timer is set is displayed.
12. Press **F2** to display the results of the CHRON command.
13. To return to the EZLK6210 panel, press **F3**.
14. To create a new timer or to copy the timer you created, press **F4** to display the panel shown in Figure 149.

```
EZLK6201          Set CHRON Otions panel   NTV6D OPER2    07/19/01 19:53:21
 Target: NTV6D    Target Network ID: USIBMNT  Operid: OPER2
IP Addr:
   Port:             Remote Targ .........................................
CHRON Type 1 1 EVERY             : Select an option and press enter.         :
             2 AT                :                                           :
             3 AFTER             :     1 Create a new timer                  :
                                 :     2 Copy this timer                     :
Save . . . 2 1 Yes   2 No        :                                           :
Clock. . . 1 1 Local 2 GMT       :                                           :
Timerid. . SYS01440              : F1=Help F2=Display Results      F6=Roll   :
Route. . . OPER2                 :                                F12=Cancel :
                                 :.........................................:
Scheduled. 07/19/01 19:53:21                                Refresh 2 1 Yes 2 No
Recovery . 1 1 Ignore  2 Autolgn  3 Purge                   Test. . 2 1 Yes 2 No
                                                            Debug . 2 1 Yes 2 No
Remark  This timer periodically displays a list of active operators.
Command list status=ops


Command ===>
F1=Help  F2=Display results F3=Return      F4=Options                F6=Roll
                            F9=Set Timer  F10=Notify  F11=Preview   F12=Cancel
```

Figure 149. Timer Options Panel to Create a New Timer or Copy a Timer

Type **1** to create a new timer of the same type or type **2** to copy a timer. You can copy a timer only if it was set previously.

Purging (Deleting) Timers

To purge a timer, type **3** or **P** in the input field beside the timer you want to purge and press **Enter**.

Note: Although **D** for Delete is not an option on the Timer Management panel, it is supported.

Figure 150 shows a timer being purged.

```
EZLK6000              TIMER MANAGEMENT    NTV6D OPER2    07/19/01 20:12:00
                                                          1 TO    6 OF    6
 Target: NTV6D    Target Network ID:          Operid: OPER2     Selected:    6
IP Addr:                                                       Purged:    0
   Port:          Remote Target Date and Time:

Filter criteria:
Type one action code. Then press enter.
  1|A=Add  2|C=Display/Change  3|P=Purge  4=Add CHRON timer
    Timer ID  Scheduled           Type   Interval   Task      Save   Catchup
 _  IDLEOFF   07/19/01 20:12:19   EVERY  00:10:00   AUTO1
              IDLEOFF 10000
 d  SYS00001  07/19/01 20:12:48   CHRON  00:01:00   OPER2
              list status=ops
 _  EZLRSET   07/20/01 00:01:00   AT                PPT
              EXCMD AUTO1 EZLEASTM
 _  PSTS      07/23/01 02:00:00   EVERY  MONDAY     AONMSG1
              DBMAINT EZLSTS 7
 _  PNPDA     07/23/01 04:00:00   EVERY  MONDAY     AONMSG1
              DBMAINT NPDA 7
 _  PNLDM     07/23/01 06:00:00   EVERY  MONDAY     AONMSG1
              DBMAINT NLDM 7


Command ===>
F1=Help      F2=End         F3=Return                F5=Refresh    F6=Roll
F7=Backward  F8=Forward                          F11=Reset Target  F12=Cancel
```

Figure 150. Example of Purging a Timer

After you press Enter to purge a specific timer, the panel shown in Figure 151 on page 270 is displayed. In the following example, the Total Purged Timers is now set to **1**, and **F9=Purged Timers** is displayed.

```
EZLK6000              TIMER MANAGEMENT    NTV6D OPER2    07/19/01 20:12:52
                                                          1 TO    5 OF    5
 Target: NTV6D    Target Network ID:          Operid: OPER2     Selected:    5
IP Addr:                                                        Purged:    1
   Port:          Remote Target Date and Time:

Filter criteria:
Type one action code. Then press enter.
  1|A=Add  2|C=Display/Change  3|P=Purge  4=Add CHRON timer
    Timer ID  Scheduled           Type   Interval   Task      Save   Catchup
 _  IDLEOFF   07/19/01 20:12:19   EVERY  00:10:00   AUTO1
              IDLEOFF 10000
 _  EZLRSET   07/20/01 00:01:00   AT                PPT
              EXCMD AUTO1 EZLEASTM
 _  PSTS      07/23/01 02:00:00   EVERY  MONDAY     AONMSG1
              DBMAINT EZLSTS 7
 _  PNPDA     07/23/01 04:00:00   EVERY  MONDAY     AONMSG1
              DBMAINT NPDA 7
 _  PNLDM     07/23/01 06:00:00   EVERY  MONDAY     AONMSG1
              DBMAINT NLDM 7


 EZL971I REQUESTED TIMERS WERE DELETED ON NTV6D
Command ===>
F1=Help      F2=End         F3=Return                 F5=Refresh    F6=Roll
F7=Backward  F8=Forward     F9=Purged Timers      F11=Reset Target  F12=Cancel
```

Figure 151. Active Timer Panel After a Purge

Reinstating Timers

To display purged (or deleted) timers, press **F9** on the Active Timer panel.

To reinstate a purged timer enter a **1** in the input field beside the timer you want to reinstate and press **Enter**. The Change Timer panel that is appropriate for the timer you requested to be reinstated is displayed.

Follow the steps listed previously for changing timers and make any necessary changes before setting the timer.

Figure 152 on page 271 shows an example of a Purged Timer panel.

```
EZLK6000              TIMER MANAGEMENT    NTV6D OPER2    07/19/01 20:13:54
                                                          1 TO    1 OF    1
 Target: NTV6D    Target Network ID:          Operid: OPER2     Selected:    5
IP Addr:                                                        Purged:    1
   Port:          Remote Target Date and Time:


Type one action code. Then press enter.
  1|R=Reinstate
    Timer ID  Scheduled           Type   Interval   Task      Save   Catchup
 r  SYS00001  07/19/01 20:12:48   CHRON  00:01:00   OPER2
              list status=ops




Command ===>
F1=Help      F2=End         F3=Return                              F6=Roll
F7=Backward  F8=Forward     F9=Active Timers                      F12=Cancel
```

Figure 152. Example of Purged (or Deleted) Timer Panel

The following panel is shown after the requested timer has been set. Note the following changes on the panel:

- The timer is no longer displayed.
- The Selected field is increased by 1.
- The Purged field is decreased by 1.

. Press **F9** to display your active timers.

Figure 153 on page 272 shows an example of changes on the panel.

```
EZLK6000              TIMER MANAGEMENT    NTV6D OPER2    07/19/01 20:17:00
                                                          0 TO    0 OF    0
 Target: NTV6D    Target Network ID:          Operid: OPER2     Selected:    6
IP Addr:                                                        Purged:    0
   Port:          Remote Target Date and Time:


Type one action code. Then press enter.
  1|R=Reinstate
    Timer ID  Scheduled           Type   Interval   Task      Save   Catchup









Command ===>
F1=Help      F2=End         F3=Return                              F6=Roll
F7=Backward  F8=Forward     F9=Active Timers                      F12=Cancel
```

Figure 153. Purged (or Deleted) Timer Panel After Reinstating

Chapter 18. Debugging Automation

In automating your enterprise using the NetView program, the unexpected occasionally happens: a command list that was supposed to handle a problem does not handle it; a message that was supposed to be automated was not; an alert that was supposed to be suppressed was not; a timed command does not run when it was supposed to; and so on.

Even in the most comprehensive automated environment, human intervention is sometimes required to solve a problem that automation was not designed to handle and to update automation when it fails to detect or recover a problem. The remainder of this chapter contains problem scenarios followed by problem determination steps and possible solutions.

Determining Why a Message Is Not Automated by the Automation Table

If a message was not automated by the automation table, first consider the message type. If the message is a log-only message (a message that only goes to the network log), it is not subject to processing by the automation table or by the ASSIGN command. An example of a log-only message is CNM154I.

If the message is processed by the operating system before being forwarded to NetView, complete the following steps to determine why the message was not automated by the automation table:

1. Determine whether AUTO(NO) is specified for the message in MPF. In MPF, specifying AUTO(NO) either as a default or specifically on an MPF entry for a message prevents the message from being forwarded to the NetView program for automation. If AUTO(NO) is specified in your MPF table for this message, AUTO(YES) or AUTO(token) needs to be specified if you want the message to be processed by the NetView program.
2. If you are using the MVS subsystem interface (SSI) rather than extended consoles for automation, determine whether the SSI address space is active. Issue the command `d a,l` from the MVS operating system console to return a list of active system address spaces (among other information), one of which is be the NetView subsystem address space application name. If the NetView subsystem address space is inactive, it can be activated by starting the NetView subsystem procedure (CNMPSSI as shipped with NetView).
3. Determine whether the NetView CNMCSSIR task is active. Issue the NetView command, LIST STATUS=OPT, to find out if the CNMCSSIR task is active. If it is not active, the NetView program does not receive unsolicited system messages over the subsystem interface.
4. If you are using MVS extended consoles, you must have:
   - An extended console with the AUTO(YES) attribute
   - The task with load module name CNMCSSIR active

   Optionally, you can have another task receive AUTO(YES) messages.

Checking Other Areas

Use the following additional steps to determine why a message was not automated:

1. Determine whether the installation exit DSIEX02A, DSIEX16, or DSIEX17 is changing or deleting the message. If you have an active DSIEX02A, DSIEX16, or DSIEX17 exit routine, it can affect the message. DSIEX02A and DSIEX17 can change or delete the message prior to automation, and DSIEX16 can affect the message or automation actions scheduled by the automation table.
2. Determine whether a TRAP in a REXX or HLL program, an &WAIT in a NetView command list language command list, or a PIPE command is suppressing the message. The message is not processed by the automation table or logged to the network log if:
   - It is being processed on a NetView task that has an active TRAP AND SUPPRESS (REXX and HLL).
   - It is being processed on a NetView task that has a &WAIT that is waiting for the message with &WAIT SUPPRESS in effect (NetView command list language).
   - It is issued within a PIPE command without the EXPOSE stage.
3. Issue a NetView AUTOTBL STATUS command to find out which automation table is currently active and determine whether this is the correct automation table.
4. Determine whether the automation table is receiving the message. You can accomplish this by adding the following statement to your automation table:

   ```
   IF MSGID = 'XYZ123I' THEN
      EXEC(CMD('MSG OPER1 AUTOMATION IS RECEIVING XYZ123I'))
      CONTINUE(Y);
   ```

   This statement sends OPER1 a message (DSI039I) when the message that is to be automated is received by the automation table. This statement does not affect any other processing of the message by subsequent statements in the automation table because of the CONTINUE(Y) action, which allows later automation table statements in the table to also process the message. Message DSI039I identifies the task that processed the message.
5. Trace the processing of a message or MSU through the automation table using the TRACE action. The TRACE action sets a trace tag in the AIFR and an indicator that the AIFR is to be traced as it is processed by the automation table. Detailed trace information is displayed on the console by message BNH370I for each part of each automation table statement that analyzes the AIFR.

   An example automation table statement to trace a message whose text begins with the characters WAC follows:

   ```
   IF (LABEL: STATEMENT1) TEXT = 'WAC' . THEN
     TRACE('TRCTAG01');
   ```
6. Use the AUTOCNT command to generate a detailed automation table usage report, then determine whether multiple statements in the automation table match the message. A message detail usage report shows how often an automation table statement was compared against messages and how often it was matched with messages.

Reading the Message Detail Report

Table 20 shows how to interpret some of the data from the detail report.

Table 20. Determining Why a Message Was Not Automated Using the Detail Report

Indicators	Possible explanation
COMPARE COUNT > 0 MATCH COUNT = 0	The automation table statement might be coded incorrectly, in which case the automation statement never matches the message

Table 20. Determining Why a Message Was Not Automated Using the Detail Report (continued)

Indicators	Possible explanation
MATCH COUNT = 0 COMPARE COUNT = 0	It is possible that a prior statement in the automation table matches the message and prevents the statement from being processed

If a command was scheduled, determine which of the following situations prevented it from running:

- It was sent to a task that was not logged on.

  You can use the LIST STATUS=OP command to determine whether the task that was supposed to receive the command is logged on, although it does not tell you if the task was logged on at the time the message was automated. You can also check the network log for DWO032E messages, which are written when a command is sent to a task that is not logged on. A CNM493I message found near a DWO032E message identifies the statement in the automation table that scheduled the command.
- Another command list is running and has not finished. The following example situations might cause a command list not to finish running, thus possibly preventing other command lists from running:
  - Using an &WAIT (NetView command list) or a TRAP or WAIT (REXX) without a timeout value. The command list waits forever without a timeout value.
  - For command lists running under an autotask, using an &PAUSE (NetView command list) or a PULL (REXX) to wait for operator input in a command list, causes the command list to wait forever because no console is available to provide input.
  - Using a WTOR to the system console that never gets a reply.
  - Processing in an infinite loop, which never completes.

  To determine which command list is preventing the task from ending:
  - Use the LIST *taskname* command for a task to show whether a command list is currently running. Then enter `EXCMD taskname,RESET` to halt the command list that is currently running. This command generates a message in the NetView log that informs that the command list was reset.
  - Scan the network log for the last CNM493I message for this operator. This typically indicates the last command scheduled to that task from the automation table. However, this does not indicate commands scheduled with timer commands, started using EXCMD from other tasks, and other non-operator commands.
- Determine whether command security prevents a command or command list from being issued from the automation table. If you set AUTOSEC=CHECK using the NetView DEFAULTS command, all commands routed from the automation table are authority checked against the target task, unless SEC=BY was specified on the CMDDEF statement.

Topic:	Reference:
The AUTOTBL, AUTOCNT, and TASKUTIL commands	NetView online help
Using the TASKUTIL command	Additional information about the TASKUTIL command can be found in the *IBM Tivoli NetView for z/OS Tuning Guide*

Topic:	Reference:
The DSIEX16 and DSIEX17 installation exits	*IBM Tivoli NetView for z/OS Programming: Assembler*
DSIEX02A and XITCI installation exits	*IBM Tivoli NetView for z/OS Programming: Assembler* or *IBM Tivoli NetView for z/OS Programming: PL/I and C*
Using MPF, PROP, and OCCF	*IBM Tivoli NetView for z/OS Automation Guide*
MVS extended consoles for automation	*IBM Tivoli NetView for z/OS Automation Guide*
Command security	*IBM Tivoli NetView for z/OS Security Reference*

Determining Why an Alert Is Not Automated

To determine why an alert is not automated:

1. Determine whether the alert is blocked by a RATE statement. If you do not use an AUTORATE statement, MSUs blocked by a filter set by the RATE function are not automated.
2. If the alert is not showing up in the hardware monitor database, it might be blocked by either an SRFILTER command in the hardware monitor or an SRF action in the automation table.
3. Determine whether the intended automation statement is coded correctly. For example, when you specify a *byte* position within an MSU major vector, subvector, or subfield for the MSUSEG condition item, be sure to include key and length values. Note that *byte* position refers to position, not offset (start counting at 1, not at 0). To determine whether an MSU condition is not coded correctly, consider adding a statement similar to the following example to display portions of the MSU:

   ```
   IF MSUSEG(0000.xx.xx) = ALERT_SUBFIELD THEN
      EXEC(CMD('MSG NETOP1 ALERT 0000.xx.xx RECEIVED, xx SUBFIELD
           IS 'ALERT_SUBFIELD)
      ROUTE(ONE AUTOx))
      CONTINUE(Y);
   ```

   This can assist you in determining how to correctly code automation table statements.
4. Determine whether the installation exit XITCI or DSIEX16B is changing or deleting the alert. If you have an active XITCI or DSIEX16B exit routine, it can affect the alert. XITCI can change or delete the alert prior to automation, and DSIEX16B can affect the alert or automation actions scheduled by the automation table.
5. Issue the NetView AUTOTBL STATUS command to find out which automation table is currently active and determine whether this is the correct automation table.
6. Determine whether the automation table is receiving the alert. You can accomplish this by adding a statement like this to your automation table:

   ```
   IF MSUSEG(0000.xx) = . 'xxxxxxx' . THEN
      EXEC(CMD('MSG OPER1 AUTOMATION IS RECEIVING xxxxxxxx ALERT')
           ROUTE (ONE AUTOx))
      CONTINUE(Y);
   ```

   Note: The ROUTE statement is included because under certain conditions (for example, if BNJDSERV is not started from an OST) certain actions fail

because they cannot be processed under BNJDSERV (DST). This statement sends OPER1 a message (DSI039I) when the alert is received by the automation table.

This statement does not affect other processing of the alert by subsequent statements in the automation table because of the CONTINUE(Y) action. The CONTINUE(Y) action allows other or subsequent automation table statements in the table to also process the alert.

7. Use the AUTOCNT command to generate a detailed automation table usage report, then determine whether multiple statements in the automation table match the alert. A detailed automation table usage report shows how often an automation table statement was compared against an alert and how often it was matched with an alert.

   Table 21 shows how to interpret some of the data from the detail report.

Table 21. Determining Why an Alert Was not Automated Using the Detail Report

Indicators	Explanation
COMPARE COUNT > 0 MATCH COUNT = 0	The automation table statement might be coded incorrectly, in which case the automation statement never matches the alert
MATCH COUNT = 0 COMPARE COUNT = 0	It is possible that a prior statement in the automation table matches the alert and prevents the statement from being processed

8. Determine whether the conditions and actions are coded correctly on the automation statement.
9. Determine whether an automation table MSUSEG function has a typographical error.
10. If a command was scheduled, determine whether it was prevented from running because:
    - It was sent to a task that was not logged on.

      You can use the LIST STATUS=OP command to determine whether the task that was supposed to receive the command is logged on, although it does not tell you if the task was logged on at the time the alert was automated. You can also check the network log for DWO032E messages, which are written when a command is sent to a task that is not logged on. A CNM493I message found near a DWO032E message identifies the statement in the automation table that scheduled the command.
    - Another command list is running and has not finished. The following example situations might cause a command list not to finish running, thus possibly preventing other command lists from running:
      – Using an &WAIT (NetView command list) or a TRAP or WAIT (REXX) without a timeout value. The command list waits forever without a timeout value.
      – Using an &PAUSE (NetView command list) or a PULL (REXX) to wait for operator input in a command list. Because no console is available to provide input, the command list wait forever. This applies only to command lists running under an autotask.
      – Using a WTOR to the system console that never gets a reply.
      – Processing in an infinite loop, which never completes.

      To determine which command list is preventing the task from ending:
      – Use the LIST *taskname* command for a task to show whether a command list is currently running. Then enter `EXCMD taskname,RESET` to halt the

command list that is currently running. This command generates a message in the NetView log that informs that the command list was reset.

– Scan the network log for the last CNM493I message for this operator. This typically indicates the last command scheduled to that task from the automation table. However, this does not indicate commands scheduled with timer commands, started using EXCMD from other tasks, and other non-operator commands.

Topic:	Reference:
RATE, AUTORATE statements	*IBM Tivoli NetView for z/OS Administration Reference*
SRFILTER, AUTOTBL, AUTOCNT, TASKUTIL commands	NetView online help
Using the TASKUTIL command	Additional information about the TASKUTIL command can be found in the *IBM Tivoli NetView for z/OS Tuning Guide*
MSUSEG condition item	*IBM Tivoli NetView for z/OS Automation Guide*
XITCI installation exit	*IBM Tivoli NetView for z/OS Programming: Assembler* or *IBM Tivoli NetView for z/OS Programming: PL/I and C*
DSIEX16B installation exit	*IBM Tivoli NetView for z/OS Programming: Assembler*

Determining Why an Alert Is Not Displayed on the Tivoli Enterprise Console

To determine why a NetView alert is not displayed on the Tivoli Enterprise Console:

1. Determine whether the NetView alert passed the NetView TECROUTE filter (defined on the SRFILTER command). To see the current definition for the TECROUTE filter, enter the command `DFILTER TECROUTE`. See the *IBM Tivoli NetView for z/OS Command Reference Volume 1* for information on how to code the TECROUTE filter. The TECROUTE filter can also be set by the automation table.
2. Verify that Event Services has started. Ensure that the Event Services startup procedure is called by your NetView startup procedure. If it is not, you can add it and restart NetView, or you can run the Event Services startup procedure alone to start it without recycling NetView.
3. Determine whether the NetView subsystem interface (SSI) is active. If it is not, stop and restart the NetView program-to-program interface (PPI) with the SSI active.
4. Check your Tivoli event filters to determine whether the event was screened out by a filter.
5. Check the Tivoli rules for event processing to determine whether a rule has screened out this event.
6. Verify that the .baroc file for IBM Tivoli NetView for z/OS V5R3 has been installed on the Tivoli Enterprise Console server. The .baroc file defines all the classes of events that can be sent to the Tivoli Enterprise Console by NetView.
7. If you have customized the NetView class definition statements (CDS) file, check for the following errors:
   - Verify the syntax in the CDS file. A syntax error results in a NetView error message, and the event is not sent to the Tivoli Enterprise Console.

- Ensure all slot names are specified in the CDS file are matches for slot names in the .baroc file. A mismatch does not result in a NetView error message, but the event is not displayed at the Tivoli Enterprise Console. Change the slot name in the CDS file or add an entry to the .baroc file for the slot name.

Determining Why a Tivoli Enterprise Console Event Is Not Forwarded to NetView

To determine why a Tivoli Enterprise Console event is not forwarded to NetView:

1. Determine whether the Tivoli Enterprise Console rule base has been properly defined to forward this event to IBM Tivoli NetView for z/OS V5R3. Check the following items:
   - Has a rule been defined? If not, refer to the Tivoli Global Enterprise Manager library for information about defining a rule base.
   - Has the correct host name been defined in the rule base? The event might have been forwarded to a different NetView host. Also, if the host name defined in the rule base is not a valid NetView host name, the event might not have been forwarded at all.
   - Is the syntax of the Tivoli Enterprise Console rule base correct? Debug syntax errors.
   - Has the rule base been compiled and loaded on the T/EC server? See *Tivoli Enterprise Console User's Guide* for information on how to compile and load the rule base.
2. Verify that Event Services has started. Ensure that the Event Services startup procedure is called by your NetView startup procedure. If it is not, you can add it and restart NetView, or you can run the Event Services startup procedure alone to start it without recycling NetView.
3. Determine whether the NetView subsystem interface (SSI) is active. If it is not, stop and restart the NetView program-to-program interface (PPI) with the SSI active.
4. Verify that the NetView hardware monitor is active. If it is not, check your NetView startup procedure for the hardware monitor startup command, and start the hardware monitor.
5. Determine whether the NetView recording filters (ESREC and AREC) have been defined to pass this particular event through their filters. See the SRFILTER command definition in *IBM Tivoli NetView for z/OS Command Reference Volume 1* and "Using Hardware Monitor Filters" on page 208 for help in changing the ESREC and AREC filter definitions.

Determining Why a Command List Does Not Complete

Sometimes, a command list is not processed correctly. For example, you might know from message CNM493I that the command list was called by automation; however, one of the commands from the command list might not have been issued.

Use the following steps to determine why one or more commands from a command list did not run:

1. Determine whether command security prevented the command list from being issued. Command security can be defined by:
   - The NetView command authorization table
   - An SAF product, such as RACF

If command security prevented the command list from running, message DSI213I in the netlog indicates that the command list is being protected.

Look in the CNMCMD members for a CMDDEF statement. If you use a synonym for the command list, the command identifier in the CMDDEF statement needs to match the command security in effect.

If you set AUTOSEC=CHECK using the NetView DEFAULTS command, all commands and command lists routed from the automation table are authority checked against the target task, unless SEC=BY was specified on the CMDDEF statement.

If your security administrator has set up command security to protect your command list, refer to the *IBM Tivoli NetView for z/OS Administration Reference* to get your security matching your expectations.

2. Verify that the command list was called correctly in the following way:

If called from...	Then...
Automation table	Verify that it ran under an active task. Unless you specify otherwise, the network log contains a CNM493I message for each command list called from the automation table.
A TIMER command	Verify that the timed command was scheduled to run, and that the task that was to run the command was active.
Another command list	Check to see that the logic path to call the command list was taken in the prior command list.

3. Trace the processing of the command list. You can use the REXX TRACE instruction and the NetView command list &CONTROL statement to:
   - Control the amount of feedback during processing
   - Indicate how statements are interpreted
   - Indicate whether statements complete processing

   Tracing helps identify problems such as:
   - Logic errors in the command list that produce unexpected results
   - Severe errors that halt processing
   - WAIT instructions or &WAIT control statements that continues processing while waiting for a message
   - The use of &PAUSE (NetView command list) or PULL (REXX) to wait for operator input in a command list running under an autotask causes the autotask to wait forever because no console is available to provide input.
   - Nested command lists that cause problems
4. Use the TASKUTIL command to determine whether the command did not run because another command, with a higher priority, was issued first and prevented the command from running. The TASKUTIL command can show if the task is currently running another command list.

In addition, the following NetView commands can affect how command lists are processed:

CMD, DEFAULTS, OVERRIDE
These commands can effect the priority at which a command is run.

RESET
This command can be used to cancel a command list that is running.

Topic:	Reference:
TRACE, PULL instruction	*TSO/E REXX/MVS Reference*

Topic:	Reference:
WAIT instruction	*IBM Tivoli NetView for z/OS Programming: REXX and the NetView Command List Language*
&CONTROL, &PAUSE statement	*IBM Tivoli NetView for z/OS Programming: REXX and the NetView Command List Language*
&WAIT statement	*IBM Tivoli NetView for z/OS Programming: REXX and the NetView Command List Language*
CMD, DEFAULTS, OVERRIDE, RESET, TASKUTIL commands	NetView online help
Using the TASKUTIL command	Additional information about the TASKUTIL command can be found in the *IBM Tivoli NetView for z/OS Tuning Guide*

Determining Why a Timed Command Does Not Run

To determine why a timed command did not run:

1. Determine whether command security protects the timer command or prevents the task from issuing the command. For instance, the command, its keywords, or values might be protecting using a NetView command authorization table or an SAF product such as RACF.

   In addition, depending on which task is checked for command authorization, the level of authorization at the source of the timer command might be wrong. To ensure that your timer command security meets your expectations, see the *IBM Tivoli NetView for z/OS Administration Reference*.
2. Verify that you specified the correct timer command. For example, if you want to schedule the STATREP command to run at 11:00 a.m., but you specify `after 11:00,statrep`, the command runs 11 hours from when you enter it, not at 11:00 a.m. (You can use the AT command to schedule the command at 11:00 a.m.).
3. Determine whether the command was scheduled for the following day because of an incorrect time specification on the AT command. Issue the LIST TIMER=ALL,OPER=ALL command to list all currently scheduled timed commands. If the timed command is listed there, but is scheduled to run on the following day, it is possible the time was specified incorrectly. An important thing to remember is that the timer command AT uses a 24 hour clock, so if you want to schedule a command for 6:00 p.m., specify 18:00, and not 6:00. For example, if you specify the AT 6:00,STATREP command after 6 a.m., the command is scheduled for 6:00 a.m. on the next day.
4. Determine whether the task that was supposed to run the command is logged off. The task that is to run the scheduled command needs to be active for the command to be issued. It is a good idea to schedule timer commands from autotasks that are always active, or to specify the PPT operand on the timer command so that they run on the NetView PPT task, which is always active. However, the PPT task and autotasks cannot process full-screen commands.
5. Determine whether a timer command scheduled to run under the NetView PPT task is not allowed to run under the PPT. In this case, schedule the command to run under an autotask or other operator task.
6. Determine whether the timer command was issued successfully. For example, it needs to have been issued from a command list but the command list never completed because of a syntax error in the command. The NetView log contains the syntax error message.

7. Determine whether the command was scheduled to a task but did not run because of a command list that is already running, but never finished. The following example situations might cause a command list to continue running, thus possibly preventing other command lists from running:
   - Using an &WAIT (NetView command list) or a TRAP or WAIT (REXX) without a timeout value. The command list waits forever without a timeout value.
   - Using an &PAUSE (NetView command list) or a PULL (REXX) to wait for operator input in a command list. Because no console is available to provide input, the command list waits forever. This applies only to command lists running under an autotask.
   - Using a WTOR to the system console that never gets a reply.
   - Processing in an infinite loop, which never completes.

   See "Determining Why a Command List Does Not Complete" on page 279 for additional information on determining why a command list did not run.
8. Determine whether the system went down and the timed command was not saved or restored.

Topic:	Reference:
AFTER, AT, EVERY command	NetView online help
&PAUSE statement	*IBM Tivoli NetView for z/OS Programming: REXX and the NetView Command List Language*
&WAIT statement	*IBM Tivoli NetView for z/OS Programming: REXX and the NetView Command List Language*
TRAP, WAIT instructions	*IBM Tivoli NetView for z/OS Programming: REXX and the NetView Command List Language*
PULL statement	*TSO/E REXX/MVS Reference*

Determining Why Automation Is Taking Too Much Processing Time

You can use the following NetView commands to help you determine how to tune your NetView automation processing:

TASKMON

This command displays processor, storage, message queuing, penalty time, and input/output statistics for tasks running in NetView. Use this information to determine:

- Which tasks are taking too much processing time
- Which tasks are delayed by resource penalties
- Which tasks have excessive input/output that LOADCL procedures might help
- Which tasks have excessive message queuing activity or are causing delays in other tasks

TASKUTIL

This command shows total processing time (processor usage), and shows system and NetView percentages separately for each active NetView task. You can use this information to spot which autotask is using the most processing time to find which autotasks need help.

AUTOCNT

This command is used to determine how the automation table is being utilized by generating:

- Detailed usage reports that show on a statement-by-statement basis how often each statement has been compared and how often it has been matched. These numbers can be used to determine whether the table needs to be restructured.
- Summary reports that show the total number of commands processed from the automation table and the average messages and average alerts processed per minute. This information can help you spot increased system processing as a result of running a large number of commands and having automation process large numbers of messages and alerts.

You can then tune your NetView automation processing by:

- Placing the most heavily matched statements at the top of the automation table. Because a preprocessed, internal version of the automation table is searched in a top-down method, this saves processing.
- Suppressing system messages, where possible, using the operating system message processing facility (MPF in MVS, PROP in VM, OCCF in VSE).
- Using the XITCI exit to process alerts, and use assembler rather than a high level language for quickest processing.
- Using BEGIN and END statements to segment the automation table logically. Because the automation table skips the entire BEGIN/END section if it does not match the message or alert, this improves performance.
- Using the LOADCL command to load into storage those command lists that are most frequently used. This decreases the processing load and increased performance savings because the command lists are not loaded to and deleted from main storage every time they are run.
- Using the automation table when possible to automate messages or alerts, rather than of using command lists. This saves the processing time required to load and process the command list. The AUTOCNT summary usage report can give you an idea of how many commands are processed from the automation table.
- Using compiled REXX command lists instead of interpreted REXX command lists. Most command lists, especially those that do a lot of mathematical computations, benefit from being compiled.

Topic:	**Reference:**
TASKUTIL, AUTOCNT commands	NetView online help
LOADCL command	*IBM Tivoli NetView for z/OS Programming: REXX and the NetView Command List Language*
Using the TASKUTIL command	Additional information about the TASKUTIL command can be found in the *IBM Tivoli NetView for z/OS Tuning Guide*
Using the AUTOCNT command	Additional information about the AUTOCNT command can be found in the *IBM Tivoli NetView for z/OS Tuning Guide*
Using MPF, PROP, OCCF	*IBM Tivoli NetView for z/OS Automation Guide*
Using the XITCI exit	*IBM Tivoli NetView for z/OS Programming: Assembler*
TASKMON	NetView Online Help

Determining Why a Message Is Routed to the Wrong Operator

Check the following things to determine why an operator received a message meant for another operator.

- Check to see that the correct automation table statement is acting on the message.
- If the message is being routed using the ASSIGN command (ASSIGN PRI for solicited messages and ASSIGN COPY for unsolicited messages), check to see that it is being routed correctly.

  If the message is being routed using the ASSIGN PRI command, check the list of operators who are to receive the message. Because only the first operator who is logged on receives the message, ensure that an incorrect operator was not added near the beginning of the list.

  You can also check to see that specific ASSIGN commands targeted at a message or message block do not override more general ASSIGN commands for the same message or message block. For example, if message XYZ123I is processed by the NetView program, operators assigned to receive MSG=XYZ123I receive the message, and operators assigned to receive MSG=XYZ* do not. Operator assignments can be verified using the NetView LIST command.
- Check to see that the EXEC(ROUTE) command in the automation table and the MSGROUTE command from a command list are used correctly. If the ONE option is used to route a message to only one operator, and not to all the operators in a list of operators or operator groups, the intended operator is the first operator in the list of operators that can receive the message.
- If you have an installation exit routine for DSIEX02A, DSIEX16, or DSIEX17, examine the exit code to ensure that it is not changing the routing for the message.

Topic:	**Reference:**
ASSIGN, LIST commands	NetView online help
EXEC(ROUTE) action	*IBM Tivoli NetView for z/OS Automation Guide*
MSGROUTE command	*IBM Tivoli NetView for z/OS Programming: REXX and the NetView Command List Language*
Solicited and unsolicited messages	"How Messages Flow" on page 384
Exits DSIEX16 and DSIEX17	*IBM Tivoli NetView for z/OS Programming: Assembler*
Exit DSIEX02A	*IBM Tivoli NetView for z/OS Programming: Assembler* or *IBM Tivoli NetView for z/OS Programming: PL/I and C*

Determining Why a Pipe Command Does Not Process Correctly

If a PIPE command does not process correctly, it is possible that the command and its messages are not correlated. Pipelines also support a variety of DEBUG options. You can use the HOLD stage to determine whether a command and its messages are correlated. For more information, refer to *IBM Tivoli NetView for z/OS Programming: Pipes*.

Part 5. Problem Diagnostics

Chapter 19. Proactive Investigating

Problem diagnosis involves the requesting of additional information to let you further analyze the cause of a status change from satisfactory to unsatisfactory. You can then resolve the problem situation and decide on the proper action to bypass or resolve the unsatisfactory condition.

Chapter 19, "Proactive Investigating" provides problem scenarios that illustrate how to solve potential problems before they affect the status of your network. The tools used to solve these problems are the NetView Graphic Monitor Facility, command facility, status monitor, and hardware monitor.

Chapter 20, "Reactive Investigating," on page 299 provides problem scenarios that illustrate how to solve problems that have already occurred. The tools used to solve these problems are the NetView management console, session monitor, hardware monitor, VTAM commands, NPM, AON, and command facility.

Preventing Problems

Proactive investigating involves resolving potential problems before they affect the network. You can accomplish this by monitoring the status of various network components (such as controllers, links, and so on) and studying response time trends. Use the following scenarios to investigate potential network problems. Table 22 gives an overview of the problem scenarios that are described in this chapter. For each scenario, the table lists the product used to solve the problem and the types of resources involved.

Table 22. Proactive Scenarios Cross Reference

Problem Scenario	Component Used to Resolve Problem	Resources Involved
Analyzing system performance using TASKUTIL	Command facility	Subarea
Initiating error recovery	Status monitor	Subarea
Displaying the status of a resource	Status monitor	Subarea
Identifying intermittent problems	Hardware monitor	Subarea
Determining controller status	Hardware monitor	Subarea
Checking the status of the session monitor and hardware monitor databases	Command facility	Subarea
Anticipate excessive use of task resources	Command facility Automate messages BNH162I and BNH163I	Task-specific processor, storage, I/O, task-to-task messages
Anticipate depletion of the NetView address space storage	Command facility Automate messages BNH162I and BNH163I	NetView storage

Analyzing System Performance Using TASKUTIL (Command Facility)

You can use the TASKUTIL or the newer TASKMON command to display performance information, including processor utilization, queue lengths, storage use, and active command lists. Consider setting an EVERY timer under an autotask to call TASKUTIL or TASKMON at least once a day (or even once every hour). The output from TASKUTIL can be compared to the output from the previous day and used to diagnose performance or storage problems.

For example, if you enter:

```
taskutil type=dst
```

A response similar to Figure 154 is received (by default, command responses are also sent to the network log).

```
DWO022I
TASKNAME TYPE DPR     CPU-TIME N-CPU% S-CPU% MESSAGEQ STORAGE-K  CMDLIST
-------- ---- --- ------------ ------ ------ -------- --------- --------
AAUTSKLP DST  249     22019.13  49.02   9.37        0     87521      N/A
BNJDSERV DST  250      4466.25   7.35   1.41        0       357      N/A
DSIELTSK DST  253      4731.99   7.24   1.38        0        31      N/A
DSICRTR  DST  251      1362.16   1.97   0.38        0        32      N/A
DSILOG   DST  254       624.64   1.40   0.27        0        23      N/A
DSIAMLUT DST  248      1145.74   1.34   0.26        0        26      N/A
AAUTCNMI DST  249        94.44   0.33   0.06        0       463      N/A
BNJDSE36 DST  249         0.04   0.00   0.00        0        25      N/A
CNMTAMEL DST  249         0.36   0.00   0.00        0        49      N/A
CNM01LUC DST  251       306.54   0.00   0.00        0        43      N/A
DSIGDS   DST  254         1.89   0.00   0.00        0        46      N/A
DSIHPDST DST  252         2.15   0.00   0.00        0        39      N/A
DSIKREM  DST  250         2.15   0.00   0.00        0       549      N/A
DSIROVS  DST  251         0.03   0.00   0.00        0        13      N/A
DSISVRT  DST  253         0.93   0.00   0.00        0       105      N/A
DSIUDST  DST  250         2.59   0.00   0.00        0        14      N/A
DSI6DST  DST  251        28.98   0.00   0.00        0        41      N/A
NETVIEW  OTHR N/A          N/A   0.00   0.00      N/A       N/A      N/A
NETVIEW  SRB  N/A       4026.90   5.93   1.13      N/A       N/A      N/A
NETVIEW  TOTL 157      54766.96 100.00  19.11      253    157477      N/A
SYSTEM   TOTL N/A          N/A    N/A  63.70      N/A       N/A      N/A
```

Figure 154. TASKUTIL Command Output

For each task, the task name (TASKNAME), task type (TYPE), dispatching priority (DPR), and processor usage (CPU-TIME) is displayed. In addition, you can use the following information (shown in Figure 154) to diagnose performance or storage problems.

Table 23. TASKUTIL Output Description

Field Name/Description	How to Use
N-CPU% (NetView program CPU utilization) Relative contribution of the task to the NetView program processor utilization, based on a maximum of 100%.	• If this value is continuously high for an operator task, autotask, distributed task, or NNT, this can indicate an endless loop condition in a command list or argument. The active command list is displayed in the `CMDLIST` field. • If this value is low, with the same command list active and message buildup for an operator task, autotask, distributed task, or NNT, this can indicate that the command list is stuck in a WAIT.
S-CPU% (system CPU utilization) Contribution of the task to the total system processor utilization, based on a maximum of 100%.	• If this value is continuously high for an operator task, autotask, distributed task, or NNT, this can indicate an endless loop condition in a command list or argument. The active command list is displayed in the `CMDLIST` field. • If this value is low, with the same command list active and message buildup for an operator task, autotask, distributed task, or NNT, this can indicate that the command list is stuck in a WAIT.
MESSAGEQ Number of messages currently backed up on the 3 public message queues of the task (HIGH, NORMAL, and LOW).	• If this value is high, with the same command list active and low processor usage for an operator task, autotask, distributed autotask, or NNT, this can indicate that the command list is stuck in a WAIT. • If this value continues to grow for a task during a steady state period when you are expecting the workload activity of the NetView program to be fairly uniform, and if the total system processor utilization is near 100%, this can indicate that the NetView program is not getting dispatched frequently enough to do its work. Continued growth results in continued NetView storage growth, which can lead to storage abends. If you detect such a condition, consider ending low-priority processor-intensive applications to relieve the system processor constraint. If the NetView program regularly experiences message growth, consider making the MVS dispatching priority for the NetView address space more favorable.
STORAGE-K Amount of pooled and non-pooled queued storage, in kilobytes, currently being used by the task.	If this value continues to rise for a task, this can indicate that the task is getting queued storage but not freeing it properly.
CMDLIST Current active command list running on the task, if any.	If the same command list is active, with message buildup and low processor usage for an operator task, autotask, distributed autotask, or NNT, this can indicate that the command list is stuck in a WAIT.

Topic:	Reference:
Tuning your system using TASKUTIL	*IBM Tivoli NetView for z/OS Tuning Guide*
TASKUTIL command	NetView online help

Initiating Error Recovery (Status Monitor)

You can use the status monitor to initiate error recovery. The status monitor tries to reactivate nodes that have failed and have been made inactive by VTAM. You can also specify in VTAMLST the nodes that cannot be reactivated automatically by specifying NOMONIT when defining the node for the status monitor. All the nodes marked as NOMONIT are stored in a reactivation exclusion list. You can add nodes to this list using the MONIT STOP command or the MONOFF command list.

For example, to stop the automatic node reactivation function of all nodes, enter:

```
monit stop,all or monoff all
```

You can remove nodes from this list (to allow reactivation) using the MONIT START command or MONON command list (so long as NOMONIT was not specified in the VTAMLST file for the particular node). For example, to start the automatic node reactivation function of all nodes, enter:

```
monit start,all or monon all
```

To start automatic reactivation for LINE27, enter:

```
monit start,line27 or monon line27
```

You can also initiate error recovery using Automated Operations Networks (AON). AON recovers network resources by monitoring critical VTAM messages and taking automated action based on preset tailored criteria. AON reacts to adverse conditions of network resources and notifies operators of these conditions, when appropriate. Recovery criteria can be set based on resource type, resource naming convention, explicit resource name, or network-wide settings. A variety of parameters and options can be selected to control when and how recovery takes place.

Topic:	Reference:
MONIT, MONON, MONOFF commands	NetView online help

Displaying Resource Status (Status Monitor)

As a network operator, one of the first things you do after logging on to the NetView program is to monitor the network resources you are responsible for controlling. You can use the status monitor to collect and summarize information on the status of resources defined in a VTAM domain. You can then use this information to activate, inactivate, or display the resources.

Complete the following steps to monitor the status of resources and to activate inactive resources using the status monitor:

1. Enter the STATMON command to access the Domain Status Summary panel of the status monitor. A panel similar to Figure 155 is displayed.

```
STATMON.DSS                    DOMAIN STATUS SUMMARY                    15:24
HOST: HOST01                *1*     *2*     *3*     *4*

                       ACTIVE  PENDING   INACT    MONIT    NEVACT   OTHER
 .....3 NCP/CA/LAN/PK  .....2   ......   ......   ......   .....1   ......
 ....17  LINES         ....14   .....1   ......   ......   .....2   ......
 ....47  PUS/CLUSTERS  ....45   .....1   ......   .....1   ......   ......
 .....1 SWITCHED/XCA   .....1   ......   ......   ......   ......   ......
 .....1  PU/XCA LINE   .....1   ......   ......   ......   ......   ......
 .....1  LU/XCA PU     .....1   ......   ......   ......   ......   ......
 .....2 LOCAL MAJ NDS  .....2   ......   ......   ......   ......   ......
 .....1  PUS           .....1   ......   ......   ......   ......   ......
 ....13  LUS/TERMS     ....11   ......   .....2   ......   ......   ......
 .....3 APPL MAJ NDS   .....3   ......   ......   ......   ......   ......
 ....87  APPLICATIONS  ....27   ......   ......   ......   ......   ....60
 .....1 CDRM MAJ NDS   .....1   ......   ......   ......   ......   ......
 .....5  CDRMS         .....5   ......   ......   ......   ......   ......
 .....1 CDRSC MAJ NDS  .....1   ......   ......   ......   ......   ......
 .....2  CDRSCS        .....2   ......   ......   ......   ......   ......
 ------ -------------  ------   ------   ------   ------   ------   ------
 ...185 TOTAL NODES    ...117   .....2   .....2   .....1   .....3   ....60

 CMD==>
 TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
```

Figure 155. Domain Status Summary Panel

The panel displays information about resources. The resources listed are divided into major and minor nodes. The major nodes are NCP/CA/LAN/PK, SWITCHED/XCA, LOCAL MAJ NDS, APPL MAJ NDS, CDRM MAJ NDS, and CDRSC MAJ NDS. Under each major node are the minor nodes (individual resources) that make up the major node. By using this panel, you can find and correct problems before users report them, or before other resources are affected.

The status monitor displays status condition names, called states, near the top of the panel. A resource can be in any of six states: ACTIVE, PENDING, INACT, MONIT, NEVACT, and OTHER. Each state is associated with a color. For a description of these states, see "Understanding the Status Monitor Panel Colors" on page 115.

Notice that two of the logical units or terminals have become inactive.

2. To display detailed information about the inactive units, insert any character except a blank before the first period under the INACT column of LUS/TERMS and press Enter. A panel similar to Figure 156 on page 292 is displayed.

```
STATMON.DSD(DESC)            DOMAIN STATUS DETAIL (DESCRIPTION)      12:57 A
HOST: HOST1                 *1*     *2*     *3*     *4*
                         ACTIVE    PENDING    INACT     MONIT    NEVACT     OTHER
?...13  LUS/TERMS        ?...11    ?.....    ?....2    ?.....    ?.....    ?.....
-------------------------------------------------------------------------------
? DISPLAY          |   NODE ID.  DESCRIPTION          NODE ID.  DESCRIPTION
 ? APPLS           |
 ? LINES           | ? A01A445   TERMINAL
 ? PUS/CLSTRS      | ? A01A446   TERMINAL
 ? LUS/TERMS       |
 ? CDRMS           |
 ? CDRSCS          |
  ? ACT            |
  ? EVERY          |
  ? INACT          |
 ? PENDING         |
 ? BFRUSE          |
? VARY INACT       |
 ? I     ? F       |
? VARY ACT         |
 ? ONLY  ? ALL     |

CMD==>
TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
```

Figure 156. Domain Status Detail Panel

The right side shows the inactive resources for one major node followed by a brief description. The left side shows you a list of available VTAM commands. You can use these commands to display information about resources (DISPLAY), activate resources (VARY ACT), or deactivate resources (VARY INACT).

3. To activate each resource, type any character except a blank or question mark (?) over the question mark next to the resource and over the question mark next to the VARY ACT command and press **Enter**.

   The command facility displays the following messages:

   ```
   * CNM01    V NET,ACT,ID=A01A445
   * CNM01    V NET,ACT,ID=A01A446
     CNM01    IST097I  VARY     ACCEPTED
     CNM01    IST097I  VARY     ACCEPTED
     CNM01    IST093I  A01A445 ACTIVE
     CNM01    IST093I  A01A446 ACTIVE
   ```

   The last two messages tell you that the resources are now active.

4. Press Enter to return to the status monitor.

Topic:	Reference:
Monitoring and controlling resources using the status monitor	"Using the Status Monitor (SNA Subarea)" on page 114

Identifying Intermittent Problems (Hardware Monitor)

You can use the hardware monitor to predict where problems are likely to occur by monitoring key temporary error counters and looking for trends in the frequency of temporary errors. You can set the hardware monitor to check the frequency of these errors and to notify you if the frequency is greater than specified. By tracking the error rate trends, you might be able to predict performance degradation and take action to prevent a problem from becoming serious.

Intermittent problems are often related to performance problems. For example, if a resource alternates between active and inactive, try to see if a correlation exists between the problem and the time when it occurs. If the problem occurs during a period of high system usage, this can indicate a performance problem. You might then have to tune the performance of your system (by rerouting or redistributing tasks) to solve the problem.

You can use the hardware monitor to monitor alerts and to display statistical data. For additional information, see "Monitoring the Network Using the Hardware Monitor Panels" on page 145. You might want to keep in mind the following failure-cause code points used to identify intermittent problems:

Hex value	Description
0411	INTERMITTENT STORAGE CONTROLLER ERROR
0412	INTERMITTENT WORKSTATION CONTROLLER ERROR
0413	INTERMITTENT COMMUNICATIONS SUBSYSTEM CONTROLLER ERROR

Topic:	Reference:
Modifying the Code Point tables	*IBM Tivoli NetView for z/OS Customization Guide*
List of code points provided by the NetView program	"Codes and Messages" in *IBM Tivoli NetView for z/OS Troubleshooting Guide*
Alert types	*SNA Formats*

Determining Controller Status (Hardware Monitor)

You can use the hardware monitor to determine the status of a controller. To use the hardware monitor, complete the following steps:

1. Enter **npda** from the command line to access the hardware monitor main menu. A panel similar to Figure 157 on page 294 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/02 12:43:59
NPDA-01A                          * MENU *               HOST DOMAIN: CNM09



SEL#   PRODUCES:
( 1)    ALERTS-DYNAMIC DISPLAY
( 2)    TOTAL EVENTS DISPLAY
( 3)    TOTAL STATISTICAL DATA DISPLAY
( 4)    HELP MENU DISPLAY


       REQUEST DATA FROM NETWORK RESOURCES:
( 5)    SNA CONTROLLERS (CTRL)
( 6)    MODEMS AND ASSOCIATED LINKS (TEST)


                        DATA TYPES INITIALIZED/PURGED
AL.. (8/18/01)   EV.. (8/18/01)   ST.. (8/18/01)   GMFALERT.. (8/18/01)

ENTER SEL#

 ???
CMD==>
```

Figure 157. Hardware Monitor Main Menu

2. Select option **5** to display the Controller Information Display panel. A panel similar to Figure 158 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/02 12:49:32
NPDA-02E          * CONTROLLER INFORMATION DISPLAY *              PAGE 1 OF 1

DOMAIN: CNM01

  THE CTRL COMMAND IS USED TO SOLICIT LINK TEST COUNTS, SUMMARY ERROR
  COUNTERS, AND RELEASE LEVEL INFORMATION FROM SNA CONTROLLERS.

  IF YOU ENTER THE RESOURCE NAME FOR A CONTROLLER, THE HARDWARE MONITOR WILL
  PROVIDE A DESCRIPTION OF THE CTRL COMMAND SET AND ALLOW YOU TO SELECT ONE.

  THE RESOURCE NAME, IDENTIFIED AS THE VARIABLE RESNAME BELOW, IS THE
  NETWORK NAME OF AN SNA CONTROLLER.  THE ACTUAL RESOURCE NAME MAY BE FOUND
  ON THE LINE ABOVE THE NETWORK FIGURE ON MOST HARDWARE MONITOR DISPLAYS.



NOTE:  NON-HARDWARE MONITOR COMMANDS (EXCEPT 'NCCF') ARE TAKEN AS RESOURCE
       NAMES.

ENTER RESNAME

 ???
CMD==> A03P041
```

Figure 158. Hardware Monitor Controller Information Display Panel

3. Enter the name of the controller for which to display information in the command line. A panel similar to Figure 159 on page 295 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/02 12:49:47
NPDA-CTRL         * CONTROLLER (CTRL) SELECTION MENU *            PAGE 1 OF 1

DOMAIN: CNM01                RESNAME: A03P041

 SEL#    CTRL                          DESCRIPTION

 (1) LINK - LINK DATA  RETRIEVES LINK TEST COUNTS FROM AN SNA CONTROLLER
                       AND PRESENTS THE RESULTS ON DISPLAY NPDA-23A.

 (2) LVL - RELEASE     RETRIEVES RELEASE LEVEL INFORMATION FROM AN SNA
     LEVEL DATA        CONTROLLER AND PRESENTS RESULTS ON DISPLAY NPDA-21A.

 (3) SEC - SUMMARY     RETRIEVES SUMMARY ERROR COUNTS FROM AN SNA CONTROLLER.
     ERROR COUNTERS    DISPLAY NPDA-41A IS PRESENTED FROM WHICH THE USER CAN
                       THEN DISPLAY THE DETAILED COUNTER DATA.

 NOTE: NOT ALL SNA CONTROLLERS SUPPORT THE ABOVE FUNCTIONS


 ENTER SEL#

 ???
CMD==> 1
```

Figure 159. Hardware Monitor Controller Selection Menu Panel

4. Select option **1** to display link data for the controller. A panel similar to Figure 160 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/02 12:49:51
NPDA-23A            * LINK DATA FOR SNA CONTROLLER *          PAGE   1 OF   2

 CNM01       A03A62     A03L04     A03P041
            +--------+            +--------+
 DOMAIN     |  COMC  | ---LINE--- |  CTRL  |
            +--------+            +--------+
DATE/TIME: 04/12 12:49      ID: 01784679(3274)



                SECONDARY CONTROLLER SDLC LINK TEST COUNTS

                       RECEIVED         TRANSMITTED

                            10                10




 ???
CMD==>
```

Figure 160. Hardware Monitor Link Data Panel

The two secondary controller SDLC link test counters, RECEIVED and TRANSMITTED, display the number of times that the A03P041 controller received the SDLC link test and the number of times that it transmitted it back. In this case, the A03P041 controller received the link test 10 times and transmitted it

back to the host 10 times. This indicates that the A03P041 controller has no problems because it retransmitted everything that it received.

5. Enter the NetView RETURN command or press a PF key set to that command to return to the Controller Selection Menu and select option 2 to display release level data. The NetView supplied default key for the RETURN command is PF3. A panel similar to Figure 161 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/02 12:50:37
NPDA-21A          * RELEASE LEVEL FOR SNA CONTROLLER *         PAGE   1 OF   1

 CNM01       A03A62     A03L04     A03P041
            +--------+            +--------+
 DOMAIN     |  COMC  |----LINE----|  CTRL  |
            +--------+            +--------+
DATE/TIME: 04/12 12:50      ID: 01784679(3274)


01E66565 65240000 010200C1 21006308 08000800 42010710 00040000 0B000001
DA0B0B01 1F0B0303 002324D1 54890009 0119015B 006638FF FEFFFEA5 5A000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 08467990 00000000 00650065 00000000 00000000 000003C0
88000009 811981FF FE000000 00000000 00410000 00000000 00000000 00000000
00000C08 07200000 00000000 00000000 00FFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
FF111400 00104000 00000000 00000000 00050100 28005000 C80190F0 00000000
00000000 00000000 00000000 00000000 0000



 ???
CMD==>
```

Figure 161. Hardware Monitor Release Level Panel

This panel contains engineering change level information. The information can include the finance system controller microcode and the patch level, displayed in hexadecimal. This information is useful in tracking down problems by helping you determine what functions are supported (or are not supported) by the specified change level.

6. Enter the NetView RETURN command or press a PF key (the NetView default is PF3) to return to the Controller Selection Menu and select option 3 to display the most recent events for the controller. A panel similar to Figure 162 on page 297 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER1     04/12/02 12:50:45
NPDA-41A                   * MOST RECENT EVENTS *              PAGE   1 OF   1

 CNM01       A03A62     A03L04     A03P041
            +--------+            +--------+
 DOMAIN     |  COMC  |----LINE----|  CTRL  |
            +--------+            +--------+
SEL#  DATE/TIME  EVENT DESCRIPTION:PROBABLE CAUSE                    ETYP
( 1) 04/12 12:50 SNA SUMMARY:COMMUNICATIONS                          SNA









 ENTER ST (STAT), SEL# (ACTION), OR SEL# PLUS D (EVENT DETAIL)

 ???
CMD==>
```

Figure 162. Hardware Monitor Most Recent Events Panel

Topic:	Reference:
Using the NetView CTRL command to determine the status of a controller	NetView online help
RECFMS record formats containing change level information	"RECFMS Record Formats" in *IBM Tivoli NetView for z/OS Troubleshooting Guide*

Checking Session Monitor and Hardware Monitor Database Status (Command Facility)

The NetView program uses VSAM key-sequenced data sets for the session monitor and hardware monitor databases. Each component has a primary and secondary database.

Follow these steps to monitor the active database for the component and, when it becomes full, switch to the alternate database:

1. From the command facility, enter the following command to display the space used on the hardware monitor database:

   ```
   listcat bnjdserv
   ```

   Note: For the session monitor database, use AAUTSKLP instead of BNJDSERV.
2. Figure 163 on page 298 shows the response to the LISTCAT command.

```
LISTCAT Listcat of Active VSAM Data Base for BNJDSERV 09:07:03 Page 1 of 1
VSAM ACB Options: LSR, ADR, KEY, SEQ, DIR, OUT
Cluster Information:
          DDNAME: BNJLGPR        KEYLEN: .........76      RKP: ..........0
     BSTRNO: ..........0    STRNO: .........11   STRMAX: ..........2
           BUFSP: ..........0
     DATA Component Information:
           LRECL: ........4086     CINV: ........4096
           BUFND: ..........12    BUFNO: ..........0
            NEXT: ..........6       FS: ..........28
            NCIS: ........1516     NSSS: ..........3
           NEXCP: ......151037    NLOGR: ........5249    NRETR: ......455779
           NINSR: .......11804    NUPDR: .......18641    NDELR: ........6565
          AVSPAC: .....2945024   ENDRBA: .....4587520  HALCRBA: .....4587520
     INDEX Component Information:
           LRECL: ........4089     CINV: ........4096
           BUFNI: ..........0    BUFNO: ..........0
            NEXT: ..........7     NIXL: ..........2
           NEXCP: ........7132    NLOGR: ..........5
          AVSPAC: .......53248   ENDRBA: .......73728  HALCRBA: .......73728


 ENTER= Refresh  PF1= Help  PF2= End  PF3= Return
```

Figure 163. LISTCAT BNJDSERV Output

Pay particular attention to the following values:

DDNAME
This value shows whether the primary or secondary database is active

AVSPAC, HALCRBA
These values are continually updated with the number of bytes available in the DATA component. This number changes based on extents allocated by VSAM. If the available space is near zero, the database is near full and you need to switch to the alternate database.

NIXL This value shows the index record level. If this number is greater than 3, you can improve the database performance by reorganizing the database.

3. To switch the hardware monitor database from primary to secondary, enter:

```
dbauto npda switch
```

Note that this NetView panel has the PF keys listed on the panel, and that you cannot use the NetView DISPFK command from this panel.

Topic:	Reference:
Maintaining hardware monitor databases (including switching to a secondary database using the DBAUTO command)	"Maintaining the Hardware Monitor Database" on page 225
Maintaining session monitor databases (including switching to a secondary database using the DBAUTO command)	"Using and Maintaining the Session Monitor Database" on page 228
DBAUTO command	NetView online help

Chapter 20. Reactive Investigating

In reactive investigating, you react to a problem that has already occurred. You learn about this problem in monitoring the problem or through a phone call. In general, you have some idea about the location of the problem and the kind of problem that has occurred.

Table 24 contains an overview of the scenarios that are covered in this chapter. For each scenario, the table lists the product used to solve the problem and the types of resources involved. Note that all scenarios might not be applicable, depending on which option of NetView is installed.

Table 24. Reactive Investigating Cross Reference

Problem Scenario	Product Used to Resolve the Problem	Page
Finding and repairing the cause of a hung session	Session monitor	299
Finding and repairing the cause of a broken session	Session monitor	302
Handling a line failure	Hardware monitor	306
Determining if a virtual route is blocked	VTAM commands	312
Identifying modem problems	Status monitor, session monitor, hardware monitor	312
Identifying and terminating looping or hung NetView tasks	Command facility	319
Measuring response time with control units using the RTM feature	Session monitor	320
Resolving sluggish network performance	NetView Performance Monitor	322

Hung Session (Session Monitor)

In the following scenario, an end user at terminal T11 reports that the directions on his screen (generated by an application program) ask for data to be entered, but the keyboard is locked. You can:

1. Enter **sess t11** from the session monitor command line to display the session list for resource T11. A panel similar to Figure 164 on page 300 is displayed:

```
NLDM.SESS                                                            PAGE 1
                                   SESSION LIST
NAME: T11                                                        DOMAIN: CNM01
------------------------------------------------------------------------
      ***** PRIMARY *****  **** SECONDARY ****
 SEL#   NAME   TYPE  DOM     NAME   TYPE  DOM     START TIME       END T
 ( 1) BADAPPL   LU   CNM01   T11    LU   CNM01  11/22 15:13:40  *** ACTIVE ***
 ( 2) VTAM      SSCP CNM01   T11    LU   CNM01  11/22 14:10:20  *** ACTIVE ***
 ( 3) TSO0001   LU   CNM01   T11    LU   CNM01  11/22 15:00:00  11/22 15:10:40















END OF DATA
ENTER SEL# (CONFIG), SEL# AND CT (CONN. TEST), SEL# AND STR (TERM REASON)
CMD==>
```

Figure 164. Session List Panel

The display shows that both the SSCP-LU and application LU sessions are active. According to the end user, however, the keyboard is locked and data cannot be entered. Because a contradiction exist, you need to look at the path information unit (PIU) trace data.

2. Select **1** to display the Session Configuration Data panel for the BADAPPL-T11 session. A panel similar to Figure 165 is displayed.

```
NLDM.CON                  SESSION CONFIGURATION DATA                 PAGE 1
-------------- PRIMARY ---------------+-------------- SECONDARY -------------
NAME BADAPPL   SA 0000000B  EL 0008   |   NAME T11      SA 00000004  EL 00DC
--------------------------------------+--------------------------------------
DOMAIN CNM01                                                    DOMAIN CNM01
               +-------------+                  +-------------+
A11M           |   CP/SSCP   |                  |             |
PUSA11  (0000) | SUBAREA PU  | ----  VR 00 ---  | SUBAREA PU  | NA04818 (0000)
               +------+------+       TP 00      +------+------+
                      |                                |
               +------+------+       ER 00      +------+------+
BADAPPL (0008) |     LU      |      RER 00      |     CUA     | DSDLC21
               +-------------+                  +------+------+
                                                       |
                                                +------+------+
                                                |     PU      | DPU3275A(00DB)
                                                +------+------+
                                                       |
                                                +------+------+
                                                |     LU      | T11     (00DC)
                                                +-------------+

SELECT PT, ST (PRI, SEC TRACE), RT (RESP TIME), P
CMD==>
```

Figure 165. Session Configuration Data Panel

This panel shows how each LU (BADAPPL and T11) is connected to its own subarea. From this panel you can now access trace data.

3. Enter `pt` on the command line to display the primary PIU trace for the session between terminal T11 and application BADAPPL. Note that the trace facility must be set either through the initial session monitor definition (in AAUPRMLP) or through the TRACE command. A panel similar to Figure 166 is displayed.

```
NLDM.PIUT                SESSION TRACE DATA                          PAGE    1
---------- PRIMARY ----------------+-------- SECONDARY ---------------+- DOM -
NAME BADAPPL  SA 0000000B  EL 0008  | NAME T11    SA 00000004  EL 00DC | CNM01
-----------------------------------+-----------------------------------+-------
SEL#   TIME   SEQ# DIR   TYPE    ******** REQ/RESP HEADER ******** RULEN SENS N
( 1) 11:28:56 0018 P-S BIND      ....OC.DR.........................   37
( 2) 11:28:58 0016 S-P (+)RSP    ....OC.DR.........................    1
( 3) 11:29:03 0019 P-P SDT       ....OC.DR.........................    1
( 4) 11:29:04 0017 S-P (+)RSP    ....OC.DR.........................    1
( 5) 11:29:10 0020 P-S DATA      ....OC.ER.......BB................    9
( 6) 11:29:10 0021 P-S DATA      ....OC.ER............CD...........   48
( 7) 11:30:03 0018 S-P DATA      ....OC.ER............CD...........   32
( 8) 11:30:12 0022 P-S DATA      ....OC.ER........EB...............   28
( 9) 11:36:10 0023 P-S DATA      ....OC.ER.......BB................    9
(10) 11:36:12 0024 P-S DATA      ....OC.ER.........................   49









END OF DATA
ENTER SEL# or COMMAND
CMD==>
```

Figure 166. Session Trace Data Panel

Figure 166 shows the primary trace data. Each trace entry has the time-of-day, sequence number, flow direction (P-S/S-P), and PIU type. Important indicators in the Request/Response Header (RH) are formatted. The trace response data is described in the following list:

OC Only one in chain
DR Definite response
ER Exception response

The first four trace entries show the session getting established, and the next five trace entries show a normal exchange of data. The BB/EB indicators show bracket protocol is in effect. Each flow direction change is signaled by a change direction (CD) flag.

In this scenario, the error source is the host application program. The NAU named BADAPPL did not insert a change direction (CD) flag in trace 10. Therefore, the terminal did not unlock the keyboard and the operator cannot respond with more data.

Further resolution of this problem is up to the BADAPPL programmer.

Topic:	Reference:
Using the session monitor panels	"Session Monitor Scenarios" on page 94

Broken Session (Session Monitor)

The following scenario illustrates the loss of a session in a cross-domain environment. In this scenario, a user (with terminal ID A04T0011) is using an application when the system logs the user off. The user calls to report the problem. You can:

1. Enter **sess a04t0011** at the command prompt to display the session list for terminal a04t011. A panel similar to Figure 167 is displayed.

```
NLDM.SESS                                                          PAGE    1
                                SESSION LIST
NAME: A04T0011                                                  DOMAIN: CNM02
------------------------------------------------------------------------------
      ***** PRIMARY *****  **** SECONDARY ****
 SEL#   NAME   TYPE  DOM     NAME   TYPE  DOM     START TIME       END TIME
( 1) A02M     SSCP CNM02  A04T0011 LU   CNM02  06/06 18:11:17   *** ACTIVE ***
( 2) TSO0101  LU   CNM01  A04T0011 LU   CNM02  06/06 20:34:58   06/06 20:45:48
                                                                 
                                                                 
                                                                 
                                                                 
                                                                 
                                                                 
                                                                 
                                                                 
                                                                 
END OF DATA
ENTER SEL# (CONFIG), SEL# AND CT (CONN. TEST), SEL# AND STR (TERM REASON)
CMD==>
```

Figure 167. Session List Panel

   The active SSCP-LU session (option 1) indicates that the user terminal is still active. The inactive LU-LU session (option 2) between application TSO0101 and terminal A04T0011 is the one about which the user called.

   The panel also shows that application TSO0101 is in domain CNM01 and that terminal A04T0011 is in domain CNM02. This is a cross-domain session.

2. Select option **2** to display the Session Configuration Data panel for the inactive session. A panel similar to Figure 168 on page 303 is displayed:

```
NLDM.CON                  SESSION CONFIGURATION DATA                  PAGE    1
-------------- PRIMARY ---------------+-------------- SECONDARY --------------
NAME TSO0101   SA 00000001  EL 0008   |   NAME A04T0011  SA 00000004  EL 005A
-------------------------------------+---------------------------------------
DOMAIN CNM01                                                 DOMAIN CNM02
               +-------------+                 +-------------+
A01M           |   CP/SSCP   |                 |             |
A01MPU  (0000) | SUBAREA PU  | ---   VR 01 --- | SUBAREA PU  | A04NV4  (0000)
               +------+------+       TP 00     +------+------+
                      |                             |
               +------+------+       ER 02     +------+------+
TSO0101 (0008) |     LU      |      RER 01     |    LINK     | A04L00
               +-------------+     INOP        +------+------+
                                                       |
                           COSNAME INTERACT    +------+------+
                           LOGMODE M23278I     |     PU      | A04P001 (0013)
                                               +------+------+
                                                       |
                                               +------+------+
                                               |     LU      | A04T0011(005A)
                                               +-------------+

SELECT PT, ST (PRI, SEC TRACE), RT (RESP TIME), P, ER, VR
CMD==>
```

Figure 168. Session Configuration Data Panel

Review the information on the panel. This panel shows the path between the session from the primary LU (TSO0101) to its host PU (A01MPU) and from the secondary LU (A04T0011) to its NCP (A04NV4). It also shows the explicit route between them for this session. The explicit route is identified by an explicit route number (in this case, the explicit route number is 02).

Notice the term INOP that is displayed in the center of the panel. INOP indicates that the explicit route the session was using became inoperative. This occurred because a node or transmission group (TG) in the route became inoperative.

3. Enter **er** to display the explicit route. A panel similar to Figure 169 on page 304 is displayed.

```
NLDM.ER                  SPECIFIC ER CONFIGURATION                  PAGE    1
-------------------------------------------------------------------------------
SUBAREA1 00000001   SUBAREA2 00000004  ER  02 | NODES (TOTAL/MIGRATION): 04/00
-------------------------------------------------------------------------------
                             (A)
                              V
 +-----+ NAME: A01MPU      +-----+ NAME: A02MPU
 | INN |   SA: 00000001    | INN |   SA: 00000002
 +--+--+ SSCP: A01M        +--+--+ SSCP: A02M
    |                          |
1) TG01  INOP: UNPLANNED  3) TG02
    |                          |
 +--+--+ NAME: A03NV4      +--+--+ NAME: A04NV4
 | INN |   SA: 00000003    | INN |   SA: 00000004
 +--+--+ SSCP: A01M        +--+--+ SSCP: A02M
    |
2) TG01
    |
    V
   (A)

END OF DATA
ENTER SEL# (FOR TG DETAIL)
CMD==>
```

Figure 169. Specific ER Configuration Panel

Notice the placement of the notation `INOP: UNPLANNED` next to item 1, `TG01`. This indicates that the explicit route is inoperative, because either the host PU (A01MPU) or the transmission group between A01MPU and A03NV4 (TG01) became inactive.

4. Enter the COPY command in the command line to store the Specific ER Configuration panel in the network log. The system programmer can use the information when further investigating this problem.
5. Tell the user to log on to the TSO application again and perhaps establish another route.
6. Confirm that the session is active by entering **sess a04t0011**. The panel shown in Figure 170 on page 305 is displayed.

```
NLDM.SESS                                                          PAGE    1
                                SESSION LIST
NAME: A04T0011                                                  DOMAIN: CNM02
------------------------------------------------------------------------------
      ***** PRIMARY *****  **** SECONDARY ****
 SEL#   NAME   TYPE  DOM     NAME   TYPE  DOM     START TIME       END TIME
( 1) TSO0101  LU   CNM01  A04T0011 LU   CNM02  06/06 20:49:03   *** ACTIVE ***
( 2) A02M     SSCP CNM02  A04T0011 LU   CNM02  06/06 18:11:17   *** ACTIVE ***
( 1) TSO0101  LU   CNM01  A04T0011 LU   CNM02  06/06 20:34:58   06/06 20:54:48









END OF DATA
ENTER SEL# (CONFIG), SEL# AND CT (CONN. TEST), SEL# AND STR (TERM REASON)
CMD==>
```

Figure 170. Session List Panel

7. Enter **1** to look at the active session configuration and to determine the route. A panel similar to Figure 171 is displayed. Note that a different explicit route (ER 03) is used for this session.

```
NLDM.CON                 SESSION CONFIGURATION DATA                 PAGE    1
-------------- PRIMARY ---------------+-------------- SECONDARY --------------
NAME TSO0101   SA 00000001  EL 0008   |   NAME A04T0011  SA 00000004  EL 005A
--------------------------------------+--------------------------------------
DOMAIN CNM01                                                DOMAIN CNM02
              +-------------+                +-------------+
A01M          |   CP/SSCP   |                |             |
A01MPU  (0000)| SUBAREA PU  | ---   VR 07 --- | SUBAREA PU  | A04NV4  (0000)
              +------+------+       TP 00     +------+------+
                     |                             |
              +------+------+       ER 03     +------+------+
TSO0101 (0008)|     LU      |      RER 02     |    LINK     | A04L00
              +-------------+                 +------+------+
                                                     |
                           COSNAME INTERACT  +------+------+
                           LOGMODE M23278I   |      PU     | A04P001 (0013)
                                             +------+------+
                                                     |
                                             +------+------+
                                             |     LU      | A04T0011(005A)
                                             +-------------+

SELECT PT, ST (PRI, SEC TRACE), RT (RESP TIME), P, ER, VR
CMD==>
```

Figure 171. Session Configuration Data Panel

8. Enter **er** to view the explicit route. A panel similar to Figure 172 on page 306 is displayed.

```
NLDM.ER                  SPECIFIC ER CONFIGURATION                  PAGE    1
-------------------------------------------------------------------------------
SUBAREA1 00000001   SUBAREA2 00000004  ER  03 | NODES (TOTAL/MIGRATION): 03/00
-------------------------------------------------------------------------------
                              (A)
                               V
 +-----+ NAME: A01MPU      +-----+ NAME: A04NV4
 | INN |   SA: 00000001    | INN |   SA: 00000004
 +--+--+ SSCP: A01M        +--+--+ SSCP: A02M
    |
1) TG03
    |
 +--+--+ NAME: A02MPU
 | INN |   SA: 00000002
 +--+--+ SSCP: A02M
    |
2) TG02
    |
    V
   (A)

END OF DATA
ENTER SEL# (FOR TG DETAIL)
CMD==>
```

Figure 172. Specific ER Configuration Panel

Note that the new TSO session has been established. The route is now going directly from the host PU (A01MPU) in subarea 1 (SA: 00000001) to the host PU (A02MPU) in subarea 2 (SA: 00000002). It no longer passes through NCP A03NV4.

Because this panel shows the new session route, the information on the panel might help the system programmer when further investigating this problem. Enter the COPY command from command line to store the Specific ER Configuration panel to the network log.

The user can continue working while the inoperative route is being repaired.

Topic:	Reference:
Using the session monitor panels	"Session Monitor Scenarios" on page 94

Line Failure (Hardware Monitor)

The following scenario illustrates how to handle a link error caused by a faulty line:

1. Enter **npda ald** from the command line to access the Alerts-Dynamic panel. A panel similar to Figure 173 on page 307 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER6     04/12/01 11:03:45
NPDA-30A                      * ALERTS-DYNAMIC *

    DOMAIN RESNAME  TYPE TIME  ALERT DESCRIPTION:PROBABLE CAUSE
     CNM99 A31P061  CTRL 11:02 LINK ERROR:LINE
     CNM01 A22P033  CTRL 10:07 ERROR TO TRAFFIC RATIO EXCEEDED:X.25 NETWORK
     CNM01 A41P056  CTRL 10:06 DEVICE DETECTED ERROR:DEVICE
     CNM01 A41P056  CTRL 10:06 DELAYED ALERT:COMMUNICATION ADAPTER
     CNM01 A31P092  CTRL 10:05 TEMPORARY CONTROL UNIT ERROR:HARDWARE









DEPRESS ENTER KEY TO VIEW ALERTS-STATIC

 ???
CMD==>
```

Figure 173. Alerts-Dynamic Panel

Notice that CNM01 is the focal point for CNM99, the entry point.

2. Press Enter to view the Alerts-Static panel. A panel similar to Figure 174 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER6     04/12/02 11:04:20
NPDA-30B                      * ALERTS-STATIC *

SEL# DOMAIN RESNAME TYPE TIME  ALERT DESCRIPTION:PROBABLE CAUSE
( 1) CNM99 A31P061  CTRL 11:02 LINK ERROR:LINE
( 2) CNM01 A22P033  CTRL 10:07 ERROR TO TRAFFIC RATIO EXCEEDED:X.25 NETWORK
( 3) CNM01 A41P056  CTRL 10:06 DEVICE DETECTED ERROR:DEVICE
( 4) CNM01 A41P056  CTRL 10:06 DELAYED ALERT:COMMUNICATION ADAPTER
( 5) CNM01 A31P092  CTRL 10:05 TEMPORARY CONTROL UNIT ERROR:HARDWARE









DEPRESS ENTER KEY TO VIEW ALERTS-DYNAMIC OR ENTER A TO VIEW ALERTS-HISTORY
ENTER SEL# (ACTION),OR SEL# PLUS M (MOST RECENT), P (PROBLEM), DEL (DELETE)

 ???
CMD==>
```

Figure 174. Alerts-Static Panel

Notice that the first alert on the panel is a link error from the distributed node CNM99.

Note: To obtain a description of all the available options from this panel, see "Monitoring the Network Using the Hardware Monitor Panels" on page 145 or enter **help** to access the help menu and select PROMPTS.

3. Select option **1** to obtain detailed information on the alert and recommended actions for the link error. A panel similar to Figure 175 is displayed.

```
N E T V I E W          SESSION DOMAIN: CNM01    OPER6        04/12/02 11:04:52
NPDA-45A           * RECOMMENDED ACTION FOR SELECTED EVENT *       PAGE 1 of 1
 CNM099      A31N43H    A31L06     A31P061
            +--------+            +--------+
 DOMAIN     |  COMC  |----LINE----|  CTRL  |
            +--------+            +--------+
USER    CAUSED - NONE

INSTALL CAUSED - NONE

FAILURE CAUSED - LSL 1 LINE
                 REMOTE NODE
       ACTIONS - D209 - RUN TRANSMIT/RECEIVE TEST
                 D219 - RUN LINE ANALYSIS TEST
                 D000 - IF PROBLEM PERSISTS THEN DO THE FOLLOWING
                 D227 - CHANGE TO BACKUP SPEED
                 D218 - RUN REMOTE NODE-DCE INTERFACE WRAP TEST
                 D005 - CONTACT APPROPRIATE SERVICE REPRESENTATIVE


ENTER ST TO VIEW MOST RECENT STATISTICS, OR D TO VIEW DETAIL DISPLAY

 ???
CMD==>
```

Figure 175. Recommended Action Panel

This panel includes a diagram of the configuration of resources. The rightmost resource (described in the **RESNAME** field of the Alerts-Static panel) is the one most affected by the event described in the panel.

Note the resource names at each end of the line (A31L06). The resource names are A31N43H and A31P061. You need these two names to run a line analysis test.

4. For this scenario, assume that action D209 (RUN TRANSMIT/RECEIVE TEST) has been tried and the results are positive (for example, no failures were detected). The next recommended action is D219 (RUN LINE ANALYSIS TEST). Enter `action d219` to get more information on how to run the line analysis test. A panel similar to Figure 176 on page 309 is displayed.

```
CNM3G019                    D219  RUN DCE TEST


Select  To get information about

   1    Local Self-Test with modem/DCE Wrap Plug

   2    Line Analysis Test (analog lines only)

   3    Modem on DSU/CSU and Line Status Test

   4    Transmit/Receive Test



 Type a number (1 through 4) and press ENTER.


 TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
 Action===>
```

Figure 176. D219 Run DCE Test Panel

This is the help panel menu for running the data communication equipment (DCE) tests.

5. Select option **2** to get more information on the line analysis test. A panel similar to Figure 177 is displayed.

```
CNM3GB19              D219  RUN LINE ANALYSIS TEST



A severe line impairment has been found in the inbound, outbound, or
both connections.

Use the LA (Line Analysis) option of the hardware monitor TEST command on
both the first and second link segments to provide the line characteristics and
to determine the failing segment.  The results are presented on a single page
display (NPDA-24B), accompanied by normal or acceptable limit values.  This
test can be run only on analog lines.

Report this trouble to the telephone company, indicating the values you have
recorded for all line parameters.  Emphasize any values that are beyond the
acceptable limits.







TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
Action===>
```

Figure 177. D219 Run Line Analysis Test Panel

Because this alert originated from the distributed node CNM99, change to that domain to run the line analysis test for this alert.

6. Enter **npda sdomain cnm99** to change to the CNM99 domain. A panel similar to Figure 178 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM99    OPER6     04/12/02 11:05:40
NPDA-01A                          * MENU *               HOST DOMAIN: CNM01



SEL#   PRODUCES:
( 1)    ALERTS-DYNAMIC DISPLAY
( 2)    TOTAL EVENTS DISPLAY
( 3)    TOTAL STATISTICAL DATA DISPLAY
( 4)    HELP MENU DISPLAY


       REQUEST DATA FROM NETWORK RESOURCES:
( 5)    SNA CONTROLLERS (CTRL)
( 6)    MODEMS AND ASSOCIATED LINKS (TEST)


                        DATA TYPES INITIALIZED/PURGED
AL.. (8/18/01)   EV.. (8/18/01)   ST.. (8/18/01)   GMFALERT.. (8/18/01)

ENTER SEL#
BNJ911I SESSION DOMAIN NOW CNM99   , WAS CNM01
 ???
CMD==>
```

Figure 178. Hardware Monitor Main Menu

7. Enter **test** to run the line analysis test for the link error received at CNM01. A panel similar to Figure 179 is displayed.

```
Tivoli NetView        SESSION DOMAIN: CNM99    OPER6         04/12/02 11:06:20
NPDA-02D              * TEST INFORMATION DISPLAY *                Page 1 of 1
DOMAIN: CNM99

  THE HARDWARE MONITOR SUPPORTS TWO SETS OF TEST COMMANDS (LPDA-1 AND LPDA-2).
  IF YOU ENTER TWO RESOURCE NAMES, THE HARDWARE MONITOR WILL DETERMINE THE
  PROPER COMMAND SET.

  THE RESOURCE NAMES ARE DEFINED BELOW AS THE VARIABLES RESNAME1 AND
  RESNAME2.  ACTUAL RESOURCE NAMES MAY BE FOUND ON THE LINE ABOVE THE NETWORK
  FIGURE ON DISPLAYS SUCH AS RECOMMENDED ACTIONS AND MOST RECENT EVENTS.

  RESNAME1 = THE NETWORK NAME OF A COMMUNICATION OR NETWORK CONTROLLER
             (COMC OR CTRL,  RESPECTIVELY) AT THE CONTROL END OF THE LINK.
  RESNAME2 = THE NETWORK NAME OF THE CONTROLLER (CTRL) AT THE REMOTE END
             OF THE LINK.

NOTE:  NON-HARDWARE MONITOR COMMANDS (EXCEPT 'NCCF') ARE TAKEN AS RESOURCE
       NAMES.

ENTER RESNAME1 RESNAME2

 ???
CMD==>
```

Figure 179. Test Information Display Panel

This is the test information display panel. The hardware monitor supports two sets of link problem determination aid (LPDA) test commands: LPDA-1 and

LPDA-2. The hardware monitor determines which command is issued. Both of these commands are used to isolate line and modem problems.

8. Enter **a31n43h a31p061** (the two resource names). A panel similar to Figure 180 is displayed.

```
Tivoli NetView        SESSION DOMAIN: CNM99    OPER6         04/12/02 11:07:39
NPDA-LPDA2              * LPDA-2 COMMAND MENU *                   Page 1 of 1
DOMAIN: CNM99     RESNAME1: A31N43H    RESNAME2: A31P061    LINK SEG LVL: 1

 SEL#      TEST                          DESCRIPTION

 (1)  MLS-MODEM AND     RETRIEVES A COMPREHENSIVE SET OF DCE (MODEM OR DSU/CSU)
      LINE STATUS       AND LINE DATA AND PRESENTS THE RESULTS ON DISPLAY
                        NPDA-22B/C.
 (2)  TRI-TRANSMIT      CAUSES A DCE (MODEM OR DSU/CSU) PAIR TO EXCHANGE ONE OR
          RECEIVE       MORE SEQUENCES OF PREDEFINED BIT PATTERNS OVER THE LINE
          TEST          AND REPORT THE RESULTS ON DISPLAY NPDA-25B.
 (2 XX)                 THE NUMBER OF SEQUENCES (XX) MAY BE ENTERED AS AN
                        OPTION FROM 1 TO 10 FOR THE TRANSMIT RECEIVE TEST.


 (3)  LA-LINE ANALYSIS  RETRIEVES LINE PARAMETERS SUCH AS SIGNAL TO NOISE
                        RATIO AND PRESENTS RESULTS ON DISPLAY NPDA-24B
                        (FOR ANALOG LINES ONLY).
                        FOR SEL# 2 ENTER ALSO A SPACE FOLLOWED BY 1-10 TO
ENTER SEL#              SPECIFY THE NUMBER OF TEST SEQUENCES.  DEFAULT IS 1

 ???
CMD==>
```

Figure 180. LPDA-2 Command Menu Panel

9. Select option **3** to perform the line analysis test. A panel similar to Figure 181 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM99    OPER6         04/12/02 11:08:33
NPDA-24B            * LINE ANALYSIS-LINK SEGMENT LEVEL 1 *          Page 1 of 1

 CNM99       A31N43H      A31L06  C1   A31P061
            +--------+ +-+        +-+ +--------+
 DOMAIN     |  COMC  | |M|--LINE--|M| |  CTRL  |
            +--------+ +-+        +-+ +--------+
 ROUND TRIP DELAY: 0 MSEC
                           LOCAL             REMOTE             ACCEPTABLE
                           MODEM             MODEM              LIMITS
TYPE-MODEL  MODEM ADDRESS: 5865-02, 01       5865-03, C1
FREQUENCY SHIFT:            0 HZ              0 HZ              MAX 6 HZ
2ND HARMONIC DISTORTION:   22 DB             40 DB              MIN 27 DB
3RD HARMONIC DISTORTION:   40 DB             40 DB              MIN 32 DB
SIGNAL TO NOISE RATIO:     40 DB             40 DB              MIN 22 DB
PHASE JITTER:               0 DEG PP          0 DEG PP          MAX 15 DEG P
RECEIVE LEVEL, LEAST:      -1, -1 DBM         0, -1 DBM         MIN -32 DBM
IMPULSE HITS:               0                 0                 15 IN 15 MIN
RLSD LOSSES:                0                 0
TRANSMIT LEVEL:             0 DBM             0 DBM
SPEED:                     9.6 KBPS(FULL)    9.6 KBPS(FULL)

 ???
CMD==>
```

Figure 181. Line Analysis-Link Segment Level 1 Panel

This panel displays the line parameters (such as frequency shift) for the local modem (attached to A31N43H) and the remote modem (attached to A31P061). It also displays the acceptable limits for each of the line parameters.

Notice that the second harmonic distortion value for the local modem is highlighted in bold (on the actual panel, it is highlighted in red), indicating that the value has fallen below the minimum acceptable limit value of 27DB.

You can now report the link error to the telephone company, indicating the values from this panel for all the line parameters.

10. Enter `sdomain cnm01` to get back to the focal point.

Topic:	Reference:
Using the hardware monitor panels	"Monitoring the Network Using the Hardware Monitor Panels" on page 145

Blocked Virtual Route (VTAM)

You can use the VTAM DISPLAY ROUTE command to display the status of virtual routes and to test virtual routes. The TEST operand lets you test all routes between the host subarea and any destination subarea for their ability to transfer data. The following example tests all virtual routes starting at node a0453le and ending at subarea address 01:

```
d net,route,destsub=01,netid=netc,origin=a0453le
```

The following output is displayed:

```
IST097I DISPLAY ACCEPTED
IST535I ROUTE DISPLAY 14 FROM SA 4 TO SA 1
IST808I ORIGIN PU = A0453LE DEST PU = C01NPU NETID = NETC
IST536I VR  TP    STATUS   ER       ADJSUB  TGN  STATUS  CUR MIN MAX
IST537I  0   1    INACT     5            1    1  ACTIV3
IST537I  1   1    INACT     1            3    1  INOP
IST537I  2   1    INACT     0           31    1  INOP
IST537I  4   1    INACT     6            3    1  INOP
IST537I  5   1    BLCKD     7           31    1  INOP
IST537I  7   1    INACT     3         1023    1  INOP
IST314I END
```

To obtain a description for a specific status, type `status` followed by the status keyword. For example, to obtain a description for the BLCKD status, enter:

```
status blckd
```

Also, the session monitor can be used to display and test virtual routes.

Topic:	Reference:
VTAM DISPLAY ROUTE command	Refer to the *VTAM Library.*
Using the NetView Performance Monitor to determine if a virtual route is blocked	*NetView Performance Monitor User's Guide*
Using the session monitor to determine if a virtual route is blocked	"Typical LU-LU Session for an SNA Subarea Network" on page 94

Modem Problems (Status Monitor, Hardware Monitor, Session Monitor)

In this scenario, a user calls early in the morning and reports that the terminals in the location are not working. You can:

1. Ask the user for the control unit ID. For this scenario, the control unit is A04P051. To display the status of the control unit, type `statmon a04p051` and press Enter. A panel similar to Figure 182 is displayed.

```
STATMON.NSD(DESC)              NODE STATUS DETAIL (DESCRIPTION)        16:25
HOST: HOST1            *1*   *2*   *3*   *4*
 ? A04L05              ACTIVE  PENDING   INACT    MONIT    NEVACT   OTHER
?.....4 PUS/CLUSTERS  ?......  ?......  ?.....4  ?......  ?......  ?.....
--------------------------------------------------------------------------------
? DISPLAY       |   NODE ID.  DESCRIPTION          NODE ID.  DESCRIPTION
 ? APPLS        |
 ? LINES        | ? A04P051 **PU
 ? PUS/CLSTRS   | ? A04P052   PU
 ? LUS/TERMS    | ? A04P053   PU
 ? CDRMS        | ? A04P054   PU
 ? CDRSCS       |
  ? ACT         |
  ? EVERY       |
  ? INACT       |
 ? PENDING      |
 ? BFRUSE       |
? VARY INACT    |
 ? I     ? F    |
? VARY ACT      |
 ? ONLY  ? ALL  |

CMD==>
TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
```

Figure 182. Status Monitor Node Status Detail (Description) Panel with List of VTAM Commands

Review the information on the panel. Notice that the control unit (A04P051) is highlighted in bold (on the actual panel, the control unit is displayed in red), indicating that it is inactive.

2. Enter the NetView SMENU command to access the Node Status Detail (Description) panel with the DETAIL FORMAT menu. The NetView supplied default PF key value for SMENU is PF24. A panel similar to Figure 183 on page 314 is displayed.

```
STATMON.NSD(DESC)               NODE STATUS DETAIL (DESCRIPTION)        16:33
HOST: HOST1            *1*   *2*   *3*   *4*
 ? A04L05              ACTIVE  PENDING   INACT    MONIT    NEVACT   OTHER
?.....4 PUS/CLUSTERS  ?......  ?......  ?.....4  ?......  ?......  ?.....1
-------------------------------------------------------------------------------
DISPLAY:        |   NODE ID.  DESCRIPTION           NODE ID.  DESCRIPTION
 HIGHER NODE    |
  ? SUMMARY     | ? A04P051   PU
  ? DETAIL      | ? A04P052   PU
 THIS NODE      | ? A04P053   PU
  ? SUMMARY     | ? A04P054   PU
  ? DETAIL      |
                |
                |
                |
----------------|
DETAIL FORMAT:  |
                |
  ? ANALYSIS    |
                |
                |
                |

CMD==>
TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
```

Figure 183. Status Monitor Node Status Detail (Description) Panel with Display/Detail Format Menu

3. Check the status of the NCP to which the line is attached. Select A04L05 from the upper-left corner of the panel and `DISPLAY:HIGHER NODE DETAIL` from below the dashed line.

   Remember that to make a selection, move the cursor to the appropriate areas on the panel, replace the question marks next to A04L05 and `DISPLAY:HIGHER NODE DETAIL` with any character, and press Enter. The Node Status Detail (Description) panel with status for line A04L05 is displayed.

```
STATMON.NSD(DESC)              NODE STATUS DETAIL (DESCRIPTION)        16:33
HOST: HOST1           *1*   *2*   *3*   *4*
 ? A04NV4             ACTIVE  PENDING   INACT    MONIT    NEVACT   OTHER
?....15  LINES       ?....11  ?......  ?.....1  ?......  ?.....3  ?.....1
-------------------------------------------------------------------------------
DISPLAY:        |   NODE ID.  DESCRIPTION           NODE ID.  DESCRIPTION
 HIGHER NODE    |
  ? SUMMARY     | ? A04NPML   LINE
  ? DETAIL      | ? A04L00    LINE
 THIS NODE      | ? A04L01    LINE
  ? SUMMARY     | ? A04L02    LINE
  ? DETAIL      | ? A04L03    LINE
                | ? A04L04    LINE
                | ? A04L05    LINE
---------------| ? A04L06    LINE
DETAIL FORMAT:  | ? A04L07    LINE
                | ? A04L08    LINE
  ? ANALYSIS    | ? A04L09    LINE
                | ? A04KC     LINE
                | ? A04KD     LINE
                | ? A04KG     LINE

CMD==>
TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
```

Figure 184. Displaying the Status for Line A04L05

You can determine that the NCP (A04NV4) is active because it is displayed in green on a color terminal. Because the NCP is active, the problem involves the line.

4. Enter the NetView SVTAM command to access the Node Status Detail (Description) panel. To return to the first menu, you can press PF10, the NetView supplied default PF key value, instead of the SVTAM command.

```
STATMON.NSD(DESC)              NODE STATUS DETAIL (DESCRIPTION)        16:34
HOST: HOST1           *1*   *2*   *3*   *4*
 ? A04NV4             ACTIVE  PENDING   INACT    MONIT    NEVACT   OTHER
?...15  LINES        ?....11  ?......  ?.....1  ?......  ?.....3  ?.....
-------------------------------------------------------------------------------
? DISPLAY       |   NODE ID.  DESCRIPTION           NODE ID.  DESCRIPTION
 ? APPLS        |
 ? LINES        | ? A04NPML   LINE
 ? PUS/CLSTRS   | ? A04L00    LINE
 ? LUS/TERMS    | ? A04L01    LINE
 ? CDRMS        | ? A04L02    LINE
 ? CDRSCS       | ? A04L03    LINE
  ? ACT         | ? A04L04    LINE
  ? EVERY       | ? A04L05    LINE
  ? INACT       | ? A04L06    LINE
 ? PENDING      | ? A04L07    LINE
 ? BFRUSE       | ? A04L08    LINE
? VARY INACT    | ? A04L09    LINE
 ? I     ? F    | ? A04KC     LINE
? VARY ACT      | ? A04KD     LINE
 ? ONLY  ? ALL  | ? A04KG     LINE

CMD==>
TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
```

Figure 185. Status for Line A04L05 and Available VTAM Commands

5. Activate the line and its attached resources by moving the cursor to the appropriate areas on the panel to select **VARY ACT**, **ALL**, and **A04L05** and pressing Enter. The command facility panel is displayed.

```
NCCF                      Tivoli NetView   CNM01 OPER3    04/12/02 16:35:00
* CNM01    V NET,ACT,ID=A04L05,SCOPE=ALL
  CNM01    IST097I  VARY     ACCEPTED
  CNM01    IST3801  ERROR FOR ID = A04L05 - REQUEST: ACTLINK , SENSE:
           08220000
  CNM01    IST105I  A04L05   NODE NOW INACTIVE
------------------------------------------------------------------------









???
```

Figure 186. Command Facility Response from Attempting to Activate Line A04L05

The attempt to activate the line fails, but a sense code is displayed (SENSE: 08220000).

6. Type `sense 08220000` and press Enter to determine the meaning of the sense code. A description of the sense code is displayed.

```
NLDM.SENS               SENSE CODE DESCRIPTION                      PAGE  1
-------------------------------------------------------------------------------

 SENSE DATA:
    CATEGORY - (08) Link procedure failure: A link-level procedure has failed
    MODIFIER - (22) because of link equipment failure, loss of contact with a
      BYTE 2 - (00) link station, or an invalid response to a link command.
      BYTE 3 - (00) This is not a path error, since the request being
                    rejected was delivered to its destination.









ENTER 'R' TO RETURN TO PREVIOUS DISPLAY - OR COMMAND
CMD==>
```

Figure 187. Sense Code Description for Line Activation Failure

The sense code description explains that the failure occurred when the communication controller tried to make contact with the local modem. The modem might be turned off, the EIA communication cable might be disconnected, or the control unit might not be installed properly.

The failed activation attempt is recorded as an event. Each installation has filters to determine which events become alerts. Assume this event passed the filters and became an alert. To continue the investigation, refer to the Alerts-History panel.

7. Type `npda alh` and press Enter to display the Alerts-History panel.

```
N E T V I E W          SESSION DOMAIN: CNM01    OPER3     04/12/02 16:36:00
NPDA-31A                     * ALERTS-HISTORY *              PAGE   1

SEL# DOMAIN RESNAME TYPE TIME  ALERT DESCRIPTION:PROBABLE CAUSE
( 1) CNM01 A04L05   LINE 07:41 DSR ON CHECK:LOCAL MODEM OFF/LOCAL MODEM
( 2) CNM01 P51K74   CTRL 07:41 DTR DROP:DEVICE
( 3) CNM01 LNE524   LINE 07:41 TIMEOUT:DEVICE/REMOTE MODEM OFF/COMMUNICATIONS
( 4) CNM01 LNE528   LINE 07:41 TIMEOUT:DEVICE/REMOTE MODEM OFF/COMMUNICATIONS
( 5) CNM01 A03L02   LINE 07:41 MODEM ERROR:LOCAL MODEM OFF/LOCAL MODEM
( 6) CNM01 A03L02   LINE 07:41 MODEM ERROR:LOCAL MODEM OFF/LOCAL MODEM
( 7) CNM01 A03L02   LINE 09:32 TIMEOUT:DEVICE/REMOTE MODEM OFF/COMMUNICATIONS
( 8) CNM01 A03L02   LINE 09:31 MODEM ERROR:LOCAL MODEM OFF/LOCAL MODEM
( 9) CNM01 A03L02   LINE 09:31 SELF TEST-NO RESPONSE:MODEM OFF/LOCAL MODEM
(10) CNM01 A03L02   LINE 09:30 SELF TEST-NO RESPONSE:MODEM OFF/LOCAL MODEM
(11) CNM01 A03L02   LINE 09:31 SELF TEST-NO RESPONSE:MODEM OFF/LOCAL MODEM
(12) CNM01 A03L02   LINE 09:30 SELF TEST-NO RESPONSE:MODEM OFF/LOCAL MODEM
(13) CNM01 A03P051  TERM*09:30 POWER OFF/INVALID ADDRESS:DEVICE
(14) CNM01 A03P051  TERM*09:30 POWER OFF/INVALID ADDRESS:DEVICE
(15) CNM01 A03L05   LINE 09:32 TIMEOUT:DEVICE/REMOTE MODEM OFF/COMMUNICATIONS
 ENTER SEL# (ACTION),OR SEL# PLUS M (MOST RECENT), P (PROBLEM), DEL (DELETE)

 ???
CMD==>
```

Figure 188. Alerts-History Panel Containing the Alert Associated with the Failure of Line A04L05

8. Find the alert on the Alerts-History panel. The description for alert indicates that this alert is probably caused by one of two things: the local modem is powered off for resource A04L05 or the modem has a problem. Type 1 and press Enter to display the recommended corrective actions for this problem. A panel similar to Figure 189 is displayed.

```
N E T V I E W          SESSION DOMAIN: CNM01    OPER3     04/12/02 16:37:00
NPDA-45A          * RECOMMENDED ACTION FOR SELECTED EVENT *     PAGE  1 OF  1
 CNM01       A03NV4     A03L05
            +--------+
 DOMAIN     |  COMC  |----LINE----
            +--------+
USER    CAUSED - LOCAL MODEM POWER OFF
       ACTIONS - D001 - CORRECT THEN RETRY

INSTALL CAUSED - CABLE
       ACTIONS - D022 - CHECK PHYSICAL INSTALLATION

FAILURE CAUSED - LOCAL MODEM
                 LOCAL MODEM INTERFACE CABLE
       ACTIONS - D022 - CHECK PHYSICAL INSTALLATION
                 D002 - RUN MODEM TESTS
                 D005 - CONTACT APPROPRIATE SERVICE REPRESENTATIVE



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

???
CMD==>
```

Figure 189. Recommended Action Panel for Line A04L05 Failure

9. Continue your investigation by following the recommended actions in sequence. Notice that `USER CAUSED` tells you that the problem might be that the modem is not on. Ensure the modem is on.
10. Next, refer to the `INSTALL CAUSED` on the panel. It tells you that the cable might not be installed properly. Determine whether the cable is installed correctly. After examining the cable, you find that the connection between the modem and cable has come loose. Restore the connection.
11. When the cable is reconnected, activate the line and its attached resource. On the command line, enter:

    ```
    act a04l05,all
    ```

    The command facility panel is displayed with messages showing that the resource is being activated. Clear the display and return to the hardware monitor.
12. Ask the user to log on again. The user tells you that logon is successful.
13. Follow your organizational procedure for submitting a problem report.

Topic:	Reference:
ACT command	NetView online help
Explanations of alert flags	NetView online help: **HELP NPDA 'DOMAIN'** For domain alert flags **HELP NPDA 'RESNAME'** For resource alert flags **HELP NPDA 'PROBABLE CAUSE'** For probable cause alert flags

Hung or Looping NetView Tasks (Command Facility)

If you notice that a command procedure processes much slower than usual, you can use the TASKUTIL command to help determine the cause of the problem. To do this, complete the following steps:

1. From the NetView command facility, issue the TASKUTIL command. Note that you must be logged on to a different operator ID from the one in which the command procedure is running. For example:

   ```
   taskutil type=ost duration=5
   ```

   This command measures NetView task utilization for 5 seconds and displays the results on your operator console. An example of the output follows:

```
 NCCF                      Tivoli NetView   CNM01 OPER2    04/12/02 15:14:35
* CNM01    TASKUTIL
' CNM01
DWO022I
TASKNAME TYPE DPR    CPU-TIME N-CPU% S-CPU% MESSAGEQ STORAGE-K  CMDLIST
-------- ---- --- ----------- ------ ------ -------- ---------  -------
OPER1    OST  251       66.94  99.86  84.00        6        66  CLIST1
OPER2    OST  251        0.93   0.11   0.09        0        59  **NONE**
OPER3    OST  251        0.47   0.00   0.00        0        83  **NONE**
NETVIEW  OTHR N/A         N/A   0.00   0.00      N/A       N/A       N/A
NETVIEW  SRB  N/A        5.34   0.03   0.03      N/A       N/A       N/A
NETVIEW  TOTL  32       92.40 100.00  84.11        6      3625       N/A
SYSTEM   TOTL N/A         N/A    N/A 100.00      N/A       N/A       N/A
END DISPLAY
```

High CPU utilization indicates the command procedure is in a loop. In this example, task OPER1 was using 99.86% of the CPU used by the NetView program and this was 84.00% of the total system CPU usage. The problem might be a loop in command list CLIST1 because CLIST1 is identified as being active and work is queued to the task.

2. Cancel the looping command list by using the following EXCMD command:

   ```
   excmd oper1,cancel
   ```

3. If the EXCMD command is not effective, log off the terminal.
4. If the logoff attempt is not successful, stop the operator task by using the following STOP command, where *luname* is the terminal ID from which OPER1 is logged on to the NetView program: `stop op=oper1,force` or `stop force=`*`luname`*

Topic:	Reference:
EXCMD, STOP, TASKMON, LOGTSTAT, and TASKURPT command	NetView online help

Measuring Response Time with Control Units Using RTM (Session Monitor)

One of the objectives of monitoring the response time is to detect performance degradation before it becomes visible to the user. Session response time data is measured and accumulated by control units having the response time monitor (RTM) feature. Examples of control units having the RTM feature include the 3274 and 3174 control units. The session monitor collects the response time data on command and when the session ends, and displays the data in various formats. The control units accumulate the measured response times into ranges of time that are specified by the performance class definitions. Sessions are associated with certain performance classes, and each performance class has associated with it a specific response time objective. You can display response-time graphs that show how the actual response time compares to a specified objective.

Response time data is displayed in one of the following ways:

- Response time summary for a terminal LU
- Response time trend for a terminal LU
- Response time for a session by collection period

Response time and configuration data for each session can be written to an external log as the response time data is collected, allowing other programs to process it.

In the following scenario, a user calls at 13:30 to complain about the terminal response time. The user also states that the response time has been getting slower since logging on at 11:20. To solve the problem, you can perform the following steps:

1. Determine the terminal ID (LU name) of the user. In this case, the terminal ID is LU3440.
2. Enter `nldm rtsum lu3440 * *` to display the summary of the response time data for LU3440 for the past hour. A panel similar to Figure 190 on page 321 is displayed:

```
NLDM.RTSUM                  RESPONSE TIME SUMMARY                    PAGE   1

LUNAME: LU3440           PERFORMANCE CLASS: TSO                 DOMAIN: NC10

                  RESPONSE TIME FROM 02/21 12:30 to 13:31

                                                    ACT:  75%  UNDER  5 SEC
 100% |                                             OBJ:  80%  UNDER  5 SEC
  90% |                                                           |
  80% |                                                           V
  70% |                                              ***************
  60% |                                             |----+----+----+----|
  50% |                                             0%  25%  50%  75% 100%
  40% |                    35%
  30% |             23%     ****                    NUMBER OF TRANS:  60
  20% |   17%     ****      ****      12%      13%  LAST TRANS TIME:  6   SEC
  10% |  ****     ****      ****     ****     ****  AVG RESP TIME:    4.3 SEC
   0% ------------------------------------------------
       0 -  1 S   -  3 S   -  5 S   - 10 S   OVER 10 S
 CUM % :  17%      40%      75%      87%     100%


ENTER 'R' TO RETURN TO PREVIOUS DISPLAY - OR COMMAND
CMD==>
```

Figure 190. Response Time Summary Panel

You notice that the user response time is actually 75% under 5 seconds, and the objective is for 80 per cent of the transactions to be completed in under 5 seconds. Because the user response times do not meet the response time objective, the horizontal bar is highlighted (or shown in red, depending on the terminal type).

At this point, inform the appropriate support personnel of the slow response time.

3. Because the user complained about a continually degrading response time, enter **nldm rtrend lu3440 11:20 *** to check the response times trend for LU3440. A panel similar to Figure 191 on page 322 is displayed:

```
NLDM.RTREND                                                        PAGE   1

LUNAME: LU3440           PERFORMANCE CLASS: TSO                DOMAIN: NC10

                       TRANSACTIONS UNDER  5   SECONDS

           96%
 100%  |    ***   93%   90%         85%
  90%  |    ***   ***   ***   82%   ***   80%                     78%
  80%  | -- *** - *** - *** - *** - *** - *** - 70% ------------ *** ---------
  70%  |    ***   ***   ***   ***   ***   ***   ***               ***
  60%  |    ***   ***   ***   ***   ***   ***   ***               ***
  50%  |    ***   ***   ***   ***   ***   ***   ***               ***
  40%  |    ***   ***   ***   ***   ***   ***   ***               ***
  30%  |    ***   ***   ***   ***   ***   ***   ***         22%   ***
  20%  |    ***   ***   ***   ***   ***   ***   ***         ***   ***
  10%  |    ***   ***   ***   ***   ***   ***   ***    0%   ***   ***
   0% ------------------------------------------------------------------
       11:20 11:30 11:45 12:00 12:15 12:30 12:45 13:00 13:15 13:30 13:42
       02/21


ENTER 'R' TO RETURN TO PREVIOUS DISPLAY - OR COMMAND
CMD==>
```

Figure 191. Response Time Trend Panel

You notice that the user response time has become worse in the last hour. The last bar suggests that the trend might have been reversed, but not enough time has elapsed since 13:30 to decide whether the response time is now approaching its previous level.

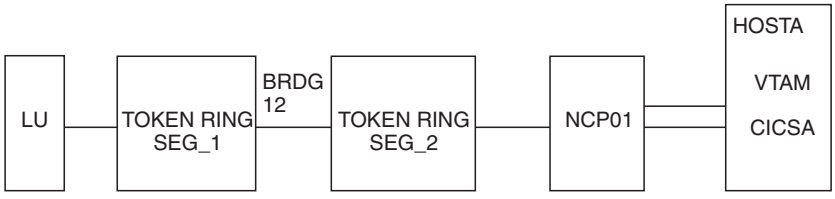
4. Log a problem report. You can now display the configuration for this session using the Session Configuration Data panel of the session monitor. See "Using the Session Monitor (SNA Subarea, SNA Advanced Peer-to-Peer Networking)" on page 90 for additional information on using the session monitor.

   Use the information obtained, along with other problem determination tools (such as Hardware monitor and Network performance monitor) to locate problems which were identified along this session path.

Topic:	Reference:
AUTOCOLL, COLLECT, RTREND, RTSUM, QUERY RANGE, SET RANGE command	NetView online help

Sluggish Network Performance (NetView Performance Monitor)

The following scenario shows how to use the NetView program in conjunction with NetView Performance Monitor to solve a typical user problem. In this case, a user is experiencing sluggish network performance. The user is connected from the LU USR01 to a VTAM application (CICSA) using the following configuration:



The user calls to report the problem. To resolve the problem, you can:

1. Ask the user for the terminal identifier. In this case, the terminal identifier is USR01. In addition, the user terminal is in session with CICSA running on HostA.
2. Enter **sess usr01** from the session monitor command line to list the sessions for resource USR01. A panel similar to Figure 192 is displayed.

```
NLDM.SESS                                                          PAGE    1
                                SESSION LIST
NAME: USR01                                                     DOMAIN: A02NV
--------------------------------------------------------------------------------
      ***** PRIMARY *****  **** SECONDARY ****
 SEL#   NAME   TYPE  DOM     NAME   TYPE  DOM     START TIME       END TIME
 ( 1) CICSA    LU   A02NV  USR01    LU   A02NV  01/25 10:17:35  *** ACTIVE ***
 ( 2) A02N     SSCP A02NV  USR01    LU   A02NV  01/25 10:00:20  *** ACTIVE ***
 ( 3) NPMA02   LU   A02NV  USR01    LU   A02NV  01/25 11:49:43  *** INITF  ***









END OF DATA
ENTER SEL# (CONFIG), SEL# AND CT (CONN. TEST), SEL# AND STR (TERM REASON)
CMD==>
```

Figure 192. Session List Panel

From this panel, you can see that:

- The CICSA-USR01 session is active.
- No other USR01 sessions exist that might be affecting the network response time.

3. Select **1** to display the Session Configuration Data panel for the USR01-CICSA session. A panel similar to Figure 193 on page 324 is displayed.

```
NLDM.CON                  SESSION CONFIGURATION DATA                  PAGE    1
-------------- PRIMARY ---------------+-------------- SECONDARY --------------
NAME CICSA     SA 00000002  EL 0010   |   NAME USR01     SA 00000001  EL 07D5
-------------------------------------+---------------------------------------
DOMAIN A02NV       PCID NETA.HOSTA.E7E3F9568F3BE167               DOMAINA02NV
                +-------------+                 +-------------+
HOSTA           |   CP/SSCP   | ---         --- |             |
HOSTAPU (0000)  | SUBAREA PU  |                 | SUBAREA PU  | NCP01 (0000)
                +------+------+  SUBA TP 02     +------+------+
                       |             VR 00            |
                +------+------+      ER 05     +------+------+
   CICSA(0010)  |     LU      |     RER 0A     |    LINK     | J0003001
                +-------------+                +------+------+
                                                      |
                                SUBACOS ISTVTCOS +----+------+
                                LOGMODE MX232T   |     PU      | PU01  (0481)
                                                 +-------------+
                                                       |
                                                 +-----+------+
                                                 |     LU     | USR01 (07D5)
                                                 +------------+

SELECT PT, ST (PRI, SEC TRACE), RT (RESP TIME), P, ER, VR
CMD==>
```

Figure 193. Session Configuration Data panel

You can use this panel to obtain information about the way in which the LU is connected to the host (CCU name, Logical Link, PU name, and so on).

4. Switch to another 3270 emulation session and log on to NetView Performance Monitor. A panel similar to Figure 194 is displayed.

```
FNM00PRI                    NPM V2R1   5655-043                        E 1
                              PRIMARY OPTIONS
                                                                        CNM01

Select Option ===>

  0  User Profile           -  NPM Terminal and User Parameters          VE ***
  1  NCP Management         -  Network Data Collection and Analysis      VE ***
  2  Session Management     -  Session Data Collection and Analysis
  3  RTM Management         -  RTM Data Collection and Analysis
  4  LAN Management         -  LAN Data Collection and Analysis
  5  VTAM Management        -  VTAM Data Collection and Analysis




  9  NPM Control            -  NPM Control Functions
  P  Problem                -  Problem Determination Facilities
  T  Tutorial               -  Online Tutorial
  X  Exit                   -  NPM Logoff

PF 1=HELP      2=          3=LOGOFF    4=          5=          6=
PF 7=          8=          9=         10=         11=         12=LOGOFF
```

Figure 194. NetView Performance Monitor Primary Options Panel

5. Select **2** to display the session management panel. The panel shown in Figure 195 on page 325 is displayed.

```
FNM01SES                    NPM V2R1   5655-043                        E 1
                            SESSION MANAGEMENT
                                                                        CNM01

Select Option ===>

  1  Start Session                                                     VE ***
  2  Stop/Status Active                                                VE ***
  3  Stop/Status Deferred


  6  LU Detail Analysis
  7  Session Analysis
  8  Performance Status Display
  9  Session Monitor Display


Host Name ===> LOCAL


PF 1=HELP      2=          3=LOGOFF    4=          5=          6=
PF 7=          8=          9=         10=         11=         12=RETURN
```

Figure 195. NetView Performance Monitor Session Management Panel

6. Select **1** to start collecting data for the user LU (USR01). A panel similar to Figure 196 is displayed.

```
FNM02SCL                     NPM V2R1   5655-043
                             SESSION MANAGEMENT
                               START SESSION

Command ===>
Resource Name       ===>
Node Name           ===>
Host Name           ===> LOCAL
Session Statistics  ===> Y                  (Yes/No/Vol/Xcl/Rsp)
VTAM Log            ===> 0                  (0/1/2/3)
Minimum PIU Trace   ===> YES                (Yes/No)
GTF Trace           ===> NO                 (Yes/No)
Transit Thresholds:
  Operator          ===>   .20 :   .30      (Low:High)
  Network           ===>   .10 :   .20      (Low:High)
  Host              ===>   .10 :   .20      (Low:High)
Distribution Bounds ===>  5.00 : 10.00 : 20.00 : 30.00
Start Time          ===>  00 : 00 : 00      (hh:mm:ss)
Stop Time           ===>  00 : 00 : 00      (hh:mm:ss)
Daily               ===> NO                 (Yes/No)
PF 1=HELP      2=          3=END       4=          5=          6=
PF 7=          8=          9=         10=         11=         12=RETURN
```

Figure 196. NetView Performance Monitor Start Session Panel

This type of data collection provides statistics for each session with the host, including message volumes and transit times. In this case, you are most interested in transit time data, the length of time it takes for inbound and outbound PIUs to travel through the host, network, or both. With NetView Performance Monitor, you can split the total transit time between the following times:

- Host transit time, the length of time the PIU spends in the host

- Network transit time, the length of time the PIU spends in the network

7. Type the LU name for the user in the **Resource Name** field and press Enter. A panel similar to Figure 197 is displayed.

```
FNM03SAS                      NPM V2R1   5655-043
                              SESSION MANAGEMENT
                           SESSION MONITOR SELECTION

Command ===>
Enter Monitor Criteria for Resource USR01                Criteria
                                                      Low     :      High
Average Operator Transit Time                    ===>     .00 :       .00
Average Host Transit Time                        ===>     .00 :       .00
Average Network Transit Time                     ===>     .00 :       .00
Maximum Operator Transit Time                    ===>     .00 :       .00
Maximum Host Transit Time                        ===>     .00 :       .00
Maximum Network Transit Time                     ===>     .00 :       .00
% of Operator Trans Exceeding Transit Threshold  ===>       0 :         0
% of Host Trans Exceeding Transit Threshold      ===>       0 :         0
% of Network Trans Exceeding Transit Threshold   ===>       0 :         0
Number of Active LUs in a Summary Record         ===>       0 :         0
Average Number of PIUs per Minute                ===>       0 :         0
Average Number of Bytes per Second               ===>       0 :         0

PF 1=HELP      2=          3=END       4=          5=          6=
PF 7=          8=          9=         10=         11=         12=RETURN
```

Figure 197. NetView Performance Monitor Session Monitor Selection Panel

You can use this panel to set the low and high monitor criteria for the resource. For this scenario, the field values are left as zero.

8. Press Enter to start the collection for the selected resource. The system then returns to the Start Session panel.
9. After the collection interval has passed, enter `=2.6` to access the Session Management panel. The panel shown in Figure 198 on page 327 is displayed.

```
FNM02DNM                      NPM V2R1   5655-043
                              SESSION MANAGEMENT
                              LU DETAIL ANALYSIS

Select Option ===>
  1  Transit Time/Interval    3  Volume/Interval
  2  Distribution/Interval    4  Transit Time Summary

LU Name                 ===> USR01
Host Name               ===> LOCAL
Data Qualifiers:
  Application           ===>
  Line                  ===>
  Physical Unit         ===>
  Virtual Route Number  ===>           (0-7)
  Transmission Priority ===>           (0-2)
File Name               ===> SESSION
Date               from ===> 09 / 30 / 93 to ===> 09 / 30 / 93  (mm/dd/yy)
Time               from ===> 08 : 00 : 00 to ===> 17 : 00 : 00  (hh:mm:ss)

PF 1=HELP      2=          3=END       4=          5=          6=
PF 7=          8=          9=         10=         11=         12=RETURN
```

Figure 198. NetView Performance Monitor LU Detail Analysis Panel

10. Select **4** to display the transit time summary. A panel similar to Figure 199 is displayed.

```
FNM03SMN                      NPM V2R1   5655-043
                              SESSION MANAGEMENT
                  NPM SESSION ANALYSIS SUMMARY - LOGICAL UNIT

Command ===>
Host Name   = LOCAL        Records = 8          VR/TP =     /
Application =              Line    =            PU    =
Group       =              Node    =            LU    = USR01
Requested Date/Time: from  01/25/01  00:00:00    to  01/26/01  00:00:00
Actual Date/Time   : from  01/25/01  11:46:13    to  01/25/01  15:00:00
                     Total         Response
Transactions         635           630
                     Operator      Host            Network
Average Transit       5.85          1.12            4.73
Maximum Transit      80.19         16.70           80.15
                     PIU Count     Avg Size        Total Bytes
User Data In         1131                19              21969
User Data Out        1378               222             306403
System Data In       1480                 5               8012
System Data Out        65                 7                424


PF 1=HELP      2=          3=END       4=TRANSIT   5=VOLUME    6=DISTRIB
PF 7=          8=          9=         10=         11=         12=RETURN
```

Figure 199. NetView Performance Monitor Session Analysis Summary - Logical Unit Panel

As you can see, the transit times for the network greatly exceed the transit times for the host, indicating that the bottleneck is located in the network. You can now proceed to collect network data to isolate the problem.

11. Enter =1.9.1 from the command line to access the NCP Management Network Start panel. A panel similar to Figure 200 is displayed.

```
FNM03STD                      NPM V2R1   5655-043
                                NCP MANAGEMENT
                                NETWORK START

Command ===>

                                                          *---------------*
Interval Number   ===> 1                           <======|    Interval   |
                                                         | Num    Time   |
NCP Name          ===> NCP01                             |  1   00:03:45 |
Resource Name     ===> LINE1                             |  2   00:07:30 |
Dynamic Resource  ===> NO       (Yes/No)                 |  3   00:15:00 |
                                                         |  4   00:30:00 |
                                                         |  5   01:00:00 |
Start Time        ===> 00 : 00 : 00   (hh:mm:ss)         |  6   02:00:00 |
Stop Time         ===> 00 : 00 : 00                      |  7   04:00:00 |
Daily             ===> NO             (Yes/No)          *---------------*



PF 1=HELP      2=          3=END       4=          5=          6=
PF 7=          8=          9=         10=         11=         12=RETURN
```

Figure 200. NetView Performance Monitor NCP Management Network Start Panel

You can use this panel to perform network data collection and analysis.

12. To see if the problem exists on the line that connects the TIC to the SEG2 LAN, type the line name (LINE1) in the **Resource Name** field.

    Then, specify the interval period in the **Interval Number** field.

    Note: You can obtain the TIC name by using the NetView Session Configuration Data panel to obtain the Logical Link name and then checking the NCP gen definition to determine the related Physical Link and the TIC name.

13. Press Enter to display the second NCP Management Network Start panel. A panel similar to Figure 201 on page 329 is displayed.

```
FNM03STM                      NPM V2R1   5655-043
                                NCP MANAGEMENT
                                NETWORK START

Command ===>

Host Name = LOCAL      NCP Name = NCP01      Resource Name = LINE1

Data Destinations      NPMLOG  VSAM   SMF   ALERT   GLOBAL
  Detail           ===> YES    YES    YES    N/A     N/A
  Monitor          ===> YES    YES    YES    NO      YES
Resolve Monitors   ===> NO     (Yes/No)

Monitor Criteria                                      LOW        : HIGH
  Negative polls/minute     (0-2147483646)     ====> 0          : 0
  Positive polls/minute     (0-2147483646)     ====> 0          : 0
  PDUs/minute               (0-2147483646)     ====> 0          : 0
  Bytes/second              (0-2147483646)     ====> 0          : 0
  Line utilization          (0-100)            ====> 0          : 0
  Error count               (0-2147483646)     ====> 0          : 0


PF 1=HELP      2=          3=END       4=          5=          6=
PF 7=          8=          9=         10=         11=         12=RETURN
```

Figure 201. NetView Performance Monitor NCP Management Network Start Panel

In this case, you want to collect data to verify that the line is working.

14. Press Enter to start collection on the selected resource and wait for the collection interval to end.
15. Enter `=1.9.4` from the command line to access the NCP Management Network Review Data panel. A panel similar to Figure 202 is displayed.

```
FNM02RVM                      NPM V2R1   5655-043
                                NCP MANAGEMENT
                                NETWORK REVIEW

Command ===>

Host Name        ===> LOCAL
Resource Name    ===> LINE1            (Name/Monitor)
Review File Name ===> REVIEW

Start Date       ===> 09 / 30 / 93     (mm/dd/yy)
Stop  Date       ===> 09 / 30 / 93

Start Time       ===> 00 : 00 : 00     (hh:mm:ss)
Stop  Time       ===> 00 : 00 : 00

Data Type        ===> DETAIL           (Detail/Monitor)



PF 1=HELP      2=          3=END       4=          5=          6=
PF 7=          8=          9=SUMMARY  10=         11=         12=RETURN
```

Figure 202. NetView Performance Monitor NCP Management Network Review Panel

16. Type `Detail` in the **Data Type** field and press Enter. A panel similar to Figure 203 is displayed.

```
 FNM03RVL                      NPM V2R1   5655-043
                                 NCP MANAGEMENT
                               NETWORK REVIEW DATA

Command ===>

Host Name = LOCAL      Resource Name = LINE1     Data Type = LINE DETAIL
Date/Time: from  01/25/01    11:45:00  to   01/25/01  15:00:00

End       Interval   Queue  Msgs  Bytes  Line-Ut   Polls/Min          Retransmit
Time      hh:mm:ss  Length  /Min  /Sec   Pri  Sec  Rate %Neg  Errors  PIUs Bytes
11:45:00  00:15:00       0    21   108    19    0   281   98       0     0     0
12:00:00  00:15:00       0    76   244    41    0   216   91       0     0     0









 PF 1=HELP      2=          3=END       4=          5=          6=
 PF 7=          8=          9=SUMMARY  10=         11=         12=RETURN
```

Figure 203. NetView Performance Monitor NCP Management Network Review Data Panel

This panel displays detail data for lines, PUs, and LUs. You can spot problems by analyzing the following fields:

- Line Utilization (Line-Ut)
- Errors (Errors)
- Retransmitted Bytes (Retransmit Bytes)

In general, the following three conditions are the reasons for poor response time:

- High traffic on a line

  This condition is indicated by high line utilization, a low number of errors, and a low number of retransmissions.
- Excessive noise

  This condition is indicated by high line utilization and a high number of errors.
- No activity

  This condition, which can be caused by a mechanical failure, is indicated by zero line utilization.

17. Repeat steps 11 on page 328 through 16 (specifying the NCP name, NCP01, in the **Resource Name** field of the NCP Management Network Start panel). A panel similar to Figure 204 on page 331 is displayed.

```
FNM03RVP                      NPM V2R1   5655-043
                                NCP MANAGEMENT
                              NETWORK REVIEW DATA

Command ===>

Host Name = LOCAL       Resource Name = NCP01      Data Type = NCP DETAIL
Date/Time: from: 01/25/01  11:45:00  to  01/25/01  12:00:00
Slowdown Limit: 17

 End       Interval    CCU   <-  Free Buffer ->      Channel     Interval
 Time      hh:mm:ss   Util   QLen   High    Low    Interm Hold   Slowdown
 11:45:00  00:15:00     63   1366   1366   1362         1    2          0
 12:00:00  00:15:00     63   1364   1365   1362         2    2          0









 PF 1=HELP      2=          3=END       4=          5=          6=
 PF 7=          8=          9=SUMMARY  10=         11=         12=RETURN
```

Figure 204. NetView Performance Monitor NCP Management Network Review Data Panel

This panel displays CCU utilization, slowdown, and buffer information. In this case, the CCU Utilization (**CCU Util** field) looks almost high, indicating that the NCP might be the cause of the poor response time. You can now proceed to obtain TIC data.

18. Repeat steps 11 on page 328 through 16 on page 330 (specifying the TIC name, TIC1, in the **Resource Name** field of the NCP Management Network Start panel). See the note in 12 on page 328 to determine how to obtain the TIC name.

    A panel similar to Figure 205 is displayed.

```
FNM03RVN                      NPM V2R1   5655-043
                                NCP MANAGEMENT
                     NETWORK REVIEW DATA FOR NTRI RESOURCES

Command ===>

Host Name = LOCAL       Resource Name = TIC1        Data Type: PHYLINK DETAIL
Date/Time: from 01/25/01  11:45:00  to  09/30/01  12:00:00

End       Interval  Queue IFrames Bytes Time   Retransmit  TIC  Congest  Active
Time      hh:mm:ss Length    /Min  /Sec Outs IFrames Bytes Util   Count   Conns
11:45:00  00:15:00      0      21   108            0     0   83       0       5
12:00:00  00:15:00      0      76   244            0     0   76       0       3









 PF 1=HELP      2=          3=END       4=          5=          6=
 PF 7=          8=          9=SUMMARY  10=         11=         12=RETURN
```

Figure 205. NetView Performance Monitor NCP Management Network Review Data for NTRI Resources Panel

You can use the data in this panel to help you determine if the problem is caused by the TIC or the host or NCP. If the TIC utilization (**TIC Util** field) or the congestion count (**Congest Count** field) is high, the TIC is the probable cause of the low response time. If the outbound queue length (**Queue Length** field) or the number of retransmissions (**Retransmit Frames** or **Retransmit Bytes** fields) is too high, the host or NCP is the probable cause of the low response time.

In this scenario, the TIC utilization value for both intervals is very high. This indicates that the TIC is the probable cause of the sluggish performance.

19. Notify the system programmer. If too much data is flowing through the TIC, the system programmer can then redistribute the attached resources by using another TIC.

Topic:	Reference:
Using NetView Performance Monitor	*NetView Performance Monitor User's Guide*
Using the session monitor panels	"Session Monitor Scenarios" on page 94

Using the NetView Help Desk

The NetView help desk can provide problem determination data and circumvent or resolve resource problems. To access the help desk, enter:

```
helpdesk
```

Choose from the following topics that are listed in the help desk:

```
               NETVIEW HELPDESK TOPICS

1     Introduction

0     Contents

1     If a terminal is not working
2     If a transaction or an application is not working
3     If there is slow response time
4     If there are problems identified through network monitoring
5     If you need help using NetView
6     If an agent or service point problem occurs
7     If you want to display status and statistics
8     If you want to gather trace data
9     Common checklists
```

Chapter 21. Managing Problems

Problem management is a function that lists, creates, displays, and updates problem reports. Problem reports are records that identify known problems with individual resources and are stored in the Information/Management database.

You can also use the NetView AutoBridge product to automate problem reporting, allowing problem records to be created in response to alerts, messages, message services units, and application data. You can then use the Problem Management Bridge/MVS to take that problem information and notify RETAIN® or another vendor electronically and automatically. The RETAIN system and other vendors systems supply an application that converts the problem record to a format that is compatible with their system. The Problem Management Bridge/MVS then manages the transfer of the problem data between Information/Management and RETAIN or the vendor system.

Using the Hardware Monitor

Use the hardware monitor Information/Management link to send event data to Information/Management and open problem records. From the hardware monitor Alerts-Static, Alerts-History, Most Recent Events, and Event Summary panels, you can transfer problem data directly into an Information/Management problem record. Include the NetView operator ID in an Information/Management privilege class that has authority to update Information/Management records. The data transferred from the hardware monitor to Information/Management is shown in Table 25:

Table 25. Hardware Monitor to Information/Management Data Transfer

NPDA Field Name	Length (Bytes)	V2 Info/Mgmt Field Name	Length (Bytes)
Resource Name (see note)	8–40	Resource Names	8–40
EV/AL DESC:PROB CAUSE	48	Description Abstract	45 (might be truncated)
Date	8	Date Occurred	8
Time	5	Time Occurred	5
Operator ID	8	Reported By	8
Constant (NPDA)	4	Reporter Dept	4
Domain Name	5	System Name	5
Action Panel ID	8	Action Panel ID	8
Detail Event Description	1040	Free Form Description	1040
Recommended Action	1120	Free Form Status	1120
Resource Type	4–20	Resource Types	4–20

Note: The hardware monitor sends as many as five resource names to define the failing resource. For example, an IBM 3710 Network Controller can send resource names in the following order:

1. NCP name
2. LINE name

3. PU name
4. LINE name
5. PU name

You can then enter additional data about a specific problem into Information/Management.

Creating a Problem Report

Complete the following steps to create a problem report from the hardware monitor.

1. From a NetView command line, enter the hardware component Alerts-Dynamic Display:

   ```
   npda ald
   ```

   A panel similar to Figure 206 is displayed. This single-page panel continuously shows the system being monitored. As failures occur, each alert is shown at the top of the panel, and the alert at the bottom of the panel is removed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER9     04/12/02 10:49:03
NPDA-30A                     * ALERTS-DYNAMIC *

    DOMAIN RESNAME  TYPE TIME  ALERT DESCRIPTION:PROBABLE CAUSE
     CNM01 P51G76   CTRL 10:35 ERROR TO TRAFFIC RATIO EXCEEDED:COMMUNICATIONS
     CNM01 P51R74   CTRL 10:33 ERROR TO TRAFFIC RATIO EXCEEDED:COMMUNICATIONS
     CNM01 P51G76   CTRL 10:32 ERROR TO TRAFFIC RATIO EXCEEDED:COMMUNICATIONS
     CNM01 K5180    LINE 10:24 MODEM CHECK:LOCAL MODEM-LSL1 OFF/LOCAL MODEM
     CNM01 P51K74   CTRL 10:21 TIMEOUT:DTR DROP
     CNM01 P51G76   CTRL 10:17 POWER OFF DETECTED:DEVICE OFF/DEVICE
     CNM01 P51K74   CTRL 10:15 TIMEOUT:DEVICE OFF/REMOTE MODEM OFF/COM









DEPRESS ENTER KEY TO VIEW ALERTS-STATIC

???
CMD==>
```

Figure 206. Alerts-Dynamic Panel

The top of the Alerts-Dynamic panel shows the date and time the panel was last updated and the domain name. Each alert is displayed on a separate line according to the following format:

RESNAME
The name of the resource associated with the alert

TYPE The resource type

TIME The time the alert was received from the system

ALERT DESCRIPTION:PROBABLE CAUSE
An abbreviated message describing the error that has occurred and the probable cause. The probable cause is the component that is most likely to have caused the failure.

2. Press **Enter** to switch to the Alerts-Static panel. A panel similar to Figure 207 is displayed.

```
Tivoli NetView         SESSION DOMAIN: CNM01    OPER9     04/12/02 10:49:26
NPDA-30A                      * ALERTS-STATIC *

SEL# DOMAIN RESNAME TYPE TIME  ALERT DESCRIPTION:PROBABLE CAUSE
( 1) CNM01 P51G76   CTRL 10:35 ERROR TO TRAFFIC RATIO EXCEEDED:COMMUNICATIONS
( 2) CNM01 P51R74   CTRL 10:33 ERROR TO TRAFFIC RATIO EXCEEDED:COMMUNICATIONS
( 3) CNM01 P51G76   CTRL 10:32 ERROR TO TRAFFIC RATIO EXCEEDED:COMMUNICATIONS
( 4) CNM01 K5180    LINE 10:24 MODEM CHECK:LOCAL MODEM-LSL1 OFF/LOCAL MODEM
( 5) CNM01 P51K74   CTRL 10:21 TIMEOUT:DTR DROP
( 6) CNM01 P51G76   CTRL 10:17 POWER OFF DETECTED:DEVICE OFF/DEVICE
( 7) CNM01 P51K74   CTRL 10:15 TIMEOUT:DEVICE OFF/REMOTE MODEM OFF/COM









DEPRESS ENTER KEY TO VIEW ALERTS-DYNAMIC OR ENTER A TO VIEW ALERTS-HISTORY
ENTER SEL# (ACTION),OR SEL# PLUS M (MOST RECENT), P (PROBLEM), DEL (DELETE)

???
CMD==>
```

Figure 207. Alerts-Static Panel

3. Type the alert number followed by `p` in the **CMD==>** field to create the problem report. For example, to create a problem report for alert 4, enter `4 p` in the **CMD==>** field. A message similar to the following message is displayed in reverse video at the bottom of the panel:

   ```
   BNJ276I PROBLEM FILED BY INFORMATION/MANAGEMENT, ID IS 00000426
   ```

Note: The Information/Management load library SBLMMOD1 must be one of the concatenated libraries for this process to work. For more information on configuring Information/Management to work with the NetView program, see the Information/Management library.

Using NetView AutoBridge/MVS

You can use NetView AutoBridge/MVS to automate problem reporting. NetView AutoBridge can be driven from NetView alerts, messages, message services units (MSUs), and application data. It uses the NetView Bridge, has checkpoint and host processing capability, and can be used to search the database before creating additional problem tickets. It is not necessary to use the NetView management console or the hardware monitor to create problem records for the events identified to the NetView AutoBridge.

For example, the following message can produce the standard Information/Management problem record shown in Figure 208 on page 336.

```
EZL501W 08:31 : RECOVERY FOR PU TA1P42A HALTED - 4 ERRORS SINCE
15:30 ON 08/11/93 - CRITICAL ERROR THRESHOLD EXCEEDED
```

```
BLG0B100                  PROBLEM REPORTER ENTRY           PROBLEM: ________

Enter problem reporter data; cursor placement or input line entry allowed.
 1. Reported by......<R> NETVIEW________  13. Problem type......... HARDWARE
 2. Reporter dept....... AUTOBRIDGE_      14. Problem status....<R> OPEN____
 3. Reporter phone...... _____________    15. User problem number.. ________
 4. Date occurred....... 08/12/01         16. Initial priority..... 02
 5. Time occurred....... 08:31            17. Outage.............. ________
 6. Network name........ CNM01___         18. Rerun time.......... ________
 7. System name......... VTAMV311         19. Network impact...... ________
 8. Program name........ ________         20. System impact....... ________
 9. Device name......... TA1T42A_         21. Program impact...... ________
10. Key item affected... PU______         22. Device impact....... ________
11. Date fix required... ________         23. User form number..... ________
12. Time fix required... _____            24. Location code........ ________
                                          26. Outage type.......... UN

25. Description......<R> TA1T42A CRITICAL ERROR THRESHOLD EXCEEDED____
```

```
BLG1TDDE                      DESCRIPTION TEXT                      LINE

08/12/01   RECOVERY FOR PU TA1T42A HALTED -  4 ERRORS SINCE 15:30 ON 08/
```

Figure 208. Sample Information/Management Problem Reporter Panel

The previous message can also produce the following Information Integration Facility record:

```
BTN0B100                      PROBLEM DATA                    PROBLEM: 00000001

  1. Callers name.....<R> NETVIEW________  13. Problem type......... HDW
  2. Callers dept........ AUTOBRIDGE_      14. Problem status....<R> OPEN_____
  3. Callers phone #..... _____________    15. Severity............. _
  4. Date occurred....<R> 08/12/01         16. Initial priority..... 02
  5. Time occurred....<R> 08:31            17. Location............. RALEIGH_
  6. Dev/Comp name....... TA1T42A_         18. Contact name... LAPOINTE_______
  7. Related problem #... ________         19. Contact phone.. 919-555-5386

    (NPDA) Components affected

 20. Gen. device type.... PU               40. Program name....... ________
 21. Comp model.......... __________       41. Vendor component #. ___________
 22. Serial #............ ________         42. Program version.... ____
 23. System name......... ________         43. Release level...... ____
 24. Network name........ ________         44. Fix level.......... ________
 25. Description......<R> TA1T42A CRITICAL ERROR THRESHOLD EXCEEDED ___
```

Figure 209. Sample IIF Problem Reporter Panel

To accomplish this, install and customize the NetView AutoBridge/MVS product. You can then further customize the NetView AutoBridge by mapping selected alerts and messages.

Implementing NetView AutoBridge

Complete the following steps to implement the NetView AutoBridge:

1. Define the record data. Determine what data to send in the record and its origin. The Information/Management API references an alias table for required and optional field definitions. If a required field, such as Problem Status, cannot be determined by the originating MSU or message, you can define a default value in the Information/Management alias table or the NetView AutoBridge process table. You can then decide what fields to produce or parse from the MSU or message to *fill in* the remainder of the record.
2. Decide which MSUs and messages need to drive the NetView AutoBridge. Identify alerts and error messages which need to result in an Information/Management problem record. For example, the AON message, EZL501I, reports that a critical threshold has been exceeded. This condition requires manual intervention; thus it is a good candidate for creating a problem record.
3. Determine the create versus update and search criteria. You can conditionally create or update or unconditionally create records. Conditional processing means that a preliminary search is performed, and based on the search results, a create or update transaction is performed. Unconditional create means that a new record is always created.

   Consider the search criteria. You can choose to search just on a resource name, which can result in updating a record regardless of how it was created. That means that any open problem record for this resource created by help desk personnel or other automation gets updated. You can alternately choose to create a new record if the existing record did not originate from the NetView AutoBridge.
4. Customize the NetView program, Information/Management, and NetView AutoBridge in the following way:

Table 26. Customizing the NetView Program, Information/Management, and AutoBridge

NetView Customization	NetView AutoBridge Customization	Information/Management Customization
1. Customize the automation table to trigger the NetView AutoBridge for the selected MSUs and messages. 2. Add the necessary autotasks and profiles and command model statements. 3. Add the NetView AutoBridge data sets to the NetView startup procedure. 4. Create a VSAM file for checkpointed problem records and define the associated DSTs.	1. Code the process table. This defines actions to take, such as adding or parsing data and creating or updating a record. 2. Code the mapping table. This specifies the data from the incoming MSU or message to put into the Information/ Management record. 3. Code the initialization table. This defines the database target address, table names, retry counts and intervals, dispatchers, and adapters.	1. Code the field panel and structured word index in the PIDT table and the alias names and their default values in the alias table (PALT). 2. Create a new session member for postprocessing the record. 3. Create a mapping reference record to define how a record is postprocessed.

Topic:	Reference:
Using the NetView AutoBridge	NetView AutoBridge library

Topic:	Reference:
Collecting problem data using the NetView Bridge	*Tivoli NetView for OS/390 Bridge Implementation* (available from Version 1, Release 4 only) Publication number: SC31-8238-03
Using the Information Integration Facility	Information/Management library

Part 6. Appendixes

Appendix A. Message Format

Most messages have the following format:

```
type domid code msgno text
```

Where:

type Message type. For more information on message type symbols, refer to HDRMTYPE in the DSITIB macro.

domid Domain or application of the message origin

code Code (see "Message Codes")

msgno Message number you can use to look up more information in *IBM Tivoli NetView for z/OS Messages and Codes Volume 1 (AAU-DSI)* and *IBM Tivoli NetView for z/OS Messages and Codes Volume 2 (DUI-IHS)*, or using the online help.

text Text of the message

Message Codes

The following are message codes that indicate the origin or destination of a message:

B The command came from the NetView Web browser.

P The message came from the PPT.

% The message was sent only to the authorized receiver of the messages (assigned with PRI).

P% The message was sent to the authorized receiver and came from the PPT.

***** The message was sent to a secondary receiver (assigned with SEC).

P* The message was sent to a secondary receiver (assigned with SEC) from the PPT.

+ The message has been copied and sent to this receiver (assigned with COPY).

? The message is an important message echoed to the system console by the status monitor. The question mark prevents the echoed message from being logged as an important message by the status monitor.

In some cases, the initial portion of the message (*type domid code*) is displayed on a line by itself as a title, and the remainder of the message (*msgno text*) is on the following line.

Appendix B. NetView Component Hierarchies

This section describes the following NetView component hierarchies:

Using the Help Panels

Use the NetView HELP command to obtain help on components, panel fields, commands, messages, sense codes, and return and feedback codes. Entering `help` or pressing PF1 (if your PF keys use the NetView-supplied defaults) takes you to the "Help Overview" for the current component.

Entering `help netview` or pressing PF1 from the NetView MAINMENU panel opens the NetView Help Facility Main Menu, similar to the screen shown in Figure 210.

```
CNMKNEEW             Tivoli NETVIEW HELP FACILITY MAIN MENU


Select  To get information about

   1    Operator's overview of the NetView Program
   2    Using the NetView Help Desk for operators
   3    Using NetView online message help
   4    Using command and command list help
   5    Finding help on VTAM in NetView
   6    Finding help on IBM LAN Network Manager
   7    Finding help on RODM (Resource Object Data Manager)
   8    Finding help on GMFHS (Graphic Monitor Facility Host Subsystem)
   9    Help for the NETVIEW stage (NetView Pipelines)
   A    All NetView commands
   I    Finding help in the Index
   P    Help for PIPE syntax

Type a value (1 to 9, A, I, or P) and press ENTER.



TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
Action===>
```

Figure 210. NetView Help Facility Main Menu

Navigating the Help Panel Hierarchy

Figure 211 on page 344 shows the general relationship of the NetView help panels.

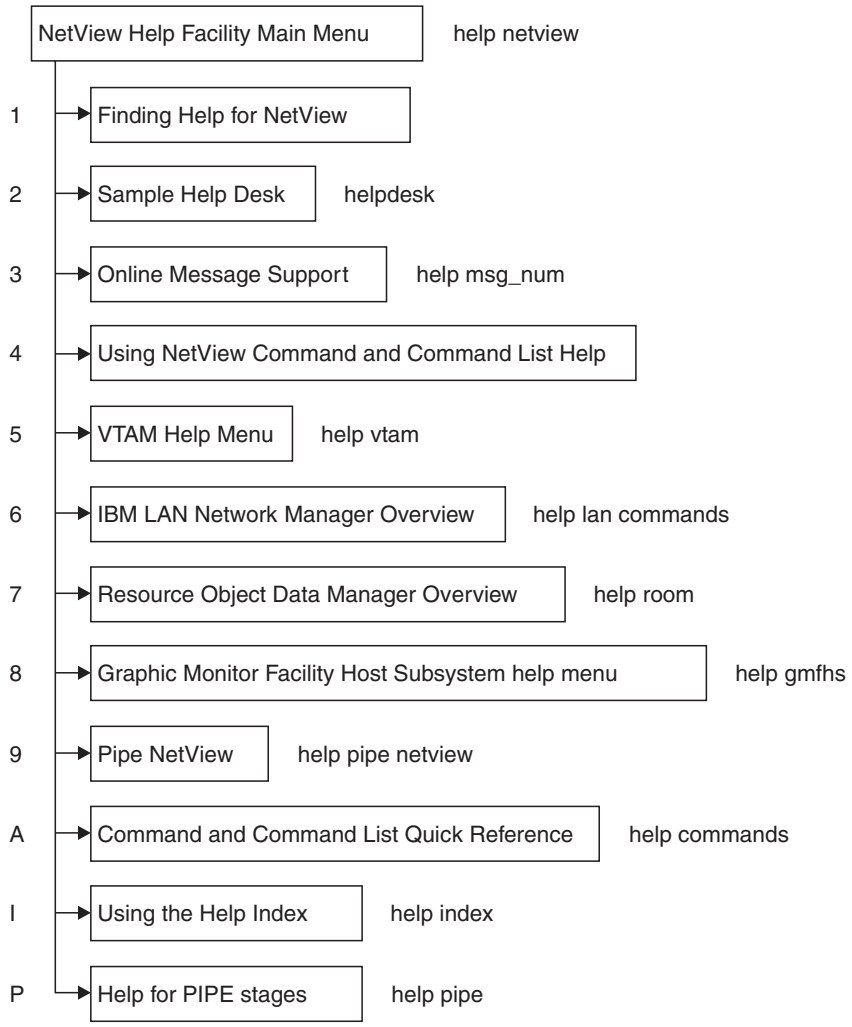


Figure 211. Help Panel Hierarchy

Using Default Hierarchies

In general, you can also use the default hierarchies which are applicable for most commands and components:

- HELP COMMANDS
- HELP command
- HELP message_id
- HELP component
- HELP component COMMANDS
- HELP component command

Using the Hardware Monitor Panels

Many hardware resources in a network send information and error records to the host system. The hardware monitor collects this information and arranges and displays the data to help you with problem determination.

Navigating the Hardware Monitor Panel Hierarchy

Figure 212 shows the general relationship of the hardware monitor panels. You can usually arrive at a specific panel in several ways. You can move down the hierarchy of panels, or you can use an explicit hardware monitor command, as shown in the left column in Figure 212, to go directly to the information you need.

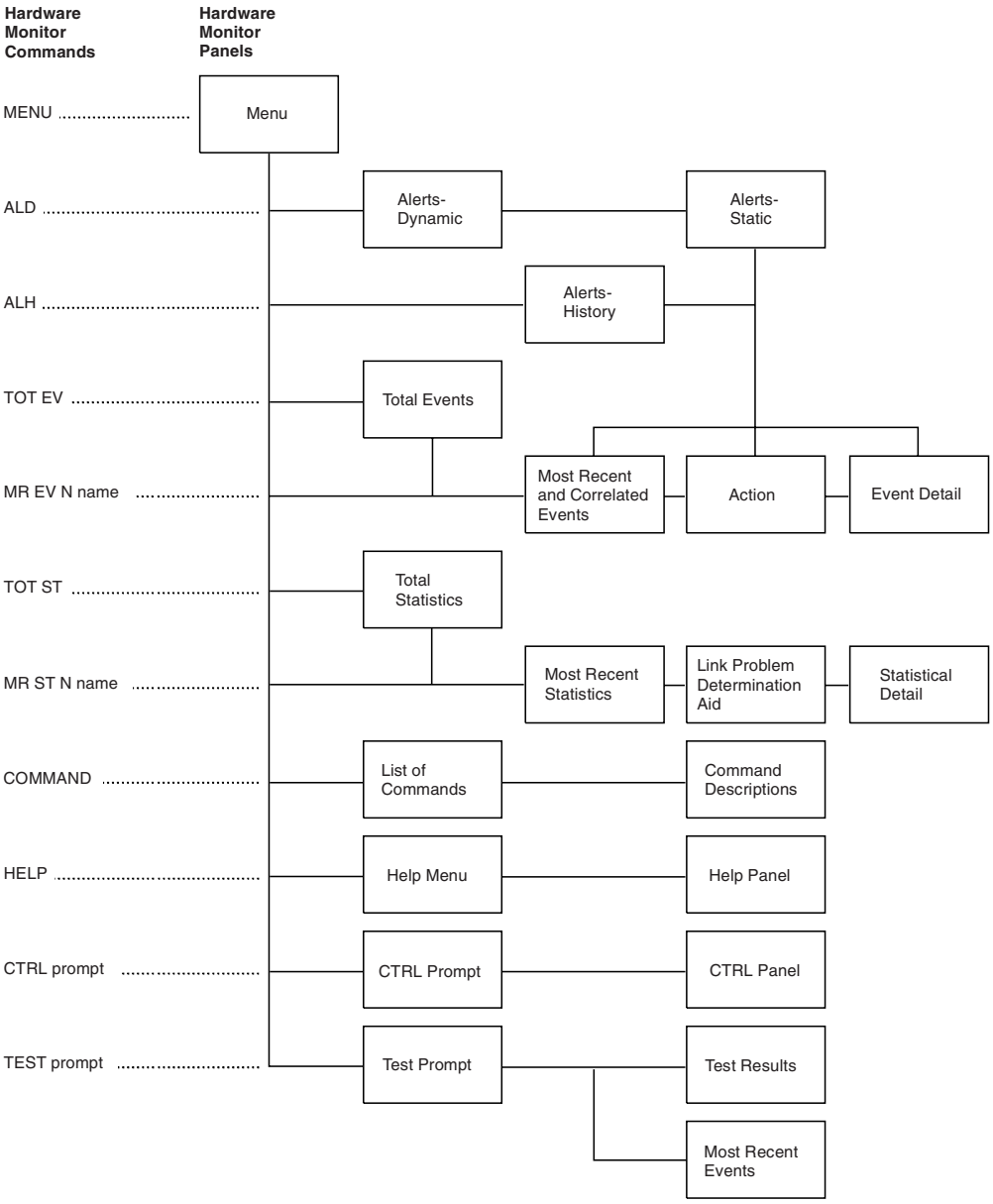


Figure 212. Hardware Monitor Panel Hierarchy

The panels in Figure 212 are described in the following list:

Menu Panel
Provides a selection of different hardware monitor functions and shows database initialization dates. This panel also indicates with which domain you are in session and the domain to which you are attached.

Alerts-Dynamic Panel
Provides a continuously updated single page of alerts retrieved from the

database, presented in reverse chronological order. A C in column 80 indicates that there might be correlated records for the listed resource.

Alerts-Static Panel
Similar to the dynamic panel, but can hold alerts (take a "snapshot" of the Alerts-Dynamic panel) so you can continue to work on problems. From this panel, you can also enter a problem in the Information/Management (MVS only) system. See "Creating a Problem Report" on page 334 for additional information. A C in column 80 indicates that correlated records are available for the listed resource. You can enter CE to display the related records.

Alerts-History Panel
Displays all alerts on the database. This can be a multipage panel.

A C in column 80 indicates that correlated records are available for the listed resource. You can enter CE to display the related records. From this panel, you can also enter a problem in the Information/Management system.

The Information/Management system does not support the printing of double-byte character set (DBCS) characters. Unexpected results can occur.

Total Events Panel
Provides summary totals of events about specific resources.

Most Recent and Correlated Events Panel
Provides a listing of the events in the database for a specified resource or correlated resource in reverse chronological order. A C in column 68 indicates that correlated records are available for the listed resource. From this panel, you can also enter a problem in the Information/Management system.

Information/Management does not support the printing of DBCS characters. Unexpected results can occur.

Action Panel
Provides a recommended action to bypass or resolve the event, or the actual action taken to fix a previously reported problem. This can be a multipage panel.

Event Detail Menu Panel
Provides a selection of information panels with different levels of detail.

The Event Detail Menu is available for network management vector transport (NMVT) record types only.

Total Statistics Panel
Displays summary of statistical data about specific resources.

Most Recent Statistics Panel
Provides a reverse chronological listing of the statistics on the database for the specific resource.

Link Problem Determination Aid Panel
Provides a list of tests initiated by the communication controller that provide data circuit-terminating equipment (DCE) status, attached device status, and the overall quality of a communications link.

Statistical Detail Panel
Provides a list of temporary error counter values recorded for physical and virtual links.

List of Commands Panel
Provides details and examples of how to use hardware monitor commands. You can also reach this panel from the hardware monitor HELP menu.

Command Descriptions
Provides individual command descriptions including the format and description of operands, and, where applicable, usage notes, examples, and responses.

Help Menu
Provides access to help for using the hardware monitor.

Help Panel
Provides help for terms and prompts seen on the panels. This panel also provides general information on how to use the panels and the hardware monitor.

CTRL Prompt Panel
Describes the CTRL command and prompts you for a resource name.

CTRL Panel
Provides link test counts, summary error counts, most recent events, and release level information from the SNA controller retrieved as a result of the CTRL command.

Test Prompt Panel
Describes the use of the TEST command and prompts for resource names.

Test Results Panel
Displays the status of the modems or line or both. Also displays the current and transition states of the Electronic Industries Association (EIA) leads for a selected remote station. For the line, analog and digital parameters are listed.

You can request help for any of the fields on NetView panels. To search for an explanation of a term shown on a hardware monitor panel, enter:

```
help npda 'term'
```

Where *term* specifies one or more words on a panel. If you do not specify a component, all component fields are searched.

To leave the panel hierarchy and return to the component you were using before you entered the hardware monitor, enter the NetView END command or press a PF key with that setting. The NetView supplied PF key setting for END is PF2.

Understanding the Hardware Monitor Panel Terminology

To make the best possible use of the hardware monitor, you need to know how the different components in your system or network are connected to each other and to the host controller. You also need to understand how the hardware monitor sees your configuration, because the probable cause terminology used by the hardware monitor might be unfamiliar to you.

Figure 213 on page 348 gives you more information on how the hardware monitor's physical components and levels are related to each other in one typical configuration.

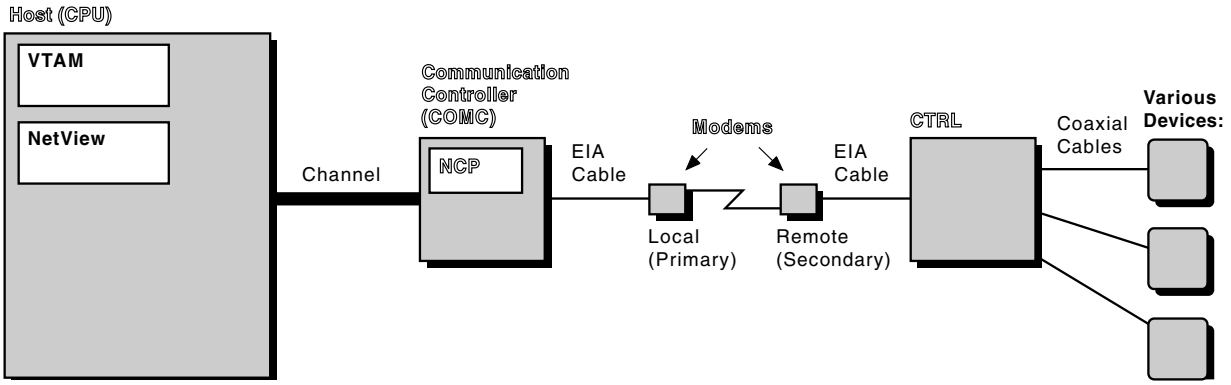


Figure 213. Hardware Monitor Physical Components and Levels

The following abbreviations are associated with the hardware monitor:

COMC
Communication controller, such as 3704, 3705, 3720, 3725, or 3745

CPU Central processing unit, the processor, the host computer

LINE The communication path between the COMC and CTRL, including the local and remote modems

CTRL The cluster controller on the remote end of the line, such as a 3174, 3274, 3276, 8100, or 3777

DEV The terminal connected to the cluster controller, such as a 3278, or 8775

CHAN
Channel—the path between the host processor and a channel-attached device

LCTL A cluster controller attached to the processor by the channel

LDEV A device attached to a channel-attached cluster controller

Table 27. Symbolic Names for Locally Attached Devices

Type	Name	Description
CPU	CPU (SSSSS)	For processor devices (such as 3090™)
CPU	$LOCAL	For the 43X1 loop adapter and the 3274 MDL 1A
CHAN	CH (XX)	For channels (such as 2860) running in an MVS environment
LCTL	LCTL (XXYZ)	For local SNA display controllers (such as 3274 MDL 1A)
LCTL	LCTL (XXY)	For local non-SNA display controllers (such as 3272)
LCTL	LCTL (User-defined)	For local display controllers (such as 3274)
TCU	TAPE (XXY)	For tape controllers (such as 3803)
SCU	DASD (XXY)	For DASD storage controllers (such as 3830)
IOCU	ICOU (XXY)	For printer controllers
LDEV	LDEV (XXYZ)	For local non-SNA display devices (such as 3277)
(NNNN)	TDEV (XXYZ)	For tape devices (such as 3420)
(NNNN)	DDEV (XXYZ)	For DASD devices (such as 3350)
(NNNN)	IODV (XXYZ)	For printer devices

This table uses the characters XX, Y, and Z to describe the first, second, third, and fourth hexadecimal characters, respectively, of the channel unit address.

XX Represents either a channel number or a channel path ID.

XXY Represents a controller on a channel.

XXYZ Represents a device on a controller. These characters might also represent a controller when the device cannot be addressed.

NNNN
Is the numerical IBM machine type designator expressed in decimal.

SSSSS
Is the resource serial number expressed in decimal.

Resource names and types, all leading or embedded blanks, all characters below X'40', and characters with a value of X'FF' are converted to an underscore (_). Names and types consisting of all blanks are converted to all underscores.

Using the Session Monitor Panels

The session monitor collects and correlates data about Systems Network Architecture (SNA) sessions (subarea and Advanced Peer-to-Peer Networking). The session monitor also helps identify network problems and conditions that might cause errors. Some examples of this are failing or unresponsive terminals, lost path information units (PIUs), buffer errors, and resource status errors.

The session monitor collects data about same-domain, cross-domain, and cross-network SNA sessions (subarea and Advanced Peer-to-Peer Networking), and maintains the collected data on a session basis. The SNA sessions can involve non-SNA terminals supported by the Network Terminal Option (NTO). These NTO sessions look like normal SNA sessions to the host. The session monitor also collects data about data flows for certain non-SNA terminals that are not supported by NTO. To collect data for cross-domain sessions, a session monitor must be available in each domain. To collect data for cross-network sessions, a session monitor must be available in each gateway host on the session path and at the session end points. To collect data for SNA Advanced Peer-to-Peer Networking sessions, a session monitor must be available at the interchange node.

Navigating the Session Monitor Panel Hierarchy

Figure 214 on page 350 shows the general relationship of the session monitor panels. You can usually arrive at a specific panel in several ways. You can move down the hierarchy of panels, or you can use an explicit session monitor command, as shown in the left column in Figure 214, to go directly to the information you need.

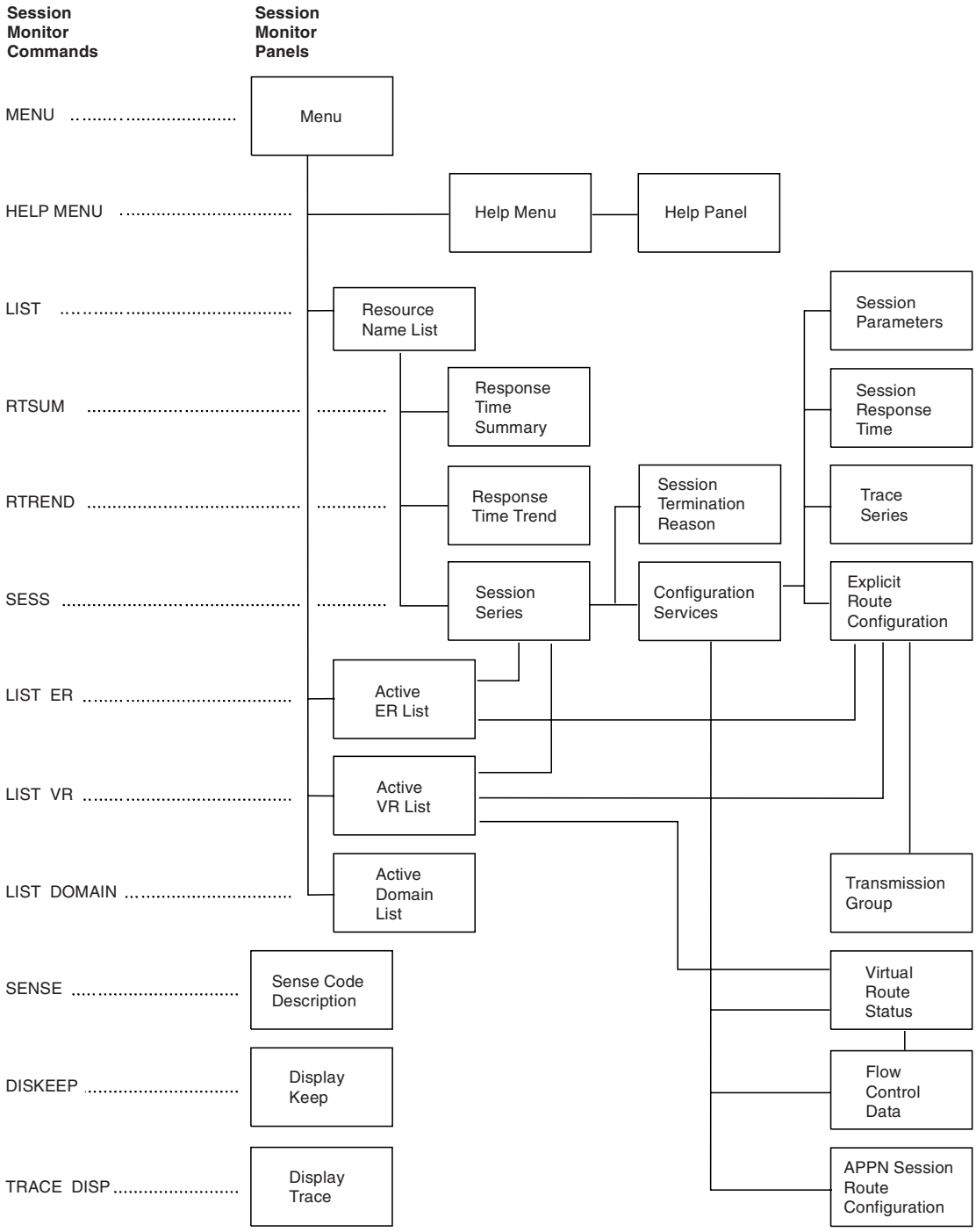


Figure 214. Session Monitor Panel Hierarchy

The panels in Figure 214 are described in the following list:

Menu Panel
Provides for the selection of the resource list type, list of domains, active explicit routes (ERs), or active virtual routes (VRs) for which you want information.

Help Menu
Lists and describes the session monitor commands for which online help is available.

Help Panel
Describes the syntax of the command selected from the previous help panel.

Resource Name List Panel
Displays a list of resources for which data is available. From this panel, you can view the Response Time Summary, Response Time Trend, or Session Series panels.

Response Time Summary Panel
Is a series of graphs showing the percentage of transactions in each response time range for a specified period of time. Graphing is done for a specific logical unit in a given domain. This series of graphs can be a multipage panel. The various performance classes have different pages.

Response Time Trend Panel
Is a graph for a specific terminal logical unit that shows the percentage of transactions with response times that are less than a specified maximum objective for each data collection period. You can specify a maximum, or your system programmer can set up the limits. The objective is displayed on the panel.

Session Series Panel
Shows a list of sessions for the resources you name on the command. From this panel, you can view session configuration data, start a session connectivity test for an active session, or display the reason code and sense code for an inactive session.

Session Termination Reason Panel
Presents in detail a description of the reason codes and sense codes associated with UNBIND, BIND failures or INIT failures. These reason codes and sense codes are displayed only for LU-LU sessions.

Configuration Services Panel
Shows the local network configuration for a selected session. You can shift the panel to the left or right to view adjacent network configurations using the NetView LEFT and RIGHT commands, or PF keys with those settings. The NetView supplied session monitor PF key setting for LEFT is PF10, and for RIGHT is PF11. From this panel, you can display trace information, session parameters, explicit route information, session response time, active virtual route status, Advanced Peer-to-Peer Networking route data, and flow control data.

The INIT failure configuration panel shows the configuration of SSCPs that attempted to establish the selected failed session.

Note: This function depends on the session monitor being fully functional in each SSCP that attempted to establish the session.

Session Parameters Panels
Display the session parameters for a given session. You can have the information interpreted or displayed in hexadecimal.

Session Response Time Panel
Is a graph of the percentage of transactions in each response time range for each data collection period of a session. Each data collection period is a separate page, beginning with the earliest period. To display the most recent period, enter the BOTTOM command.

Trace Series Panel
Provides trace data for the type of trace you requested on the previous

panel. Whether you get a formatted or unformatted list depends on the trace you requested and whether you have HEX set on or off.

Explicit Route Configuration Panel
Provides a configuration for an explicit route. Explicit route information includes the translation of subarea PU addresses into network names, wherever possible. From this panel, you can select a panel to view transmission group detail information.

Active ER List Panel
Lists the active explicit routes for which data is available. From this panel, you can display a list of sessions using a specific explicit route or display the configuration of the explicit route.

Active VR List Panel
Lists the active virtual routes for which data is available. From this panel, you can display the virtual route status, display a list of sessions, or display the configuration of the virtual route.

Active Domain List Panel
Lists other known domains. This panel also shows the status of sessions that have been started to each of these domains.

Transmission Group Panel
Displays a list of all the SSCPs that have activated links on either side of the selected transmission group. If SSCP names are not available, their subarea addresses are displayed in EBCDIC.

Virtual Route Status Panel
Lists the virtual route status data from the virtual route end points. From this panel, you can display flow control data.

Flow Control Data Panel
Displays primary or secondary stage data, or both, for a TG ending in either an NCP or VTAM.

APPN Session Route Configuration Panel
Displays the route configuration through the SNA Advanced Peer-to-Peer Networking networks. You can shift the panel for more data in the primary or secondary directions by issuing PAR or SAR, respectively.

Sense Code Description Panel
Presents in detail a description for sense codes.

Display Keep Panel
Lists the PIU KEEP counts that have been set for a specific network name or for a name pair, or the DASD session keep counts for the global keep count or for a specific name pair.

Display Trace Panel
Lists the specific resource names that have been activated or deactivated for tracing with the TRACE command. The first resource listed (GLOBAL) reflects the setting of the TRACE ALL function. If global trace is ON, you can use TRACE STOP to deactivate the trace for all sessions with the specified resource. The session monitor lists the specific network names that have been deactivated. If global trace is OFF, you can use the TRACE START to activate the trace for all sessions with the specified resource. The session monitor lists the specific resource names that have been activated.

For an online explanation of a panel, enter:

```
help nldm.panelname
```

Where *panelname* is the name of the panel, found in the upper left corner of each session monitor panel. For example, to receive help for the main menu, enter:

```
help nldm.menu
```

For an explanation of the fields shown on the panels, enter:

```
help nldm 'term'
```

Where *term* specifies one or more words on a panel. You can request help for any of the terms on the panels.

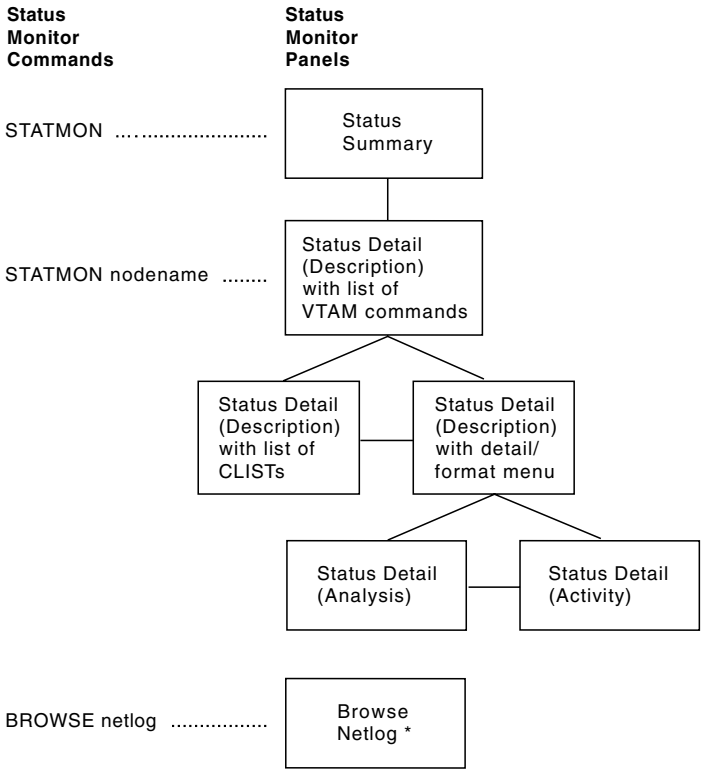
To leave the panel hierarchy and return to the component you were using before you entered the session monitor, enter the NetView END command or press a PF key with that setting. The NetView supplied PF key setting for END is PF2.

Using the Status Monitor Panels

The status monitor collects and summarizes information on the status of resources defined in a VTAM domain. The status monitor can automatically restart failing network resources and monitor important NetView messages.

Navigating the Status Monitor Panel Hierarchy

Figure 215 shows the general relationship of the status monitor panels. You can usually arrive at a specific panel in several ways. You can move down the hierarchy of panels, or you can use an explicit status monitor command, as shown in the left column in Figure 215, to go directly to the information you need.



* This panel is also accessible from any of the other status monitor panels

Figure 215. Status Monitor Panel Hierarchy

The panels in Figure 215 on page 353 are described in the following list:

Status Summary Panel
When you access this panel by typing `statmon`, this panel displays every type of major and minor resource (node) within your domain. For each resource type, this panel displays the total resource count and the number of resources that fall into each of the status monitor's interpretation of VTAM states.

When you access this panel from the Status Detail panel that contains the detail/format menu (by selecting a resource and `SUMMARY` from the `DISPLAY: HIGHER NODE` option), this panel displays, for the specified resource type, the total resource count and the number of resources that fall into the status monitor's interpretation of VTAM states.

Status Detail Panels
By selecting any total in the Domain Status Summary, you can display the Domain Status Detail panel for that resource type. For example, if you select LINES, the Domain Status Detail panel displays all of the lines for the domain identified in the header section.

Initially, the Domain Status Detail panel is presented in description format with a list of available VTAM commands that can be applied to the listed resources. In this format, each listed resource is followed by a description of the resource. You can press the following keys to toggle to a different format:

SCLIST
Displays the command lists that you can run against one or more of the displayed resources. The NetView supplied status monitor PF key setting for SCLIST is PF11.

SMENU
Displays activity and analysis information for the selected resources displayed on the status monitor screen. The analysis format summarizes the status of each displayed node over a period of time. The activity format, available only for application programs and application program major nodes, summarizes the message traffic to and from the listed application programs or terminal LUs.

From the detail/format menu you can also select a resource and `DETAIL` from the `DISPLAY: THIS NODE` option to display information for that specific resource. At this point, the status monitor panels display information only for that resource.

Network Log Panel
By selecting one of the message indicators at the top of a status monitor panel you can look at messages that are written to the active network log. Depending on the indicator you selected, the messages are highlighted in different colors. You can also look at the network log by entering `browse netlog`*x* where *x* is either `a` for the active log, `i` for the inactive log, `p` for the primary log or `s` for the secondary log. :edl

To leave the panel hierarchy and return to the component you were using before you entered the status monitor, enter the NetView END command or press a PF key with that setting. The NetView supplied PF key setting for END is PF2.

Using the RODMView Panels

Use RODMView to simplify the process of adding, deleting, changing, and querying fields and data in RODM.

Navigating the RODMView Panel Hierarchy

Figure 216 shows the general relationship of the RODMView panels. The main panel is the starting point for all subsequent panels. Each RODMView panel has a corresponding Help panel, accessed by pressing PF1. From each Help panel, you can access the Keys Help panel, which describes how to use the RODMView-specific PF keys. Unlike NetView PF keys, RODMView PF keys cannot be changed interactively, nor displayed with DISPFK. From any RODMView panel, use PF keys PF14 through PF22 to display the RODMView input panels as shown in Figure 216.

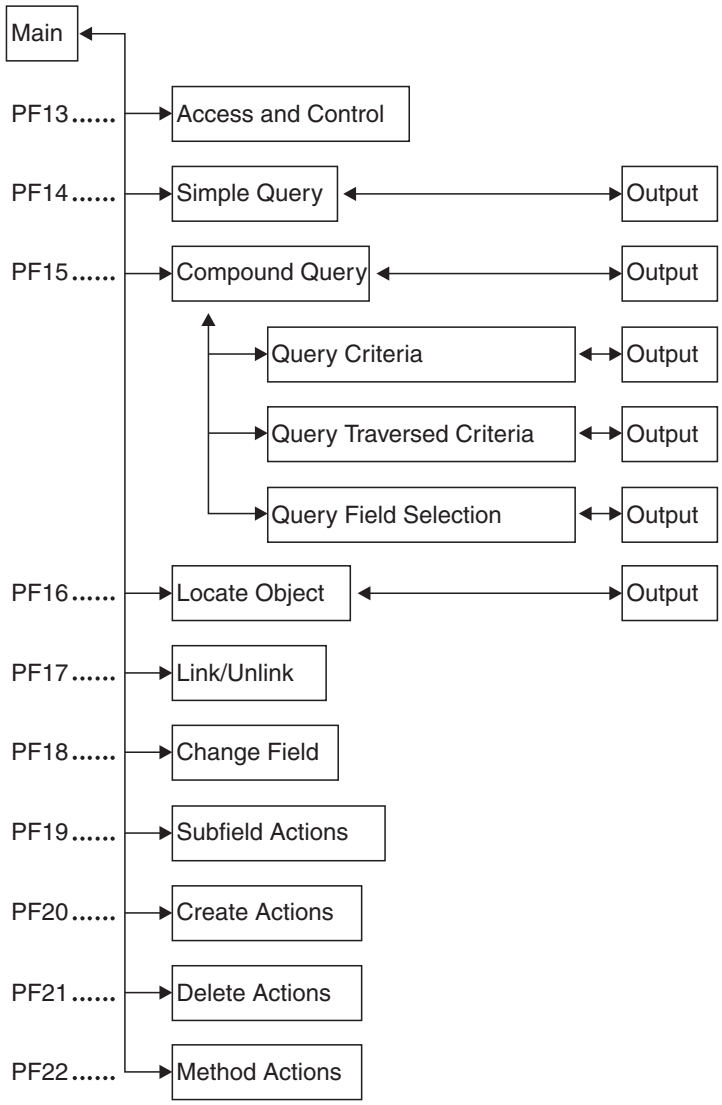


Figure 216. RODMView Panel Hierarchy

For a description of the panels in Figure 216, refer to *IBM Tivoli NetView for z/OS Resource Object Data Manager and GMFHS Programmer's Guide*.

You can get function equivalent to the RODMView panels through the NetView EKGV commands. The EKGV commands do not display the RODMView panels. For a list and descriptions of the RODMView commands, refer to the NetView online help.

Appendix C. Interpreting Session Data

You can use the session monitor to provide information about sessions and resources in pure SNA subarea, pure SNA Advanced Peer-to-Peer Networking, or mixed networks. This section provides scenarios that show:

- Typical SNA subarea and SNA Advanced Peer-to-Peer Networking configurations and the network management data available at the session monitor in each of the network nodes
- The session monitor data resulting from taking over or giving back one or more endpoints in a session

For additional information on defining SNA Advanced Peer-to-Peer Networking session configurations, refer to the *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components* .

Sessions-Data Availability Scenarios

In the SNA Advanced Peer-to-Peer Networking environment, a VTAM interchange node and the NCP it owns are viewed logically as a single SNA Advanced Peer-to-Peer Networking node (referred to as a composite network node), allowing them to interact with other SNA Advanced Peer-to-Peer Networking nodes. At the same time, they continue to provide subarea support. Using Session PD support, the user can view both SNA Advanced Peer-to-Peer Networking and SNA subarea information for a single session. The session configuration and the placement of the session monitor in the session path determines the amount of data available locally to the user. For optimal session PD, the user should be at an interchange node. Here, both SNA Advanced Peer-to-Peer Networking and SNA subarea data is available locally.

The following scenarios represent some of the configurations you can set up. These scenarios show examples of how SNA subarea and SNA Advanced Peer-to-Peer Networking nodes can be connected together and the network management data that is available in these different combinations. In each of the configurations, all CPs are VTAM V4R1 with NetView V2R4 or later.

SNA Session

The configuration shown in Figure 217 on page 358 is composed of an LU-LU session in a pure SNA subarea network. An SSCP-SSCP session exists between SSCP1 and SSCP2.

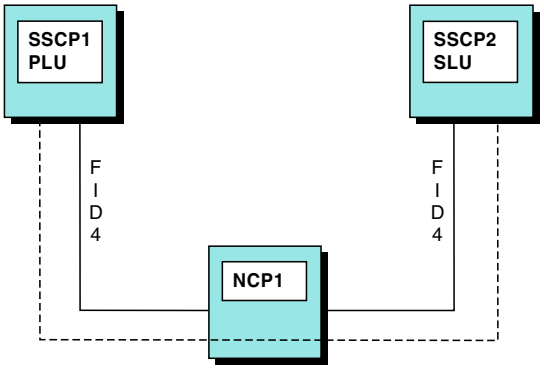


Figure 217. SNA Session

Node	Available data
SSCP1	• Session awareness (SAW) data • Subarea route data (explicit route and virtual route)
SSCP2	• SAW data • Subarea route data (explicit route and virtual route)

SNA Advanced Peer-to-Peer Networking Session through a Composite Node

The configuration shown in Figure 218 is composed of an LU-LU session going through a composite node. This configuration contains two NCP subarea nodes. CP-CP sessions exist between CP1-CP2 and CP2-CP3.

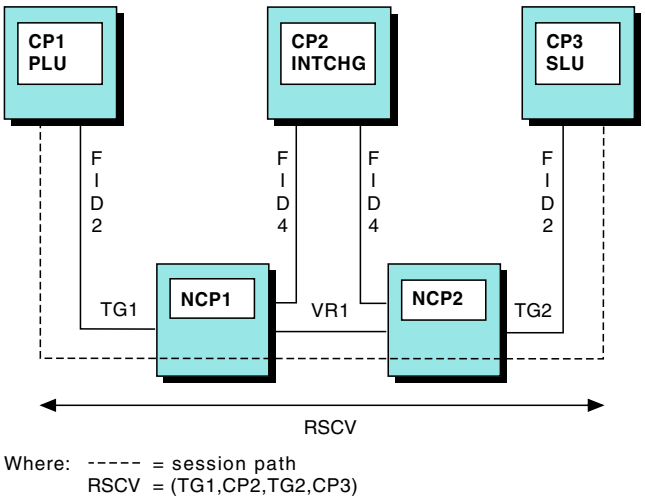


Figure 218. SNA Advanced Peer-to-Peer Networking Sessions through Composite Nodes

Node	Available data
CP1	• Session awareness (SAW) data, including the Route Selection Control Vector (RSCV) for the session • Complete Advanced Peer-to-Peer Networking Session Route Configuration (built from the RSCV) from the Session Configuration display • Flow control data for TG1 in the secondary direction • Subarea route data (by issuing a Set Domain to CP2)
CP2	• SAW data, including Virtual Route (VR) information • Complete Advanced Peer-to-Peer Networking Session Route Configuration (built from the RSCV) from the Session Configuration display • Origin flow control data (data for TG1 in the primary direction) by soliciting NCP1 • Destination flow control data (data for TG2 in the secondary direction) by soliciting NCP2
CP3	• SAW data, including the RSCV for the session • Complete Advanced Peer-to-Peer Networking Session Route Configuration (built from the RSCV) from the Session Configuration display • Flow control data for TG2 in the primary direction • Subarea route data (by issuing a Set Domain to CP2)

SNA Advanced Peer-to-Peer Networking Session through Non-Adjacent Composite Nodes

The configuration shown in Figure 219 consists of a single network with multiple non-adjacent composite nodes. The network has multiple VRs: an internal VR for NCP1 and another VR between NCP2 and NCP3.

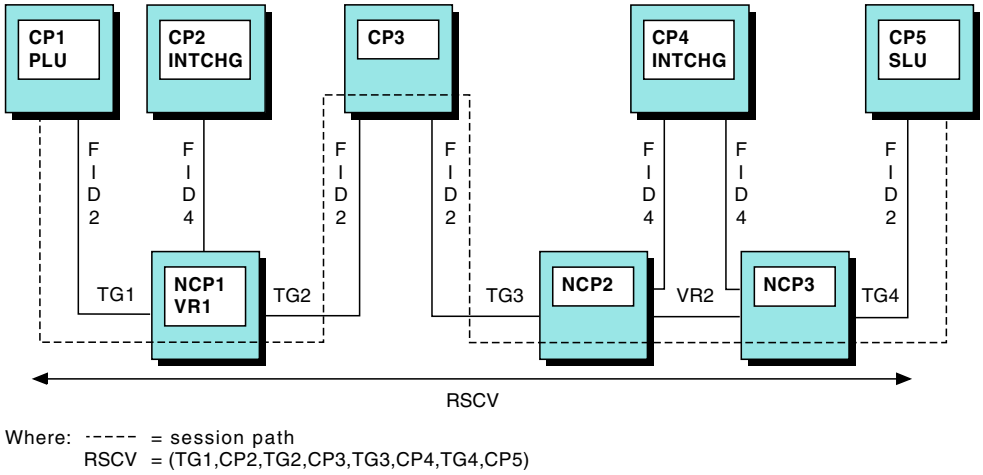


Figure 219. SNA Advanced Peer-to-Peer Networking Session through Nonadjacent Composite Nodes

Node	Available data
CP1	• Session awareness (SAW) data, including the Route Selection Control Vector (RSCV) for the session • Complete Advanced Peer-to-Peer Networking Session Route Configuration (built from the RSCV) from the Session Configuration display • Flow control data for TG1 in the secondary direction • Subarea route data (by issuing a Set Domain to CP2 or to CP4)
CP2	• SAW data, including Virtual Route (VR) information for VR1 • Complete Advanced Peer-to-Peer Networking Session Route Configuration (built from the RSCV) from the Session Configuration display • Origin flow control data (data for TG1 in the primary direction) by soliciting NCP1 • Destination flow control data (data for TG2 in the secondary direction) by soliciting NCP1
CP3	• Session awareness (SAW) data, including the Route Selection Control Vector (RSCV) for the session • Complete Advanced Peer-to-Peer Networking Session Route Configuration (built from the RSCV) from the Session Configuration display • Origin flow control data (data for TG2 in the primary direction) by soliciting NCP2 • Destination flow control data (data for TG3 in the secondary direction) by soliciting NCP3
CP4	• SAW data, including Virtual Route (VR) information for VR2 • Complete Advanced Peer-to-Peer Networking Session Route Configuration (built from the RSCV) from the Session Configuration display • Origin flow control data (data for TG3 in the primary direction) by soliciting NCP2 • Destination flow control data (data for TG4 in the secondary direction) by soliciting NCP3
CP5	• SAW data, including the RSCV for the session • Complete Advanced Peer-to-Peer Networking Session Route Configuration (built from the RSCV) from the Session Configuration display • Flow control data for TG4 in the primary direction • Subarea route data (by issuing a Set Domain to CP4 or to CP2)

SNA Advanced Peer-to-Peer Networking Session through Adjacent Composite Nodes

The configurations shown in Figure 220 on page 361 and Figure 221 on page 362 consist of a single network with adjacent composite nodes. These nodes can be connected in two ways. Figure 220 on page 361 shows them connected with a Casual Connection (FID2). Figure 221 on page 362 shows them connected with a VR.

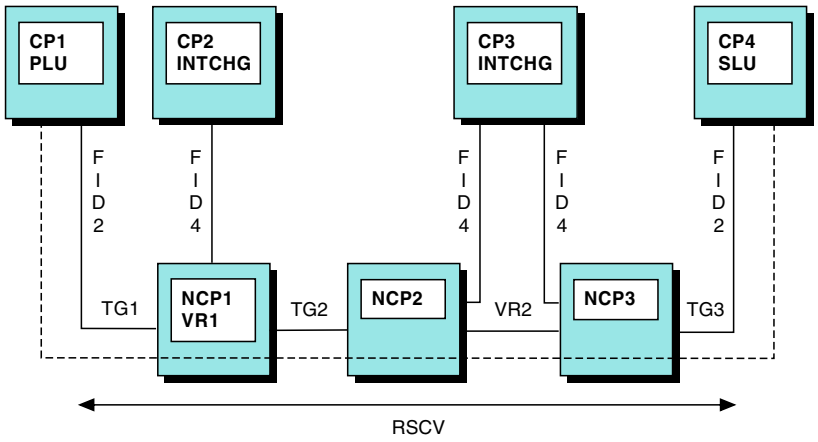


Figure 220. SNA Advanced Peer-to-Peer Networking Session through Adjacent Composite Nodes with FID2 Connection

Table 28 displays the data available with a Casual connection.

Table 28. Data Available for SNA Advanced Peer-to-Peer Networking Session through Adjacent Composite Nodes with Casual Connection

Node	Available data
CP1	• Session awareness (SAW) data, including the Route Selection Control Vector (RSCV) for the session • Complete Advanced Peer-to-Peer Networking Session Route Configuration (built from the RSCV) from the Session Configuration display • Flow control data for TG1 in the secondary direction • Subarea route data (by issuing a Set Domain to CP2 or CP3)
CP2	• SAW data, including Virtual Route (VR) information for VR1 • Complete Advanced Peer-to-Peer Networking Session Route Configuration (built from the RSCV) from the Session Configuration display • Origin flow control data (data for TG1 in the primary direction) by soliciting NCP1 • Destination flow control data (data for TG2 in the secondary direction) by soliciting NCP1
CP3	• SAW data, including Virtual Route (VR) information for VR2 • Complete Advanced Peer-to-Peer Networking Session Route Configuration (built from the RSCV) from the Session Configuration display • Origin flow control data (data for TG2 in the primary direction) by soliciting NCP2 • Destination flow control data (data for TG3 in the secondary direction) by soliciting NCP3
CP4	• SAW data, including the RSCV for the session • Complete Advanced Peer-to-Peer Networking Session Route Configuration (built from the RSCV) from the Session Configuration display • Flow control data for TG3 in the primary direction • Subarea route data (by issuing a Set Domain to CP3 or CP2)

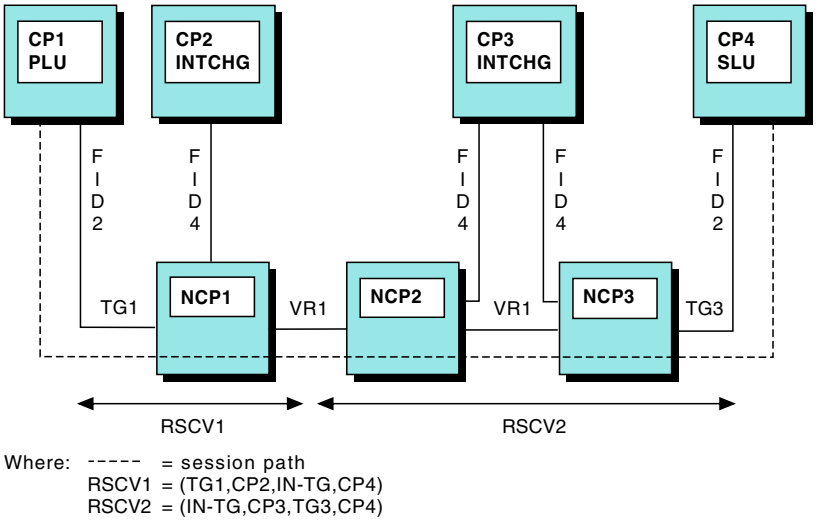


Figure 221. SNA Advanced Peer-to-Peer Networking Session through Adjacent Composite Nodes with VR Connection

Table 29 displays the data available with a VR connection.

Table 29. Data Available with SNA Advanced Peer-to-Peer Networking Session through Adjacent Composite Nodes with a VR Connection

Node	Available data
CP1	• Session awareness (SAW) data, including the local Route Selection Control Vector (RSCV), RSCV1, for the node • Advanced Peer-to-Peer Networking Session Route Configuration (built from the RSCV1) from the Session Configuration display The adjacent RSCV (RSCV2) can be viewed by issuing a SAR command from the session monitor Advanced Peer-to-Peer Networking Session Route Configuration panel • Flow control data for TG1 in the secondary direction • Subarea route data (by issuing a Set Domain to CP2 or CP3)
CP2	• SAW data, including the local RSCV (RSCV1) and Virtual Route (VR) information for VR1 for the node • Advanced Peer-to-Peer Networking Session Route Configuration (built from the RSCV1) from the Session Configuration display RSCV2 data can be viewed by issuing a SAR command from the session monitor Advanced Peer-to-Peer Networking Session Route Configuration panel • Origin flow control data (data for TG1 in the primary direction) by soliciting NCP1
CP3	• SAW data, including the local RSCV (RSCV2) and Virtual Route (VR) information for VR1 for the node • Complete Advanced Peer-to-Peer Networking Session Route Configuration (built from RSCV2) from the Session Configuration display RSCV1 data can be viewed by issuing a PAR command from the session monitor Advanced Peer-to-Peer Networking Session Route Configuration panel • Destination flow control data (data for TG3 in the secondary direction) by soliciting NCP3

Table 29. Data Available with SNA Advanced Peer-to-Peer Networking Session through Adjacent Composite Nodes with a VR Connection (continued)

Node	Available data
CP4	• SAW data, including the local RSCV (RSCV2) for the node • Complete Advanced Peer-to-Peer Networking Session Route Configuration (built from the RSCV2) from the Session Configuration display RSCV1 data can be viewed by issuing a PAR command from the session monitor Advanced Peer-to-Peer Networking Session Route Configuration panel • Flow control data for TG3 in the primary direction • Subarea route data (by issuing a Set Domain to CP3 or CP2)

SNA Advanced Peer-to-Peer Networking Session through a SNI Gateway

The configuration shown in Figure 222 consists of two composite nodes connected through a gateway NCP. This configuration always results in multiple RSCVs.

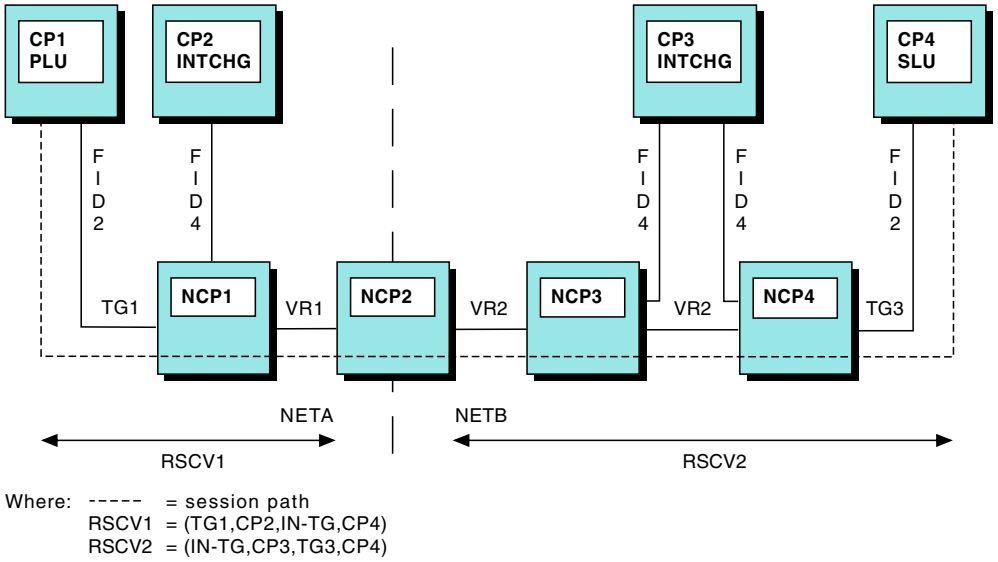


Figure 222. SNA Advanced Peer-to-Peer Networking Session through SNI Gateway

Node	Available data
CP1	• Session awareness (SAW) data, including the RSCV for NETA (RSCV1) for the session • Configuration data for NETA from the SAW data • Configuration data for NETB, including the RSCV for NETB (RSCV2), can be viewed by issuing a RIGHT command from the session monitor Session Configuration Data panel, or by issuing a SAR command from the session monitor Advanced Peer-to-Peer Networking Session Route Configuration panel • Flow control data for TG1 in the secondary direction

Node	Available data
CP2	• SAW data, including the RSCV for NETA (RSCV1) • Configuration data for NETA from the SAW data • Configuration data for NETB, including the RSCV for NETB (RSCV2), can be viewed by issuing a RIGHT command from the session monitor Session Configuration Data panel, or by issuing a SAR command from the session monitor Advanced Peer-to-Peer Networking Session Route Configuration panel • Origin flow control data (data for TG1 in the primary direction) by soliciting NCP1
CP3	• SAW data, including the RSCV for NETB (RSCV2) • Configuration data for NETB from the SAW data • Configuration data for NETA, including the RSCV for NETA (RSCV1), can be viewed by issuing a LEFT command from the session monitor Session Configuration Data panel, or by issuing a PAR command from the session monitor Advanced Peer-to-Peer Networking Session Route Configuration panel • Destination flow control data (data for TG3 in the secondary direction) by soliciting NCP4
CP4	• SAW data, including the RSCV for NETB (RSCV2) • Configuration data for NETB from the SAW data • Configuration data for NETA, including the RSCV for NETA (RSCV1), can be viewed by issuing a LEFT command from the session monitor Session Configuration Data panel, or by issuing a PAR command from the session monitor Advanced Peer-to-Peer Networking Session Route Configuration panel • Flow control data for TG3 in the primary direction

Session between 2 SNA Advanced Peer-to-Peer Networking Subnetworks with a LEN Connection

The configuration shown in Figure 223 on page 365 consists of 2 SNA Advanced Peer-to-Peer Networking subnetworks joined with a LEN connection. This type of connection results in multiple RSCVs for the session.

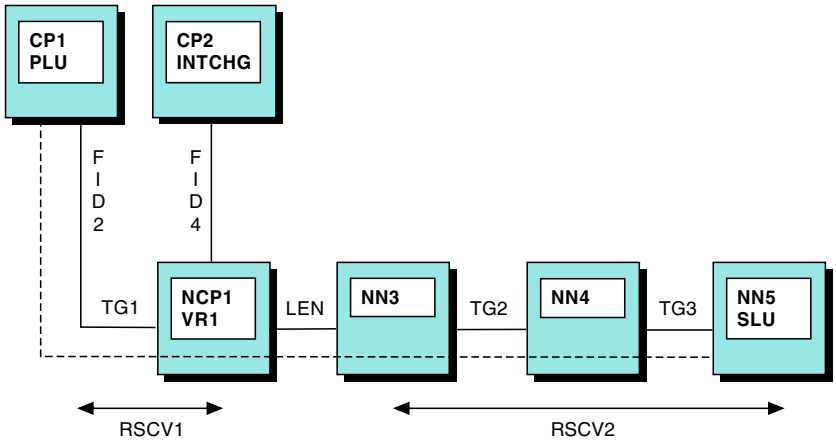


Figure 223. Session between 2 SNA Advanced Peer-to-Peer Networking Subnetworks through a LEN Connection

Node	Available data
CP1	• Session awareness (SAW) data, including the Route Selection Control Vector (RSCV1) for the first subnetwork for the session • Advanced Peer-to-Peer Networking Session Route Configuration (built from RSCV1) The RSCV for the second subnetwork (RSCV2) can be viewed by issuing a SAR command from the session monitor Advanced Peer-to-Peer Networking Session Route Configuration panel • Flow control data for TG1 in the secondary direction • Subarea route data (by issuing a Set Domain to CP2)
CP2	• SAW data, including Virtual Route (VR) information • RSCV1 • RSCV2, including the name for its primary end (NN3), along with an indicator to identify it as a LEN RSCV • Complete Advanced Peer-to-Peer Networking Session Route Configuration (built from RSCV1 and RSCV2) • Flow control data for TG1 in the primary direction

SNA Session through an Advanced Peer-to-Peer Networking Network

The configuration shown in Figure 224 on page 366 illustrates a session using a DLUS-DLUR pipe to cross an Advanced Peer-to-Peer Networking network.

The Advanced Peer-to-Peer Networking network consists of two network nodes, and is indicated by the RSCV designation. The pipe is established and controlled by the DLUS (dependent LU server) and DLUR (dependent LU requestor) functions.

SSCP-LU (**1**) and SSCP-PU (**2**) sessions exist between the VTAM (CP1) and the LU and PU that it owns. The LU is also the SLU in an SLU-PLU session (**3**) with an application in CP2.

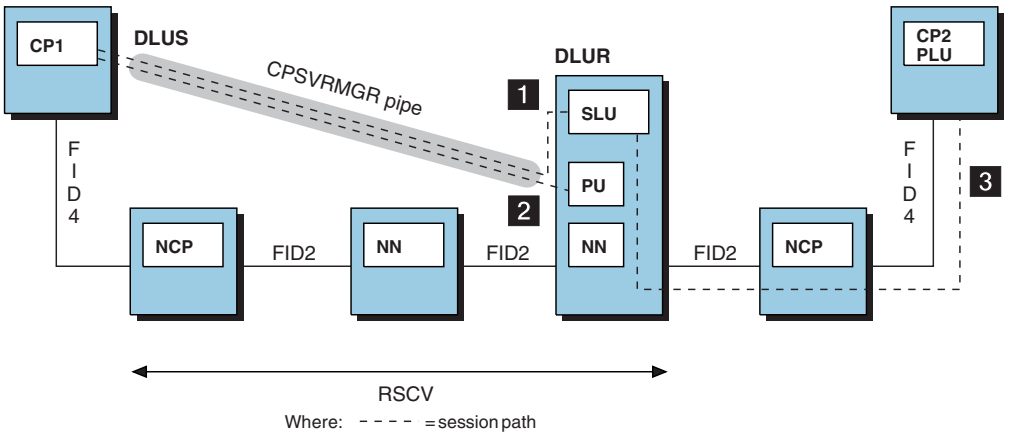


Figure 224. SNA Session through an Advanced Peer-to-Peer Networking Network

Node	Available data
CP1	• Session awareness (SAW) data for all sessions, including the LU 6.2 session pipe between the DLUS and DLUR • Complete Advanced Peer-to-Peer Networking Session Route Configuration for the two LU-LU sessions between the DLUS and DLUR, and the application LU to dependent LU session (3)
CP2	• SAW data for the SLU-PLU session (3) • Complete Advanced Peer-to-Peer Networking Session Route Configuration for the SLU-PLU session (3)

SSCP Takeover/Giveback Scenarios

The following four scenarios of SSCP Takeover/Giveback are processed:

- In the first scenario, the session monitor receives awareness that one endpoint of the session has been given up, while local awareness of the other endpoint is not available in the current domain. Another local VTAM takes over the connection to the endpoint that was given up.
- In the second scenario, the session monitor receives awareness that both endpoints of the session have been given up. Another local VTAM takes over the connection to both endpoints in a session.
- In the third and fourth scenarios, one endpoint of a session has been given up, while local awareness of the other endpoint is still available in the current domain.

Note that VTAM sends takeover and giveback notifications to the session monitor when they occur, at which time the takeover and giveback indicators can be seen on the session monitor panels. However, each time the session monitor restarts and requests SAW data for currently active sessions, VTAM no longer knows if these active sessions were previously involved in takeovers or givebacks. Therefore, the session monitor at that time has no takeover or giveback knowledge for any active sessions (even if it knew about a given session before the session monitor was restarted).

The following sample configurations illustrate these scenarios. For each one, the data available to the NetView operator is described.

SSCP Takeover/Giveback of NCP BF Connection - Scenario 1

In the configuration shown in Figure 225, an LU-LU session exists between LUA and LUB, where CP2 is the owner of the NCP BF connection to the adjacent link station ALS2. When the session is started, session monitor in CP1 and CP2 receives SAW data for the session. When CP2 loses ownership of the connection to ALS2, CP3 takes over the connection.

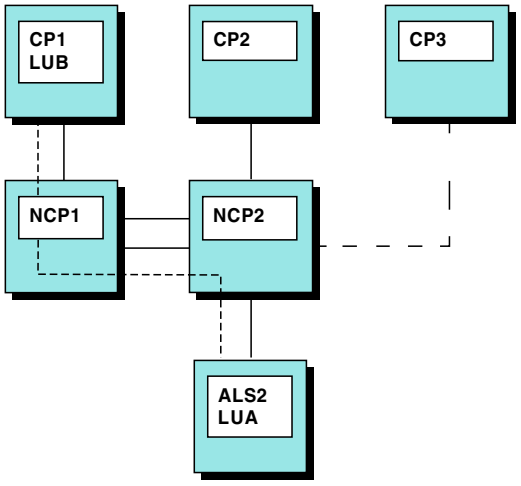


Figure 225. SSCP Takeover/Giveback of NCP BF Connection - Scenario 1

Table 30 shows the data available before and after CP3 takes over the connection to ALS2.

Table 30. Data Comparisons for Takeover/Giveback Scenario 1

Node	Initial State	After Giveback	After Takeover
CP1	Session monitor receives SAW data for the session.	No change.	No change. Session monitor still thinks CP2 owns the connection to ALS2.
CP2	Session monitor receives SAW data for the session.	• If the line between the NCPs is PUTYPE=4, the session is displayed on the session monitor session list with an end time (the time when CP2 lost its awareness of the session) and with a GIVEBACK indicator. • If the line between the NCPs is PUTYPE=2, the session is displayed on the session monitor session list as ACTIVE and with a GIVEBACK indicator. • The resource names are displayed with a GBK (giveback) indicator.	No change.

Table 30. Data Comparisons for Takeover/Giveback Scenario 1 (continued)

Node	Initial State	After Giveback	After Takeover
CP3	Session monitor is not aware of the session.	The session monitor has no awareness of the session. It becomes aware of the session after the session is taken over.	• The session is displayed on the session monitor session list as ACTIVE and with a TAKEOVER indicator. • The resource names are displayed with a TOV (takeover) indicator. • Because of the limited data received in the takeover notification, some Session PD route functions can be limited.

SSCP Takeover/Giveback of NCP BF Connection - Scenario 2

In the configuration shown in Figure 226, an LU-LU session exists between LUC and LUD, where CP1 is the owner of the NCP BF connection to the adjacent link stations ALS1 and ALS2. The connection can be either an SNA Advanced Peer-to-Peer Networking connection or a LEN connection. When the session is started, session monitor in CP1 receives SAW data for the session. When CP1 loses ownership of the connection to ALS1 and ALS2, CP2 takes over that connection.

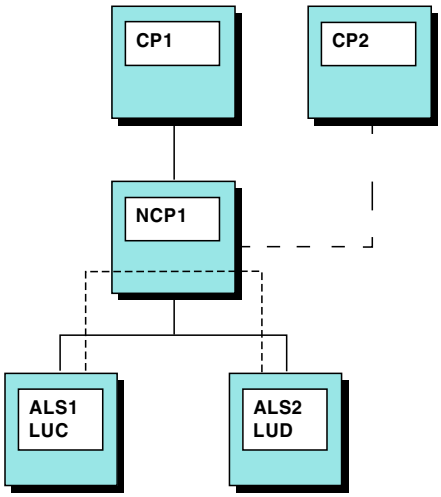


Figure 226. SSCP Takeover/Giveback of NCP BF Connection - Scenario 2

Table 31 shows the data available before and after CP2 takes over the connection to ALS1 and ALS2.

Table 31. Data Comparison for Takeover/Giveback Scenario 2

Node	Initial State	After Giveback of both links	After Takeover of both links
CP1	Session monitor receives SAW data for the session.	• The session is displayed on the session monitor session list with an end time and with a GIVEBACK indicator. • The resource names are displayed with a GBK (giveback) indicator.	No change.

Table 31. Data Comparison for Takeover/Giveback Scenario 2 (continued)

Node	Initial State	After Giveback of both links	After Takeover of both links
CP2	Session monitor is not aware of the session.	Session monitor is not aware of the session. It becomes aware of the session after the session is taken over.	• The session is displayed on the session monitor session list as ACTIVE and with a TAKEOVER indicator. • The resource names are displayed with a TOV (takeover) indicator. • Because of the limited data received in the takeover notification, some Session PD route functions can be limited.

SSCP Takeover/Giveback of NCP BF Connection - Scenario 3

In the configuration shown in Figure 227, an LU-LU session exists between LUA and LUB, where CP1 is the owner of the NCP BF connection to the adjacent link station ALS1. When the session is started, session monitor in CP1 receives SAW data for the session. When CP1 loses ownership of the connection to ALS1, CP2 takes over that connection.

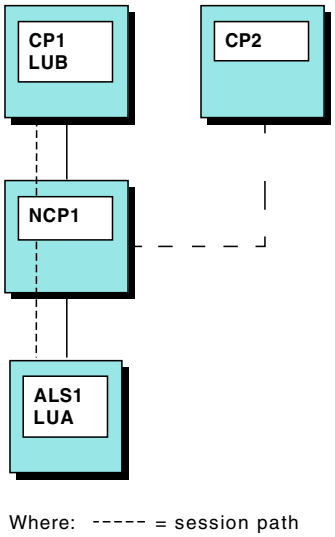


Figure 227. SSCP Takeover/Giveback of NCP BF Connection - Scenario 3

Table 32 shows the data available before and after CP2 takes over the connection to ALS1.

Table 32. Data Comparison for Takeover/Giveback Scenario 3

Node	Initial State	After Giveback	After Takeover
CP1	Session monitor receives SAW data for the session.	• The session is displayed on the session monitor session list as ACTIVE and with a GIVEBACK indicator • The resource names are displayed with a GBK (giveback) indicator.	No change.

Table 32. Data Comparison for Takeover/Giveback Scenario 3 (continued)

Node	Initial State	After Giveback	After Takeover
CP2	Session monitor is not aware of the session.	Session monitor is not aware of the session. It becomes aware of the session after the session is taken over.	• The session is displayed on the session monitor session list as ACTIVE and with a TAKEOVER indicator. • The resource names are displayed with a TOV (takeover) indicator. • Because of the limited data received in the takeover notification, some Session PD route functions can be limited.

SSCP Takeover/Giveback of NCP BF Connection - Scenario 4

In the configuration shown in Figure 228, an LU-LU session exists between LUA and LUB, where CP1 is the owner of the NCP BF connection to the adjacent link station ALS1. In contrast to the previous scenario, LUB is located at CP2. When the session is started, session monitor in CP1 receives SAW data for the session. When CP1 loses ownership of the connection to ALS1, CP2 takes over that connection.

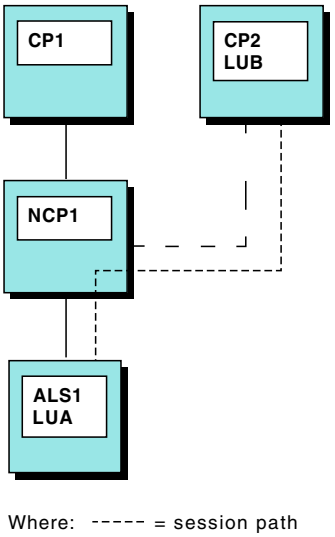


Figure 228. SSCP Takeover/Giveback of NCP BF Connection - Scenario 4

Table 33 shows the data available before and after CP2 takes over the connection to ALS1.

Table 33. Data Comparison for Takeover/Giveback Scenario 4

Node	Initial State	After Giveback	After Takeover
CP1	Session monitor receives SAW data for the session.	• The session is displayed on the session monitor session list with an end time and with a GIVEBACK indicator. • The resource names are displayed with a GBK (giveback) indicator.	No change.

Table 33. Data Comparison for Takeover/Giveback Scenario 4 (continued)

Node	Initial State	After Giveback	After Takeover
CP2	Session monitor receives SAW data for the session.	No change. Session monitor has SAW data for the session.	• The session is displayed on the session monitor session list as ACTIVE and with a TAKEOVER indicator. • The resource names are displayed with a TOV (takeover) indicator. • Because of the limited data received in the takeover notification, some Session PD route functions can be limited.

Appendix D. Using the NetView Library

The NetView library includes these publications, grouped by task.

Note: Most of the publications are also available on the Web at http://www.ibm.com/software/tivoli/products/netview-zos/.

Table 34. The IBM Tivoli NetView for z/OS Library

Automation	• *IBM Tivoli NetView for z/OS Automation Guide*
Customization	• *IBM Tivoli NetView for z/OS Automated Operations Network Customization Guide* • *IBM Tivoli NetView for z/OS Customization Guide* • *IBM Tivoli NetView for z/OS Programming: Assembler* • *IBM Tivoli NetView for z/OS Programming: Pipes* • *IBM Tivoli NetView for z/OS Programming: PL/I and C* • *IBM Tivoli NetView for z/OS Programming: REXX and the NetView Command List Language*
Diagnosis	• *IBM Tivoli NetView for z/OS Troubleshooting Guide*
Training	• *Introducing Tivoli NetView for OS/390: A Tutorial for Network Operators* (available from Version 1, Release 4 only) Publication number: SK2T-6097-03 • *Introducing Tivoli NetView for OS/390: A Tutorial for System Programmers* (available from Version 1, Release 4 only) Publication number: SK2T-6097-03
Installation and Administration	• *IBM Tivoli NetView for z/OS Administration Reference* • *IBM Tivoli NetView for z/OS Installation: Getting Started* • *IBM Tivoli NetView for z/OS Installation: Migration Guide* • *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components* • *IBM Tivoli NetView for z/OS Installation: Configuring Graphical Components* • *IBM Tivoli NetView for z/OS Tuning Guide*
Operation	• *IBM Tivoli NetView for z/OS Automated Operations Network User's Guide* • *IBM Tivoli NetView for z/OS NetView Management Console User's Guide* • *IBM Tivoli NetView for z/OS SNA Topology Manager Implementation Guide* • *IBM Tivoli NetView for z/OS User's Guide* • *Tivoli NetView for OS/390 Bridge Implementation* (available from Version 1, Release 4 only) Publication number: SC31-8238-03 *IBM Tivoli NetView for z/OS Web Application User's Guide*
Programming	• *IBM Tivoli NetView for z/OS Application Programmer's Guide* • *IBM Tivoli NetView for z/OS Resource Object Data Manager and GMFHS Programmer's Guide*

Table 34. The IBM Tivoli NetView for z/OS Library (continued)

Reference	• *IBM Tivoli NetView for z/OS Command Reference Volume 1* • *IBM Tivoli NetView for z/OS Data Model Reference* • *IBM Tivoli NetView for z/OS Messages and Codes Volume 1 (AAU-DSI)* • *IBM Tivoli NetView for z/OS Messages and Codes Volume 2 (DUI-IHS)* • *IBM Tivoli NetView for z/OS Security Reference*

Finding the Right Information

See Table 35 for information about the contents of each book. Table 35 lists NetView tasks and the publication where you can find the information about that task:

Table 35. Finding the Information That Can Help with Your Task

If your task is...	Use this book...
To change or add resource definitions.	*IBM Tivoli NetView for z/OS Administration Reference*
To write applications that send network management vector transports, formatted alerts to the NetView program, send buffers to other applications, or develop applications for the program-to-program interface	*IBM Tivoli NetView for z/OS Application Programmer's Guide*
To automate your system operations and networks	• *IBM Tivoli NetView for z/OS Automation Guide* • *IBM Tivoli NetView for z/OS Automated Operations Network User's Guide*
To send transactions between the NetView program and a database that is in another address space	*Tivoli NetView for OS/390 Bridge Implementation* (available from Version 1, Release 4 only) Publication number: SC31-8238-03
To see information about NetView commands, their syntax diagrams, and attributes	*IBM Tivoli NetView for z/OS Command Reference Volume 1*
To customize the NetView program	*IBM Tivoli NetView for z/OS Customization Guide*
To tailor NetView for unique requirements or design, write, and install programs in assembler	*IBM Tivoli NetView for z/OS Programming: Assembler*
To write installation exit routines, command lists, command processors, and subtasks using PIPEs in a REXX, PL/I, or C environment	*IBM Tivoli NetView for z/OS Programming: Pipes*
To write installation exit routines, command processors, and subtasks using PL/I, and C	*IBM Tivoli NetView for z/OS Programming: PL/I and C*
To write simple and advanced command lists that simplify network operator tasks	*IBM Tivoli NetView for z/OS Programming: REXX and the NetView Command List Language*
To get information about data models for topology manager, RODM, and MultiSystem Manager	*IBM Tivoli NetView for z/OS Data Model Reference*

Table 35. Finding the Information That Can Help with Your Task (continued)

If your task is...	Use this book...
To identify, classify, and report problems to IBM Software Support	*IBM Tivoli NetView for z/OS Troubleshooting Guide*
To install and prepare NetView for operation	*IBM Tivoli NetView for z/OS Installation: Getting Started*
To use, customize, and operate MultiSystem Manager	*IBM Tivoli NetView for z/OS MultiSystem Manager User's Guide*
To use the NetView management console to monitor and control networks	*IBM Tivoli NetView for z/OS NetView Management Console User's Guide*
To read about the new function added to the NetView program in this release	*IBM Tivoli NetView for z/OS Installation: Migration Guide*
To streamline the NetView installation by performing tasks prior to installation and to estimate resources for a NetView installation	*IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*
To define resources to RODM for the NetView Graphic Monitor Facility host subsystem (GMFHS), to automate network operations for resources, to write RODM applications and methods, to create RODM data models, and to define exception views	*IBM Tivoli NetView for z/OS Resource Object Data Manager and GMFHS Programmer's Guide*
Set up NetView security	*IBM Tivoli NetView for z/OS Security Reference*
To use SNA topology manager and CMIP	*IBM Tivoli NetView for z/OS SNA Topology Manager Implementation Guide*
To control and improve NetView performance using tuning values	*IBM Tivoli NetView for z/OS Tuning Guide*
To train novice users	*Introducing IBM Tivoli NetView for z/OS*
To monitor and control, investigate and solve problems, and automate networks and systems	*IBM Tivoli NetView for z/OS User's Guide*

Because the formerly separate Automated Operations Network/MVS and MultiSystem Manager MVS/ESA™ products have been merged with IBM Tivoli NetView for z/OS, the information for these products has been merged with the NetView library. The following table contains the type of information and the information unit where it now resides.

Table 36. Information Map for MultiSystem Manager and Automated Operations Network Components

Information Type	AON	MSM	Location
Control file entries, focal-point services, reporting, message processing, and file control manager interface	X		*IBM Tivoli NetView for z/OS Administration Reference*
Getting started, using and implementing SNA, LAN, and TCP/IP automation	X		*IBM Tivoli NetView for z/OS Automation Guide*

Table 36. Information Map for MultiSystem Manager and Automated Operations Network Components (continued)

Information Type	AON	MSM	Location
DDF design, DDF statements, DDF commands, implementing DDF, customized procedures, command processors, common routines, user exits, VTAM messages, SNBU modem configurations, control file manager, extending TCP/IP, and definition tables	X		*IBM Tivoli NetView for z/OS Automated Operations Network Customization Guide*
Getting started (SNA and TCP/IP), using and setting timers, maintaining tasks and logs, cross-domain functions, automation, getting network status, displaying resources with AutoView, displaying VTAM commands, peer-to-peer networking, processing X.25 protocols, browsing data, tailoring the NetView program, NetView component hierarchies, command synonyms and fastpath reference, operator interface, querying databases, deleting objects, issuing commands, managing VTAM options, and solving problems with the help desk	X		*IBM Tivoli NetView for z/OS Automated Operations Network User's Guide*
AON/SNA, AON/TCP, and MultiSystem Manager commands	X	X	*IBM Tivoli NetView for z/OS Command Reference Volume 1*
Initialization and recovery	X		*IBM Tivoli NetView for z/OS Troubleshooting Guide*
Planning and requirements, tailoring the NetView program, gateways, and focal points, defining AON, testing installations, verifying installation and components, and implementing the SNA component	X	X	• *IBM Tivoli NetView for z/OS Installation: Getting Started* • *IBM Tivoli NetView for z/OS Installation: Migration Guide* • *IBM Tivoli NetView for z/OS Installation: Configuring Graphical Components* • *IBM Tivoli NetView for z/OS Installation: Configuring Additional Components*
All messages	X	X	• *IBM Tivoli NetView for z/OS Messages and Codes Volume 1 (AAU-DSI)* • *IBM Tivoli NetView for z/OS Messages and Codes Volume 2 (DUI-IHS)*

Table 36. Information Map for MultiSystem Manager and Automated Operations Network Components (continued)

Information Type	AON	MSM	Location
Getting started, using and customizing, operation of agents and MultiSystem Manager, managing alerts, using global variables, using agents, solving problems, and samples		X	*IBM Tivoli NetView for z/OS MultiSystem Manager User's Guide*
Workstation interface overview; installing, using, tailoring, and programming workstation interface; enabling automation in progress (AIP)	X		*IBM Tivoli NetView for z/OS NetView Management Console User's Guide*
Protecting commands	X		*IBM Tivoli NetView for z/OS Security Reference*
Tuning for performance and compiling REXX functions	X		*IBM Tivoli NetView for z/OS Tuning Guide*

NetView Help Information

The NetView program offers online help for both the workstation and the host. NetView help information is designed for users who are unfamiliar with the NetView commands and for users who need help interpreting NetView panels. The Help Desk is also provided to help you solve specific problems.

Host

Table 37 contains help commands that, provide information for NetView components, panels, panel fields, commands, return codes, and so forth.

Host help information is provided online in an indexed format. The following table contains the types of available help and the command for each type:

Table 37. Types of Help Information

To obtain help for...	Enter...
NetView commands	HELP *commands*
NetView components	HELP *component*
NetView commands by component	HELP *component* command
NetView messages	HELP *msgid*
NetView product	HELP NetView
VTAM return codes and feedback codes	RCFB *code, feedback_code*
SNA sense codes	SENSE *sense_code*
VTAM status codes	STATUS *code*
Explicit and virtual route status codes	ERST *code* and VRST *code*
Recommended actions for hardware monitor panels	ACTION *number*
Field descriptions	HELP *component 'field'*
The Help Desk	HELPDESK
Help index	INDEX *letter*

Workstation

Extensive, context-sensitive, workstation help information is provided for the NetView management console. The information provides help for all functions, windows, fields, and buttons. Workstation help offers the following functions:

- A comprehensive hypertext system that you can use to link to more detailed or related information
- A detailed index
- Color graphics
- Search capability
- Print capability

Using Online Help

The NetView program provides online information that includes host help panels and workstation help.

Note: You can also access all of the help panels from the Web application.

Using Host Help

Use Table 38 to obtain help for various NetView components, panels, panel fields, commands, return codes, and so on. While you are viewing a help panel, if the top line contains `Panel 1 of nn`, this indicates that more information is on subsequent panels. You can press the Enter key to continue to the next panel of information. You can also use the NetView VIEW component BACK and FORWARD commands, or PF keys set to those commands, to page backwards and forwards through help panel sequences. The NetView-supplied value for PF7 is BACK, and for PF8 is FORWARD, and the default scroll value is by page. If you enter a number on the command line and use a PF key set to BACK or FORWARD, it scrolls that number of lines.

Navigating in Help Panels

To return to the first help panel that you accessed, use the NetView VIEW component ENTRYPNT command or a PF key set to that command, such as the NetView-supplied value for ENTRYPNT which is PF11. To leave the help facility, enter END or press a PF key set to END, such as PF2.

Table 38. Getting Help

To obtain help for...	Enter...
Action codes from hardware monitor panels	`action code`
Explicit route status codes	`erst code`
The Help Desk	`helpdesk`
The Online Index	`index character`
NetView commands (all)	`help commands`
NetView commands (any)	`help command`
NetView commands by component	`help component commands`
NetView components	`help component`
NetView messages	`help msgid`
NetView product	`help netview`
Panel fields	`help 'term'`

Table 38. Getting Help (continued)

To obtain help for...	Enter...
Panel fields by component	`help component 'term'`
SNA sense codes	`sense sense_code`
Virtual route status codes	`vrst code`
VTAM return codes and feedback codes	`rcfb return_code,feedback_code`
VTAM status codes and status modifiers	`status code`

Summary

When you need information to perform NetView tasks, refer to the following sources:

- The printed library describes how to: plan, install, customize, automate tasks, write application programs, tune, operate, set up security, and diagnose problems.
- The softcopy bookshelf places the NetView library online, provides search capability, and hypertext links.
- Host help, workstation, and message help information is available online, providing help for your current task.
- The NetView library is available online from the IBM Tivoli NetView for z/OS Web site. Point your browser to http://www.ibm.com/software/tivoli/products/netview-zos/.

Appendix E. How Data Is Sent to the NetView for z/OS Program

This appendix describes how data is sent to the NetView for z/OS program.

The NetView program implements a structure that enables open network management. The structure has three parts:

- The *focal point* provides centralized network management support to control functions such as change management and operations control. The NetView program can act as a focal point application.
- The *entry point* is a distributed point of control for all SNA devices that send information to the focal point and receive commands from the focal point. The IBM AS/400 computer and the IBM 3174 establishment controller are two examples of entry point hardware products. An NCP (Network Control Program) application is an example of an entry point software product.
- The *service point* is the distributed point of control for non-SNA resources. A service point is SNA-addressable and can convert SNA information to a format for the attached components. It can also act as a gateway, converting non-SNA information to an SNA format. NetView (AIX), Tivoli NetView Service Point, IBM LAN Network Manager, Service Point Application (SPA) Router, and Remote Operations Support (ROPS) are some examples of service point products that enable NetView to manage non-SNA resources.

Figure 229 on page 382 shows the relationship between the three types of applications.

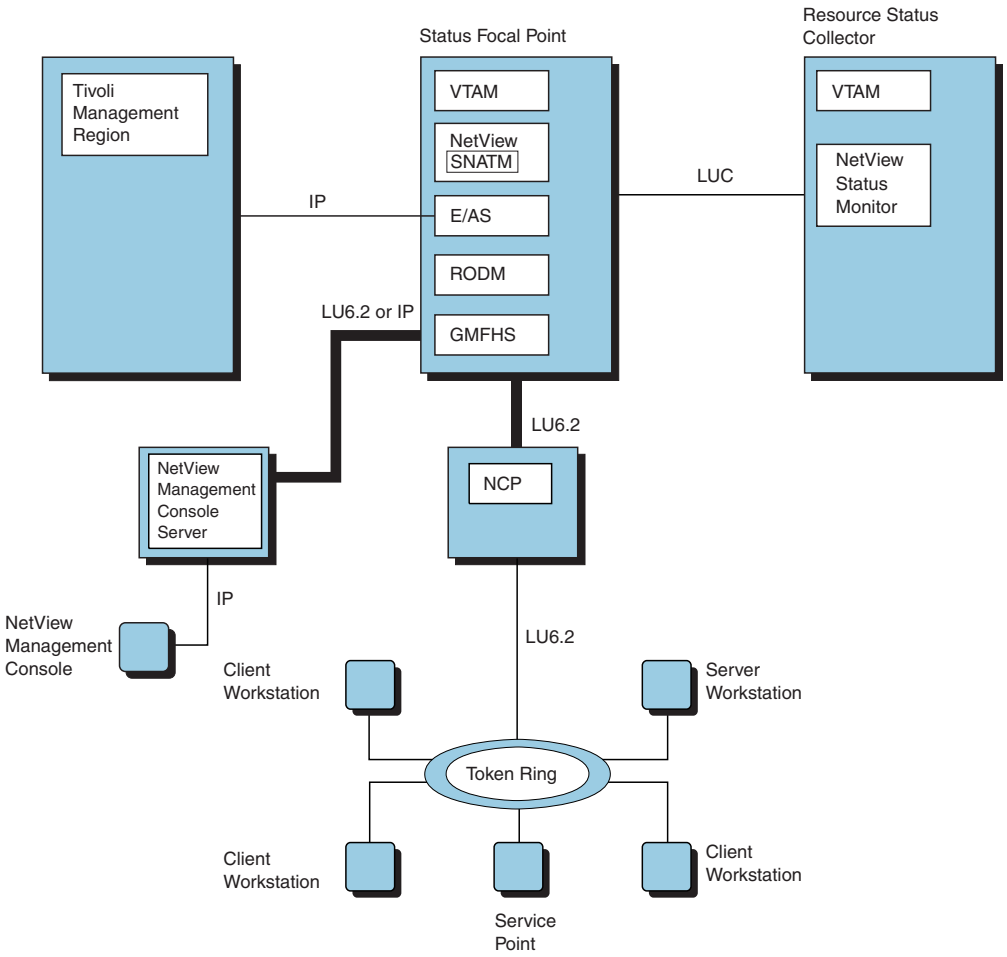


Figure 229. Network Management Structure

In a focal point NetView, data is received from distributed NetView programs. Messages can be filtered out at several levels by NetView or operating system filters, such as PROP on VM, OCCF on VSE, and MPF on MVS. For example, messages can be filtered at the distributed operating system, then at the distributed NetView program, and finally at the focal point NetView program.

Alerts can be filtered using the SVFILTER and SRFILTER commands. In addition, you can use the SRFILTER command to forward alerts to the focal point. See "Alert Forwarding" on page 164 for additional information on forwarding alerts. Refer to the NetView online help for additional information on the SVFILTER and SRFILTER commands.

To help you analyze problems, you need to know how data gets to NetView. Problems are often identified by resources sending events, statistics, or alerts. See Figure 230 on page 383 for some of the command destinations and for some of the sources of events, statistics, alerts, and messages.

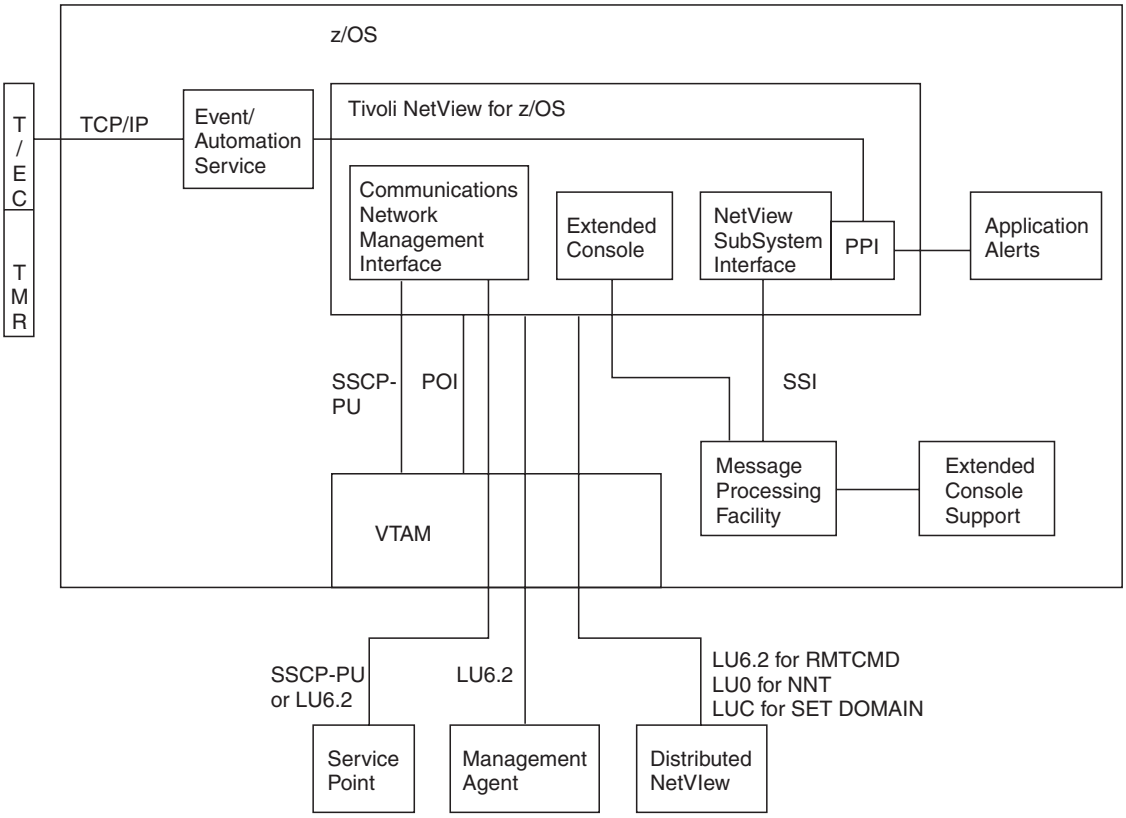


Figure 230. Data Flows to NetView

How Commands and Responses Flow

The NetView operator can issue commands from the NetView program and receive responses. The NetView operator can issue commands to the z/OS operating system, to z/OS subsystems or applications, or to any resource with an IP address. For example, if VTAM is the destination of the NetView operator command, the response to the command flows back to NetView through the VTAM programmed operator interface (POI). NetView receives the response, which it then passes through the NetView automation table.

The NetView program might be the destination of the command. If the destination is the local NetView program, the response passes through the NetView automation table. If the destination is the remote NetView program, the operator uses the RMTCMD command to send the command to the remote NetView program. The response to the command passes through the automation table on the remote NetView program and then through the automation table of the local NetView program.

Service point applications might be the destination of a command. The operator uses the RUNCMD command to send the command to the service point application. NetView receives the response to the command through the CNMI and then passes it through the NetView automation table.

In general, the NetView program passes command response messages (and not, for example, return codes) through the NetView automation table (including responses to commands sent from the MVS console or from a NetView workstation).

How Events, Statistics, and Alerts Flow

The NetView program collects network data. The data comes from both hardware and software and can be grouped into the following categories:

- Events (including SNMP traps, Tivoli Enterprise Console events, common base events, and SNA events)
- Statistics
- Alerts

Events are exception conditions detected by a device about itself or on behalf of a device it controls. Events can be records of permanent errors and other warning and exception conditions. Statistics include information describing the number of transmissions and retransmissions for traffic on a line. An alert is an event that is considered critical and requires operator attention. Whether an event is important enough to be considered an alert can be determined by a filter. This filtering decision is made using criteria set in your installation based on how you want to manage and control your network and what information the operators need to see.

Selected alerts can be forwarded from the hardware monitor through the Event/Automation Service to a Tivoli Enterprise Console in a Tivoli management region.

The Common Event Infrastructure, an IBM component technology, can also be used to manage Common Base Events generated by the NetView program from selected messages and management services units (MSUs). Use the correlation engine to specify criteria which allows messages and MSUs to be routed as you direct. The *IBM Tivoli NetView for z/OS Automation Guide* contains additional information about Common Base Events and using the Common Event Infrastructure for routing data.

How Messages Flow

If the destination for a message is known, the NetView program treats the message as a *solicited message*. The NetView program queues solicited messages to the known destination task. An example of a solicited message is a command response message. If the destination for a message is unknown, the NetView program treats the message as an *unsolicited message*. Unsolicited messages originate in the network or system to notify an operator of a condition or event that might require action. See Figure 230 on page 383 for some of the sources of unsolicited messages.

The z/OS operating system, subsystems, and applications are designed to issue unsolicited messages that are displayed to the z/OS operator. The z/OS message processing facility (MPF) can control whether a system message is displayed to the z/OS operator, made available for NetView automation, written to the system log, or any combination including discarding the message. However, message handling specified in the MPF can be overridden or altered by the NetView message revision table, including availability to NetView automation. In fact, the message revision table can replace the MPF. If the message is available for automation, the NetView program accepts the message from the z/OS operating system and passes it through the NetView automation table, which determines whether automatic processing needs to occur.

Communications Server enables an application to act as a programmed operator using the VTAM programmed operator interface (POI). The NetView program acts as a VTAM programmed operator and, in this role, receives unsolicited messages from the VTAM program.

A NetView task might issue unsolicited messages. If the task resides on the same NetView program that is performing automation, that NetView program passes the messages through the automation table. If the task resides on a remote NetView, the messages pass first through the automation table on the remote NetView program. The messages can then be routed to the local NetView program (such as when the task is started by using the RMTCMD command from the local NetView program) and passed through the automation table of the local NetView program.

Service point applications might generate unsolicited messages that flow on the management session (LU 6.2 or SSCP-PU) to the focal point NetView. The NetView program receives these messages from VTAM using the communications network management interface (CNMI) and then passes them through the NetView automation table.

Selected messages can be forwarded from NetView automation through the Event/Automation Service to a Tivoli Enterprise Console in a Tivoli management region.

For more information about solicited and unsolicited messages, see the *IBM Tivoli NetView for z/OS Automation Guide*.

Appendix F. Using the Tivoli NetView for z/OS Tivoli Enterprise Portal Agent

Use the Tivoli NetView for z/OS Tivoli Enterprise Portal Agent to manage your network from the Tivoli Enterprise Portal using NetView for z/OS take action commands. You can also manage both TCP/IP availability and performance data from the Tivoli Enterprise Portal. The NetView program provides the TCP/IP availability data and OMEGAMON XE for Mainframe Networks V3.1 provides the TCP/IP performance data.

The NetView for z/OS Tivoli Enterprise Portal Agent runs on a Windows or UNIX system or on a Linux system on an IBM System z platform and communicates with the NetView for z/OS program using a socket client program. A NetView autotask initiates the connection to the NetView for z/OS Tivoli Enterprise Portal Agent by issuing the NACMD command either manually or at NetView initialization. The NACMD command is a long-running command processor, which waits for take action commands from the NetView for z/OS Tivoli Enterprise Portal Agent and sends command responses back to the agent. The agent receives the command responses, and upon request, displays the data at the Tivoli Enterprise Portal. Where applicable, the data displayed at the Tivoli Enterprise Portal can include graphs of the data. The STOPNA command stops the socket client program.

AUTONA is the default autotask used for NACMD command processing. You can specify a different autotask on which to run the NACMD by changing this statement in the NetView style sheet or its included members:

```
function.autotask.NAOPER=AUTONA
```

The NetView style sheet and its included members contain all of the values that can be customized for NACMD.

Use the Tivoli Enterprise Portal to interact with your applications and operating system through the take action commands. These take action commands are provided by the NetView for z/OS Tivoli Enterprise Portal Agent:

- Browse NetView Logs (NALBRW)
- View TCP/IP Connection Data (NATCPCON)
- Format Packet Trace (FMTPACKT)
- Purge Packet Trace (PKTS PURGE)
- View Session Data (NASESMG)
- View Session Configuration Data (SESSC)
- View DVIPA Definition and Status (NAEDVPT)
- View DVIPA Sysplex Distributors (NAEDVP1)
- View DVIPA Distributor Targets (NAEDVP2)
- View DVIPA Connections (NAEDVP3)
- Issue NetView Command

Note: The Take Action dialog box shows NANVCMD *command=xxxxxxxx*, where *xxxxxxxx* is the argument value specified by the user in the Edit Argument Values dialog box. The *xxxxxxxx* value is the actual NetView command that is issued. For more information about the take action commands, see the NetView for z/OS Tivoli Enterprise Portal Agent online help.

When you issue a take action command and send it to the NetView program, the command response is displayed in a workspace. The workspace is the working area of the Tivoli Enterprise Portal window, divided into panes to show different types of views. The following workspaces are provided by the NetView for z/OS Tivoli Enterprise Portal Agent:

- DVIPA Connections
- DVIPA Definition and Status
- DVIPA Distributor Targets
- DVIPA Sysplex Distributors
- Formatted Packet Trace
- NetView Audit Log
- NetView Command Response
- NetView Log
- Session Data
- TCPIP Connection Data

For more information about these workspaces, see the NetView for z/OS Tivoli Enterprise Portal Agent online help.

Special Usage Considerations

Each NetView for z/OS workspace has no data initially. A take action command must be issued, and the appropriate workspace refreshed, to view the data.

The NetView Audit Log workspace provides information regarding the NetView take action commands. This workspace displays messages indicating the following conditions:

- The command was received by the NetView program.
- A command response was sent by the NetView program to the NetView for z/OS Tivoli Enterprise Portal Agent.
- The command failed.
- The errors that were encountered issuing the command, such as a syntax error.
- The first line of a command response, for example BNH772I, is received as a result of the NATCPCON command.

Note: Error messages received from commands driven under the Issue NetView Commands, View Session Configuration, and Purge Packet Trace take action items are displayed in the NetView Command Response workspace.

The NetView for z/OS workspaces are displayed in the Tivoli Enterprise Portal under the distributed system on which you installed the NetView for z/OS Tivoli Enterprise Portal Agent

For example, if you installed NetView Tivoli Enterprise Portal Agent on a Windows computer, the Navigator tree looks similar to the following example:

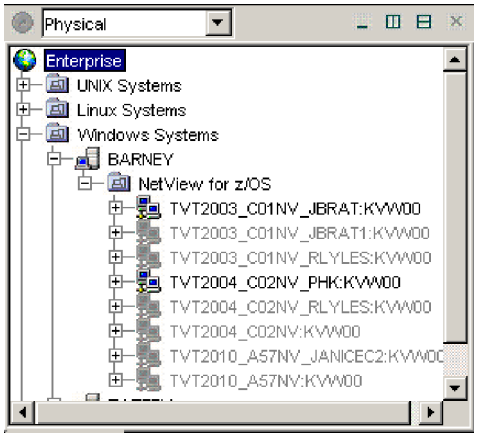


Figure 231. Navigator Tree Example

Each time an NACMD command is issued to a NetView program, the default leaf in the Navigator looks similar to the following example:

```
myhost_CNM01_AUTONA
```

where CNM01 is the NetView domain and AUTONA is the operator ID of the NetView operator who issued the NACMD.

You might choose to issue multiple NACMD commands from one NetView program for the following reasons:

- Commands issued by multiple users against the same workspace can cause unexpected results for a user
- Improved throughput and performance
- Workspace security

If a Tivoli Enterprise Portal user issues a time-consuming NetView for z/OS take action command, the command might time out. A BNH808I message is received in the NetView Audit Log workspace. When the BNH808I message is issued, the command running on the operator task on the NetView host is not stopped. If the BNH808I message persists on subsequent NetView for z/OS take action commands, the operator can wait for the command to finish, or can take the following steps to free up the NetView operator task:

1. Issue the RESET command to stop the command. If this does not work, issue the RESET IMMED command.
2. End the NetView operator task.

Linking to OMEGAMON XE for Mainframe Networks Workspaces

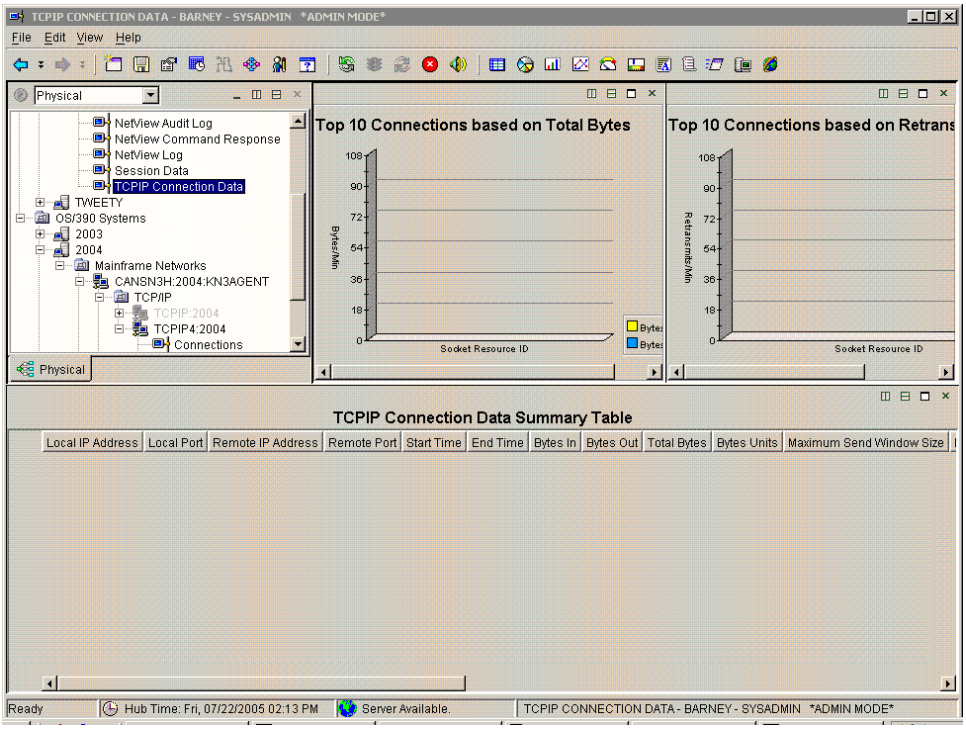
If you have OMEGAMON DE and OMEGAMON XE for Mainframe Networks V3.1 installed, the links between the NetView workspaces and the OMEGAMON XE for Mainframe Networks workspaces are operable. Links are available from the following workspaces:

- The NetView for z/OS TCPIP Connection Data workspace to the OMEGAMON XE for Mainframe Networks TCP Connections Link workspace
- The NetView for z/OS DVIPA Connections workspace to the OMEGAMON XE for Mainframe Networks TCP Connections Link workspace

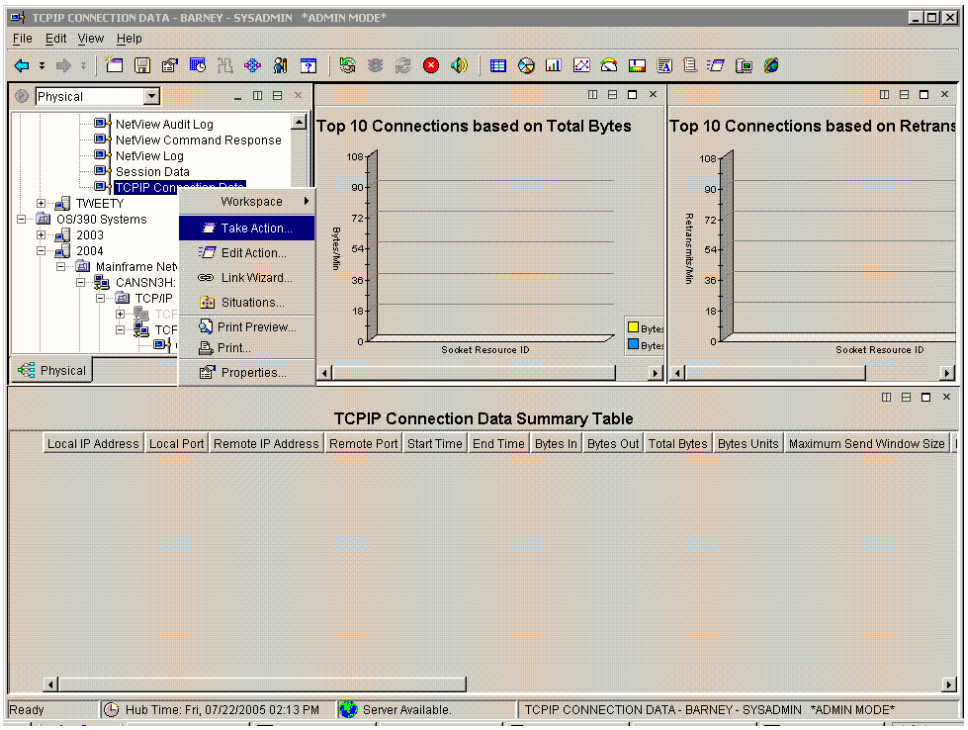
Example: Viewing the TCP/IP Availability Data

Use the following steps to view the TCP/IP availability data:

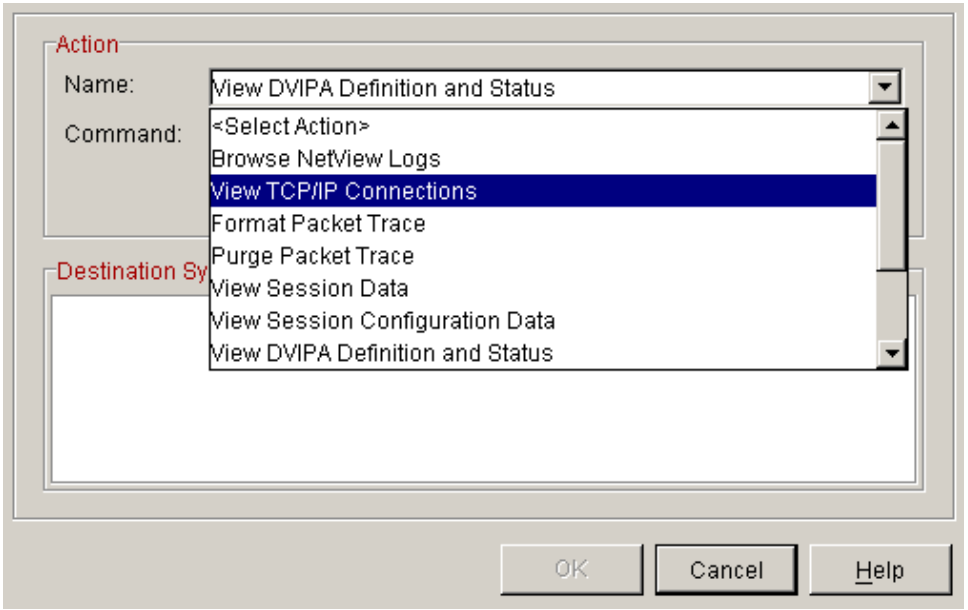
1. Under NetView for z/OS in the Tivoli Enterprise Portal Navigator tree, click the **TCPIP Connection Data** workspace. The workspace is initially empty.



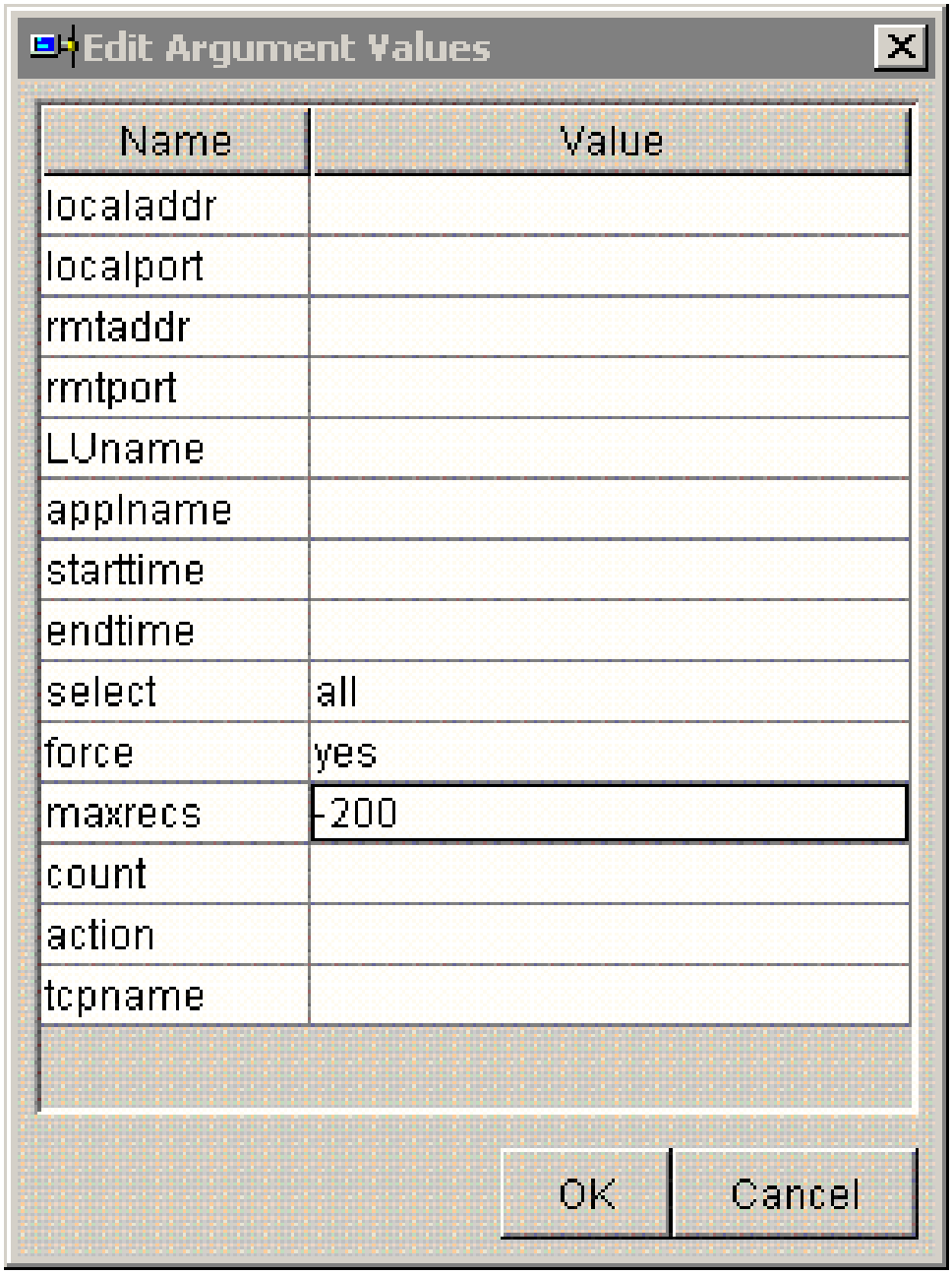
2. Right-click the workspace name.
3. Click **Take Action** in the menu.



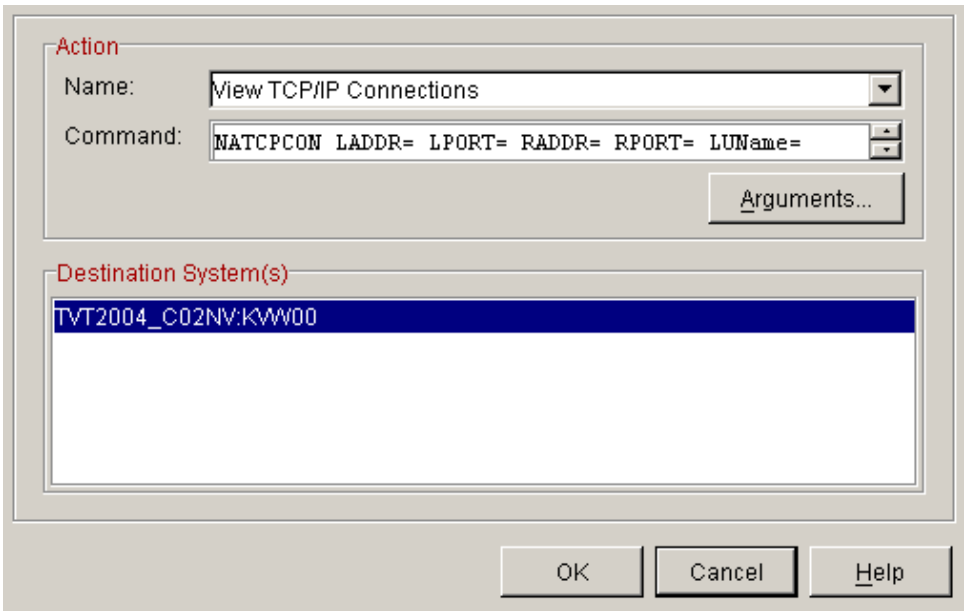
4. Select **View TCP/IP Connections** in the Take Action Command Selection.



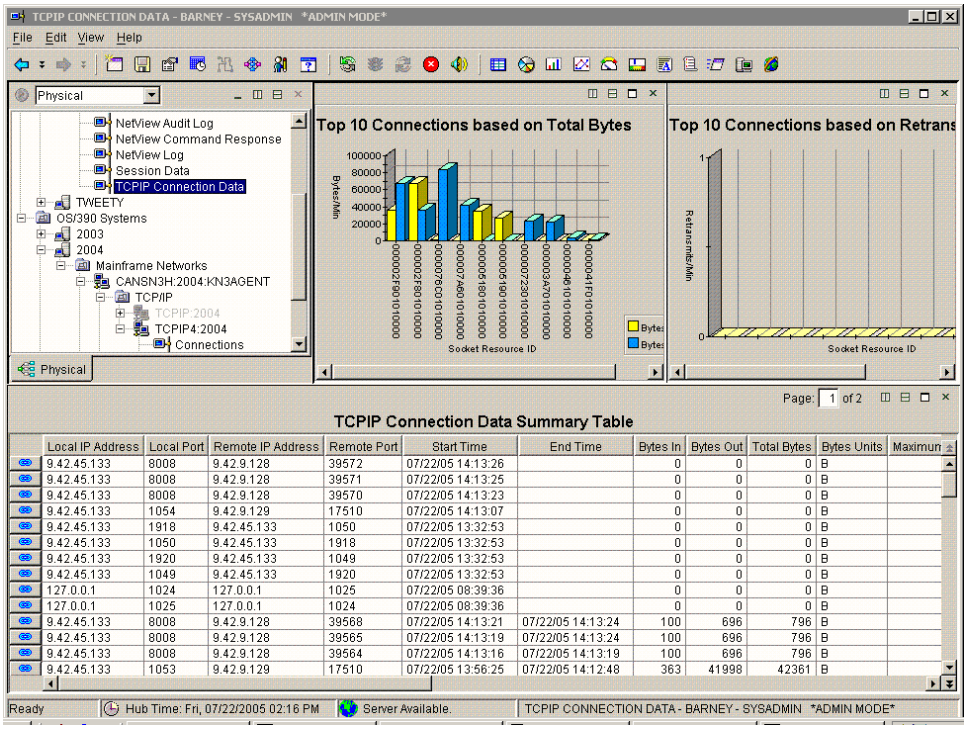
5. Specify argument values for the View TCP/IP Connections (NATCPCON) command.



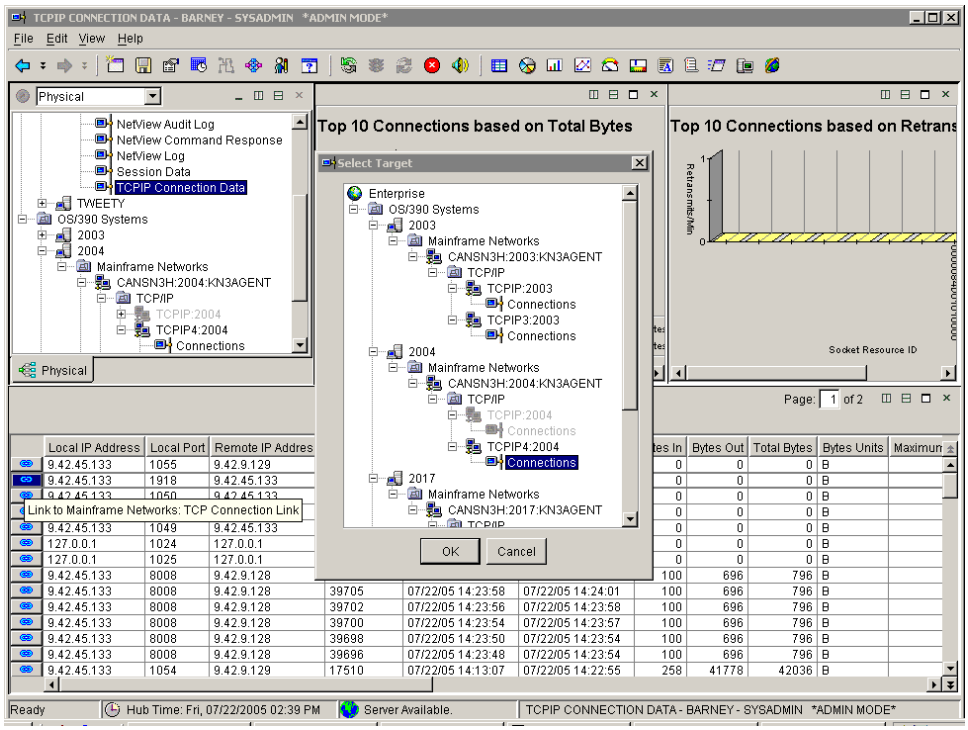
6. Select the NetView system from where you want the command to be run.

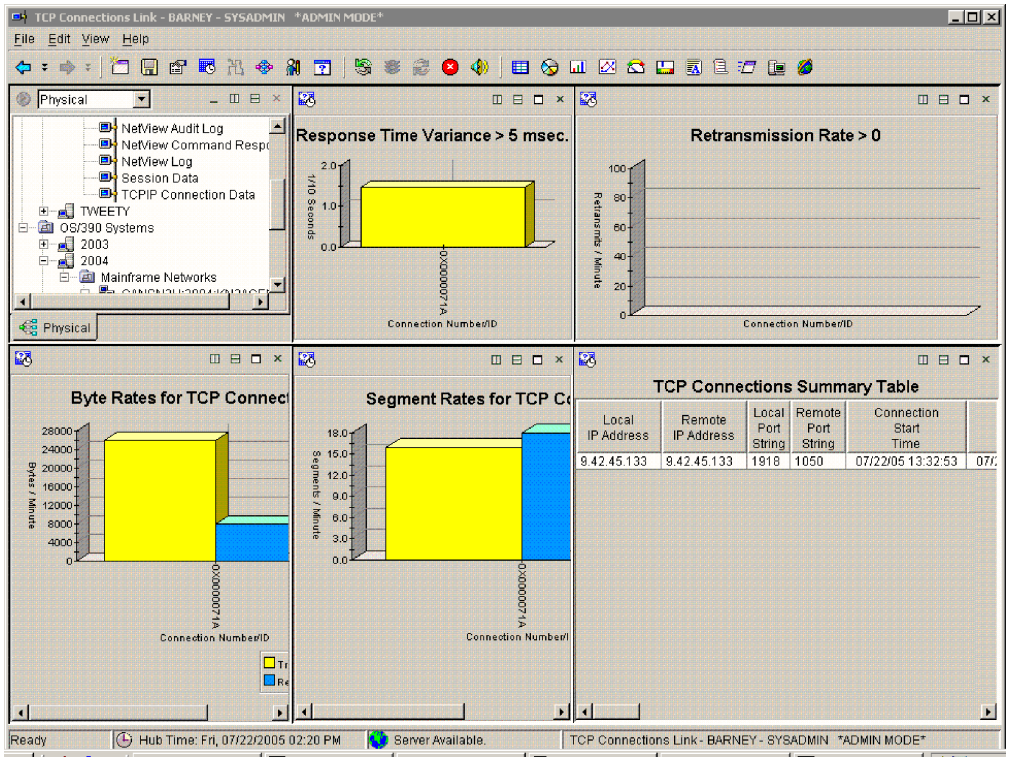


7. Refresh the TCP/IP Connection Data workspace to view the data resulting from issuing the NATCPCON command.

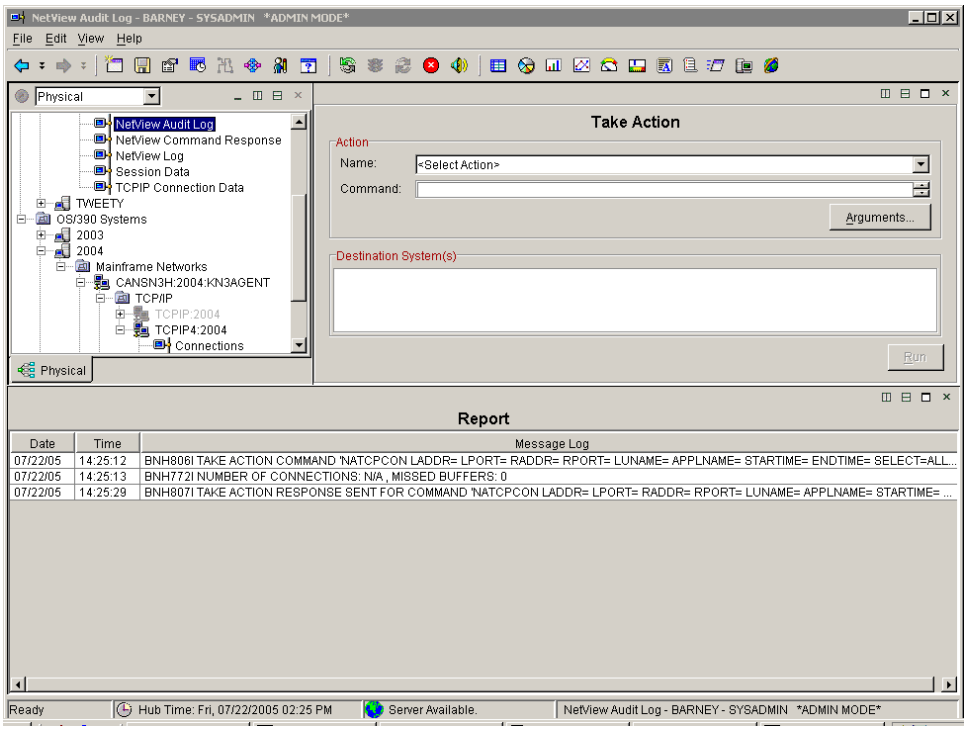


8. If you want to view the performance data for the fourth connection, select the link icon on the far left. If several systems are running OMEGAMON XE for Mainframe Networks, a list is displayed from which you can select the appropriate system. The OMEGAMON XE for Mainframe Networks TCP Connections Link workspace is displayed.





The NetView Audit Log workspace shows information related to issuing the View TCP/IP Connections take action item.


NetView Audit Log - BARNEY - SYSADMIN *ADMIN MODE*
File Edit View Help
Physical
NetView Audit Log
NetView Command Response
NetView Log
Session Data
TCPIP Connection Data
TWEETY
OS/390 Systems
2003
2004
Mainframe Networks
CANSN3H:2004:KN3AGENT
TCP/IP
TCPIP:2004
TCPIP4:2004
Connections
Physical
Take Action
Action
Name:
<Select Action>
Command:
Arguments...
Destination System(s)
Run
Report
Date
Time
Message Log
07/22/05
14:25:12
BNH806I TAKE ACTION COMMAND 'NATCPCON LADDR= LPORT= RADDR= RPORT= LUNAME= APPLNAME= STARTIME= ENDTIME= SELECT=ALL...
07/22/05
14:25:13
BNH772I NUMBER OF CONNECTIONS: N/A , MISSED BUFFERS: 0
07/22/05
14:25:29
BNH807I TAKE ACTION RESPONSE SENT FOR COMMAND 'NATCPCON LADDR= LPORT= RADDR= RPORT= LUNAME= APPLNAME= STARTIME= ...
Ready
Hub Time: Fri, 07/22/2005 02:25 PM
Server Available.
NetView Audit Log - BARNEY - SYSADMIN *ADMIN MODE*

Appendix G. Accessibility

For keyboard access in the Tivoli NetView for z/OS product, standard shortcut and accelerator keys are used. These keys are documented by the operating system. Refer to the documentation provided by your operating system for more information.

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

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

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

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

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

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

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

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Programming Interfaces

This publication documents information that is NOT intended to be used as Programming Interfaces of Tivoli NetView for z/OS.

Trademarks

IBM, the IBM logo, 3090, Advanced Peer-to-Peer Networking, AIX, AS/400, BookManager, Candle, CICS, DB2, ESCON, IMS, MVS, MVS/ESA, NetView, OMEGAMON, OS/2, OS/390, RACF, RETAIN, REXX, System z, Tivoli, Tivoli Enterprise, Tivoli Enterprise Console, TME 10, VSE/ESA, VTAM, WebSphere, z/OS, z/VM, and zSeries are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product or service names may be trademarks or service marks of others.

Index

Special characters

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z

File Number: S370/4300/30XX-50
Program Number: 5697-ENV

Printed in USA

GC31-8849-02