User’s Guide

Version 1 Release 4
## Contents

**Preface** .................................................. xiii  
Who Should Read This Document ........................................... xiii  
Prerequisite and Related Documents ................................. xiii  
What This Document Contains ................................. xiii  
Using Online Help ........................................... xiv  
Conventions Used in This Document ........................................... xv  
Platform-specific Information ........................................... xv  
Terminology ........................................... xv  
Accessing Publications Online ........................................... xvi  
Ordering Publications ........................................... xvi  
Providing Feedback about Publications ................................. xvii  
Contacting Customer Support ........................................... xvii

### Part 1. About NetView ........................................... 1

#### Chapter 1. Introducing Network Management Concepts ........................................... 3  
What Are the NetView Components? ........................................... 4  
  Command Facility ........................................... 5  
  Session Monitor ........................................... 5  
  Status Monitor ........................................... 5  
  Hardware Monitor ........................................... 5  
  SNA Topology Manager ........................................... 6  
  APPN Accounting Manager ........................................... 6  
  APPN Topology and Accounting Agent ........................................... 6  
  MultiSystem Manager ........................................... 6  
  Automated Operations Network ........................................... 6  
  Log and Member Browse ........................................... 8  
  4700 Support Facility ........................................... 8  
  Application Management Interface ........................................... 8  
  Online Help ........................................... 14  
  NetView Graphic Monitor Facility Host Subsystem ........................................... 15  
  NetView Management Console ........................................... 15  
  Resource Object Data Manager ........................................... 15  
  Event/Automation Service ........................................... 15  
What Other Programs Interact with NetView ........................................... 16  
  Any MultiSystem Manager Open Topology Agent ........................................... 17  
  Any Service Point ........................................... 17  
  Information/Management ........................................... 17  
  TSO ........................................... 17  
  TCP/IP for OS/390 ........................................... 17  
  UNIX for OS/390 ........................................... 17  
  LAN Network Manager ........................................... 18  
  MultiSystem Manager ATM Agent ........................................... 18  
  NetView AutoBridge/MVS ........................................... 18  
  NetView Performance Monitor ........................................... 18  
  MultiSystem Manager NetWare Agent ........................................... 19  
  Open Systems Interconnection Agents ........................................... 19  
  Operations Planning and Control/ESA ........................................... 19  
  Performance Reporter for MVS ........................................... 19  
  SNA Manager/6000 ........................................... 19  
  System Automation for OS/390 ........................................... 19  
  Tivoli Management Regions ........................................... 21  
  Tivoli Global Enterprise Manager ........................................... 21
Chapter 5. Managing Network and System Status ........................................ 121
Using Operations Planning and Control/ESA ........................................ 121
Using Performance Reporter ......................................................... 121
  Setup Prior to Using the Performance Reporter ............................. 122
Using NetView Performance Monitor .............................................. 122
Using NTune .............................................................................. 122

Chapter 6. Monitoring Hardware and Software Problems .................. 125
Using the Hardware Monitor ....................................................... 125
Data Collection ................................................................. 125
  Solicited Data ............................................................... 125
  Unsolicited Data ............................................................ 125
Record Types .................................................................. 127
  Statistics ...................................................................... 127
  Events ......................................................................... 127
  GMFALERLTS .................................................................. 127
  Alerts ............................................................................ 127
Secondary Recording of Event Records ........................................ 130
Monitoring the Network Using the Hardware Monitor Panels .......... 130
  Investigating Non-Network Management Vector Transport Alerts .... 131
  Investigating Network Management Vector Transport (NMVT) Alerts .. 135
Displaying Total Events ......................................................... 140
Displaying Total Statistical Data ................................................. 141
Running Modem and Link Tests ............................................... 143
Network Management for Multiple Domains .................................. 148
Alert Forwarding .................................................................... 149
Distributed Database Retrieval .................................................. 150
Event/Automation Service ....................................................... 152

Chapter 7. Managing Network Inventory ........................................ 155
Using Vital Product Data ......................................................... 155
Strategy for Implementing Filters ............................................. 199
Setting Session Awareness Data Filters in VTAM ..................... 199
Setting Session Awareness Data Filters in the Session Monitor .... 200

Chapter 12. Managing NetView Data ........................................ 203
Setting the Primary Focal Point ............................................. 203
Changing the Primary Focal Point from an Entry Point ............... 203
Changing the Backup Focal Point from an Entry Point ............... 204
Displaying the Primary and Backup Focal Points ..................... 204
Displaying the Sphere of Control for a Focal Point .................. 204
Removing an Entry Point from the Focal Point Sphere of Control.. 204
Refreshing the Focal Point Sphere of Control .......................... 205
Controlling the Processing of Problem Management Data ............ 205
Generating Alerts Using GENALERT ....................................... 205
Generating Alerts Using the PPI ........................................... 205
Setting Error Thresholds for Alerts ....................................... 206
Using and Maintaining the Network Log .................................. 206
Displaying the Network Log .................................................. 206
Log Browse Filtering ......................................................... 207
Switching the Network Log ................................................... 209
Creating and Displaying NetView Trace Data ............................ 210
Creating and Displaying Command Facility Trace Data ............... 210
Creating and Displaying Session Monitor Trace Data ................ 210
Creating and Displaying PPI Trace Data ................................... 211
Maintaining the Hardware Monitor Database ............................ 211
Switching Primary and Secondary Databases ............................ 211
Controlling the Amount of Data Retained in the Hardware Monitor Database .............................................. 212
Removing Unwanted Data from the Hardware Monitor Database .... 212
Collecting Hardware Monitor Data in an SMF Data Set ................ 212
Using and Maintaining the 4700 Support Facility Database .......... 213
Switching Primary and Secondary Databases ............................ 213
Removing Unwanted Data from the 4700 Support Facility Database .. 213
Reorganizing the 4700 Support Facility Database ....................... 213
Using and Maintaining the Session Monitor Database ................. 214
Switching Primary and Secondary Logs ................................... 214
Removing Unwanted Data from the Session Monitor Log ............. 214
Collecting Session Monitor Data in an SMF Data Set ................. 214
Maintaining the Save/Restore Database ................................... 215
Switching Primary and Secondary Databases ............................ 215
Removing Unwanted Data from the Save/Restore Database .......... 215
Reorganizing the Save/Restore Database ................................... 215
Using the MVS System Log (SYSLOG) ..................................... 215
Using and Maintaining the RODM Log ..................................... 216
Switching the Primary and Secondary RODM Logs ..................... 216
Formatting the RODM Log .................................................... 216
Copying the Contents of RODM to a Checkpoint Data Set ............ 217

Part 4. Automating the Network or System .............................. 219

Chapter 13. Using the NetView Automation Table ....................... 223
Automation Table and Alerts ................................................ 223
Setting Network and System Security ..................................... 224
Planning Message or MSU Automation .................................... 225
Browsing the Automation Tables ......................................... 225
Adding a New Automation Table Statement ............................. 226
Testing an Automation Table ................................................ 231
| Requirements for Writing Command Lists | 279 |
| Defining a Data Set                  | 279 |
| Creating a Command List              | 280 |
| Using REXX Functions                 | 281 |
| Using NetView Functions              | 282 |
| Handling Command Message Responses   | 282 |
| Displaying Panels                    | 284 |
| Issuing Messages                     | 284 |
| Obtaining Input from the Operator    | 285 |
| Issuing Commands                     | 285 |
| Storing Information in Global Variables | 285 |
| Accessing Data Set Members           | 286 |
| Parsing Input                        | 286 |
| Testing a Command List               | 287 |
| Adding a CMDMDL Statement            | 287 |
| Improving the Performance of Command Lists | 288 |
| Writing an HLL Command Processor     | 289 |
| Writing an Assembler-Language Command Processor | 290 |
| Chapter 20. Storing Information in NetView Global Variables | 293 |
| Designing Global Variables           | 293 |
| Displaying the Current Value of a Global Variable | 294 |
| Chapter 21. Optimizing Your Automation | 297 |
| Deciding Which Alerts to Filter      | 297 |
| Deciding Where to Filter Each Alert  | 297 |
| Implementing Filtering Decisions     | 297 |
| Using the RATE Statement             | 297 |
| Using the Hardware Monitor SRFILTER Command | 298 |
| Using the Automation Table SRF Function | 298 |
| Using the DSIEX16B Exit              | 298 |
| Suppressing a System Message         | 298 |
| Using MVS Message Processing Facility (MPF) | 299 |
| Suppressing VTAM Messages            | 300 |
| Chapter 22. Monitoring NetView Automation | 301 |
| Using Operations Planning and Control/ESA | 301 |
| OLTP Shutdown Triggered by OPC/ESA Deadline WTOs | 301 |
| Setting Special Resource Availability | 301 |
| Invoking the OPC/ESA Program Interface (PIF) or the API | 301 |
| Scheduling NetView Activities from OPC/ESA | 301 |
| Chapter 23. Debugging Automation     | 303 |
| Determining Why a Message Is Not Automated by the Automation Table | 303 |
| Checking Other Areas                 | 303 |
| Reading the Message Detail Report    | 304 |
| Determining Why an Alert Is Not Automated | 306 |
| Determining Why an Alert Is Not Displayed on the Tivoli Enterprise Console | 308 |
| Determining Why a Tivoli Enterprise Console Event Is Not Forwarded to NetView | 309 |
| Determining Why a Command List Does Not Complete | 310 |
| Determining Why a Timed Command Does Not Run | 311 |
| Determining Why Automation Is Taking Too Much Processing Time | 313 |
| Determining Why a Message Is Routed to the Wrong Operator | 314 |
| Determining Why a Pipe Command Does Not Process Correctly | 315 |
Part 5. Problem Diagnostics ........................................... 317

Chapter 24. Proactive Investigating .................................. 319
Preventing Problems .................................................. 319
Analyzing System Performance Using TASKUTIL (Command Facility) .... 320
Initiating Error Recovery (Status Monitor) ................................ 322
Displaying Resource Status (Status Monitor) ........................... 322
Identifying Intermittent Problems (Hardware Monitor) ................... 324
Determining Controller Status (Hardware Monitor) ....................... 325
Checking Session Monitor and Hardware Monitor Database Status (Command
Facility) .................................................................. 329

Chapter 25. Reactive Investigating ..................................... 331
Hung Session (Session Monitor) ......................................... 331
Broken Session (Session Monitor) ....................................... 334
Line Failure (Hardware Monitor) ........................................ 338
Blocked Virtual Route (VTAM) .......................................... 344
Modem Problems (Status Monitor, Hardware Monitor, Session Monitor) .... 344
Hung or Looping NetView Tasks (Command Facility) .................... 351
NetView Abends (First Failure Support Technology) ................... 351
  FASTService Option .................................................. 352
  Resolving an Abend ................................................... 352
Measuring Response Time with Control Units Using RTM (Session Monitor) 353
Sluggish Network Performance (NPM) .................................. 355
Using the NetView Help Desk ........................................... 365

Chapter 26. Managing Problems ....................................... 367
Using the Hardware Monitor ........................................... 367
Creating a Problem Report ............................................... 368
Using NetView AutoBridge/MVS ........................................ 369
Implementing NetView AutoBridge ...................................... 370

Part 6. Appendixes .......................................................... 373

Appendix A. Message Format .......................................... 375
Message Codes .................................................................. 375

Appendix B. NetView Component Hierarchies ......................... 377
Using the Help Panels ................................................... 377
  Navigating the Help Panel Hierarchy ................................ 377
  Using Default Hierarchies .......................................... 378
Using the Hardware Monitor Panels .................................... 378
  Navigating the Hardware Monitor Panel Hierarchy .................. 379
  Understanding the Hardware Monitor Panel Terminology ............ 381
Using the 4700 Support Facility Panels ................................ 383
  Navigating the 4700 Support Facility Panel Hierarchy ............... 383
Using the Session Monitor Panels ...................................... 385
  Navigating the Session Monitor Panel Hierarchy .................... 385
Using the Status Monitor Panels ....................................... 389
  Navigating the Status Monitor Panel Hierarchy ...................... 389
Using the RODMView Panels .......................................... 391
  Navigating the RODMView Panel Hierarchy ......................... 391

Appendix C. Interpreting Session Data ................................ 393
Sessions-Data Availability Scenarios ................................... 393
Preface

This document describes how Tivoli® NetView® for OS/390® (NetView) enables you to manage complex, multivendor networks and systems from a single point. The Tivoli NetView for OS/390 User’s Guide provides information for the operator and system programmer on how to use NetView as the central point to manage their networks and systems.

Who Should Read This Document

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

IBM® also provides solutions for implementing network management functions using the NetView program and associated products through a series of offerings called NetView Extra.

Prerequisite and Related Documents

To read about the new functions offered in this release, refer to the Tivoli NetView for OS/390 Installation: Migration Guide.

You can find additional product information on these Internet sites:

<table>
<thead>
<tr>
<th>Resource Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM</td>
</tr>
<tr>
<td>Tivoli Systems</td>
</tr>
<tr>
<td>Tivoli NetView for OS/390</td>
</tr>
</tbody>
</table>

The Tivoli NetView for OS/390 home page offers demonstrations of NetView, related products, and several free NetView applications you can download. These applications can help you with tasks such as:

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

What This Document Contains

The information in this document is presented according to task. Each task contains subtasks. For each subtask the following is provided:

- A description of the subtask
- The steps required to perform the subtask
- Additional references

This document is divided into the following parts.

- Part 1. About NetView on page 1 describes:
  - Various components of the NetView program
Preface

- Data flows in the NetView environment
- How to use the system console and NetView program

- "Part 2. Monitoring and Controlling the Network and System" on page 49 describes the tasks required to monitor and control the network and system.
- "Part 3. Controlling the NetView Environment" on page 177 describes the tasks required to control the NetView environment.
- "Part 4. Automating the Network or System" on page 219 describes the tasks required to automate the network or system.
- "Part 5. Problem Diagnostics" on page 317 provides scenarios for investigating and solving problem situations.
- The appendixes in this book describe:
  - Message formats
  - NetView component hierarchies
  - How to interpret session data

Using Online Help

The NetView program provides online information that includes host help panels and workstation help.

Using Host Help

Use Table 2 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 there is more information 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 will scroll 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 2. Getting Help

<table>
<thead>
<tr>
<th>To obtain help for...</th>
<th>Enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action codes from hardware monitor panels</td>
<td>action code</td>
</tr>
<tr>
<td>Explicit route status codes</td>
<td>erst code</td>
</tr>
<tr>
<td>The Help Desk</td>
<td>helpdesk</td>
</tr>
<tr>
<td>The Online Index</td>
<td>index character</td>
</tr>
<tr>
<td>NetView commands (all)</td>
<td>help commands</td>
</tr>
<tr>
<td>NetView commands (any)</td>
<td>help command</td>
</tr>
<tr>
<td>NetView commands by component</td>
<td>help component commands</td>
</tr>
<tr>
<td>NetView components</td>
<td>help component</td>
</tr>
<tr>
<td>NetView messages</td>
<td>help msgid</td>
</tr>
<tr>
<td>NetView product</td>
<td>help netview</td>
</tr>
<tr>
<td>Panel fields</td>
<td>help 'term'</td>
</tr>
<tr>
<td>Panel fields by component</td>
<td>help component 'term'</td>
</tr>
</tbody>
</table>
Table 2. Getting Help (continued)

<table>
<thead>
<tr>
<th>To obtain help for...</th>
<th>Enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNA sense codes</td>
<td>sense sense_code</td>
</tr>
<tr>
<td>Virtual route status codes</td>
<td>vrst code</td>
</tr>
<tr>
<td>VTAM® return codes and feedback codes</td>
<td>rcfb return_code,feedback_code</td>
</tr>
<tr>
<td>VTAM status codes and status modifiers</td>
<td>status code</td>
</tr>
</tbody>
</table>

Conventions Used in This Document

The document uses several typeface conventions for special terms and actions. These conventions have the following meaning:

**Bold** Commands, keywords, flags, and other information that you must use literally appear like **this**, in **bold**.

**Italics** Variables and new terms appear like **this**, in **italics**. Words and phrases that are emphasized also appear like **this**, in **italics**.

**Monospace** Code examples, output, and system messages appear like this, in a monospace font.

**ALL CAPS** Tivoli NetView for OS/390 commands are in ALL CAPITAL letters.

Platform-specific Information

For more information about the hardware and software requirements for NetView components, refer to the *Tivoli Netview for OS/390 Licensed Program Specification*.

Terminology


For brevity and readability, the following terms are used in this document:

**NetView**
- Tivoli NetView for OS/390 Version 1 Release 4
- Tivoli NetView for OS/390 Version 1 Release 3
- TME® 10 NetView for OS/390 Version 1 Release 2
- TME 10 NetView for OS/390 Version 1 Release 1
- IBM NetView for MVS Version 3
- IBM NetView for MVS Version 2 Release 4
- IBM NetView Version 2 Release 3

**MVS** MVS/ESA™, OS/390, or z/OS operating systems.

**Tivoli Enterprise™ software** Tivoli software that manages large business networks.

**Tivoli environment** The Tivoli applications, based upon the Tivoli Management Framework, that are installed at a specific customer location and that address network computing management issues across many platforms. In a Tivoli environment, a system administrator can distribute software, manage user
configurations, change access privileges, automate operations, monitor resources, and schedule jobs. You may have used TME 10 environment in the past.

**TME 10**

In most product names, TME 10 has been changed to Tivoli.

**V and R**

Specifies the version and release.

**VTAM and TCP/IP**

VTAM and TCP/IP for OS/390 are included in the IBM Communications Server for OS/390 element of the OS/390 operating system. Refer to [http://www.software.ibm.com/enetwork/commserver/about/csos390.html](http://www.software.ibm.com/enetwork/commserver/about/csos390.html).

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.

### Accessing Publications Online

The Tivoli Customer Support Web site ([http://www.tivoli.com/support/](http://www.tivoli.com/support/)) offers a guide to support services (the *Customer Support Handbook*); frequently asked questions (FAQs); and technical information, including release notes, user’s guides, redbooks, and white papers. You can access Tivoli publications online at [http://www.tivoli.com/support/documents/](http://www.tivoli.com/support/documents/). The documentation for some products is available in PDF and HTML formats. Translated documents are also available for some products.

To access most of the documentation, you need an ID and a password. To obtain an ID for use on the support Web site, go to [http://www.tivoli.com/support/getting/](http://www.tivoli.com/support/getting/).

Resellers should refer to [http://www.tivoli.com/support/smb/index.html](http://www.tivoli.com/support/smb/index.html) for more information about obtaining Tivoli technical documentation and support.

Business Partners should refer to [Ordering Publications](http://www.tivoli.com/support/Prodman/html/pub_order.html) for more information about obtaining Tivoli technical documentation.

**Note:** Additional support is also available on the NETVIEW CFORUM (Customer Forum) through the IBMLink™ system. This forum is monitored by NetView developers who answer questions and provide guidance. When a problem with the code is found, you are asked to open an official problem management record (PMR) to get resolution.

### Ordering Publications

Order Tivoli publications online at [http://www.tivoli.com/support/Prodman/html/pub_order.html](http://www.tivoli.com/support/Prodman/html/pub_order.html) or by calling one of the following telephone numbers:

- U.S. customers: (800) 879-2755
- Canadian customers: (800) 426-4968
Providing Feedback about Publications

We are very interested in hearing about your experience with Tivoli products and documentation, and we welcome your suggestions for improvements. If you have comments or suggestions about our products and documentation, contact us in one of the following ways:

- Send e-mail to pubs@tivoli.com.
- Fill out our customer feedback survey at http://www.tivoli.com/support/survey/.

Contacting Customer Support

The Tivoli Customer Support Handbook at http://www.tivoli.com/support/handbook provides information about all aspects of Tivoli Customer Support, including the following:

- Registration and eligibility
- How to contact support, depending on the severity of your problem
- Telephone numbers and e-mail addresses, depending on the country you are in
- What information you should gather before contacting support
Part 1. About NetView

Chapter 1. Introducing Network Management Concepts

What Are the NetView Components? 

Command Facility 
Session Monitor 
Status Monitor 
Hardware Monitor 
SNA Topology Manager 
APPN Accounting Manager 
APPN Topology and Accounting Agent 
MultiSystem Manager 
Automated Operations Network
  AON/LAN Automation 
  AON/SNA Automation 
  AON/TCP Automation
Log and Member Browse 
4700 Support Facility 
Application Management Interface 
  Sending Instrumentation Data to the Topology Server 
  NetView Instrumentation 
Online Help 
NetView Graphic Monitor Facility Host Subsystem 
NetView Management Console 
Resource Object Data Manager 
Event/Automation Service

What Other Programs Interact with NetView 

Any MultiSystem Manager Open Topology Agent 
Any Service Point 
Information/Management 
TSO 
TCP/IP for OS/390 
UNIX for OS/390 
LAN Network Manager 
MultiSystem Manager ATM Agent 
NetView AutoBridge/MVS 
NetView Performance Monitor 
MultiSystem Manager NetWare Agent 
Open Systems Interconnection Agents 
Operations Planning and Control/ESA 
Performance Reporter for MVS 
SNA Manager/6000 
System Automation for OS/390 
  System Operations 
  CICS Automation Feature 
  IMS Automation Feature 
  OPC Automation Feature 
  Processor Operations 
  I/O Operations 
Tivoli Management Regions 
Tivoli Global Enterprise Manager 
NetFinity 
Tivoli NetView 
VTAM 

How Is Data Sent to NetView?
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>How Commands and Responses Flow</td>
<td>23</td>
</tr>
<tr>
<td>How Events, Statistics, and Alerts Flow</td>
<td>24</td>
</tr>
<tr>
<td>How Messages Flow</td>
<td>24</td>
</tr>
<tr>
<td>What Are Network Management Tasks?</td>
<td>25</td>
</tr>
<tr>
<td>Chapter 2. Getting Started</td>
<td>29</td>
</tr>
<tr>
<td>Starting NetView</td>
<td>29</td>
</tr>
<tr>
<td>Replying to a Message</td>
<td>30</td>
</tr>
<tr>
<td>Stopping NetView</td>
<td>30</td>
</tr>
<tr>
<td>Issuing a NetView Command from MVS</td>
<td>31</td>
</tr>
<tr>
<td>Using NetView from a 3270 Session</td>
<td>32</td>
</tr>
<tr>
<td>Logging on to NetView from a 3270 Session</td>
<td>32</td>
</tr>
<tr>
<td>Understanding the Panel Layout</td>
<td>36</td>
</tr>
<tr>
<td>Session Identification Line</td>
<td>37</td>
</tr>
<tr>
<td>Message Area</td>
<td>37</td>
</tr>
<tr>
<td>Response Area</td>
<td>39</td>
</tr>
<tr>
<td>Command Entry Area</td>
<td>39</td>
</tr>
<tr>
<td>Moving between the Components</td>
<td>40</td>
</tr>
<tr>
<td>Issuing Commands</td>
<td>40</td>
</tr>
<tr>
<td>Using Program Function Keys</td>
<td>41</td>
</tr>
<tr>
<td>Listing PF and PA Keys</td>
<td>41</td>
</tr>
<tr>
<td>Controlling the NetView Screen</td>
<td>42</td>
</tr>
<tr>
<td>Using NetView from the NetView 3270 Management Console</td>
<td>43</td>
</tr>
<tr>
<td>Workstation and Host Environments</td>
<td>43</td>
</tr>
<tr>
<td>Logging on to NetView from the NetView 3270 Management Console</td>
<td>43</td>
</tr>
<tr>
<td>Customizing Your Console</td>
<td>44</td>
</tr>
<tr>
<td>Using the Command Facility Panel</td>
<td>44</td>
</tr>
<tr>
<td>Using a Full-Screen Session Panel</td>
<td>44</td>
</tr>
<tr>
<td>Logging Off</td>
<td>45</td>
</tr>
<tr>
<td>Using the NetView Web Server</td>
<td>45</td>
</tr>
<tr>
<td>The Autotask</td>
<td>46</td>
</tr>
<tr>
<td>The HTML Files</td>
<td>46</td>
</tr>
<tr>
<td>Usage Notes</td>
<td>47</td>
</tr>
</tbody>
</table>
Chapter 1. Introducing Network Management Concepts

Today's network environment is extremely complex due to the wide variety of choices available from both connectivity and vendor points of view. The network environment is open, allowing products of many types to communicate with each other. This complexity and high degree of connectivity requires a comprehensive management facility. Tivoli NetView for OS/390 (NetView) provides the ability to manage a complex multivendor network from a central point of control.

Tivoli NetView for OS/390 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. Both the Graphical Enterprise and Procedural Features of the NetView program can act as focal point applications.

- The **entry point** is a distributed point of control for all SNA devices that send information to the focal point and receiving commands from the focal point. The IBM AS/400® computer and the IBM 3174 establishment controller are two examples of entry point hardware products. The Procedural or Unattended features acting as distributed NetViews, and an NCP (Network Control Program) application are examples of entry point software products.

- 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. TME 10 NetView (AIX), Tivoli NetView Service Point, IBM LAN Network Manager, OS/2® Service Point Application (SPA) Router and Remote Operations Support (ROPS) and First Failure Support Technology™ (FFST) are some examples of service point products that enable NetView to manage non-SNA resources.

Figure 1 on page 4 shows the relationship between the three types of applications.
What Are the NetView Components?

Tivoli NetView for OS/390 (NetView) provides a comprehensive set of management functions from an MVS/ESA host and a graphical workstation. See Figure 2 on page 3 for the relationship between the host and workstation components. Some of these components may not be available on your system, depending on which NetView feature you have installed.
Command Facility

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

This component is available with the Unattended feature, the Procedural feature, and the Graphical Enterprise feature of NetView.

Session Monitor

The session monitor component provides information about SNA sessions (subarea and APPN) 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 VTAM sense code information for problem determination.

This component is available with the Procedural feature and Graphical Enterprise feature of NetView. The Unattended feature of NetView only contains the data collection part of this component and not the user interface.

Status Monitor

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

This component is available with the Procedural feature and Graphical Enterprise feature of NetView. The Unattended feature of NetView only contains the data collection part of this component and not the user interface.

Hardware Monitor

The hardware monitor component collects and displays events and statistical data for both hardware and software applications to identify failing resources in a network. It provides probable cause and recommended actions to enable operators to perform problem determination more efficiently.
This component is available with the Procedural feature and Graphical Enterprise feature of NetView. The Unattended feature of NetView only contains the data collection part of this component and not the user interface.

**SNA Topology Manager**
The SNA topology manager (SNATM) is a function of the NetView program that performs dynamic collection and displays APPN®, subarea, and LU topology and status. Topology and status data is stored in RODM for use by NMC. This component is available with the Graphical Enterprise feature of NetView.

**APPN Accounting Manager**
The APPN accounting manager (APPNAM) is a function of Tivoli NetView for OS/390 that starts and stops the collection of APPC session and conversation accounting information from APPN topology and accounting agents. The collected data can be written to either SMF (System Management Facility) or an external log.

This component is available with the Graphical Enterprise feature of NetView.

**APPN Topology and Accounting Agent**
The APPN accounting agent collects session level data at either session end points or intermediate nodes on the session path. The accounting agent supplies information such as conversation data, session data, or intermediate session data about various resources. The forwarding of collected data can be triggered by either the agent or the APPN accounting manager.

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

**MultiSystem Manager**
MultiSystem Manager provides for the further integration of management function on the NetView platform. It allows the NetView operator to view and manage resources that have been identified and are managed locally by products such as LAN Network Manager or Novell’s NetWare.

The topology and status of these resources are dynamically managed through the RODM and graphical workstation components of the NetView program. Refer to the [Tivoli NetView for OS/390 MultiSystem Manager User’s Guide](#) for more detailed information.

**Automated Operations Network**
The Automated Operations Network (AON) uses NetView automation facilities to automate the recovery of network resources. AON can monitor messages and alerts, then automatically invoke recovery actions. AON also provides an automated help desk to assist with resolving network problems, and generates reports so 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.
AON/LAN Automation
You can use the AON/LAN feature operating under the NetView program to extend automation capabilities to token-ring LAN resources such as LAN Network Managers (LNMs), adapters, bridges, segments, and controlled access units (CAUs).

AON/LAN Automation shows you the status of the resources, notifies you when changes occur in the LAN environment, and lets you know if intervention is required. AON/LAN Automation provides automatic recovery of bridges and LNMs, such as automated switching of an LNM from observing to controlling.

AON/LAN has a Remote Analysis Performance agent that gathers remote LAN trace data, then forwards the data to NetView to be used for other automation tasks. AON/LAN also provides a help desk to assist with solving command LAN problems.

AON/SNA Automation
The AON/SNA feature extends automation capabilities to VTAM SNA networks and systems. Specifically, the AON/SNA provides the following functions:

- Automatic switched network backup (SNBU)
  SNBU enables you to switch modems to a lower speed when a communication line experiences temporary errors, such as noise or poor line quality, or switch from a leased line to a dialed line when a communication line experiences permanent errors.
- Support for X.25 support interface between data terminal equipment and packet switching networks
  This function enhances problem determination for packet-switching networks by providing an exit to trap hardware alerts from X.25 resources and translate them into meaningful alerts. From these alerts, you can gain a clear interpretation of the error, including the meaning of the error bytes and recommended actions.
- Support for the APPN environment
  APPN is a robust, flexible, easy-to-use networking solution for client/server and distributed applications. AON enables you to define critical APPN resources and sessions between those resources to be monitored for failures. AON provides menu-driven commands that simplify VTAM topology and directory database management. Such an environment accepts operator commands for common APPN VTAM functions and enables active monitoring of control points and control point sessions.
- Support for the SNA environment
  AON provides automated recovery of VTAM subarea resources, such as NCPs, lines, and PUs.
  AON also provides a help desk for problem determination for your VTAM subarea resources.

AON/TCP Automation
You can use AON/TCP to assist you with management of your TCP/IP resources by proactively monitoring critical resources and by responding to network events.

AON/TCP provides support for NetView for AIX®, as a service point, and TCP/IP for OS/390. The NetView for AIX support can detect performance problems involving disk space, CPU utilization, and security authorization failures.

When you use TCP/IP for OS/390, you can issue any IP or UNIX® command. For example, Ping, Tracerte, Netstat, from NetView, display connections such as...
TN3270, FTP, SMTP, and then diagnose problems for those connections. You can also manage IP resources and NetView TSO and UNIX servers. The proactive monitoring capabilities exploits SNMP functions for MIB polling. For example, identify a failed interface, or check MIB thresholding for example, checking customer defined performance MIBs for key routers.

Log and Member Browse

The browse facility enables you to view local or remote NetView data set members including the NetView log, NetView parameters, and NetView panels.

This component is available with the Unattended feature, the Procedural feature and the Graphical Enterprise feature of NetView.

4700 Support Facility

The 4700 Support Facility provides information about the 47xx finance communications systems.

This component is available with the Procedural feature and Graphical Enterprise feature of NetView. The Unattended feature of NetView only contains the data collection part of this component and not the user interface.

Application Management Interface

The application management interface is an interface between instrumentation code and the topology display service. Instrumentation, through an API provided by the interface, provides management information used to build graphical displays for the topology console.

Software entities (called components), their possible connections to other components, and component and connection monitors are defined in a business model. A component can be defined in the business model to be an application, a subset of an application, a group of applications, or system or middle-ware entities.

When instrumentation code registers a component with the application management interface, a representing icon is displayed on the topology console. When instrumentation code makes a connection, a line is displayed on the topology console showing the connection.

A monitor provides information on the operational or performance characteristics of a component or connection. For example, a state monitor can be defined for a component which indicates whether a component is running or stopped. A CPU utilization monitor can be defined to measure usage of CPU resources. An events—sent monitor can be defined to measure the number of work elements sent on a connection.

Thresholding specifications may be established for any specific component or connection monitor so that only pertinent information is sent to the topology display service. For example, you can set the CPU utilization monitor to flag values less than 20 percent as normal severity, values greater than 20 percent as warning, and values greater than 60 percent as severe.

Instrumentation code that uses the application management interface can come from a variety of sources:
- NetView instrumentation
- Instrumentation code shipped with other products (for example, CICS)
• User-written instrumentation. Refer to the *Tivoli Global Enterprise Manager Instrumentation Guide* for information about how to create a business model and how to instrument your software so that it can be managed by GEM.

**Sending Instrumentation Data to the Topology Server**

Application management data flows across the NETCONV session or through the event/automation service and the Tivoli Enterprise Console (TEC).

Commands flow from the topology server across the NETCONV session to NetView/390. These may be user initiated tasks or topology server requests for data.

You can choose the route over which instrumentation events are sent from NetView/390 to the topology server based on these considerations:

• Directly across the NETCONV session
  - Can be used with or without GEM
  - Easier to setup
  - There is no history function available on the workstation
  - Instrumentation events cannot be sent if the NETCONV session ends

• Indirectly through the event/automation service and TEC
  - Requires GEM
  - Requires TCP/IP
  - The event/automation service must be configured and started, and IHSAAPMF must be included in the message adapter format file
  - TEC must be configured and started
    - GEM Event Service must be installed
    - The files `interapp.baroc` and `interapp.rls` must be imported to your rules base
    - The topology server address must be entered in the file `ihsttec.cfg`

Instrumentation events are created from messages issued from the Application Management Interface. These messages are BNH351I — BNH354I. Automation table samples are provided to route the messages to the appropriate module for sending to the topology server. Sample DSIAMIN is used to send directly across the NETCONV session, and sample DSIAMIT is used for the event/automation service and TEC path.

**NetView Instrumentation**

NetView instrumentation consists of two different subsystems. The topology display subsystem is available if you have NetView management console (NMC) or Tivoli Global Enterprise Manager (GEM). For other subsystems, including the event flow subsystem, the GEM product must be installed. Refer to the *Tivoli NetView for OS/390 Customization Guide* for more information about customizing.

**Topology Display Subsystem:** The topology display subsystem consists of the following components:

• RODM
• GMFHS
• SNATM
• PPI
• CNMTAMEL
• Other managers (for example, MSM)
Connections are reported between topology display subsystem components and workstation servers.

*Common Task Components:*

- **Query State**
  Select this task to query the current state of the selected component.

- **Set Pulse**
  Select this task to modify the polling interval associated with the heartbeat monitor for the selected component.

- **Query Connections**
  Retrieves the connection instances to and from the selected component.

- **Query Thresholds**
  Queries thresholds for all monitors associated with the selected component.

- **Query Polling Intervals**
  Queries the polling intervals associated with all monitors defined for the selected component.

*Common Monitor Tasks:*

Monitors are provided to measure availability and resource utilization of the topology display subsystem components. All monitors have the following tasks:

- **Set threshold**
  Sets the conditions when threshold events are sent

- **Set polling interval**
  Sets the interval between times the current value of a monitor is checked against the thresholds established by Set Threshold

- **Query value**
  Retrieves the current value of the monitor

- **Query threshold**
  Retrieves the current threshold severity level

The STATE monitor is common to all components.

*RODM Component:*

The following tasks are available:

- **Warm start RODM**
  Select this task to warm start RODM. To change the options, modify the NetView INIT member DSIAMII.

- **Stop RODM**
  Select this task to stop RODM

- **Cold start RODM**
  Select this task to cold start RODM. RODM will be started using the options 'type=coldforc,init=ekglislm'. To change the options, modify the NetView INIT member DSIAMII. After cold starting RODM, you must restart GMFHS.

The following RODM connection is available:

- **RODM-MGR**
  In this connection the manager component uses RODM to store and retrieve data.

*GMFHS Component:*

The following tasks are available:

- **Start GMFHS**
  Select this task to start GMFHS. To change the options, modify the NetView INIT member DSIAMII.

- **Stop GMFHS**
  Select this task to stop GMFHS
DISPLAY SUBTASK STATUS  Retrieves status and queue depth for all the GMFHS subcomponents

The following component monitors are available:

IPC QUEUE  Reports the number of buffers queued to the IPC subtask.

VIEWMGR QUEUE  Reports the number of buffers queued to the View Manager subtask.

VSTATMGR QUEUE  Reports the number of buffers queued to the View Status Manager subtask.

The following GMFHS connections are available:

RODM-MGR  The manager component uses RODM to store and retrieve data.

PPI  GMFHS uses this connection to communicate with CNMTAMEL which is in the NetView address space.

The following CNMTAMEL connections are available:

IP NETCONV  GMFHS uses this connection to send and receive data to and from the workstation data server. The connection uses the IP transport. The connection is removed when the NETCONV session is stopped.

LU6.2 NETCONV  GMFHS uses this connection to send and receive data to and from the workstation data server. The connection uses the SNA LU6.2 transport. The connection is removed when the NETCONV session is stopped.

The following connection monitor is available:

TDS STATE  Reports on the connection between CNMTAMEL and the workstation data server. This monitor is mapped to the IP NETCONV and LU6.2 NETCONV connections.

SNATM Component:  The following tasks are available:

Start SNATM  Select this task to start SNATM

Stop SNATM  Select this task to stop SNATM

The following SNATM connection is available:

RODM-MGR  In this connection, SNATM uses RODM to store and retrieve data.

RODMMGR Component:  The following connection is available:

RODM-MGR  In this connection, the RODMMGR uses RODM to store and retrieve data.

Event Flow Subsystem:  The event flow subsystem consists of the following components:

• Event services

• MSM agent
- Message adapter
- Alert adapter
- Event receiver

**Event Services Component:** The event services instance is displayed for NetView to represent its alert and messaging facilities. Connections to other event services instances show alert focal pointing connections.

The following event services tasks are available along with the common tasks described in “Common Task Components” on page 10:

- **Start NPDA** Issue STARTCNM NPDA command if NPDA is not active
- **Stop NPDA** Issue STOPCNM NPDA command

The following component monitors are available with the event services component:

- **CPU UTIL** Combined CPU utilization of BNJDSERV and CNMCSSIR
- **STOR USAGE** Combined storage usage of BNJDSERV and CNMCSSIR
- **IO RATE** Combined I/O rate of BNJDSERV and CNMCSSIR
- **MSG INQUEUE** Combined message inqueue rate of BNJDSERV and CNMCSSIR
- **MSG OUTQUEUE** Combined message outqueue rate of BNJDSERV and CNMCSSIR
- **AVSTOR24** Available NetView storage below the line
- **AVSTOR32** Available NetView storage above the line
- **STATE - UP/DOWN** Status of BNJDSERV and CNMCSSIR
- **BNJDSERV CPU** CPU utilization of BNJDSERV
- **BNJDSERV STOR** Storage usage of BNJDSERV
- **BNJDSERV IO** I/O rate of BNJDSERV
- **BNJDSERV MSGIN** Message inqueue rate of CNMCSSIR
- **BNJDSERV MSGOUT** Message outqueue rate of CNMCSSIR
- **CNMCSSIR CPU** CPU utilization of CNMCSSIR
- **CNMCSSIR STOR** Storage usage of CNMCSSIR
- **CNMCSSIR IO** I/O rate of CNMCSSIR
- **CNMCSSIR MSGIN** Message inqueue rate of CNMCSSIR
- **CNMCSSIR MSGOUT** Message outqueue rate of CNMCSSIR

STATE and CPU UTIL are set up with initial thresholds and are polled every 10 minutes. Other monitors need to be customized for your environment.

The following event services connections are supported:

- **SNA ALERT** Represents the forwarding of alerts
- **OS390_MESSAGE** Represents the forwarding of messages
PPI SNA ALERT Represents the forwarding of alerts across the PPI

The following connection monitor is available:

**SNA ALERTS SENT** Rate of alerts forwarded from one NPDA to another

*MSM Agent Component:* An MSM agent instance is displayed for each agent being managed by MSM (based on information stored in RODM). A connection to the event services component represents alert forwarding.

The common tasks are described in "Common Task Components" on page 10 and the common monitors are described in "Common Monitor Tasks" on page 10.

The following connection monitor is available:

**SNA ALERTS SENT** Rate of alerts forwarded from this MSM agent to NPDA. This monitor must be customized for your environment.

The STATE monitor is set up with initial thresholds.

The following MSM agent connection is supported:

**SNA ALERT** Represents forwarding of alerts

*Message Adapter Component:* An instance is displayed for each event automation service message adapter. A connection to an event service component represents message flow from NetView. A connection to a Tivoli Enterprise Console (TEC) component represents event flow to TEC.

The following message adapter tasks are available along with the common tasks described in "Common Task Components" on page 10:

- **Start** Start the message adapter
- **Stop** Stop the message adapter
- **Recycle adapter** Stop then start the message adapter

The following component monitors are available:

**OS390 MSGS REC** Rate of messages received by message adapter. This monitor needs to be customized for your environment.

**TEC EVENTS SENT** Rate of TEC events sent by message adapter. This monitor needs to be customized for your environment.

The following message adapter connections are supported:

**TEC EVENT** Represents the arding of TEC events

**OS390_MESSAGE** Represents the forwarding of messages

*Alert Adapter Component:* An instance is displayed for each event automation service alert adapter. A connection to an event service component represents alert flow from the component. A connection to a TEC component represents event flow to TEC.
The following alert adapter tasks are available along with the common tasks described in "Common Task Components" on page 10:

Start
Start the alert adapter

Stop
Stop the alert adapter

Recycle Adapter
Stop then start the alert adapter

The following component monitors are available:

**SNA ALERTS REC**
Rate of alerts received by alert adapter. This monitor must be customized for your environment.

**TEC EVENTS SENT**
Rate of TEC events sent by alert adapter. This monitor must be customized for your environment.

The following alert adapter connections are supported:

**TEC EVENT**
Represents the forwarding of TEC events

**PPI SNA ALERT**
Represents the forwarding of alerts across the PPI

*Event Receiver Component:* An instance is displayed for each event automation service event receiver. A connection to an event service component represents alert flow to NetView. A connection to a TEC component represents event flow to TEC.

The following event receiver tasks are available along with the common tasks described in "Common Task Components" on page 10:

Start
Start the event receiver

Stop
Stop the event receiver

Recycle adapter
Stop then start the event receiver

The following component monitors are available:

**SNA ALERTS SENT**
Rate of alerts sent to NPDA. This monitor must be customized for your environment.

**TEC EVENTS REC**
Rate of events received from TEC. This monitor must be customized for your environment.

The following event receiver connections are supported:

**TEC EVENT**
Represents the forwarding of TEC events

**PPI SNA ALERT**
Represents the forwarding of alerts across the PPI

**Online Help**

There are many types of online help available on the host and workstation, depending on your installation and configuration. They include:

- Host NetView help panels
- NMC help files
- NetView online books, which can be viewed using BookManager/READ
- Helpdesk

This help is available with the Procedural feature and Graphical Enterprise feature of NetView.
NetView Graphic Monitor Facility Host Subsystem

The NetView Graphic Monitor Facility Host Subsystem component maintains the status of resources in RODM and supplies the NetView management console (NMC) workstation with information about RODM resources. For instance, GMFHS allows an NMC operator to monitor and control Novell NetWare LANs or SNA APPN resources.

NetView Management Console

The NetView management console (NMC) uses interactive graphics to display color-coded views that represent network resources being monitored. From the views, you can interactively control resources and see the status changes reflected in the view updates. If used with GMFHS and RODM, it can monitor and control both SNA and non-SNA resources.

This component is available with the Graphical Enterprise feature of NetView.

Resource Object Data Manager

The 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. Use RODMView to simplify the process of adding, deleting, querying, and changing classes, objects, and fields in RODM.

The NetView GMFHS program uses RODM to maintain status information for resources controlled by service points, SNA APPN resources, and relationships between these resources and SNA subarea resources. For instance, you can use the NetView program and NetView MultiSystem Manager MVS/ESA to maintain LAN and client/server data using RODM. The NetView program can then use this information to dynamically build graphical views on a workstation using NMC. When resource status changes occur in RODM, methods will automatically update views that currently include those resources.

Event/Automation Service

The Event/Automation Service (E/AS) serves as a gateway for event data between the Tivoli NetView for OS/390 management environment, the Tivoli Management Region environment, and SNMP trap managers. With this gateway function, you can manage all network events from the management platform of your choice.

The E/AS converts Tivoli NetView for OS/390 alerts and messages into Tivoli Enterprise Console (TEC) events before forwarding the event data to a TEC in the Tivoli Management Region. As a result, all network events can be managed from a Tivoli Enterprise Console. For more information on Tivoli Enterprise Consoles, refer to Tivoli Enterprise Console User’s Guide.

The E/AS also converts Tivoli NetView for OS/390 alerts into SNMP traps before forwarding the trap data to an SNMP manager. The E/AS performs the function of an SNMP sub-agent, and sends the converted alert data to an SNMP agent for eventual forwarding to an SNMP manager.

The E/AS also converts TEC events that arrive from a Tivoli Management Region into alerts before forwarding the alert to Tivoli NetView for OS/390 through the Alert Receiver PPI mailbox. As a result, all network events can be managed from the Hardware Monitor.
Finally, the E/AS converts SNMP traps that arrive from SNMP managers into alerts before forwarding the alert to Tivoli NetView for OS/390 through the Alert Receiver PPI mailbox.

What Other Programs Interact with NetView

NetView 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. This book provides examples of ways to use NetView and to manage your network and system using NetView, other products, or both.

Many other products complement the NetView program to provide a comprehensive set of enterprise management functions. Some of these products’ relationship to the NetView program are covered in this book, and provide functions such as:

- Automation
- Managing SNA APPN networks
- Managing resources connected by service points, including LANs
- Controlling consoles
- Simplifying other tasks

Some automation products are now components of System Automation for OS/390 and their names have changed as shown in the following list:

**Automated System Control/MVS**
   System Automation for OS/390

**Target System Control Facility**
   Processor Operations

**Automation Operation Control**
   System Operations

**ESCON® Manager**
   I/O Operations

For more information about the programs described here, refer to the documentation in the appropriate library. See [Figure 3 on page 17](#) for a graphical representation of the relationship between host and workstation products. This book describes how to use these products to monitor, control, and automate your network and system.
Each of these products is described in the following section.

**Any MultiSystem Manager Open Topology Agent**

Any customer-written or vendor-written manager and agent application that follows the rules established by the MultiSystem Manager component of Tivoli NetView for OS/390 can be used.

**Any Service Point**

Any service point product that supports an architected data flow and can be monitored by Tivoli NetView for OS/390.

**Information/Management**

Information/Management (INFO) is a systems management application that provides a change database and integration services for Tivoli NetView for OS/390.

**TSO**

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

**TCP/IP for OS/390**

NetView operators or programs may interact with TCP/IP for OS/390 with the TSO stage or UNIX stage, as AON does. TCP/IP also supports several NetView functions; such as, the JAVA Client, and the Web Server. You can use the IPCMD command to issue any linemode TCP/IP for OS/390 command from NetView.

**UNIX for OS/390**

NetView operators or programs may interact with UNIX for OS/390 with the UNIX stage. For more information see the help for PIPE UNIX. You can use the IPCMD command to issue any linemode UNIX command from NetView.
LAN Network Manager

LAN Network Manager (LNM) lets you manage multisegment IBM token-ring networks, broadband and baseband IBM PC networks, and IBM 8209 LAN Bridge that interconnect a token-ring segment and an Ethernet segment. You can manage your LAN centrally using the Graphical Enterprise configuration of Tivoli NetView for OS/390 or locally using the operator interface at the LAN workstation.

The MultiSystem Manager component of Tivoli NetView for OS/390 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 (NMC), 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.

The Automated Operations Network component of Tivoli NetView for OS/390 provides toolkits for enhancing the 3270-based automation of TCP/IP, SNA (both subarea and APPN), and token-ring LAN resources.

MultiSystem Manager ATM Agent

The MultiSystem Manager ATM Agent works with the Nways® ATM Campus Manager for AIX, an integrated suite of network management applications for campus networks. Nways Campus Manager ATM automatically discovers, maps, and monitors campus ATM devices such as hubs, concentrators, and bridges.

The MultiSystem Manager component of Tivoli NetView for OS/390 communicates with an agent running in the Nways ATM Campus Manager and is able to gather topology and status information about the resources it manages and display this information using NMC. MultiSystem Manager can also correlate information from Nways ATM Campus Manager with information provided by other MultiSystem Manager agents, such as IP or LNM, letting you view system information and network connectivity from a single interface.

NetView AutoBridge/MVS

The NetView AutoBridge provides an MVS-based interface between NetView and Information/Management. Problem records can be created automatically in the Information/Management database based on the type of alert detected by NetView. Information/Management combines alert information with information already in its database to provide complete, detailed problem reports.

AutoBridge allows NetView and NetView Graphic Monitor Facility operators to view problem records without having to sign on to Information/Management (using the EYLEXUSR sample provided with the AutoBridge product). Specific problem records can be extracted from Information/Management, displayed on the NetView console, modified, and returned to the problem database. This interface between NetView and Information/Management speeds and simplifies help desk operations.

NetView Performance Monitor

NetView Performance Monitor (NPM) is a performance and accounting tool that collects, monitors, and analyzes communications network data. NPM helps you measure network performance, determine the source of a problem, identify potential problems, and plan for growth. NPM also collects accounting data that you can use...
to bill network customers. With NMC and NPM on the same workstation, Graphical Enterprise Tivoli NetView for OS/390 users can issue NPM commands from NMC to collect and view performance data.

MultiSystem Manager NetWare Agent
NetWare is a LAN management product for Novell NetWare LANs. When used with the NetWare agent, the MultiSystem Manager component of Tivoli NetView for OS/390 can gather topology and status information about the resources managed by NetWare and display this information using NMC.

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.

Three OSI agent applications collect information for transmission to NetView. Two of these applications are provided by NetView and run on the OS/2 Communications Manager/2 platform: a topology agent application that gathers information about APPN and an accounting agent. A third agent application is provided by VTAM and gathers topology information about SNA and APPN.

Operations Planning and Control/ESA
Operations Planning and Control/ESA (OPC/ESA) is designed for scheduling and controlling workloads in any operating environment where communication with MVS/ESA can be established. OPC/ESA increases the opportunities for centralized control of product workload across your environment. For example, you can use OPC/ESA with Tivoli NetView for OS/390 to schedule activities by business cycle or dependencies, control real resources, automatically report and respond to abnormal workload conditions, or manage your disaster recovery plan.

Performance Reporter for MVS
Performance Reporter for MVS 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 MVS or VM systems, IMS, CICS®, and networks. Performance Reporter for MVS 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 Performance Reporter for MVS can be used to fine tune the performance of Tivoli NetView for OS/390.

SNA Manager/6000
System Network Architecture (SNA) Manager/6000 integrates the end-user interfaces of IBM’s SNA, TCP, and non-TCP/IP managers onto a single RISC/6000 workstation. SNA Manager/6000 works with Tivoli NetView for OS/390 to provide SNA subarea topology and status to Tivoli NetView (for AIX), allowing a Tivoli NetView operator access to topology and status information from a single interface. All of the SNA automation capabilities of NetView are available when you are using a SNA Manager/6000 workstation.

System Automation for OS/390
System Automation for OS/390 is a comprehensive automation product for System/390® applications. System Automation for OS/390 centralizes operations,
such as initial microcode load (IML), initial program load (IPL), automation of system resources, and reconfiguring local or remote target systems, of System/390 processors and operating systems. This platform enables an operator at a focal point host to control and monitor multiple target systems such as MVS, VM, VSE, and TPF, concurrently.

System Operations
System Operations, previously known as Automated Operation Control (AOC), can automate console operations by monitoring messages received from MVS subsystems and related products, comparing them to statements in the NetView automation table, and initiating actions when a match is found.

CICS Automation Feature
The CICS Automation Option provides a simple and consistent way to monitor and control all of the local and remote CICS regions within your organization. Its main menu and series of panels simplify the CICS monitor and control tasks, enabling you to perform those tasks across systems from a single operator session. For example, you can obtain detailed information on CICS subsystems and manually initiate startup or shutdown processes for a subsystem, a group of subsystems, or all of the subsystems on a specified NetView domain.

IMS Automation Feature
The IMS Automation Feature provides a single-point-of-control for IMS startup, shutdown, recovery, and extended recovery facility (XRF) takeover operations, based on the automation environment supported by the System Operations component. IMS provides new functions that are not available in NetView, IMS, or the System Operations component, resulting in a more comprehensive automation capability than is possible with these products individually.

The benefits of IMS are multiplied in an XRF IMS environment where the purpose is to maintain an alternate IMS subsystem. In such an environment, IMS switches its workload to another set of available resources (takeover) quickly and with minimal disruption. This results in reduced IMS outages (scheduled and unscheduled), enhanced operator productivity, and reduced error potential.

OPC Automation Feature
Operation Planning and Control (OPC) can issue requests that perform complex setup, shutdown, or restart activities that are not handled efficiently by OPC/ESA alone. It extends the automation platform display facility to include status information on components, such as tapes, batch jobs, or OPC-detected errors and alerts. With OPC, Tivoli NetView for OS/390 can use OPC calendar information to achieve a single-calendar definition that handles multiple systems and sites. A change in the OPC calendar can affect all the systems, ensuring consistency throughout the systems complex.

Processor Operations
The Processor Operations component, previously known as the Target System Control Facility (TSCF), is designed to centralize operations of System/390 processors and operating systems, such as initial microcode load (IML), recycling operating systems (IPL), automation, and reconfiguring local or remote target systems. Processor Operations is used to start or stop systems; System Operations (previously AOC) is used to manage applications that run on the systems that Processor Operations starts or stops.

The Processor Operations component enables an operator at a focal point host to control and monitor multiple target systems, such as MVS, VM, VSE, and TPF,
concurrently. In a parallel sysplex environment, Processor Operations 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 is extendible by user-written automation routines, and its integration with the System Operations component on the operator views of the System Operations graphical interface.

**I/O Operations**

I/O Operations is the functional area of System Automation for OS/390 that 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 NMC-based 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 and that product's level of function.

**Tivoli Management Regions**

Tivoli Management Region (TMR) is a logical representation of the physical resources of groups 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 geographical-based (all the systems in Detroit) or application-based (all the users of a set of software applications) or use any other common, defining principle. Policy regions mask the operating system and hardware differences when a management function is executing across TMRs.

The NetView hardware monitor component can display events related to TMR resources, and the Tivoli Enterprise Console can integrate information about resources managed by Tivoli NetView for OS/390 with information about TMR resources.

When used with the MultiSystem Manager TMR agent, the MultiSystem Manager component of NetView for OS/390 can gather topology and status information about the resources managed by TMR. This information is then stored in RODM and can be displayed graphically using NMC.

**Tivoli Global Enterprise Manager**

Tivoli Global Enterprise Manager (Tivoli GEM) is an open network computing management solution that extends from the mainframe to the desktop and enables management of mission-critical business applications. The Tivoli GEM provides seamless and open integration of the System/390 and distributed management solutions and the ability to manage at the business application level.

Tivoli GEM endpoint applications can send data about distributed managers and environments to NetView for integration and monitoring.

**NetFinity**

NetFinity is a suite of tools and utilities that helps you manage networked desktop and server PCs in environments that include: NetFinity Manager and Services (clients) for OS/2, Windows® 3.1, Windows for Workgroups, Windows 95, Windows NT®, and Novell NetWare.

The MultiSystem Manager component of Tivoli NetView for OS/390 communicates with an agent running in NetFinity to gather topology and status information about
system resources such as application programs, adapters, memory, and hard disks that are managed by NetFinity. MultiSystem Manager can correlate information from NetFinity with information provided by other MultiSystem Manager agents, such as IP or LNM, enabling you to view system information and network connectivity from a single interface.

**Tivoli NetView**

Tivoli NetView 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 Tivoli NetView for OS/390 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 Tivoli NetView for OS/390.

When used with the MultiSystem Manager IP agent, the MultiSystem Manager component of NetView for OS/390 can gather topology and status information about the resources managed by Tivoli NetView. This information is then stored in RODM and can be displayed graphically using NMC.

**VTAM**

VTAM provides communication facilities for Tivoli NetView for OS/390 and other applications. It also provides status information and control facilities for SNA resources. For the Graphical Enterprise feature users of Tivoli NetView for OS/390, VTAM provides the topology agent information for SNA, both subarea and APPN, resources.

**How Is Data Sent to NetView?**

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 149 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 4 on page 23 for some of the command destinations and for some of the sources of events, statistics, alerts, and messages.
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 MVS operating system, its subsystems, or its applications. 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.

NetView might be the destination of the command. If the destination is a local NetView, the response passes through the NetView automation table. If the destination is the remote NetView, the operator uses the RMTCMD command to send the command to the remote NetView. The response to the command passes through the automation table on the remote NetView and then through the automation table of the local NetView.

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 the NetView workstation command tree facility).

**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**
- **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.

**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 4 on page 23 for some of the sources of unsolicited messages.

The MVS operating system, its subsystems, and its applications are designed to issue unsolicited messages that are displayed to the MVS operator. The message processing facility (MPF) of MVS controls whether a system message is displayed to the MVS operator, made available for NetView automation, written to the system log, or any combination including discarding the message. In the case where the message is available for automation, NetView accepts the message from the MVS operating system and passes it through the NetView automation table, which determines whether automatic processing should occur.

VTAM includes the capability for 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. VTAM then passes the messages through the NetView automation table.

A NetView task might issue unsolicited messages. If the task resides on the same NetView program that is performing automation, the 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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solicited and unsolicited</td>
<td>[NetView Information Routing for Automation] in</td>
</tr>
<tr>
<td>messages</td>
<td>Tivoli</td>
</tr>
<tr>
<td></td>
<td>NetView for OS/390 Automation Guide</td>
</tr>
</tbody>
</table>

What Are Network Management Tasks?

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

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

In a multiple-host environment, you can automate NetView 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. Systems can be designed so that little or no intervention is required at the distributed host.

Table 3 on page 26 describes these categories of tasks, and the remaining chapters of this book (from Chapter 3. Monitoring and Controlling Your Network from a Workstation on page 53 to Chapter 23. Debugging Automation on page 303) further divide these categories into subcategories and actual tasks that comprise network management.
### Table 3. Major NetView Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Monitoring and Controlling the Network and System:</strong></td>
<td><em>Monitoring</em> is the examination of the entire network and system for changes in</td>
</tr>
<tr>
<td></td>
<td>the status of individual components from satisfactory to a status requiring</td>
</tr>
<tr>
<td></td>
<td>attention. NetView achieves this through receipt of status changes, alerts,</td>
</tr>
<tr>
<td></td>
<td>and messages, which are displayed for analysis. You can explicitly request</td>
</tr>
<tr>
<td></td>
<td>this status information or NetView can present it automatically. You can</td>
</tr>
<tr>
<td></td>
<td>control the amount of information collected, and you can request more</td>
</tr>
<tr>
<td></td>
<td>information such as network and system definitions to help you analyze changes</td>
</tr>
<tr>
<td></td>
<td>in status. <strong>Controlling</strong> is the taking of specific actions against individual</td>
</tr>
<tr>
<td></td>
<td>network and system components to change their status from unsatisfactory to</td>
</tr>
<tr>
<td></td>
<td>satisfactory. This includes controlling the configuration and definition of</td>
</tr>
<tr>
<td></td>
<td>the resources. NetView provides controls to limit the functions you can use</td>
</tr>
<tr>
<td></td>
<td>and the resources you can access. <strong>Accounting</strong> involves recording information</td>
</tr>
<tr>
<td></td>
<td>about the length of sessions and the amounts of data processed for sessions,</td>
</tr>
<tr>
<td></td>
<td>such as the amount of session data, the number of PIUs, and the number of</td>
</tr>
<tr>
<td></td>
<td>bytes. This information can be used to charge end users for their use of network</td>
</tr>
<tr>
<td></td>
<td>resources. <strong>Controlling</strong> is the continual adjustment of the NetView</td>
</tr>
<tr>
<td></td>
<td>environment to achieve the goals of monitoring, investigating, analyzing, and</td>
</tr>
<tr>
<td></td>
<td>controlling of network and system components.</td>
</tr>
<tr>
<td><strong>Automating the Network or System</strong></td>
<td><strong>Automating</strong> is the understanding of a consistent relationship between an</td>
</tr>
<tr>
<td></td>
<td>event and the normal reaction to that event, and storing a procedure to</td>
</tr>
<tr>
<td></td>
<td>automatically recognize the event as well as taking appropriate action. One</td>
</tr>
<tr>
<td></td>
<td>way of doing this is through analysis of messages and alerts, and the operator</td>
</tr>
<tr>
<td></td>
<td>actions taken in response to them.</td>
</tr>
</tbody>
</table>

**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. NetView achieves this through receipt of status changes, alerts, and messages, which are displayed for analysis. You can explicitly request this status information or NetView 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. NetView 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.
<table>
<thead>
<tr>
<th>Task</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diagnosing Problems</td>
<td><strong>Investigating</strong> is the requesting of additional information to enable you to 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. <strong>Solving</strong> 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.</td>
</tr>
</tbody>
</table>

*Table 3. Major NetView Tasks (continued)*

This management task is described in [Chapter 26, Managing Problems](#) on page 367.
Chapter 2. Getting Started

This chapter describes how to get started using Tivoli NetView for OS/390 (NetView) and briefly describes the interfaces and functions of NetView. It also provides an overview of the types of online information available.

Starting NetView

The Graphical Enterprise NetView host environment consists of five MVS address spaces:
- NetView program
- NetView subsystem
- Resource Object Data Manager (RODM)
- NetView Graphic Monitor Facility host subsystem (GMFHS)
- Event/automation service (E/AS)

The Procedural and Unattended features consists of three MVS address spaces:
- NetView program
- NetView subsystem
- Event/automation service (E/AS)

Usually, the address spaces are started automatically. To start the address spaces manually, enter the following commands from the system console:

- To start the NetView program, enter:
  
  \[ s \text{ pro}name \]

  Where \text{pro}name 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 11. Controlling NetView Operation" on page 187 for more information.

- To start the NetView subsystem, enter:
  
  \[ s \text{ pro}name \]

  Where \text{pro}name is the name that your system programmer assigned to the cataloged procedure for the NetView subsystem, such as CNMPSSI.

- To start event/automation service, enter:
  
  \[ s \text{ pro}name \]

  Where:

  \text{pro}name

  The name your system programmer assigned to the cataloged procedure for the event/automation service, such as IHSAEVNT.

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 \text{pro}name that your system programmer assigned to the cataloged procedure for the RODM program, such as EKGXRODM.

- To \text{cold start} the RODM program, without using the checkpoint data set, enter:
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 EKGXRRODM: 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:
  
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 217 for information about how to copy the data from the RODM data cache to a checkpoint data set.

For Graphical Enterprise feature users: To start the GMFHS program, enter:

s procname.id

Replying to a Message

Unless the MVSPARM statement in DSIDMN specifies CMDWTOR=NO, 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:

r 07,command

Where command is any of the following commands:

- CLOSE
- CLOSE DUMP
- CLOSE IMMED
- CLOSE NORMAL
- CLOSE STOP
- MSG operid,text
- MSG LOG,text
- MSG SYSP,text
- MSG ALL,text
- REPLY Pnn,text
- REPLY Lnn,text

Stopping NetView

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

\[ p \text{ procname} \]

Where \text{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 as follows:

\[ r \text{ nn}, \text{close} \]

Where \text{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:

\[ p \text{ procname} \]

Where \text{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 either:

\[ f \text{ procname}, \text{term} \]

\[ p \text{ procname} \]

Where \text{procname} is the name your system programmer assigned to the cataloged procedure for event/automation service such as IHSAEVNT.

For Graphical Enterprise feature users: To stop the RODM program, enter:

\[ f \text{ procname}, \text{term} \]

Where \text{procname} is the name that your system programmer assigned to the cataloged procedure for the RODM program, such as EKGXRODM.

For Graphical Enterprise feature users: To stop the GMFHS program, enter:

\[ f \text{ procname}, \text{term} \]

Where \text{procname} is the name that your system programmer assigned to the cataloged procedure for the GMFHS program, such as CNMGMFHS.

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:

\[ f \text{ procname}, \text{command} \]

Where \text{procname} is the name that your system programmer assigned to the cataloged procedure for the NetView program, such as CNMNETV, and \text{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:

\[ f \text{ procname}, \text{disconid} \]

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 NetView. The default command designator is the 4-character subsystem name. For example, if job T130TEST is the NetView subsystem address space job, the designator would be T130. To display the MVS console names and IDs used by the NetView program, enter the following:

\[ t130 \text{ disconid} \]
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 NetView is not required.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNMSJ009 and CNMSJ010 (NetView start procedure)</td>
<td>[Getting Ready to Start NetView](Tivoli NetView for OS/390 Installation: Getting Started) in the Tivoli NetView for OS/390 Installation: Getting Started</td>
</tr>
<tr>
<td>NetView commands</td>
<td>NetView online help</td>
</tr>
<tr>
<td>Associating an autotask with an MVS console</td>
<td>AUTOTASK command in the NetView online help</td>
</tr>
</tbody>
</table>

### 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:
   ```
   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 only accepted on the VTAM LOGON command when NetView has enabled the function through the LOGONPW command. In this case `data` is entered in the form `userid/password`.

   When you log on, NetView queries the device for screen size and color attributes if the logmode specifies to issue the query. Otherwise, NetView 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 5 on page 33 is displayed.
Note:

- If NetView 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 will be 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 will contain the value you specified.

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

3. Enter your password. You will 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 NetView using a PassTicket rather than a password if you use the Network Security Program/Secure Logon Coordinator product (NetSP/SLC V1.2) with a 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 a 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. Press Enter.

If you left the PASSWORD field blank and NetView is using a SAF product such as RACF to check passwords, the panel shown in Figure 6 is displayed.

8. 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 will not be logged on.

For example, if the operator specifies values for profile, HCL, or INITCMD which are not valid, even if the password change is valid, the operator will not be logged on, and will not receive a message at the console. However, at the next logon attempt, the operator will need 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 has been entered in the non-displayed fields, either press CLEAR or PF3/PF15 before proceeding.

9. Press Enter. A panel similar to Figure 7 on page 35 is displayed.
10. 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.

```
Figure 7. NetView News Panel
```

<table>
<thead>
<tr>
<th>CNM01</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter LOG or LOGOFF to terminate session.</td>
</tr>
<tr>
<td>Enter HELP to obtain help.</td>
</tr>
<tr>
<td>Lead operator has been notified of your logon.</td>
</tr>
<tr>
<td>To obtain help from NETWORK CONTROL CENTER, enter</td>
</tr>
<tr>
<td>MSG PPT, your question here</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CNM01</th>
</tr>
</thead>
<tbody>
<tr>
<td>!! HIGHLIGHTS OF TIVOLI NETVIEW FOR OS/390 VERSION 1 RELEASE 3 !!</td>
</tr>
<tr>
<td>- HELP DESK COMPLETELY NEW! MUCH NEW INFORMATION AND USABILITY.</td>
</tr>
<tr>
<td>- COMMAND AND MESSAGE HELP SUPPORTS FIND CMD, PAGING, EASY CUSTOMIZATION.</td>
</tr>
<tr>
<td>- ACCESS TO VSAM FILES DIRECTLY FROM REXX PROCEDURES.</td>
</tr>
<tr>
<td>- NIAF/2 ON OS/2 SUPPORTS INSTALLATION AND ADMINISTRATIVE TASKS.</td>
</tr>
</tbody>
</table>

```
Figure 8. NetView Main Menu
```

```
CMMINETV TIVOLI NETVIEW for OS/390 VERSION 1 RELEASE 4 MAIN MENU

OPERATOR ID = OPER1 APPLICATION = CNM01

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

- Browse Facility BROWSE command
- Command Facility NCCF command
- Help Facility HELP command
- Help Desk HELPDESK command
- Index of help topics INDEX command
- Hardware Monitor NPOA command
- 4700 Support Facility TARA command
- Session Monitor NLDM command
- Status Monitor STATMON command
- Automated Operations Network AON command
- System Automation for OS/390 AOC command
- News NEWS command
- PF Key Settings DISPFK command

To Exit the NetView Program LOGOFF command

TO SEE YOUR KEY SETTINGS, ENTER ‘DISPFK’

Action===>
```

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 will only display active options. For example, if the Automated Operations Network and System Automation for OS/390 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 will be able to use the BROWSE member command, but not the BROWSE NETLOGA command.

The panel in Figure 9 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.

![Figure 9. NetView Main Menu](image)

**Understanding the Panel Layout**

Type `nccf` and Press Enter to access the command facility.
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 192.

Session Identification Line
The first line of the panel, identified with the SF5800001/SF590000, gives you the name of the panel that appears 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 will 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 11 on page 38 shows a 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 "Suppressing a System Message" on page 298. See "Appendix A. Message Format" on page 375 for additional information on message formats.

To rearrange the messages on the screen, press the Enter key. This will redisplay the messages in sequential order and remove 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 disappear as the screen scrolls. Examples of exceptions include reply messages, held messages, and windowed responses.

**Reply messages** are messages to which you should reply before you delete them from the display screen. These messages appear 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 appear in high intensity (or are otherwise highlighted) and appear at the top of the message area. Specific action must be taken to remove them, such as:
- 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 there are more messages being held than can be displayed on your type of terminal, message DSI151I appears and the messages are queued. The queued messages appear 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 will return 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 will return 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 has been done.

To avoid losing information from the command entry area, you can either:
• 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, and enables you to 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 10 on page 37. 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. Some of the commands you can use are:
• AUTOWRAP
• CLOSE
• GO
• HOLD
• LOGOFF
• RESET

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

Most of these commands change how fast 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 10 on page 37. You communicate with the NetView program by entering commands here or you can invoke 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**

<table>
<thead>
<tr>
<th>To move to this component:</th>
<th>Enter:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browse facility</td>
<td>browse logname</td>
</tr>
<tr>
<td>Command facility</td>
<td>nccf</td>
</tr>
<tr>
<td>Hardware monitor</td>
<td>npda</td>
</tr>
<tr>
<td>Help facility</td>
<td>help</td>
</tr>
<tr>
<td>4700 Support Facility</td>
<td>tara</td>
</tr>
<tr>
<td>Session monitor</td>
<td>nldm</td>
</tr>
<tr>
<td>Status monitor</td>
<td>statmon</td>
</tr>
</tbody>
</table>

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`.

**Note:** If you are using the Unattended feature of NetView, the browse, help, and the 4700 support facility are not available. Also, you will not see the end user interface for the command facility, hardware monitor, session monitor, and status monitor.

The NetView program allows you to have multiple components active at the same time. The ROLL function enables you 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.

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 377. 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 appears 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 on page 41](#) shows the possible destinations and how to direct commands to
those destinations.

**Table 5. Directing Commands**

<table>
<thead>
<tr>
<th>To direct a command to</th>
<th>Use:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current operator task</td>
<td><code>command_name</code></td>
</tr>
<tr>
<td>VTAM</td>
<td><code>VTAM_command_name</code></td>
</tr>
<tr>
<td>Another task on this NetView EXCMD</td>
<td><code>EXCMD command or command prefix label</code></td>
</tr>
<tr>
<td>Remote NetView program</td>
<td><code>RMTCMD command or command prefix label</code></td>
</tr>
<tr>
<td>Service point</td>
<td><code>RUNCMD command</code></td>
</tr>
<tr>
<td>MVS</td>
<td><code>MVS command</code></td>
</tr>
</tbody>
</table>

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:

```
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:

```
monit start all
```

**Using Program Function 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.

**Listing PF and PA Keys**

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

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

```
dispfk nccf
```

A scrollable window similar to the one following 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.
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, allowing you to type a component name on the command line, then press PF4 to see that component’s PF keys. 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 58 on page 103.

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

```
list key=pfnn
```

Where `nn` is the PF key number. See “Defining Program Function Keys” on page 189 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 189 for more information.
Using NetView from the NetView 3270 Management Console

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

This section describes the following topics:

- Workstation and host environments
- 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

Workstation and Host Environments

The NetView 3270 management console environments follow:

- OS/2 Warp 4.0
- Windows 95 and 98
- Windows NT 4.0
- AIX 4.22
- Sun Solaris 2.x
- Sun OS 4.x
- HPUX 9.x and 10.x

You will also need the Java runtime 1.1.7. For specific hardware and software requirements, refer to the Read.me file for the NetView 3270 management console.

The following conditions must exist in the host environment to enable the NMC-3270:

- Host TCP/IP must be started. This must be done each time you IPL the system. To start TCP/IP, issue an MVS command similar to the following:
  
  ```
  S TCPIP32.TCP32
  ```

  For further information, refer to the MVS/ESA OS/390 TCP/IP Users Guide. The start-up profile is in TCP32.PROFILE.TCPIP.

- Tivoli NetView for OS/390 and the DSITCPIP optional task must be running. Issue the following command to start the optional task:
  
  ```
  START TASK=DSITCPIP
  ```

  Security authorization is required to issue the START command.

Logging on to NetView from the NetView 3270 Management Console

To log on to NetView 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 will be prompted to re-enter it for verification. A command facility panel is then displayed.

**Customizing Your Console**

You can customize your console as follows:

- 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 as follows:
   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 pulldown. A dialog box is displayed.
2. Enter the name of the full-screen session to be added.
3. Enter the initial command to invoke 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. This enables you to 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 only in effect 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 pulldown. A dialog box is displayed.

2. Select the name of the full-screen session to be modified 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 only in effect 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 pulldown. 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 only in effect for the current session.

**Logging Off**

To log off NetView:

1. Select Connection Services on the menu bar.

2. Select Logoff from the pulldown. 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 pulldown. This logs you off NetView if you have not already logged off and ends the NetView 3270 management console session.

**Using the NetView Web Server**

Operators can enter a NetView line-mode command, access session monitor, or the network log, or browse a data set through a Web browser. With the NetView Web server function, NetView provides HTML files that enable you to enter NetView commands, link to another HTML file, and create your own HTML file. The Web server function supports HTTP 1.0 protocol on Netscape and Microsoft Internet Explorer Version 4.0 or higher. The BROWSE command, and most online help panels, are also supported.

**Note:** When using the BROWSE command without specifying a DDNAME, the default search order is different than the search order used with NCCF BROWSE. Refer to the BROWSE command in the NetView online help for details on the search order. The BROWSE NETLOG function is supported on Netscape, Hot Java, and Microsoft Internet Explorer Version 4.0 or higher.
To access the NetView Web server, enter the following URL from a Web browser:
http://hostname:portnumber

Where:

hostname
The host name of the NetView host machine

portnumber
The port number as defined in DSIWBMEM. The default is 80.

The first time you issue a command to access NetView, or link to another HTML file from a Web browser, you will be prompted for your NetView operator ID and password. If the operator ID and password are valid, NetView access is granted and the command you entered will be executed, or the link requested, will be sent.

If the operator is not already logged on, NetView starts it as an attended autotask, and the command is sent to the task for execution. The operator, who is started as an autotask, will remain logged on until the autotask is logged off. The autotask can also be logged off by using a NetView CLIST or REXX EXEC similar to CNME1057 (IDLEOFF).

Note: If Web server security has not been enabled by specifying WEBSEC=CHECK on either the OPTIONS statement in DSIDMNK or on the REFRESH command, commands can still be entered from the Web browser even though an operator has logged off of the NetView operator ID. When Web security is not enabled, the Web server logs the NetView operator ID on again when a command is entered. To prevent unauthorized use, an operator must close the Web browser.

The Autotask

When the DSIWBTSK DST is started, it will establish communication with TCP/IP using the port number specified in DSIWBMEM. DSIWBTSK also starts the autotask DSIWEB, if it is not already active. When NetView receives an access request, DSIWEB reads in the HTML file and any requested files that reside on DSIOPEN.

Notes:
1. DSIOPEN and DSIWEB must have read access to DD CNMPNL1.
2. You may want to restrict access to the DSIWEB task from the EXCMD command by using scope-of-command authorization, the NetView command authorization table, or a SAF product such as RACF.

For more information, refer to the Tivoli NetView for OS/390 Security Reference.

The HTML Files

NetView provides the following HTML files (in DD CNMPNL1) including:

CNMHFCMD or CNMHTCMD (nonframe support)
Sent to the Web browser in response to the opening request from the browser.

CNMHFRSP or CNMHTRSP (nonframe support)
Contains the command response that is sent to the browser.

NetView provides the following graphics (GIF) files in DD DSIOPEN:
CNMGTIVS
Contains the Tivoli logo.

CNMGNETV
Contains the NetView logo.

For information about customizing these files, refer to “Designing HTML Files” in the Tivoli NetView for OS/390 Customization Guide.

Usage Notes

When using the NetView Web server, consider the following:

• When browsing a member of a NetView data set using the Web server, specify the member name rather than a synonym for the member name. For example, you do not use BR HELPDESK, use BR CNME1026.

• Only the first 1000 lines of data are sent to the Web browser. Additional lines over 1000 are discarded.

• NetView provides the capability through command authorization checking for the WEBCMD command to specify which operators are authorized to access the Web server.

• NetView provides additional security for the Web server by requiring an operator ID and password to be respecified after the interval specified by the IDLETIME control statement in member DSIWBMEM or on the REFRESH command, and through the WEBSEC keyword on either the OPTIONS statement in DSIDMNM or on the REFRESH command.

• When the SESMGET command is invoked from the Web browser, it creates a Web page from the AAU975I and AAU976I messages. This page consists of a list of specified sessions. You can view the configuration of any session that you select from the list. The configuration information is formatted from AAU978I messages, which contain most, but not all, of the configuration information known to the specified session monitor (NLDM). To view the configuration of a session from another session monitor, issue the SESMGET command to that session monitor.

For more information about the OPTIONS statement, refer to the Tivoli NetView for OS/390 Administration Reference. For more information on the REFRESH command, refer to the online help.
# Part 2. Monitoring and Controlling the Network and System

## Chapter 3. Monitoring and Controlling Your Network from a Workstation

- Using the NetView Management Console .................................................. 53
- Using the SNA Topology Manager .............................................................. 55
  - SNA Topology Manager ......................................................................... 56
- Using the APPN Accounting Manager ...................................................... 57
- Monitoring Resources Using Systems Automation for OS/390 ...................... 57
  - Graphical Enterprise Window (Cluster View) ........................................ 58
  - System Trend Window ........................................................................... 59
  - Transfer TSCF ...................................................................................... 60
  - Application Detail and Trends ............................................................... 61

## Chapter 4. Monitoring and Controlling Network Configuration

- Monitoring Network Resources ................................................................. 63
  - Monitoring SNA (Subarea and APPN) Resources .................................. 63
  - Monitoring Non-SNA Resources ............................................................. 64
- Using VTAM Commands (SNA Subarea, SNA APPN) .................................. 64
  - Checking the Status of a Resource ...................................................... 64
  - Controlling Resources Defined to VTAM .............................................. 65
  - Reloading and Reactivating an NCP ..................................................... 65
- Using NetView Commands (SNA Subarea, SNA APPN) ............................... 66
  - Using the APPLSPEN Command ......................................................... 66
  - Using the DISG Command ....................................................................... 66
  - Using the RMTCMD Command .............................................................. 68
    - Sending Commands ............................................................................... 68
    - Listing the Autotasks You Started ..................................................... 69
    - Restricting Access before Using the RMTCMD Command ................. 69
- Using Labels to Route Commands ............................................................... 69
  - Label Syntax .................................................................................................. 70
  - Label Usage ............................................................................................... 70
- Using the LAN Command List ..................................................................... 71
- Using the TOPOSNA Command .................................................................. 74
  - Monitoring Topology Information ......................................................... 74
  - Monitoring Critical LUs ........................................................................... 75
  - Displaying the Status of Monitoring Requests ....................................... 75
- Using the ACCTSNA Command .................................................................. 75
  - Retrieving Accounting Information ....................................................... 75
  - Sending Accounting Data Automatically .............................................. 75
  - Displaying the Status of an Accounting Agent ....................................... 76
- Using the Session Monitor (SNA Subarea, SNA APPN) ............................... 76
  - Session Response Time Data ................................................................. 77
  - Session Trace Data .................................................................................... 78
  - Network Accounting and Availability Measurement Data ....................... 79
  - Route Data .................................................................................................. 79
  - Session Awareness Data ........................................................................... 79
  - Setting Up the Session Monitor ............................................................... 80
  - Session Monitor Scenarios ....................................................................... 80
- Typical LU-LU Session for an SNA Subarea Network ...................................... 80
- Typical CP-CP Session for an SNA APPN Network ...................................... 87
- Typical LU-LU Session for an SNA APPN Network ...................................... 90
- SNA Session through an APPN Network .................................................... 96
- Typical Takeover/Giveback Session ........................................................... 97
- SESSMDIS Command ..................................................................................... 99
Chapter 3. Monitoring and Controlling Your Network from a Workstation

This chapter is only applicable to users who have installed the Graphical Enterprise feature.

This chapter describes how to manage your network from a workstation using the NetView management console (NMC), NetView Resource Manager (NRM), NetView MultiSystem Manager, SNATM, and Automated Operations Control/MVS.

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 either a Windows or OS/2 system 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 NMC, you can do the following:

• Monitor and control large portions of complex communication networks, including SNA subarea and APPN 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, access a NetView or non-SNA command line to issue your own commands, or use command trees to send commands.

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

NMC 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 NMC can display it. The NMC topology server forwards topology and status information collected from these sources to all signed-on client workstations.

Figure 13 illustrates the connection between host NetView and the NMC.

Figure 13. Host-to-Workstation Connection

The service point in Figure 13 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.

You can also use the SNA Manager/6000 to view RODM-defined resources, but using a RISC/6000 workstation running AIX, rather than OS/2.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examples of non-SNA networks attached to service points</td>
<td>Defining Your Network to GMFHS in the Tivoli NetView for OS/390 Resource Object Data Manager and GMFHS Programmer's Guide</td>
</tr>
</tbody>
</table>
Monitoring Resource Utilization Using NetView Resource Manager

NetView Resource Manager (NRM) enables you to graphically monitor and manage NetView tasks for resource utilization and status via NMC. You can monitor all NetViews in your enterprise via one NMC.

NRM is comprised of manager and agent NetView hosts. The agent host forwards local resource utilization information to one or more manager host(s). The manager host then processes resource utilization information for agent hosts (including itself), and provides a graphical interface (NMC) to monitor all of your NetViews. A manager host can also forward data to one or more manager host(s). You can use TCP/IP or SNA to communicate between these NetViews.

NRM is started with the INITNRM command, manually or at NetView initialization. CNMSTYLE contains all of the values that can be customized for NRM. AUTONRM is the autotask used for NRM processing.

NRM enables you to set thresholds for the following types of resources:
- CPU
- I/O
- MQS rates
- storage
- message queue count

When a resource reaches a threshold, a status change is sent to NMC. Reaching a threshold will not cause any action to be taken on the task. The NRM manager NetView uses the following functions:
- RODM
- RMTCMD
- HardWare Monitor
- TCP/IP Alert Receiver (if your communication method is TCP/IP)

The NRM agent NetView uses the RMTCMD function.

For more information about setting up and using NRM see:

Using the SNA Topology Manager

The NetView Graphical Enterprise feature can manage SNA subarea and Advanced Peer-to-Peer Networking® (APPN) resources using the NetView SNA topology manager. SNA topology manager collects topology information from VTAM agents and APPN topology and accounting agents.
APPNTAA works with corresponding Communications Manager/2 functions to gather and record data about your APPN networks.

The VTAM accounting agent collects topology information from SNA resources, both subarea and APPN.

**SNA Topology Manager**

The SNA topology manager provides a dynamic, centralized network management system for SNA subarea and APPN networks. It uses existing NetView components, including RODM and GMFHS, to manage and display SNA subarea and APPN topology data at the NMC 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 APPN networks. The agent application supplies topology information about nodes and links in response to requests from the manager application. VTAM V4R3 provides a topology agent for APPN and subarea topology information, and the APPN topology and accounting agent provides APPN topology and accounting information for OS/2 APPN networks using Communications Manager/2. Communication between the NetView system and the node containing the agent is over an SNA LU 6.2 session. 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 APPN 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 APPN 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 NMC to display configuration and status in graphic views. Operators can start network and local topology monitoring dynamically using the NMC 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 APPN networks: by their nature, these networks change configuration and status frequently as nodes establish and terminate 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 appearing 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 NMC commands at the NMC workstation
  - Customized command sets at the NMC 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 14 shows an overview of the SNA topology manager environment.

Using the APPN Accounting Manager

The APPN accounting manager provides the ability to start and stop the collection of APPC session and conversation accounting information. It retrieves this accounting information from the APPN topology and accounting agent. It then formats the data and writes it to either SMF or an external log. The APPN accounting manager is controlled using the ACCTSNA command. Session-level data can be collected at the session endpoints or at intermediate nodes on the session path. Conversation-level data can only be collected at the session endpoints. Collection can be triggered by the agent using a timer or threshold, or by the APPN accounting manager using the ACCTSNA RETRIEVE command.

Monitoring Resources Using Systems Automation for OS/390

The terminology used here is System Operations (previously known as AOC) terminology, not NetView terminology.

The System Operations Graphical Interface works with NMC to:

- 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 15 shows the relationships between the windows in the AOC Graphic Interface and NMC:

Figure 15. Relationships between the AOC Graphic Interface and NMC Views

The shaded blocks represent NMC views, using System Operations terminology

**Graphical Enterprise Window (Cluster View)**

The cluster view contains all your resources. It is an NMC view, not an AOC/MVS specific view.
**System Trend Window**

On the left side of [Figure 17 on page 60](#) is the System Trend window, this AOC/MVS window provides additional information about the system in the NMC view. Shown under the menu bar is the system name, location, and its fit in your complex.

Displayed graphically is the average workflow. You also have the option of adjusting the frequency of updates to the trend graph. You can access the numbers used to plot the graph from this window by clicking at any point on the graph line. You will see the numbers up to and including that point in time.
From this window, using the Transfer pull-down menu, you can issue commands using the Processor Operations component of Systems Automation for OS/390 and the Resource Measurement Facility (RMF).

**Transfer TSCF**

As shown in the upper part of the window, the commands are sent to the same system you are monitoring. Each radio button sends a specific command to the system.

For example, select Target Summary to display a window similar to the screen shown in [Figure 20 on page 61](#). At this time, you are in the TSCF program and all of its options are available to you.
Application Detail and Trends

Below are the Application Detail and Trends windows. Select what applications that you want to monitor and the criteria at which you want the system to alert you that there is a potential problem.

To see the Application Trend window:

1. Click one of the applications.
2. Click Selection.
3. Click Trend in the pull-down menu.

Where the System Trend window shows the overall system utilization, the Application Trend window shows information on an application over a period time. As with the System Trend window, you can use the Transfer pull-down menu to access the system, send commands to the system, receive more information about the application, and receive status information on the jobs, queues, and printers to name a few.

Figure 19. Application Detail Window

Figure 20. Application Trend Window
<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring resources using SDF and the AOC Graphic Interface</td>
<td><em>Automated Operations Control/MVS Operations</em></td>
</tr>
</tbody>
</table>
Chapter 4. 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, to help you analyze 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

There are various programs that you can use to monitor your network. You can use some of these programs to monitor only specific types of resources, for example, SNA (subarea and APPN) or LAN resources.

For Graphical Enterprise feature users, to monitor your entire network (consisting of hardware and software, SNA and non-SNA resources), use the graphical workstations.

Monitoring SNA (Subarea and APPN) Resources

To monitor and control the network, use a combination of the following:
- Status monitor
- Hardware monitor
- Session monitor
- NetView Graphic Monitor Facility host subsystem
- SNA topology manager
- User-written command lists
- Messages and message indicators
- Alerts
- The NetView Graphic Monitor Facility

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 APPN networks. In an SNA APPN 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 APPN network act as end nodes or entry points and will 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 APPN) 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 NMC and service points.

For Graphical Enterprise feature users: In general, the status of non-SNA resources can be monitored from a view on an NMC 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. In the following example:

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

The following responses are sent:

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

Using VTAM Commands (SNA Subarea, SNA APPN)

When VTAM activates a resource, it owns that resource. Session requests and alerts from that resource are delivered to the owning VTAM. The hierarchical structure used in the resource definition allows you to 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 as well as 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 on either the OPTIONS statement in DSIDMN 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 21 on page 63 is displayed.
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 APPN)" on page 66, and refer to the NetView online help.

Controlling Resources Defined to VTAM

You can use VTAM commands to control SNA (subarea and APPN) 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=nrulo505,inact`

2. To reactivate the resource, enter:
   
   `v net,id=nrulo505,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 APPN)

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:

```
applspen a01a701,act
```

The system responds with messages similar to the following:

```
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 E7FF38CE6EEB49AD7
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:

```
disg a04p1092
```

A panel similar to Figure 22 on page 67 is displayed.
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 23 on page 68 is displayed.

---

**Figure 22. 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 23 on page 68 is displayed.
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:
   \[ \text{rmtcmd lu=cnm02,act ncp2} \]
   
   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:
   \[ \text{rmtcmd lu=cnm02,dis ncp2} \]
   
   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 24**:

![Sample Output from the RMTSESS Command](image)

**Figure 24. 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.
**Label 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.

```
netid..domain_name/:your_id:command
```

**Note:** When an operator ID is specified in a label, NetView routes your command as EXCMD would.

When an `domain_name` is specified in a label, NetView routes your command as RMTCMD does.

**Label Usage**

Error conditions and messages, including authority checking, typically apply as if you had entered an RMTCMD or EXCMD command. Unlike RMTCMD or EXCMD, the label syntax causes correlated responses from the command to be returned to the originator. For further details, refer to the description of the NetView RMTCMD and EXCMD commands in the NetView online help.

You must enter a blank before any command, immediately after the colon. No blanks may be used within the label.

- **netid** Specifies the VTAM network ID that should be used for routing the command. If a value is specified, the netid value must be followed by a period (.). If you do not specify a value or enter an asterisk (*.), the default is to use the `netid` chosen by VTAM based on the value of `domain_name`.

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

- **operator_id** Specifies the name of the operator task where the command should process. If you specify a `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 will 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.

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:

```
* NTVE /AUTO1: QRYGLOBL TASK,VARS=*
! NTVE QRYGLOBL TASK,VARS=*
' NTVE
BNH031I NETVIEW GLOBAL VARIABLE INFORMATION
BNH031I COMMAND ISSUED AT: 05/23/96 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 25. Querying the Values of a Task Global Variable**

A label may be used anywhere a regular NetView command can be entered, except on the assembler interface described in "Designing Your Module" in *Tivoli NetView for OS/390: Customization: Using Assembler*.

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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENDTASK, REFRESH, RMTCMD command</td>
<td>NetView online help</td>
</tr>
<tr>
<td>Defining RMTCMD and RMTCMD Security</td>
<td><em>Configuring NetView for Your Environment</em> in <em>Tivoli NetView for OS/390 Installation: Configuring Additional Component</em></td>
</tr>
<tr>
<td>Security Definitions (RMTSEC and RMTSECUR parameters)</td>
<td><em>NetView Definition Statement Reference</em> in <em>Tivoli NetView for OS/390 Administration Reference</em></td>
</tr>
</tbody>
</table>

**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 LNMSPL, enter:
lan qnetwork status 1nmsp1

Figure 26 is displayed.
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=1nmsp1 adp list seg=0002

Figure 27 is displayed.
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=1nmsp1 adp query adp=10005a258085 seg=0002 attr=pcinfo

Figure 28 on page 73 shows the response.
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:
   
   `lan sp=lnmsp1 adp query adp=10005a258085 seg=0002 attr=attach`

   Figure 29 on page 74 shows the response.
Notice that the microcode level of the adapter as well as the adapter address of the nearest active upstream neighbor (NAUN) is shown.

Using the TOPOSNA Command

This section is only applicable to users who have installed the Graphical Enterprise feature.

To control the collection of SNA subarea and APPN 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

There are three categories of topology information:

Network topology

For APPN, 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 APPN, local topology consists of the node where the topology is being collected as well as 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 will be 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 ACCTSNA Command**

This section is only applicable to users who have installed the Graphical Enterprise feature.

To control the collection of APPC session and conversation accounting information, use the ACCTSNA command to start the accounting management control object (AMCO) manually. The agent cannot send any notifications and the accounting manager cannot retrieve data until the ACCTSNA START request completes.

**Retrieving Accounting Information**

There are three types of accounting information:

- Conversation endpoint data
- Intermediate session data
- Session endpoint data

To collect accounting information, use the ACCTSNA RETRIEVE command. For example, to collect conversation endpoint data accounting information from the agent residing at node APPNNT1.NODE1, enter:

```
acctsna retrieve node=appnnt1.node1,acctdata=convers
```

**Sending Accounting Data Automatically**

You can setup automatic notification to the accounting manager based on thresholds at the APPN topology and accounting agent. The agent notifies the accounting manager when the threshold has been exceeded, and the accounting manager automatically retrieves this data when it receives a notification. This threshold is defined using the ACCTSNA SETDEFS command. For example, to cause a notification to be sent to the accounting manager when the buffer is 75% full, enter:
Displaying the Status of an Accounting Agent
You can display the status of the data collection at an agent using the ACCTSNA DISPLAY command. For example, to display the status of conversation endpoint accounting data collection at APPNNET1.NODE1, enter:
acctsna display,node=appnnet1.node1,acctdata=convers

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN Commands</td>
<td>IBM Local Area Network Host Information</td>
</tr>
<tr>
<td>SNATM capabilities</td>
<td>Tivoli NetView for OS/390 SNA Topology Manager and APPN Accounting Manager Implementation Guide</td>
</tr>
<tr>
<td>LAN command list, RUNCMD command, ACCTSNA commands, TOPOSNA commands</td>
<td>NetView online help</td>
</tr>
</tbody>
</table>

Using the Session Monitor (SNA Subarea, SNA APPN)

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 APPN) 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, as well as SNA APPN 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 appear to 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 APPN, 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 APPN route data
- APPN 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 30 on page 77 for an overview of the sources of session monitor data.
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. Once 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, an invalid data count field (DCF)
- 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 monitorKEEPDISC 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 "Defining the Data Logs" in the Tivoli NetView for OS/390 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. The session monitor allows you 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
- APPN 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
  - 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 [Defining NetView Components] in the [Tivoli NetView for OS/390 Installation]. 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 APPN sessions, a session monitor must be available at the Interchange node.

Session Monitor Scenarios

The following scenarios 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 help nldm 'term', where term specifies one or more words of the field. The following scenarios illustrate:

- An LU-LU session for an SNA subarea network
- A CP-CP session for an SNA APPN network
- An LU-LU session for an SNA APPN or mixed network
- A SNA Session Through an APPN Network (DLUR/DLUS)
- An LU-LU session for an SNA APPN 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 31 on page 81 is displayed.
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 32 is displayed.

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.

**Figure 31. Session Monitor Main Menu**

**Figure 32. Resource Name List Panel**
3. Locate the desired 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 33 is displayed.

Figure 33. Session List Panel

This panel lists the active and terminated 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 34 on page 83 is displayed.
This panel shows how each LU is physically connected to its own subarea. Note that even though AR (APPN Route) is listed as an option, LU-LU sessions across pure SNA subarea networks do not have APPN route data. If you choose this option, you will receive a message stating that APPN 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 35 is displayed:

**Figure 34. Session Configuration Data Panel**

This panel shows how each LU is physically connected to its own subarea. Note that even though AR (APPN Route) is listed as an option, LU-LU sessions across pure SNA subarea networks do not have APPN route data. If you choose this option, you will receive a message stating that APPN 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 35 is displayed:

**Figure 35. 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 at the right margin.

6. 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.

7. 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 will not be able to access primary or secondary trace data, the PT and ST options, from the Session Configuration Data panel. The KEEPPIU count is found in the AAUPRLMLP member (used to initialize the session monitor).

Depending on the session type, the following information is displayed:

<table>
<thead>
<tr>
<th>Session type</th>
<th>Information code</th>
<th>Information description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LU-LU, CP-CP</td>
<td>BIND</td>
<td>Bind</td>
</tr>
<tr>
<td>SSCP-LU</td>
<td>ACTLU</td>
<td>Logical unit</td>
</tr>
<tr>
<td>SSCP-PU</td>
<td>ACTPU</td>
<td>Physical unit</td>
</tr>
<tr>
<td>SSCP-SSCP</td>
<td>ACTCDRM</td>
<td>Cross-domain resource manager</td>
</tr>
</tbody>
</table>

For an LU-LU session, a panel similar to Figure 36 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 ---------------
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 36. 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.

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

8. Enter `r` or press the PF key with a value of RETURN (NetView default is PF3) to return to the Session Configuration Data panel.

9. Enter `er` to display the explicit route for the session. A panel similar to Figure 37 is displayed.

Figure 37. 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.

10. Press the PF key with a value of RETURN (NetView default is PF3) to return to the Session Configuration Data panel.

11. Enter `vr` to display the virtual route for the session. A panel similar to Figure 38 on page 86 is displayed.
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.

12. 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 39 on page 87).
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 APPN Network**

To monitor a CP-CP session for an SNA APPN network:

1. Type `nl_dm` at the command line to access the session monitor main menu. A panel similar to Figure 40 on page 88 is displayed:
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 41** is displayed.

![Figure 41. Resource Name List Panel](image)

3. Locate the desired 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.
command line to display the list of sessions. A panel similar to Figure 42 is displayed.

**Figure 42. Session List Panel**

This panel lists the active and terminated 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 43 is displayed.

**Figure 43. 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 80.

5. Enter `ar` to display the APPN route configuration panel. A panel similar to Figure 44 is displayed.

![Figure 44. APPN Session Route Configuration Panel](image)

This panel displays APPN nodes and connecting groups in an APPN session path.

**Typical LU-LU Session for an SNA APPN Network**

Complete the following steps to monitor an LU-LU session for an SNA APPN 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 45 on page 91](#) is displayed.
This panel lists the active and terminated 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 45 is displayed.

Figure 45. Session List Panel

This panel lists the active and terminated 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 46 is displayed.

Figure 46. Session Configuration Data Panel

See "Typical LU-LU Session for an SNA Subarea Network" on page 80 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 47 is displayed.

<table>
<thead>
<tr>
<th>NLD.M.VR</th>
<th>VIRTUAL ROUTE STATUS</th>
<th>PAGE 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAIN: CNM99</td>
<td>NETID: NETA</td>
<td>DOMAIN: CNM19</td>
</tr>
<tr>
<td>ORIGIN</td>
<td>WINDOW SIZE: MIN 1 CUR 3 MAX 3</td>
<td>DESTINATION</td>
</tr>
<tr>
<td>NAME: A04862</td>
<td>SEQ NUMBER: SENT RECEIVED</td>
<td>NAME: A03A62</td>
</tr>
<tr>
<td>SA: 0000004</td>
<td>SAMPLE 1: 0DC8 0DD0</td>
<td>SA: 0000003</td>
</tr>
<tr>
<td>PU TYPE: 4</td>
<td>VR 00 TP 00</td>
<td>PU TYPE: 4</td>
</tr>
<tr>
<td>INBND PIU POOL CURRENT: 0</td>
<td>&lt;&lt;&lt;--------</td>
<td>INBND PIU POOL CURRENT: 0</td>
</tr>
<tr>
<td>LIMIT: 10</td>
<td>SEQ NUMBER: RECEIVED SENT</td>
<td>LIMIT: 10</td>
</tr>
<tr>
<td>STATUS: 0000</td>
<td>SAMPLE 1: 0DC6 0DCE</td>
<td>STATUS: 4008</td>
</tr>
</tbody>
</table>

Figure 47. Virtual Route Status Panel

A virtual route (VR) is a logical data path from one resource to another. For an SNA APPN 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 APPN network meet. OFC requests provide flow control data in the primary direction at the point where the SNA subarea and SNA APPN 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 48 on page 93:
If you enter dfc (to display destination flow control data), a panel similar to Figure 49 is displayed:

Figure 48. Flow Control Data Panel (Origin)

If you enter dfc (to display destination flow control data), a panel similar to Figure 49 is displayed:

Figure 49. Flow Control Data Panel (Destination)

Flow control data is maintained for low-entry networking (LEN) and APPN 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 there is no connecting virtual route, 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).

- Look at the PACING DATA to determine if there are

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 vr to display the virtual route for the session.

7. Enter ar to display the APPN route configuration panel. A panel similar to Figure 50 is displayed.

![APPN Session Route Configuration Panel with Subarea Number from Primary Side](image)

In the SNA APPN environment, there is no limit to the number of APPN subnetworks that a session can flow through. 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 there are additional RSCVs 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 APPN 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** will be displayed. The corresponding PAR and SAR options are not displayed for these situations.

8. Enter **par** to scroll in the primary direction. A panel similar to Figure 51 is displayed.

![Figure 51. APPN Session Route Configuration Panel with Subarea Number from Secondary Side and OAR Prompt](image)

**Note:** The following paragraphs explain some of the abbreviations that appear on the screen:

The terms PRI-SA (see Figure 50 on page 94) and SEC-SA (Figure 51) indicate the subarea number that is associated with an APPN 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 will 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 APPN 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 51, but which shows the RSCV that the outboard CP reports.

For details about these terms, see the online help.
SNA Session through an APPN Network

Complete the following steps to monitor the SSCP-PU session that connects through an APPN 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 is new for NetView V3R1.

1. Enter `sess ps2dl2pa` from the session monitor command line or `nldm sess ps2dl2pa` from the NCCF command line to access the session list for resource ps2dl2pa. A panel similar to Figure 52 is displayed.

```
NLDM.SESS PAGE 1
SESSION LIST
NAME: PS2DL2PA
DOMAIN: CNM09

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 52. Session List Panel**

This panel lists the active and terminated 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 APPN 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 53 on page 97 is displayed.
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 APPN 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 APPN 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 APPN 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 APPN 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 54 on page 98 is displayed.
VTAM can take over or give back control of the NCP providing boundary function for some sessions. When there are takeovers and givebacks, the Session List panel can display Takeover/Giveback statuses (as shown here) as well as active and terminated status (as shown in "Typical LU-LU Session for an SNA Subarea Network" on page 80). Possible takeover/giveback notifications are:

** 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 will be 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 will be 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 panel, as well as other session monitor panels, see "Typical LU-LU Session for an SNA Subarea Network" on page 80, "Typical CP-CP Session for an SNA APPN Network" on page 87, and "Typical LU-LU Session for an SNA APPN Network" on page 90.

Due to 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 55 is displayed.

Check the following:

- The session count. If the session count is 0, there are no active sessions between the given resource types. On Figure 55, there are two active CP-CP sessions, 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.

### Table: Reference:

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description of the output</td>
<td>“Tuning for the Session Monitor” in the Tivoli NetView for OS/390 Tuning Guide</td>
</tr>
<tr>
<td>displayed from the</td>
<td></td>
</tr>
<tr>
<td>SESSMDIS command</td>
<td></td>
</tr>
<tr>
<td>NLDM panel help</td>
<td>NetView Online Help</td>
</tr>
<tr>
<td>NLDM panel Field Level Help</td>
<td>NetView Online Field Level Help help nldm 'term'</td>
</tr>
<tr>
<td>Configuration examples</td>
<td>&quot;Appendix C. Interpreting Session Data&quot; on page 393</td>
</tr>
<tr>
<td>Setting up the session</td>
<td>&quot;Defining NetView Components&quot; in the Tivoli NetView for OS/390 Installation: Configuring Additional Components and &quot;Using Session Monitor Filters” on page 195</td>
</tr>
<tr>
<td>monitor</td>
<td></td>
</tr>
</tbody>
</table>

### 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 NMC is not available.

The status monitor, like VTAM, groups resources into major and minor nodes. Figure 56 shows an example of the hierarchy that the status monitor uses. The term higher node refers to the next node up in the hierarchy. For example, in

![Status Monitor Hierarchy Diagram]

Figure 56. Status Monitor Hierarchy

Figure 56 shows 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. These states can be any of the following:

**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 6 shows how the VTAM states are generally mapped to the status monitor states:

<table>
<thead>
<tr>
<th>VTAM Status Code</th>
<th>VTAM Status</th>
<th>Status Monitor Status</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>00xx</td>
<td>Inactive</td>
<td>Inactive (INACT)</td>
<td>The exceptions are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0000 (Reset) is mapped to OTHER. This is a substate of the VTAM Inactive status and is handled differently because of multiple ownership considerations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 0002 (Released) is mapped to OTHER. This is a substate of the VTAM Inactive status and is handled differently because of multiple ownership considerations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• If the resource has been selected for re-activation by using the STATOPT statement, it is mapped to MONIT.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>01xx</td>
<td>Pending</td>
<td>Pending (PENDING)</td>
<td></td>
</tr>
<tr>
<td>02xx</td>
<td>Connectable</td>
<td>Other (OTHER)</td>
<td></td>
</tr>
<tr>
<td>03xx</td>
<td>Reactivate</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>04xx</td>
<td>Pending</td>
<td>Pending (PENDING)</td>
<td></td>
</tr>
<tr>
<td>05xx</td>
<td>Active</td>
<td>Active (ACTIVE)</td>
<td></td>
</tr>
<tr>
<td>06xx</td>
<td>Routable</td>
<td>Other (OTHER)</td>
<td></td>
</tr>
</tbody>
</table>

**Setting Up the Status Monitor**

If the status monitor does not work as described in the previous section, check to see that:

1. Resources and relationships have been defined between resources. You can define these relationships using STATOPT statements in VTAMLST. In the following example:

   ```plaintext
   LINE01  LINE  ADDR=(001,FULL),
           SPEED=56000
           STATOPT=('LINE020',NOMONIT)
   ```
resource LINE01 is assigned the description LINE020 and is excluded from automatic reactivation (NOMONIT).

2. The preprocessor, CNMNDEF, which reads the VTAMLST members and creates a member DSINDEF in DSIPARM, has been run. DSINDEF is used by the status monitor initialization process.

3. The status monitor has been defined. This can be done in the status monitor initialization member sample DSICNM. In this sample, you can specify:
   - Command lists available for execution 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 57 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/0K ......2 ...... ...... ...... ......6 ......1
......599 LINES ......2 ...... ...... ...... ......343 ......1
......599 LUS/CLUSTERS ......2 ...... ...... ...... ......844 ......13
......3260 LUS/TERMS ...... ...... ...... ...... ...... ...... ......28
......1 SWITCHED/XCA ......1 ...... ...... ...... ...... ...... ......
......2 PU/XCA LINE ...... ...... ...... ...... ...... ...... ......2
......2 LU/XCA PU ...... ...... ...... ...... ...... ...... ......2
......4 LOCAL MAJ NDS ......2 ...... ...... ...... ...... ......2
......3 PUS ...... ...... ...... ...... ...... ...... ......
......11 LUS/TERMS ...... ...... ...... ...... ...... ...... ......
......2 APPL MAJ NDS ......2 ...... ...... ...... ...... ......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 57. 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 377.
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 will switch 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 will see one or more screens similar to the one shown here:

```
Figure 58. 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 as follows:

```
   b. Type any character except a blank in the space immediately before the field you just located. For example:
c. Press Enter.
A panel similar to Figure 59 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 | ? CNM09PPPT  APPLICATION  | ? A011  APPLICATION
? LUS/TERMS | ? A  APPLICATION  | ? A012  APPLICATION
? CD RMS | ? 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
? VARY ACT | ? A008  APPLICATION  | ? CNM09006  APPLICATION
CMD==> TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
```

Figure 59. 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 60 on page 105 is displayed.
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 61 on page 106 is displayed.
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 62.

Figure 61. Domain Status Detail (Description) Panel Containing Activity and Analysis Information

Figure 62. Domain Status Detail (Description) Panel Showing only Active Applications
The DISPLAY menu on the upper left side of the panel allows you 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.

The DETAIL FORMAT menu on the lower left side of the panel allows you to ask for more status information about the resources listed on this panel. You can view an analysis of the resources’ status by typing any character over the ? field in front of ANALYSIS and pressing Enter. For resources types of APPLICATIONS and APPL MAJ NDS there is an ACTIVITY option, which lets you display application message traffic information. You can view information about the applications’ activity 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 63 is displayed.

7. Replace the question mark in front of ANALYSIS with any character and press Enter to view analysis information. A panel similar to Figure 64 on page 108 is displayed.
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 there is a change in the status of a resource. 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 do the following:

- Entering BROWSE NETLOGA
- Pressing a PF key set to BROWSE NETLOGA (such as the NetView default PF setting of PF5)
- Selecting 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 65 is displayed.

![Figure 65. Browse Network Log Panel](image)

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network log message format</td>
<td><a href="#">Appendix A. Message Format</a> on page 375</td>
</tr>
<tr>
<td>STATMON, CLRSTATS command</td>
<td>NetView online help</td>
</tr>
<tr>
<td>STATOPT statement syntax</td>
<td><a href="#">NetView Definition Statement Reference</a> in the Tivoli NetView for OS/390 Administration Reference</td>
</tr>
<tr>
<td>Defining the status monitor</td>
<td><a href="#">Defining NetView Components</a> in the Tivoli NetView for OS/390 Installation: Configuring Additional Components</td>
</tr>
</tbody>
</table>

**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 **Q** 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 will attempt to reactivate the resource every minute until the resource status is no longer INACTIVE. The resource will be 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 on a per resource basis. When global monitoring is set off, status monitor will 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 "NetView Definition Statement Reference" in the Tivoli NetView for OS/390 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. OS/2 ROPS, for instance, provides support for RUNCMD.

| Topic: Unknown service point resources | Reference: 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 execution by one of the service point applications. Following is an example of 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: RUNCMD command | Reference: NetView online help |

**Setting Up Service Points**

There are two types of transport than 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. Following is an example of an NCP configuration definition:

```plaintext
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,
   PUTFYPE=2,
   ISTATUS=ACTIVE
```

To transfer files between the NetView program and a workstation, add a host definition similar to the following for the CICS/DDM program (the following definitions are specifically for the host side of NetView/PC and an AIX service point).

```plaintext
NVIXL621 LU LOCADDR=1,
   ISTATUS=ACTIVE,
   PACING=1,
   MODETAB=NVPCTAB,
   DLOGMOD=NVPCMODE
```

Following is an example of a VTAM logmode definition:

```plaintext
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'060000000000000000002F0F0',
   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 logomode at the Group level. Following is an example of an NCP configuration:

```plaintext
NTSDLG Group DIAL=NO,
   LNCTL=SDLCL,
   REPLYTO=3,
   RNRLIMIT=3,
   TESTTO=1,
   TYPE=NCI,
   TYPE=TRN,
   TYPE=ADV,
   VIRTUAL=NO,
   ISTATUS=INACTIVE

DLOGMOD=M3SDLCQ,
MODETAB=AMODETAB,
USSTAB=AUSSTAB,
V PACING=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. Following is an example 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'06020000000000000002F00',
   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:
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:** The IBM LAN NetView Tie program allows you to 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
```

**Reference:**

<table>
<thead>
<tr>
<th>Topic</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing and configuring the Tie Program</td>
<td><em>IBM LAN NetView Tie Administration Guide</em></td>
</tr>
<tr>
<td>Tie Program commands</td>
<td><em>IBM LAN NetView Tie Getting Started</em></td>
</tr>
<tr>
<td>Managing hardware and software resources on a LAN using the IBM LAN NetView Manage program</td>
<td><em>IBM LAN NetView Manage Administration Guide</em></td>
</tr>
</tbody>
</table>

**Attaching to a NetView for AIX Service Point:** The AIX NetView Service Point program enables the host program and Service Point applications, including the NetView for AIX program, to exchange SNA MS major vectors over SNA services. The NetView for AIX program supplies the `spappld` daemon as a service point application and starts it as a part of the NetView for AIX program initialization process, enabling the NetView for AIX program to process the contents of the RUNCMD in the Simple Network Management Protocol (SNMP) environment.

On an IBM RISC System/6000®, use the System Management Interface Tool (SMIT) to set up and customize the Service Point. You can specify the logical unit profile that will be used to define the type of transport (SSCP-PU or MDS) to be used between the AIX Service Point and the NetView program.
Controlling TCP/IP Resources Attached to a Downstream NetView for AIX
Program: You can use the NetView program in conjunction with the AIX NetView Service Point program and Service Point applications including the NetView for AIX program to manage TCP/IP networks. The AIX NetView Service Point program acts as a bridge between the NetView for AIX program and the host, routing RUNCMD commands from the host to a specific NetView for AIX program. The service point application that resides on that NetView for AIX program then processes the contents of the RUNCMD.

The following example shows how to send the FINDROUTE command to a service point application (A1234567) registered with the AIX NetView Service Point program (NVSP). The FINDROUTE command is used to determine whether there is a route between two internet devices, router1 and router2, that supports SNMP.

```
runcmd sp=nvsp, appl=a1234567, findroute router1 router2
```

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetView Service Point Program</td>
<td>AIX SystemView® NetView for AIX and the Host Connection</td>
</tr>
<tr>
<td>Installing a Service Point</td>
<td>AIX NetView Service Point Installation, Operation and Programming Guide</td>
</tr>
</tbody>
</table>

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 on OS/2.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developing REXX executable files and command lists to use SPA Router and ROP Services and setting up a SPA Router and ROP Services</td>
<td>Communications Manager/2 Service Point Application Router and Remote Operations Service Guide</td>
</tr>
</tbody>
</table>

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.
Using the Automation Table to Control Resources Attached through Service Points

The NetView for AIX program, NetView/390 MultiSystem Manager, LAN Network Manager program, and so on 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 NetView/6000 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.

```plaintext
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;
END;
```

The REXX command list looks like this:

```plaintext
/* */
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 AIX NetView Service Point program and the service point application name from the SNA alert to create a RUNCMD command.

---

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 67 on page 117](#) is displayed.
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 68 is displayed.

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 69 is displayed.

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 70 is displayed.

   **Figure 69. 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 70 is displayed.

   **Figure 70. 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 71 on page 119 is displayed.
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).

**Figure 71. 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 5. Managing Network and System Status

To manage the status of your network from a workstation, use the NetView management console or the System Operation Graphical Interface (previously called AOC) 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:

- Operations Planning and Control/ESA (OPC/ESA)
- Performance reporter for MVS
- NetView Performance Monitor (NPM)
- NTune
- Automated Operations Network (AON)
- System Operations, previously known as Automated Operations Control (AOC)
  - CICS Automation Feature
  - IMS Automation Feature

Note: These products are not shipped with NetView.

Using Operations Planning and Control/ESA

Using OPC/ESA to plan and control your production workload according to your business schedules, you can:

- Define the deadlines, order of processing, and resource requirements of your production batch jobs and started tasks. This information is used by OPC/ESA to automatically start your processing in the correct order. When conflicts arise, such as when there is more processing to be started than there are resources to accommodate the processing, OPC/ESA 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 when:
  - 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 executing for longer than expected
  - Processing is getting late and deadlines are in jeopardy
  - An OPC subtask fails
  - A defined threshold has been reached on the OPC queue
- Provide a hot standby facility to maximize the availability of the controlling functions in an MVS/ESA 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 there is an MVS failure or a communications outage.

Using Performance Reporter

The Performance Reporter for MVS accepts the output of the session monitor to create a logical view of your network’s layout. 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
VTAMs 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, 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.

| Setting up the Session Monitor to log data to the external log (SMF) | "Defining NetView Components" in the Tivoli NetView for OS/390 Installation: Configuring Additional Components |

**Using NetView Performance Monitor**

You can use the NetView Performance Monitor (NPM) 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 NPM, 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

| Using NPM and NetView to solve network problems | "Sluggish Network Performance (NPM)" on page 355 |

**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 enables you to 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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using NTune</td>
<td>NTune User’s Guide</td>
</tr>
<tr>
<td>Using NTuneNCP</td>
<td>NTuneNCP Reference</td>
</tr>
</tbody>
</table>
Chapter 6. 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. These connections include:

- 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.

For Graphical Enterprise feature users: you can use the NetView management console (NMC) 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 NMC to monitor hardware problems, see "Chapter 3. Monitoring and Controlling Your Network from a Workstation" on page 53.

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 recommends actions 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 194). 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 NMC to display the GMFALERT records, which represent resources monitored by NMC.

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 has been resolved or a resource has been 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 NMC.

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 NetViews or entry point nodes.

**Figure 72** provides an illustration of hardware monitor data collection.
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 due to 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 has been resolved, are also stored on the database as events.

GMFALERTs

GMFALERT records represent events that pertain to resources monitored by NMC. If NMC is not installed, the GMFALERT records, which are a subset of NMC event report records, are recorded in the hardware monitor database. The alert history window of NMC 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 "Modifying Network Asset Management Command Lists" in the Tivoli NetView for OS/390 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 methods for forwarding alerts are:
  - The primary method makes use of 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. It is recommended that you use the ROUTE filter for forwarding alerts to the focal point. See [Network Management for Multiple Domains](#) on page 144 for more information.

An alert appears 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 7 provides a list of event types and their corresponding abbreviations and codes.

<table>
<thead>
<tr>
<th>Abbr.</th>
<th>Event Type</th>
<th>Description</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVAL</td>
<td>Availability</td>
<td>The availability status of the reported resource has changed.</td>
<td>09</td>
</tr>
<tr>
<td>BYPS</td>
<td>Alert bypass</td>
<td>A loss of availability has been 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.</td>
<td>14</td>
</tr>
<tr>
<td>CUST</td>
<td>Customer application generated</td>
<td>A program that does not have an IBM order number generated the problem record.</td>
<td>05</td>
</tr>
<tr>
<td>DLRC</td>
<td>Delayed recovery</td>
<td>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.</td>
<td>0F</td>
</tr>
<tr>
<td>ENV</td>
<td>Environment</td>
<td>A physical environmental problem has occurred.</td>
<td>0B</td>
</tr>
<tr>
<td>HELD</td>
<td>Held alert flag</td>
<td>An error condition was detected earlier, but the record was not sent at the time because there is no session 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.</td>
<td>--</td>
</tr>
<tr>
<td>IMPD</td>
<td>Impending problem</td>
<td>Availability to the user is about to be lost.</td>
<td>11</td>
</tr>
<tr>
<td>IMR</td>
<td>Intensive Mode Recording</td>
<td>An error record resulted from the user invoking intensive mode recording, a feature of the NCP. When IMR is invoked, an error record is generated each time the NCP goes through an error retry.</td>
<td>08</td>
</tr>
<tr>
<td>INST</td>
<td>Installation</td>
<td>A system definition or an incompatibility between components has been reported.</td>
<td>0C</td>
</tr>
<tr>
<td>Abbr.</td>
<td>Event Type</td>
<td>Description</td>
<td>Code</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>INTV</td>
<td>Intervention required</td>
<td>Intervention of a human operator is needed for corrective action.</td>
<td>04</td>
</tr>
<tr>
<td>NTFY</td>
<td>Notification of status change</td>
<td>Availability to the user is about to be lost. An important change of component, system, or network status requiring operator notification is required.</td>
<td>0A</td>
</tr>
<tr>
<td>PAFF</td>
<td>Permanently affected resource</td>
<td>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.</td>
<td>10</td>
</tr>
<tr>
<td>PERF</td>
<td>Performance</td>
<td>A recognized measurement of performance, such as response time, has exceeded a determined threshold.</td>
<td>03</td>
</tr>
<tr>
<td>PERM</td>
<td>Permanent error</td>
<td>Availability to the user is lost unless there is external intervention to the reporting product.</td>
<td>01</td>
</tr>
<tr>
<td>PROC</td>
<td>Operation or procedure</td>
<td>A requested function cannot be performed due to an operational or procedural error.</td>
<td>0D</td>
</tr>
<tr>
<td>REDL</td>
<td>Redundancy lost</td>
<td>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.</td>
<td>15</td>
</tr>
<tr>
<td>RSLV</td>
<td>Resolve major vector</td>
<td>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.</td>
<td>--</td>
</tr>
<tr>
<td>RSNT</td>
<td>Resent alert flag</td>
<td>The alert has been 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.</td>
<td>--</td>
</tr>
<tr>
<td>SCUR</td>
<td>Security</td>
<td>A report of an incident that can indicate a possible security violation has been detected.</td>
<td>0E</td>
</tr>
<tr>
<td>SNA</td>
<td>SNA summary</td>
<td>A record containing SNA summary error counters. The record is normally the result of a NetView hardware monitor solicitation.</td>
<td>07</td>
</tr>
<tr>
<td>TEMP</td>
<td>Temporary or recoverable error</td>
<td>A momentary loss of availability is noticeable by the user, but is recovered from without intervention external to the reporting product.</td>
<td>02</td>
</tr>
<tr>
<td>USER</td>
<td>End user generated</td>
<td>A problem record initiated by a terminal operator.</td>
<td>06</td>
</tr>
<tr>
<td>UNKN</td>
<td>Unknown</td>
<td>The severity of the alert cannot be assessed.</td>
<td>12</td>
</tr>
</tbody>
</table>
Table 7. Event Types with Abbreviations and Codes (continued)

<table>
<thead>
<tr>
<th>Abbr.</th>
<th>Event Type</th>
<th>Description</th>
<th>Code</th>
</tr>
</thead>
</table>

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 has been 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.

Recording two event records in this situation allows you to 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 focal point’s ESREC and AREC recording filters are blocked. For NetView-forwarded alerts, this would require 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 "The Automation Table" in [Tivoli NetView for OS/390 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, as well as local (non-forwarded) alerts. NetView V3 now 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

This section applies to NetView features other than the Unattended feature.

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 quote 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 325. 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 177.

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 73 is displayed.

   ![Figure 73. Hardware Monitor Main Menu](image)

2. Select option 1 to monitor the alerts. A panel similar to Figure 74 on page 132 is displayed.
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 appears 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAIN</td>
<td>The name of the domain from which the alert originated</td>
</tr>
<tr>
<td>RESNAME</td>
<td>The name of the device or other resource which is the one most affected by the event that originated the alert</td>
</tr>
<tr>
<td>TYPE</td>
<td>An abbreviation of the resource type</td>
</tr>
<tr>
<td>TIME</td>
<td>The time the alert was recorded on the database</td>
</tr>
<tr>
<td>ALERT DESCRIPTION:PROBABLE CAUSE</td>
<td>An abbreviated message describing the error that occurred and the probable cause</td>
</tr>
</tbody>
</table>

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 75 on page 133** is displayed.
The Alerts-Static panel freezes the current contents of the Alerts-Dynamic panel. It does not allow new alerts to appear 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**  This option lets you display all the alerts recorded in the database. You can then press the Enter key to page forward through the alerts.

**SEL#**  This option lets you view the recommended actions for a specific alert.

**SEL# M**  This option lets you 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**  This option lets you 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**  This option lets you 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 12 on page 42 and Figure 58 on page 103.

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 76 is displayed.

![Figure 76](image)

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 (Dnnn, Ennn, Innn, or Rnnn) 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 Dnnn actions have associated NetView-supplied panels, Ennn, Innn, and Rnnn actions do not have NetView-supplied panels. However, the NetView program allows you to 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 "Modifying and Creating Online Help Information" in the Tivoli NetView for OS/390 Customization Guide.

5. Enter **d** to display event detail information for the alert. A panel similar to Figure 77 on page 135 is displayed.
The Event Detail panel displays additional information about the event that generated the alert. There are a number of distinct formats for event detail data. 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 141.

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 78 is displayed.

![Figure 78. Hardware Monitor Main Menu](image)

2. Select option 1 to monitor the alerts. A panel similar to Figure 79 is displayed.

![Figure 79. Alerts-Dynamic Panel](image)

For a complete description of this panel, see “Investigating Non-Network Management Vector Transport Alerts” on page 131.
3. Press **Enter** to display the Alerts-Static panel. A panel similar to Figure 80 is displayed.

![Figure 80. Alerts-Static Panel](image)

For a complete description of this panel, see "Investigating Non-Network Management Vector Transport Alerts" on page 131.

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 81 is displayed.

![Figure 81. Recommended Action for Selected Event Panel](image)
5. Enter **d** to display event detail information for the alert. A panel similar to Figure 82.

```
Figure 82. 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 83 is displayed.

```
Figure 83. Event Detail, Continued
```

Note that for an NMVT alert, there is an additional **DM** option. This option lets you display more detail on the failure.
7. Enter **dm** to display the Event Detail Menu. A panel similar to Figure 84 is displayed.

```
Tivoli NetView  SESSION DOMAIN: CNM01  OPER1  04/12/99 16:43:59
NPDA-43R + EVENT DETAIL MENU +  PAGE 1 OF 1

CNM01 | GENALERT | GENALINE | C1 | GENACTRL |
      +--------+--+ +-+ +-+ +-+ +--------+
DOMAIN | COMC | IM |===LINE==| M | |=LINE--| X|-- | 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 84. Event Detail Menu, DM Option**

This panel lists available detailed information about the problem. In this example, there are five options. 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 138).

**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 143.
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 will always include an empty box. As you select lower and lower resource level displays, the pictorial representation will show the current level hardware connections.

When you select option 2, a panel similar to Figure 85 is displayed.

![Total Events Panel](image)

Figure 85. 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 86 on page 141 is displayed.
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 87 on page 142** is displayed.
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 88 is displayed.

### Figure 87. 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 88 is displayed.

### Figure 88. Total Statistical Data Panel, Level 2

This panel displays statistical record counts for the resources attached to the communication controller NTFFC.

<table>
<thead>
<tr>
<th>SEL#</th>
<th>TYPE</th>
<th>RESNAME</th>
<th>TRAFFIC</th>
<th>TEMPS</th>
<th>FROM</th>
<th>TO</th>
<th>E/T</th>
<th>MR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CHAN</td>
<td>NTCH05</td>
<td>N/A</td>
<td>0</td>
<td>N/A</td>
<td>0</td>
<td>00/00</td>
<td>00:00</td>
</tr>
<tr>
<td>2</td>
<td>CHAN</td>
<td>NTCH06</td>
<td>N/A</td>
<td>0</td>
<td>N/A</td>
<td>0</td>
<td>00/00</td>
<td>00:00</td>
</tr>
<tr>
<td>3</td>
<td>CHAN</td>
<td>NTCH07</td>
<td>N/A</td>
<td>0</td>
<td>N/A</td>
<td>0</td>
<td>00/00</td>
<td>00:00</td>
</tr>
<tr>
<td>4</td>
<td>CHAN</td>
<td>NTCH08</td>
<td>N/A</td>
<td>0</td>
<td>N/A</td>
<td>0</td>
<td>00/00</td>
<td>00:00</td>
</tr>
<tr>
<td>5</td>
<td>LAN</td>
<td>NTFFTRLN</td>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>04/06</td>
<td>12:32</td>
</tr>
<tr>
<td>6</td>
<td>LINE</td>
<td>J007V0D3</td>
<td>24</td>
<td>0</td>
<td>N/A</td>
<td>0</td>
<td>04/06</td>
<td>13:26</td>
</tr>
<tr>
<td>7</td>
<td>LINE</td>
<td>J007V0ED</td>
<td>28816</td>
<td>0</td>
<td>N/A</td>
<td>0</td>
<td>04/08</td>
<td>19:53</td>
</tr>
<tr>
<td>8</td>
<td>LINE</td>
<td>J007V001</td>
<td>20</td>
<td>0</td>
<td>N/A</td>
<td>0</td>
<td>04/06</td>
<td>13:26</td>
</tr>
<tr>
<td>9</td>
<td>LINE</td>
<td>J007V003</td>
<td>37</td>
<td>0</td>
<td>N/A</td>
<td>0</td>
<td>04/06</td>
<td>13:26</td>
</tr>
<tr>
<td>10</td>
<td>LINE</td>
<td>J007V03F</td>
<td>24</td>
<td>0</td>
<td>N/A</td>
<td>0</td>
<td>04/06</td>
<td>13:26</td>
</tr>
<tr>
<td>11</td>
<td>LINE</td>
<td>J007V05B</td>
<td>20</td>
<td>0</td>
<td>N/A</td>
<td>0</td>
<td>04/06</td>
<td>13:26</td>
</tr>
</tbody>
</table>
To display statistical record counts for the resource attached to line J007V0ED, enter 7. A panel similar to Figure 89 is displayed.

---

**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 IBM 586X 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.

<table>
<thead>
<tr>
<th>LPDA-1</th>
<th>LPDA-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote data terminal equipment interface test (DTE)</td>
<td>Line analysis test (LA)</td>
</tr>
<tr>
<td>Link status test (LS)</td>
<td>Modem and line status test (MLS)</td>
</tr>
<tr>
<td>Remote modem self-test (RST)</td>
<td>Transmit receive test (TRT)</td>
</tr>
</tbody>
</table>

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 90 on page 144 is displayed.
This panel 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 91 is displayed.

**Figure 90. Test Information Display Panel**

This panel 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 91 is displayed.

**Figure 91. LPDA-2 Command Menu Panel**
3. Select option 1 to review the modem and line status information. A panel similar to Figure 92 is displayed.

![Figure 92. Modem and Line Status, Panel 1](image)

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 93 on page 146.
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 95 is displayed:

Tivoli NetView SESSION DOMAIN: CNM01 OPER1 04/12/99 15:03:35
NPDA-2581 * TRANSMIT RECEIVE TEST-LINK SEGMENT LEVEL 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

Figure 95. 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 96 on page 148 is displayed.
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.

**Figure 96. 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.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using the ALT_ALERT statement to customize hardware monitor panels</td>
<td>Using Hardware Monitor Filters on page 194</td>
</tr>
</tbody>
</table>

**Network Management for Multiple Domains**

The hardware monitor allows an operator at a single central host domain to 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**. A focal point's sphere of control 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 97 on page 149** 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 each focal point's sphere—of—control.
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 98 for an example of an Alerts-Static panel.

This section does not apply to Unattended feature users.

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 appearing 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.

Figure 98. 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 appearing 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, as well as 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 NetViews or entry points.

The DOMAIN operand of the SVFILTER command allows the focal point operator to prevent alerts from specified entry point host domains from appearing on the operator’s Alerts-Dynamic, Alerts-Static, and Alerts-History panels.

The ROUTE option of the SRFILTER command allows the distributed host operator to 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 98 on page 149. 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 2q 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 there is no @ indicator.

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.


Distributed Database Retrieval

This section is only applicable to users who have installed the Graphical Enterprise feature and Procedural feature.

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's database, not the owning (distributed host) domain's database.
- Refer to the NPDA SDOMAIN command description in the NetView online help for restrictions that apply when distributed database retrieval is invoked 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 may 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 will be unable to retrieve the desired 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's 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 may 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’s domain name, not against the sending NetView entry point’s domain name. Therefore, if an operator enters SEL# M from the Alerts Static panel the event data may already be present on the focal point’s 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’s database rather than the focal point’s database.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using filters</td>
<td>Using Hardware Monitor Filters on page 193</td>
</tr>
<tr>
<td>Implementing filtering decisions using the XITCI exit</td>
<td>Implementing Filtering Decisions on page 297</td>
</tr>
</tbody>
</table>

**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 Tivoli NetView for OS/390 platform. By acting as a gateway between these platforms, the E/AS allows for centralized network management from any platform.

The E/AS is composed of 5 services. The Alert Adapter service converts Tivoli NetView for OS/390 alerts into Tivoli Enterprise Console events, and then forwards the events on to a Tivoli Enterprise Console (TEC). The Message Adapter service converts Tivoli NetView for OS/390 messages that originate from the automation table into TEC events, and then forwards the events on to a TEC. The Event Receiver service converts TEC events into Tivoli NetView for OS/390 alerts and forwards the alerts to the alert receiver PPI mailbox. The Alert to Trap service converts Tivoli Netview for OS/390 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 Tivoli NetView for OS/390 alerts and forwards the alerts to the alert receiver PPI mailbox.

The alert adapter service converts alert data into a TEC event through a customizable conversion rules file. 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 TEC event data through a customizable conversion rules file. This customization enables you to specify how various pieces of information from the message are encoded into the slot/value pairs that compose a TEC 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 Rreceiver service converts TEC events into NetView alerts via a customizable conversion rules file. 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 customizable conversion rules file. 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 via a customizable conversion rules file. 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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli NetView for OS/390 adapters</td>
<td>Tivoli Enterprise Console User’s Guide</td>
</tr>
</tbody>
</table>
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 will help you maintain a centralized, up-to-date inventory of system components and their relationships to one another, and will extend your 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 will be able to 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. This data enables you to control the terminal inventory of remote locations from a central site. Without this function, you would have to check all the terminals’ serial numbers by means of 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 means of a command list. In a multidomain network, VPD can also be collected at each domain and then forwarded to a focal point host. Once 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. These commands allow you to 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:

```vpadall config(atccon01),create,clist(vpdaact),add```

An example of the command list generated is shown in Figure 99.

```
BROWSE -- SYS1.COMMON.CLISTS(VPDACT)----------- LINE 0
COMMAND==>  
****************************************************************************** TOP OF DATA *******
 VPDACT CLIST
 &CONTROL ERR
 VPDLOGC START
  * RABQ48
  VPDPU ALL RABQ48 NOERROR
  * RABP48
  VPDPU ALL RABP48 NOERROR
  * SW3174
  VPDPU ALL P3174SW NOERROR
  * SW45A4XX
  VPDPU ALL P45A451C NOERROR
  * SWRAJ
  VPDPU ALL PCDRJ NOERROR
  * SWPC
  VPDPU ALL PCSW NOERROR
  * SWPSPC
  VPDLOGC END
&EXIT
****************************************************************************** BOTTOM OF DATA **********
```

Figure 99. 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'
   ```

156 User’s Guide
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

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining VPD to the NetView program</td>
<td>Refer to <a href="#">Tivoli NetView for OS/390 Installation: Configuring Additional Components</a>.</td>
</tr>
<tr>
<td>VPDALL and VPDCMD commands</td>
<td>NetView online help</td>
</tr>
</tbody>
</table>
Chapter 8. Controlling Remote Processors

The NetView program provides the ability to control remote processors. In normal operation, the NetView program communicates with a peer NetView program on the remote System/390 processor to issue commands and receive responses as well as unsolicited messages. When not available with distributed NetViews, 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 normal NetView-to-NetView communication can take over.

The NetView program can also control remote non-System/390 processors such as the AS/400 that support the host command facility (HCF) interface. Additionally, you can use the Distributed Console Access Facility (DCAF) from an OS/2 workstation such as NMC to control a remote workstation.

For information about setting NetView timer commands for remote systems and processors, see "Chapter 18. Scheduling Commands" on page 255.

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 18. Scheduling Commands" on page 255.

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 100 on page 160 is displayed.
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 101 is displayed.

**Figure 100. 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 101 is displayed.

**Figure 101. 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 102 is displayed.

![ISQETSR Target System LPAR Resource Updates: Dynamic](image)

**Figure 102. 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 103 on page 162 is displayed.
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 104 on page 163 is displayed.
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 OS/2 workstation, move the cursor to the name of the OS/2 workstation you want to monitor and press PF11. A panel similar to Figure 105 is displayed.

**Figure 104. Target System Hardware Summary Status Panel**

When you have reviewed the information, press PF3 to return to the Target System Summary panel.

**Figure 105. 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 OS/2 workstation port, move the cursor to the name of the OS/2 workstation and port letter you want to monitor and press PF10. A panel similar to Figure 106 is displayed.

<table>
<thead>
<tr>
<th>ISQEPRT</th>
<th>PS/2 Port Detail</th>
<th>Updates: Dynamic</th>
</tr>
</thead>
<tbody>
<tr>
<td>PS/2 Name : PS2NAM01</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LU Name : LU62AAB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port : 0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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: 03/18/96 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 106. 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 OS/2 workstation, move the cursor to the name of the OS/2 workstation and port letter you wish to monitor and press PF7. A panel similar to Figure 107 on page 165 is displayed.
If there is more data 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
TSCF enables you 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. The pass-through session enables you 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: Monitoring the status of the components in your TSCF configuration. | Reference: 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, OS/2-based LAN servers)
- Remote management of personal computers running OS/2, 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 running OS/2
- 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.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using the Distributed Console Access Facility</td>
<td><em>IBM Distributed Console Access Facility User’s Guide</em></td>
</tr>
</tbody>
</table>
Chapter 9. Controlling Operating System Resources

You can manage operating system resources through the NetView program, AOC/MVS, and OPC/ESA. 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, which enables you 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:

```
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, as well as the NetView subsystem router, must be started. (This only applies when MSGIFAC=USESSI, MSGIFAC=QUESSI, or MSGIFAC=QSSIAT is coded on the MVSPARM statement and the NetView subsystem is started with MSGIFAC=the same value.) Refer to "Preparing the MVS System" in the Tivoli NetView for OS/390 Installation: Getting Started.

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 the Tivoli NetView for OS/390 Installation and Administration Guide for more information.

When MVS Commands Fail

If you receive the following message:

**CNM560I**

The NetView subsystem router is not active. To start the NetView subsystem router, enter:

```
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:

```
s proccname
```

From the MVS console, where *proccname* 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 [Preparing the MVS System](#) in the *Tivoli NetView for OS/390 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**

There is no MVS console ID available. You can either ask your system programmer to define additional MVS consoles or you can enter:

```
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:

```
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:

```
getconid console=name
```

Where *name* is a different console than you first requested. The default console name is the same as your operator ID.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>MVS, GETCONID, RELCONID, DISCONID, SETCONID commands</td>
<td>NetView online help</td>
</tr>
<tr>
<td>Consoles</td>
<td><a href="#">Tivoli NetView for OS/390 Automation Guide</a></td>
</tr>
<tr>
<td>MVS System Commands</td>
<td>MVS/ESA System Commands Reference</td>
</tr>
<tr>
<td>Defining consoles</td>
<td>MVS/ESA Initialization and Tuning Reference</td>
</tr>
</tbody>
</table>

**Issuing JES2 Commands**

To issue a JES2 command, enter MVS from the NetView command facility, followed by a valid JES2 command. For example, to:
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

Do the following:
1. To display the status of prt15, enter:
   mvs $du,prt15
2. To drain prt15, enter:
   mvs $pprt15
3. To interrupt the job printing on prt15, enter:
   mvs $iprt15

Issuing JES3 commands

You can issue commands to JES3 from the NetView program. Figure 108 shows how to issue the JES3 *I S command to display the status of JES3 system resources.

![Figure 108. Issuing a JES3 Command from the NetView Program](image-url)

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:
A full–screen panel similar to Figure 109 is displayed.

Figure 109. 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:

@d a,all

A full–screen panel similar to Figure 110 on page 173 is displayed.
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:

```
jes2 du,all
```

A full-screen panel similar to Figure 111 on page 174 is displayed.
The ALL operand displays detailed information about all local JES2 controlled devices, active remote devices, and internal readers.

**Figure 111. 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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>MVS command</td>
<td>NetView online help</td>
</tr>
<tr>
<td>Setting up, displaying, and changing the AOC/MVS automation control file</td>
<td>Automated Operations Control/MVS Customization and Programming and Automated Operations Control/MVS Operations</td>
</tr>
<tr>
<td>Assigning automation operators for AOC/MVS messages</td>
<td>Automated Operations Control/MVS Operations</td>
</tr>
<tr>
<td>Managing the status of MVS resources</td>
<td>Automated Operations Control/MVS Operations</td>
</tr>
<tr>
<td>Issuing MVS and JES2 commands from AOC/MVS</td>
<td>Automated Operations Control/MVS Operations</td>
</tr>
</tbody>
</table>

**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 your enterprise's business processing needs. 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 resource 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:
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 which could not 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 there is a queue for JES initiators, 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 will be dismounted at step end if there are outstanding device requests. 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.
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using and Maintaining the Network Log</td>
<td>206</td>
</tr>
<tr>
<td>Displaying the Network Log</td>
<td>206</td>
</tr>
<tr>
<td>Log Browse Filtering</td>
<td>207</td>
</tr>
<tr>
<td>Switching the Network Log</td>
<td>209</td>
</tr>
<tr>
<td>Using Browse</td>
<td>209</td>
</tr>
<tr>
<td>Creating and Displaying NetView Trace Data</td>
<td>210</td>
</tr>
<tr>
<td>Creating and Displaying Command Facility Trace Data</td>
<td>210</td>
</tr>
<tr>
<td>Creating and Displaying Session Monitor Trace Data</td>
<td>210</td>
</tr>
<tr>
<td>Creating and Displaying PPI Trace Data</td>
<td>211</td>
</tr>
<tr>
<td>Maintaining the Hardware Monitor Database</td>
<td>211</td>
</tr>
<tr>
<td>Switching Primary and Secondary Databases</td>
<td>211</td>
</tr>
<tr>
<td>Controlling the Amount of Data Retained in the Hardware Monitor Database</td>
<td>212</td>
</tr>
<tr>
<td>Removing Unwanted Data from the Hardware Monitor Database</td>
<td>212</td>
</tr>
<tr>
<td>Collecting Hardware Monitor Data in an SMF Data Set</td>
<td>212</td>
</tr>
<tr>
<td>Using and Maintaining the 4700 Support Facility Database</td>
<td>213</td>
</tr>
<tr>
<td>Switching Primary and Secondary Databases</td>
<td>213</td>
</tr>
<tr>
<td>Removing Unwanted Data from the 4700 Support Facility Database</td>
<td>213</td>
</tr>
<tr>
<td>Reorganizing the 4700 Support Facility Database</td>
<td>213</td>
</tr>
<tr>
<td>Using and Maintaining the Session Monitor Database</td>
<td>214</td>
</tr>
<tr>
<td>Switching Primary and Secondary Logs</td>
<td>214</td>
</tr>
<tr>
<td>Removing Unwanted Data from the Session Monitor Log</td>
<td>214</td>
</tr>
<tr>
<td>Collecting Session Monitor Data in an SMF Data Set</td>
<td>214</td>
</tr>
<tr>
<td>Maintaining the Save/Restore Database</td>
<td>215</td>
</tr>
<tr>
<td>Switching Primary and Secondary Databases</td>
<td>215</td>
</tr>
<tr>
<td>Removing Unwanted Data from the Save/Restore Database</td>
<td>215</td>
</tr>
<tr>
<td>Reorganizing the Save/Restore Database</td>
<td>215</td>
</tr>
<tr>
<td>Using the MVS System Log (SYSLOG)</td>
<td>215</td>
</tr>
<tr>
<td>Using and Maintaining the RODM Log</td>
<td>216</td>
</tr>
<tr>
<td>Switching the Primary and Secondary RODM Logs</td>
<td>216</td>
</tr>
<tr>
<td>Formatting the RODM log</td>
<td>216</td>
</tr>
<tr>
<td>Copying the Contents of RODM to a Checkpoint Data Set</td>
<td>217</td>
</tr>
</tbody>
</table>
Chapter 10. Maintaining the NetView Program

Controlling NetView 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 [Overview of

Defining a NetView Command

Use the CMDMDL statements (located in DSICMD) to define commands to the
NetView program. For example, the LIST command is defined by the following
statement:

```
LIST CMDMDL 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
  the DSICMD member.

For more information about NetView prefixes and internal command names, refer to
the Tivoli NetView for OS/390 Customization Guide.

You can also include a CMDMDL statement for a command list if you want to either
provide a synonym for the command list or restrict access to the command list
using scope of command authorization. For example, to define a command list
named MYSTATUS as well as a synonym of MYSTAT, and ensure that NetView
performs an authorization check, include the following statements in DSIPARM
member DSICMD:

```
MYSTATUS CMDMDL MOD=DSICCP,SEC=CH
CMDSYN MYSTAT
```

You can define command security using scope of command authorization, the
NetView command authorization table, or a system authorization facility (SAF)
security product such as Resource Access Control Facility (RACF). In order for
changes to scope of command authorization in DSICMD to take effect, you must
recycle the NetView program. Changes to command security using the NetView
command authorization table or a SAF product do not require a recycle of the
NetView program.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMDMDL statement syntax</td>
<td>[NetView Definition Statement Reference] in the Tivoli NetView for OS/390 Administration Reference</td>
</tr>
</tbody>
</table>
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. APPN 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.

For Graphical Enterprise feature users: The NetView program uses the VTAMLST data set to define the network that is monitored by the status monitor. If SNATM 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.

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 NMC to manage non-SNA resources in your system and network, the resources and relationships between them must exist in the RODM data cache. There are several facilities which can be used for creating, updating and deleting objects and relationships in RODM:

- NetView Network Planner/2
- NetView MultiSystem Manager
- NetView SNA Topology Manager (SNATM)
- Remote Operations Manager
- NetView RODM load utility
- RODMView

The NetView Network Planner/2 program is an OS/2-based facility that 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 NMC to use.
The SNA Topology Manager collects topology information for SNA subarea and APPN resources, and stores the topology information in RODM for use with the NMC.

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 the NetView MultiSystem Manager product to manage your LAN, IP, and Open Topology Interface resources. MultiSystem Manager dynamically collects resource and configuration information from LAN topology 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 NMC to use.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Novell networks</td>
<td>MultiSystem Manager MVS/ESA for Novell Netware Networks</td>
</tr>
<tr>
<td>LAN Network Manager (LNM) networks</td>
<td>MultiSystem Manager MVS/ESA for Internet Protocol (IP) networks and MultiSystem Manager: Internet Protocol Networks</td>
</tr>
<tr>
<td>Other resources</td>
<td>MultiSystem Manager: Open Topology Interface</td>
</tr>
</tbody>
</table>

Using the NetView SNA Topology Manager

Use the NetView SNA topology manager (SNATM) to gather and record data about SNA subarea and APPN topology. The SNA topology manager collects topology data from either a VTAM agent or the APPN topology and accounting agent. The topology data collected is stored in RODM for use by NMC.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNATM usage</td>
<td><a href="#">Tivoli NetView for OS/390 SNA Topology Manager and APPN Accounting Manager Implementation Guide</a></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetView RODM load utility usage</td>
<td><a href="#">Using the RODM Load Function</a> in the <a href="#">Tivoli NetView for OS/390 Resource Object Data Manager and GMFHS Programmer's Guide</a></td>
</tr>
</tbody>
</table>
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 APPN objects, domains, gateways, non-SNA objects, and SNA shadow objects as well as 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, do the following:

1. Type `rodmview` on the NetView command facility command line and press Enter. The RODMView main menu is displayed as shown in Figure 112.

2. Select option 1 (Access and control). The Access and Control panel is displayed as shown in Figure 113 on page 183. 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.
3. Select option 10 (Method actions). The Method Actions panel is displayed as shown in Figure 114.

![Figure 114. RODMView Methods Actions Panel - EKGVMETI](image)

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 invoke it by entering the information as shown in Figure 115 on page 184.
Displaying Data Sets Used by the NetView Program

If you are authorized, you may BROWSE members of NetView datasets 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 luname=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:
<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>BROWSE command</td>
<td>NetView online help</td>
</tr>
</tbody>
</table>
Chapter 11. 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 NMC program, enter:

```plaintext
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, enter:

```plaintext
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:

```plaintext
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 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:

```plaintext
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:

```plaintext
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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional task definitions</td>
<td>NetView Definition Statement Reference in the Tivoli NetView for OS/390 Administration Reference</td>
</tr>
<tr>
<td>AUTOTASK, START, STOP, STARTCNM, and STOPCNM commands</td>
<td>NetView online help</td>
</tr>
<tr>
<td>For a list of tasks</td>
<td>NetView Tasks in the Tivoli NetView for OS/390 Installation: Getting Started</td>
</tr>
</tbody>
</table>

Controlling Resource Utilization

The resource utilization function in NetView enables you to prioritize, monitor, and limit the resource usage for various tasks in NetView. 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 CPU consumed
- Based on the rate of I/O activity
- The message-queuing traffic to and from NetView tasks
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 a SAF security product, such as Resource Access Control Facility (RACF).

For information about adding new NetView operators, when operators are defined to a SAF product or when operators are defined using DSIOPF NetView definitions, refer to "Defining Operators, Passwords, and Logon Attributes" in the Tivoli NetView for OS/390 Administration Reference.

Defining NetView Operators

Here are the steps to follow:

1. If defining operators using the NetView product rather than a SAF product, verify that there are enough application (APPL) statements defined in your APPL major node for each additional operator you want to add. The samples use member A01APPLS (CNMS0013).

2. If there are not enough APPL statements 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 ATCCONxx (CNMS0003), or add the new major node to ATCCONxx.

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 a 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 a 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 a 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 terminate the operator session.

If the operator is not logged on when you issue the REFRESH OPERS command, the operator will no longer be able to log on.

If defining operators using a 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 appears on your screen for each operator successfully deleted, then message DSI633I appears to indicate that the refresh command completed successfully.

### 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 in free-form 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.

### 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. This enables you to 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:

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Component Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETVIEW</td>
<td>The default setting, unless otherwise specified</td>
</tr>
<tr>
<td>LBROWSE</td>
<td>Log browse</td>
</tr>
<tr>
<td>MAINMENU</td>
<td>The NetView main menu panel</td>
</tr>
<tr>
<td>MBROWSE</td>
<td>Member browse</td>
</tr>
<tr>
<td>NCCF</td>
<td>Command facility</td>
</tr>
<tr>
<td>NLDM</td>
<td>Session monitor</td>
</tr>
<tr>
<td>NPDA</td>
<td>Hardware monitor</td>
</tr>
<tr>
<td>STATMON</td>
<td>Status monitor</td>
</tr>
<tr>
<td>TARA</td>
<td>4700 support facility</td>
</tr>
<tr>
<td>VIEW</td>
<td>View applications, such as the NetView WINDOW command</td>
</tr>
<tr>
<td>WINDOW</td>
<td>The NetView WINDOW command</td>
</tr>
<tr>
<td>PFKDEF</td>
<td>The PFKDEF display</td>
</tr>
</tbody>
</table>

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 appears 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.

### 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 (NMC)

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 invoke your command list RODMINST that displays a list of network management gateways defined in RODM, enter the following:

```
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 invoke your command list RODMINST that displays a list of network management gateways defined in RODM, enter the following:

```
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 change the current password for the RODM named EKGXRODM to yyyy, enter:

?orcntl pass,or=ekgxrodm,newpass=yyyy

To suppress not only the command echo but also the command response from your display and the NetView log, enter the suppression character twice. For example, to change the current password for the RODM named EKGXRODM to yyyy, and suppress both the command and command response, enter:

??orcntl pass,or=ekgxrodm,newpass=yyyy

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. An example of this is:

?excmd oper1,sdom password=xyz

**Note:** The suppression character must precede the EXCMD command; do not enter the suppression character with the queued command (SDOM command).

The suppression character is defined by the SUPPCHAR keyword in CNMSTYLE.

To automatically suppress the command echo for a command, you can include ECHO=N on the CMDMDL statement for the command in DSIPARM member DSICMD. 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 ???) you will see message:

DSI083I AUTOWRAP STOPPED

Your screen will lock 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:

autowrap 5

In the response area (next to ???) you will see the message:

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 will 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.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up your screen definitions</td>
<td>[Customizing the NetView Command Facility Panel](Tivoli NetView for OS/390 Customization Guide)</td>
</tr>
<tr>
<td>Syntax of screen definition statements</td>
<td>[NetView Definition Statement Reference](Tivoli NetView for OS/390 Administration Reference)</td>
</tr>
<tr>
<td>OVERRIDE and LIST commands</td>
<td>NetView online help</td>
</tr>
</tbody>
</table>

# Defining Receivers for Alerts and Other MDS-MUs

The NetView product allows 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, do the following:

1. Add the following statements to DSIPARM member DSCMD to define the hardware monitor generic automation receiver commands.

   DSIREGGR CMDMDL MOD=DSIREGGR,TYPE=R,RES=Y
   DSILoggr CMDMDL MOD=DSILoggr,TYPE=R,RES=Y
   DSINVGRP CMDMDL MOD=DSINVGRP,TYPE=R,PARSE=N,RES=N
   BNJNETOP CMDMDL MOD=DSIFGUSP,TYPE=D,PARSE=N,RES=Y

   If you expect your use of the generic automation receiver to be heavy, change the RES operand on the DSINVGRP CMDMDL statement from N to Y.
2. Define the operator ID to receive the alerts. If you define operators using NetView profiles, rather than in a SAF product, add the following statements to DSIPARM member DSIOPF:

```
DSINVGR OPERATOR PASSWORD=GENREC
PROFILE DSIPRFGR
```

3. If you define operators in a SAF product, such as RACF, define the IC, MSGRECVR, CTL and other values in the NETVIEW segment of the SAF product.

If you define operators in the NetView product, add a profile for the automation receiver to the DSIPRF data set as follows:

```
DSIPRFGR PROFILE IC=DSIREGGR
AUTH MSGRECVR=NO,CTL=GLOBAL
OPCLASS 1,2,6
```

Refer to "Defining Operators, Passwords, and Logon Attributes" in the Tivoli NetView for OS/390 Administration Reference for examples of various operator and autotask definitions.

4. Define and start the alert receiver autotask, DSINVGR, in CNMSTYLE.

**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 as well as from the hardware monitor alerts display screens.

**Graphical Enterprise feature and Procedural feature users**: To delete a specific alert from the hardware monitor database while viewing the Alerts Dynamic or 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, do the following:

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
   ```

**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**

**Graphical Enterprise feature and Procedural feature users**:

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**

**Graphical Enterprise feature and Procedural feature users only.**

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 116 on page 196 is displayed:
You can then use the sample REXX command list shown in Figure 117 to delete the alert filters listed:

```rexx
/* 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 117. 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 will have to run your system with the defaults disabled for a period of time before you will be able to gather the data necessary to make your filtering decisions. Ask the following questions for each alert:
   - Should its event be recorded or deleted?
   - Should the event 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, should probably be recorded and displayed by the hardware monitor.

### Setting Viewing Filters

**Graphical Enterprise feature and Procedural feature.**

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 8 shows examples of how to set specific viewing filters.

<table>
<thead>
<tr>
<th>To:</th>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not display alerts for event type IMR.</td>
<td>NPDA SVF BLOCK E IMR</td>
</tr>
<tr>
<td>Not display alerts for event type IMR</td>
<td>NPDA SVF BLOCK E IMR N GRETL</td>
</tr>
<tr>
<td>from resource GRETL.</td>
<td></td>
</tr>
<tr>
<td>Not display alerts for event type IMR</td>
<td>NPDA SVF BLOCK E IMR T COMC</td>
</tr>
<tr>
<td>from resource type COMC.</td>
<td></td>
</tr>
<tr>
<td>Not display alerts for event 04C10.</td>
<td>NPDA SVF BLOCK C 04C10</td>
</tr>
<tr>
<td>Display alerts for event 04C10 from</td>
<td>NPDA SVF PASS C 04C10 N GRETL</td>
</tr>
<tr>
<td>resource GRETL.</td>
<td></td>
</tr>
<tr>
<td>Not display alerts for product ID</td>
<td>NPDA SVF BLOCK P 5601227 6D3EF9A1 N GRETL</td>
</tr>
<tr>
<td>5601227 with an alert ID of 6D3EF9A1</td>
<td></td>
</tr>
<tr>
<td>from resource GRETL.</td>
<td></td>
</tr>
<tr>
<td>Start displaying alerts for domain CNM01.</td>
<td>NPDA SVF CLEAR D CNM01</td>
</tr>
</tbody>
</table>

### 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 invoked 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 9 shows examples of how to set specific recording filters.

**Table 9. Examples of Recording Filters**

<table>
<thead>
<tr>
<th>To:</th>
<th>Example:</th>
</tr>
</thead>
</table>
| 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 |
| 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 will apply 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 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. For Graphical Enterprise feature and Procedural feature users, 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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVFILTER, SRFILTER, and DFILTER commands</td>
<td>NetView online help</td>
</tr>
<tr>
<td>Automation table</td>
<td>[The Automation Table] in Tivoli NetView for OS/390 Automation Guide</td>
</tr>
<tr>
<td>SRF action in the automation table</td>
<td>[Automating Messages and MSUs] in Tivoli NetView for OS/390 Automation Guide</td>
</tr>
</tbody>
</table>

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

There are two basic filter types: 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. There are two statements that define the filtering rules, 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:

   ISTMG10  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 as well as 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. There are two statements that define the filtering rules, 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 10 shows examples of how to define KCLASS statements and Table 11 on page 201 shows examples of MAPSESS statements.

#### Table 10. Examples of KCLASS Statements

<table>
<thead>
<tr>
<th>To:</th>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep session awareness data and store it on the database, keeping 42 PIUs per session.</td>
<td>DASDK42  KCLASS  SAW=YES,DASD=YES,KEEPPIU=42</td>
</tr>
<tr>
<td>Keep session awareness data in storage only, keeping 10 PIUs per session.</td>
<td>STORK10  KCLASS  SAW=YES,DASD=NO,KEEPPIU=10</td>
</tr>
<tr>
<td>Keep session awareness data and store it on the database if there is trace or RTM data for the session, or if there is a BIND failure, INIT failure, or abnormal UNBIND, keeping 14 PIUs per session.</td>
<td>FAILK14  KCLASS  SAW=YES,DASD=(DATA,FAILURES),KEEPPIU=14</td>
</tr>
</tbody>
</table>
Table 10. Examples of KCLASS Statements (continued)

<table>
<thead>
<tr>
<th>To:</th>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep session awareness data and store it on the database for a maximum of 500 sessions, keeping 30 PIUs per session.</td>
<td>DASDK30 KCLASS SAW=YES,DASD=YES,KEEPPIU=30,KEEPSESS=500</td>
</tr>
</tbody>
</table>

Table 11. Examples of MAPSESS Statements

<table>
<thead>
<tr>
<th>To:</th>
<th>Example:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control session awareness data using KCLASS DASDK42 for sessions whose primary session partner is SSCP1 and whose secondary session partner name begins with CDRM.</td>
<td>M1 MAPSESS KCLASS=DASDK42,PRI=SSCP1,SEC=CDRM*</td>
</tr>
<tr>
<td>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.</td>
<td>M2 MAPSESS KCLASS=STORK10,PRI=SSCP1,SEC=??LU*</td>
</tr>
<tr>
<td>Control session awareness data using KCLASS FAILK14 for sessions whose primary session partner is SSCP1 and whose secondary session partner name begins with CICS.</td>
<td>M3 MAPSESS KCLASS=FAILK14,PRI=SSCP1,SEC=CICS*</td>
</tr>
<tr>
<td>Control session awareness data using KCLASS DASDK30 for any session that did not match a prior MAPSESS statement.</td>
<td>M4 MAPSESS KCLASS=DASDK30,PRI=<em>,SEC=</em></td>
</tr>
</tbody>
</table>

To define the session monitor filters:

1. Create DSIPARM member AAUPRMLP as follows:

   INITMOD AAUINLDM KEEPMEM=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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTAM filter table ISTMGC10</td>
<td>Refer to the VTAM Library.</td>
</tr>
<tr>
<td>DSIPARM member AAUPRMLP</td>
<td>NetView Definition Statement Reference in the Tivoli NetView for OS/390 Administration Reference</td>
</tr>
</tbody>
</table>
Chapter 12. 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:

- 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 or should 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:
   
   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:
   
   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:
   
   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:
   
   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:
   
   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:
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:
   
   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:
   
   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:

   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:

   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 focal point’s sphere of control. To do this, at the NetView console of the focal point, enter:

   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 focal point’s sphere of control to the state defined in the sphere of control configuration file. To do this, at the NetView console of the focal point, enter:

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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOCALPT commands</td>
<td>NetView online help</td>
</tr>
<tr>
<td>Setting up focal points</td>
<td>[Centralizing Operations] in the <em>Tivoli NetView for OS/390</em> Installation: Configuring Additional Components</td>
</tr>
</tbody>
</table>

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 should:

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. Invoke 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:

sratio 020 n pu08

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>GENALERT command</td>
<td>NetView online help</td>
</tr>
<tr>
<td>SRATIO command</td>
<td>NetView online help</td>
</tr>
<tr>
<td>Filtering</td>
<td>&quot;Overview of Filter Types&quot; on page 194</td>
</tr>
<tr>
<td>Alert types</td>
<td>“Chapter 9” in SNA Formats</td>
</tr>
<tr>
<td>Sending alerts using the PPI</td>
<td>[Understanding the NetView Program-to-Program Interface] in the Tivoli NetView for OS/390 Application Programmer’s Guide</td>
</tr>
</tbody>
</table>

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 DSIE1X18. Note that with TME 10 NetView release 1 and later, the BLOG command is available to accomplish this without requiring DSIE1X18.

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:

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:

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:

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 may 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 that will 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 118 is an example of the log browse interface:

Figure 118. 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 BROWSE command’s LU parameter 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 BROWSE command’s NETID parameter 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 BROWSE command’s OPERID parameter 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 OVERRIDE command’s STARTCOL parameter to set the display column when entering browse.

From Time
Indicates the starting time for the netlog display. This value corresponds to the BROWSE command’s FROM parameter 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 BROWSE command’s FROM parameter 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 BROWSE command’s TO parameter 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 BROWSE command’s TO parameter 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 \textit{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 \textit{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. Normally, NetView automatically switches to the inactive log when the active log fills up.

To display which network log is active, enter:
\texttt{list dsilog}

To switch to the secondary network log, enter:
\texttt{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.

\begin{verbatim}
NETVIEW.BRWS ------ BROWSE CNMKEYS (DSIOPEN ) --- LINE 00000 TO 00036 OF 00165
SCROLL ==> CSR
----+----1----+----2----+----3----+----4----+----5----+----6----+----7----+----
\end{verbatim}

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 will change the number of lines scrolled by the BACK and FORWARD PF keys. You can change whether the BROWSE screens have a SCROLL field using \texttt{OVERRIDE SCROLL=OFF}. For more information about the effects of the OVERRIDE command, refer to the NetView online help.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up the network log</td>
<td>\textit{Tivoli NetView for OS/390 Installation: Configuring Additional Components}</td>
</tr>
<tr>
<td>Filtering the log display using the log browse installation exit DSIEX18</td>
<td>\textit{Writing Installation Exit Routines} in \textit{Tivoli NetView for OS/390 Customization: Using Assembler}</td>
</tr>
<tr>
<td>Printing the network log (DSIPRT)</td>
<td>\textit{Defining the Data Logs} in \textit{Tivoli NetView for OS/390 Installation: Configuring Additional Components}</td>
</tr>
<tr>
<td>Message formats</td>
<td>\textit{Appendix A, Message Format} on page 375</td>
</tr>
<tr>
<td>BROWSE and FIND commands</td>
<td>NetView online help</td>
</tr>
</tbody>
</table>
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, do the following:

1. Start the DSITRACE task:
   
   \[
   \text{nccf start task=dsitrace}
   \]

2. Start the command facility trace:
   
   \[
   \text{nccf trace on,option=(mod,uexit),mode=ext,task=ost}
   \]

3. Verify trace settings:
   
   \[
   \text{nccf list trace}
   \]

4. To stop the trace, enter:
   
   \[
   \text{nccf trace end}
   \]

5. Stop the DSITRACE task:
   
   \[
   \text{stop task=dsitrace}
   \]

6. To print the trace data, use the command facility utility program DSIPRT. An example of the job to invoke this utility is located in member CNMPRT of the CNMSAMP data set.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up the command facility trace log</td>
<td>Tivoli NetView for OS/390 Installation: Configuring Additional Components</td>
</tr>
<tr>
<td>Command facility LIST, START, STOP, and TRACE commands</td>
<td>NetView online help</td>
</tr>
<tr>
<td>Reading the command facility trace data</td>
<td>&quot;Diagnostic Tools for the NetView Program&quot; in Tivoli NetView for OS/390 Diagnosis Guide</td>
</tr>
</tbody>
</table>

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, do the following:

1. To start the session monitor trace from the command facility, enter:
   
   \[
   \text{nldm trace start cpuu term1}
   \]

2. To stop the trace, enter:
   
   \[
   \text{nldm trace stop cpuu term1}
   \]

3. To display, see "Typical LU-LU Session for an SNA Subarea Network" on page 80.
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, do the following:

1. Start the MVS GTF task from the command facility. GTF should be set 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:
   ```
   mvs s gtf.gtf
   ```
2. Start the PPI trace for SSI task NETVSSI from the command facility:
   ```
   mvs f netvssi,traceppi on rcvrid=task1
   ```
3. To stop the trace, enter:
   ```
   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.

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 there is only one physical hardware monitor database, 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:

```
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:

```
dbauto npda,purge,60
```

To reclaim the space used by the purged records, reorganize the database. To do this, enter:

```
dbauto npda,reorg
```

**Note:** If the default is not desirable, you can also specify primary and secondary space allocation.

To delete all data in the database, enter:

```
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 will be recorded. You cannot select which alerts will be logged.

To start alert recording, enter:

```
npda reports on
```

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up the hardware monitor database</td>
<td><a href="#">Tivoli NetView for OS/390 Installation: Configuring Additional Components</a></td>
</tr>
<tr>
<td>Maintaining the hardware monitor database through automation</td>
<td>Refer to <a href="#">Tivoli NetView for OS/390 Installation: Configuring Additional Components</a></td>
</tr>
<tr>
<td>Using SMF logs</td>
<td>Refer to <a href="#">Tivoli NetView for OS/390 Installation: Configuring Additional Components</a></td>
</tr>
</tbody>
</table>
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:

```
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:

```
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:

```
dbauto tara,reorg
```

**Note:** Specify primary and secondary space allocation if the default is not appropriate.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up the 4700 support facility database</td>
<td>Tivoli NetView for OS/390 Installation: Configuring Additional Components</td>
</tr>
<tr>
<td>Maintaining the 4700 support facility database through automation</td>
<td>Refer to Tivoli NetView for OS/390 Installation: Configuring Additional Components</td>
</tr>
<tr>
<td>DBAUTO and LISTCAT commands</td>
<td>NetView online help</td>
</tr>
</tbody>
</table>
Using and Maintaining the Session Monitor Database

The session monitor collects data about same-domain, cross-domain, and cross-network SNA (subarea and APPN) 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:

```
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:

```
dbauto nldm,purge,60
```

To reclaim the space used by the purged records, reorganize the log. To do this, enter:

```
dbauto nldm,reorg
```

To delete all data in the log, enter:

```
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:

```
nldm record sesstats primlu1 seclu2
```

To write storage and processor utilization data to the external log enter:

```
nldm record strgdata
```
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:

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:

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:

dbauto save,reorg

Note: You might also want to specify primary and secondary space allocation if the default is not desirable.
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 invoke 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 invoke the RODM log formatter using a submit JCL, EKGRLOG. A sample job is found in member EKGRLOG of the SEKGSMP1 data set. The SYSPRINT data set contains the formatted log.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up the RODM log</td>
<td><a href="#">Tivoli NetView for OS/390 Installation: Configuring Additional Components</a></td>
</tr>
<tr>
<td>Invoking a MAPI call from a RODM method to write records to the RODM log</td>
<td><a href="#">Writing RODM Methods</a> in <a href="#">Tivoli NetView for OS/390 Resource Object Data Manager and GMEHS Programmer's Guide</a></td>
</tr>
<tr>
<td>Customizing member EKGCUST</td>
<td><a href="#">Resource Object Data Manager (RODM) Definition Statements</a> in <a href="#">Tivoli NetView for OS/390 Administration Reference</a></td>
</tr>
</tbody>
</table>

216 User's 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 to allow you to copy the contents of the RODM data cache to a checkpoint data set. RODM also allows you to load the data cache during RODM initialization from a checkpoint data set. Therefore you should 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, do the following:

From the NetView console, enter:

```
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 appears when the checkpoint is complete.

**Note:** Before starting RODM, specify one or more checkpoint data sets in the RODM procedure.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting up the RODM</td>
<td><em>Tivoli NetView for OS/390 Installation: Configuring Additional Components</em></td>
</tr>
<tr>
<td>checkpoint data set</td>
<td></td>
</tr>
<tr>
<td>MVS command</td>
<td>NetView online help</td>
</tr>
<tr>
<td>Chapter 19. Writing a NetView Command</td>
<td>279</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>Requirements for Writing Command Lists</td>
<td>279</td>
</tr>
<tr>
<td>Defining a Data Set</td>
<td>279</td>
</tr>
<tr>
<td>Creating a Command List</td>
<td>280</td>
</tr>
<tr>
<td>Using REXX Functions</td>
<td>281</td>
</tr>
<tr>
<td>Using NetView Functions</td>
<td>282</td>
</tr>
<tr>
<td>Handling Command Message Responses</td>
<td>282</td>
</tr>
<tr>
<td>Displaying Panels</td>
<td>284</td>
</tr>
<tr>
<td>Issuing Messages</td>
<td>284</td>
</tr>
<tr>
<td>Using the REXX SAY Instruction</td>
<td>284</td>
</tr>
<tr>
<td>Using MSG</td>
<td>284</td>
</tr>
<tr>
<td>Using WTO</td>
<td>284</td>
</tr>
<tr>
<td>Using WTOR</td>
<td>285</td>
</tr>
<tr>
<td>Obtaining Input from the Operator</td>
<td>285</td>
</tr>
<tr>
<td>Issuing Commands</td>
<td>285</td>
</tr>
<tr>
<td>Storing Information in Global Variables</td>
<td>285</td>
</tr>
<tr>
<td>Accessing Data Set Members</td>
<td>286</td>
</tr>
<tr>
<td>Parsing Input</td>
<td>286</td>
</tr>
<tr>
<td>Testing a Command List</td>
<td>287</td>
</tr>
<tr>
<td>Adding a CMDMDL Statement</td>
<td>287</td>
</tr>
<tr>
<td>Improving the Performance of Command Lists</td>
<td>288</td>
</tr>
<tr>
<td>Writing an HLL Command Processor</td>
<td>289</td>
</tr>
<tr>
<td>Writing an Assembler-Language Command Processor</td>
<td>290</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 20. Storing Information in NetView Global Variables</th>
<th>293</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designing Global Variables</td>
<td>293</td>
</tr>
<tr>
<td>Displaying the Current Value of a Global Variable</td>
<td>294</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 21. Optimizing Your Automation</th>
<th>297</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deciding Which Alerts to Filter</td>
<td>297</td>
</tr>
<tr>
<td>Deciding Where to Filter Each Alert</td>
<td>297</td>
</tr>
<tr>
<td>Implementing Filtering Decisions</td>
<td>297</td>
</tr>
<tr>
<td>Using the RATE Statement</td>
<td>297</td>
</tr>
<tr>
<td>Using the Hardware Monitor SRFILTER Command</td>
<td>298</td>
</tr>
<tr>
<td>Using the Automation Table SRF Function</td>
<td>298</td>
</tr>
<tr>
<td>Using the DSIEX16B Exit</td>
<td>298</td>
</tr>
<tr>
<td>Suppressing a System Message</td>
<td>298</td>
</tr>
<tr>
<td>Using MVS Message Processing Facility (MPF)</td>
<td>299</td>
</tr>
<tr>
<td>Suppressing VTAM Messages</td>
<td>300</td>
</tr>
</tbody>
</table>

| Chapter 22. Monitoring NetView Automation | 301 |
Chapter 23. Debugging Automation .......................... 303
Determining Why a Message Is Not Automated by the Automation Table . . 303
Checking Other Areas ........................................... 303
Reading the Message Detail Report ................................ 304
Determining Why an Alert Is Not Automated ............... 306
Determining Why an Alert Is Not Displayed on the Tivoli Enterprise Console ........ 308
Determining Why a Tivoli Enterprise Console Event Is Not Forwarded to NetView ........ 309
Determining Why a Command List Does Not Complete .......................... 310
Determining Why a Timed Command Does Not Run .......... 311
Determining Why Automation Is Taking Too Much Processing Time ........ 313
Determining Why a Message Is Routed to the Wrong Operator ....... 314
Determining Why a Pipe Command Does Not Process Correctly .......................... 315
Chapter 13. 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 invocation 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. This also allows you to perform routine operations automatically.

The NetView automation table enables you to examine and separate data, then take actions in response. Its purpose is for:

- 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)

The generic, automation receiver function of the NetView program enables you 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 Tivoli NetView for OS/390 Customization Guide.

Automation Table and Alerts

You can use the SRFILTER and PDFILTER commands to change recording filters. The PDFILTER command is called from a statement in the sample NetView automation table (DSITBL01) when the NetView BNJDSERV task completes initialization.
Normally, 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 normal 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’

You should 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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using the AUTOTBL and AUTOCNT commands</td>
<td>NetView online help</td>
</tr>
<tr>
<td>Protecting data sets</td>
<td>&quot;Controlling Access to Data Sets and Members&quot; in the <em>Tivoli NetView for OS/390 Security Reference</em></td>
</tr>
<tr>
<td>Protecting commands and keywords</td>
<td>&quot;Controlling Access to Commands&quot; in the <em>Tivoli NetView for OS/390 Security Reference</em></td>
</tr>
<tr>
<td>Planning security for automation</td>
<td>&quot;Security Considerations for Automation&quot; in the <em>Tivoli NetView for OS/390 Security Reference</em></td>
</tr>
</tbody>
</table>
Planning Message or MSU Automation

This comparison of automating messages and MSUs shows the steps necessary before updating an automation table.

Table 12. Planning Message and MSU Automation

<table>
<thead>
<tr>
<th>If you are automating a message:</th>
<th>If you are automating an MSU:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain a copy of the actual message (using network or system logs).</td>
<td>Look at the contents of the MSU (using the hardware monitor).</td>
</tr>
<tr>
<td>Obtain the ID of the message.</td>
<td>Get the major vector of the MSU.</td>
</tr>
<tr>
<td>Identify any specific message instances that you wish to automate (such as from a particular domain, network device, or application).</td>
<td>Identify any specific MSU instances that you want to automate (such as from a particular domain, network device, or application).</td>
</tr>
<tr>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>

Browsing the Automation Tables

You can browse your automation tables using the NetView BROWSE command. For example, if your automation table is named AUTOTAB2, you would enter:

```
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 233.

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 will not be replaced unless you use the REPLACE parameter on AUTOTBL.
Adding a New Automation Table Statement

Automation table statements define actions for the NetView program to take when it receives a specific message or MSU. See Table 13 for the statement types that make up an automation table:

### Table 13. Automation Table Statement Types

<table>
<thead>
<tr>
<th>Statement</th>
<th>Function of the statement</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALWAYS</td>
<td>Enables you to specify actions to take place for all messages and MSUs that reach that statement in the table. See Table 17 on page 223 for a list of valid actions.</td>
<td>IF conditions THEN BEGIN; IF statement1 THEN action1; IF statement2 THEN action2; ALWAYS action3; END;</td>
</tr>
<tr>
<td>BEGIN-END</td>
<td>Enables you to group statements together for processing, which improves performance by reducing the number of comparisons. A BEGIN-END section starts with a BEGIN option on an IF-THEN statement and ends with an END statement.</td>
<td>IF conditions THEN BEGIN; statements END;</td>
</tr>
<tr>
<td>IF-THEN</td>
<td>Lets you specify messages and MSUs that you want the NetView program to automate. An IF-THEN statement contains a set of conditions followed by a set of actions that the NetView program is to perform when a message or MSU meets those conditions. See Table 14, Table 15 on page 227, and Table 16 on page 228, for a list of valid conditions and Table 17 on page 229 for a list of valid actions.</td>
<td>IF conditions THEN actions;</td>
</tr>
<tr>
<td>%INCLUDE</td>
<td>Enables you to include separately coded and maintained sections of the automation table to divide your automation table maintenance among several groups or individuals.</td>
<td>%INCLUDE member1 %INCLUDE member2 %INCLUDE member3</td>
</tr>
<tr>
<td>SYN</td>
<td>Enables you to define synonyms for use later in the table. Each SYN statement includes a name and an associated value.</td>
<td>SYN %NETDOM%='RA3AN'; IF DOMAINID=%NETDOM% THEN actions;</td>
</tr>
</tbody>
</table>

Table 14, Table 15 on page 227, and Table 16 on page 228 show the valid condition items that are commonly used in an IF-THEN statement.

### Table 14. Automation Table Condition Items for Messages

<table>
<thead>
<tr>
<th>Condition Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTIONDL</td>
<td>Message is being deleted and for what reason. See also ACTIONMG and DOMACTION.</td>
</tr>
<tr>
<td>ACTIONMG</td>
<td>Explains whether the message is an action message or not. See also ACTIONDL and DOMACTION.</td>
</tr>
<tr>
<td>AREAID</td>
<td>MVS message area ID</td>
</tr>
<tr>
<td>AUTOTOKE</td>
<td>MVS message processing facility automation token</td>
</tr>
<tr>
<td>CART</td>
<td>Command and response token</td>
</tr>
<tr>
<td>DESC</td>
<td>MVS message descriptor codes</td>
</tr>
</tbody>
</table>
### Table 14. Automation Table Condition Items for Messages (continued)

<table>
<thead>
<tr>
<th>Condition item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFRAUWF1</td>
<td>MVS WTO information</td>
</tr>
<tr>
<td>JOBNAME</td>
<td>MVS originating job</td>
</tr>
<tr>
<td>JOBNUM</td>
<td>MVS assigned job number</td>
</tr>
<tr>
<td>KEY</td>
<td>Key associated with a message</td>
</tr>
<tr>
<td>MCSFLAG</td>
<td>MVS MCS flags</td>
</tr>
<tr>
<td>MSGAUTH</td>
<td>Authorized program indicator</td>
</tr>
<tr>
<td>MSGCATTR</td>
<td>MVS message-attribute flags</td>
</tr>
<tr>
<td>MSGCMISC</td>
<td>MVS miscellaneous routing flags</td>
</tr>
<tr>
<td>MSGCMLVL</td>
<td>MVS message-level flags</td>
</tr>
<tr>
<td>MSGCMSGT</td>
<td>MVS message-type flags</td>
</tr>
<tr>
<td>MSGCOJBN</td>
<td>Originating job name</td>
</tr>
<tr>
<td>MSGCPRD</td>
<td>MVS product level</td>
</tr>
<tr>
<td>MSGCSPLX</td>
<td>Name of sysplex sending message</td>
</tr>
<tr>
<td>MSGDOMFL</td>
<td>MVS delete operator message (DOM) flags</td>
</tr>
<tr>
<td>MSGGBGPA</td>
<td>Background presentation attributes</td>
</tr>
<tr>
<td>MSGGDATE</td>
<td>Date associated with a message</td>
</tr>
<tr>
<td>MSGGFGPA</td>
<td>Foreground presentation attributes</td>
</tr>
<tr>
<td>MSGGMFLG</td>
<td>MVS general message flags</td>
</tr>
<tr>
<td>MSGGMID</td>
<td>MVS message ID</td>
</tr>
<tr>
<td>MSGGTIME</td>
<td>Time that the message was issued</td>
</tr>
<tr>
<td>MSGID</td>
<td>Message ID</td>
</tr>
<tr>
<td>MSGSRCNM</td>
<td>Source name from source object</td>
</tr>
<tr>
<td>MVSRTAIN</td>
<td>MVS AMRF retain flags</td>
</tr>
<tr>
<td>NVDELID</td>
<td>NetView deletion ID as used by DOM NVDELID</td>
</tr>
<tr>
<td>PARTID</td>
<td>VSE partition ID</td>
</tr>
<tr>
<td>ROUTCDE</td>
<td>MVS routing codes</td>
</tr>
<tr>
<td>SESSID</td>
<td>Terminal access facility session ID</td>
</tr>
<tr>
<td>SYSCONID</td>
<td>System console name or number</td>
</tr>
<tr>
<td>SYSID</td>
<td>ID of originating MVS system</td>
</tr>
<tr>
<td>TEXT</td>
<td>Message text</td>
</tr>
<tr>
<td>TOKEN</td>
<td>In a message text, a string delimited by blanks</td>
</tr>
</tbody>
</table>

### Table 15. Automation Table Condition Items for MSUs

<table>
<thead>
<tr>
<th>Condition item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIER</td>
<td>Hierarchy subvectors and its subfields.</td>
</tr>
<tr>
<td>HMASPRID</td>
<td>Alert sender product ID</td>
</tr>
<tr>
<td>HMBLKACT</td>
<td>Block ID and action code of an MSU</td>
</tr>
<tr>
<td>HMCPLINK</td>
<td>Indicator that specifies whether a complex link exists</td>
</tr>
</tbody>
</table>
### Table 15. Automation Table Condition Items for MSUs (continued)

<table>
<thead>
<tr>
<th>Condition item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HMSEPNAU</td>
<td>Returns the nau name of the entry point node where the MSU originated for MSUs forwarded using the SNA-MDS/LU 6.2 alert forwarding protocol, the NV-UNIQ/LUC alert forwarding protocol, or the NetView V1R2 message and alert forwarding protocol</td>
</tr>
<tr>
<td>HMSEPNET</td>
<td>Returns the netid name of the entry point node where the MSU originated for MSUs forwarded using the SNA-MDS/LU 6.2 alert forwarding protocol</td>
</tr>
<tr>
<td>HMSEPNETV</td>
<td>Returns an indicator that specifies whether the entry point node where the MSU originated was a remote node NetView program. This function applies only to MSUs forwarded using the SNA-MDS/LU 6.2 alert forwarding protocol</td>
</tr>
<tr>
<td>HMEVTYPE</td>
<td>Event type of an MSU</td>
</tr>
<tr>
<td>HMFWDED</td>
<td>Indicator that specifies whether an MSU was forwarded from another node</td>
</tr>
<tr>
<td>HMFWDSNA</td>
<td>Returns an indicator that specifies whether an MSU was forwarded from a remote entry point node using the SNA-MDS/LU 6.2 alert forwarding protocol</td>
</tr>
<tr>
<td>HMGENCAU</td>
<td>General cause code of an MSU, in hexadecimal</td>
</tr>
<tr>
<td>HMONMSU</td>
<td>Indicator that specifies whether an MSU was submitted to automation by the hardware monitor</td>
</tr>
<tr>
<td>HMORIGIN</td>
<td>Name of the resource sending the MSU</td>
</tr>
<tr>
<td>HMSECREC</td>
<td>Indicator specifying whether the hardware monitor performs secondary recording</td>
</tr>
<tr>
<td>HMSPECAU</td>
<td>Specific component code of an MSU, in hexadecimal</td>
</tr>
<tr>
<td>HMUSRDAT</td>
<td>User data from subvector 33 of an MSU</td>
</tr>
<tr>
<td>MSUSEG</td>
<td>Segment of an MSU</td>
</tr>
</tbody>
</table>

### Table 16. Automation Table Condition Items for Messages and MSUs

<table>
<thead>
<tr>
<th>Condition item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACQUIRE</td>
<td>Acquire AIFR data</td>
</tr>
<tr>
<td>ATF</td>
<td>Automation table function</td>
</tr>
<tr>
<td>ATF(DSICGLOB)</td>
<td>Specified common global variable</td>
</tr>
<tr>
<td>ATF(DSITGLOB)</td>
<td>Specified task global variable</td>
</tr>
<tr>
<td>ATTDNED</td>
<td>Attended task indicator</td>
</tr>
<tr>
<td>AUTOMATED</td>
<td>Significant action indicator</td>
</tr>
<tr>
<td>AUTOTASK</td>
<td>Autotask indicator</td>
</tr>
<tr>
<td>CURPART</td>
<td>NetView program’s VSE partition ID</td>
</tr>
<tr>
<td>CURSYS</td>
<td>Current MVS operating system name</td>
</tr>
</tbody>
</table>
Table 16. Automation Table Condition Items for Messages and MSUs (continued)

<table>
<thead>
<tr>
<th>Condition item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISTAUTO</td>
<td>Distributed autotask indicator</td>
</tr>
<tr>
<td>DOMAIN</td>
<td>Current NetView domain name</td>
</tr>
<tr>
<td>DOMAIND</td>
<td>Originating NetView domain</td>
</tr>
<tr>
<td>HDRMTYPE</td>
<td>Message or MSU type</td>
</tr>
<tr>
<td>IFRAUI3X</td>
<td>Thirty-two bits of indicators, the first 8 are IFRAUIN3.</td>
</tr>
<tr>
<td>IFRAUIND</td>
<td>AIFR indicator flags</td>
</tr>
<tr>
<td>IFRAUIN3</td>
<td>Indicator-bit field</td>
</tr>
<tr>
<td>IFRAUSB2</td>
<td>AIFR user field</td>
</tr>
<tr>
<td>IFRAUSC2</td>
<td>AIFR user field</td>
</tr>
<tr>
<td>IFRAUSDR</td>
<td>Name of originating NetView task</td>
</tr>
<tr>
<td>IFRAUSR8</td>
<td>AIFR user field</td>
</tr>
<tr>
<td>IFRAUSRC</td>
<td>AIFR user field</td>
</tr>
<tr>
<td>IFRAUTA1</td>
<td>AIFR control flags</td>
</tr>
<tr>
<td>INTERVAL</td>
<td>Occurrence interval detection</td>
</tr>
<tr>
<td>LNPRES</td>
<td>Presentation attributes of first text buffer</td>
</tr>
<tr>
<td>LINETFLG</td>
<td>Presentation override flag (bit 16) and other flags</td>
</tr>
<tr>
<td>MVSLEVEL</td>
<td>Current MVS product level</td>
</tr>
<tr>
<td>NETID</td>
<td>VTAM network identifier</td>
</tr>
<tr>
<td>NETVIEW</td>
<td>NetView version and release</td>
</tr>
<tr>
<td>NVCLOSE</td>
<td>NetView CLOSE processing flag</td>
</tr>
<tr>
<td>OPID</td>
<td>Operator or task ID</td>
</tr>
<tr>
<td>OPSYSTEM</td>
<td>Operating system</td>
</tr>
<tr>
<td>SYSPLEX</td>
<td>Local MVS sysplex name</td>
</tr>
<tr>
<td>TASK</td>
<td>Type of task</td>
</tr>
<tr>
<td>THRESHOLD</td>
<td>Occurrence threshold detection</td>
</tr>
<tr>
<td>VALUE</td>
<td>Value of a variable</td>
</tr>
<tr>
<td>VTAM</td>
<td>VTAM level</td>
</tr>
<tr>
<td>VTCOMPID</td>
<td>VTAM component identifier</td>
</tr>
<tr>
<td>WEEKDAYN</td>
<td>Day of the week</td>
</tr>
</tbody>
</table>

Table 17 shows the valid action statements that can be used in an IF-THEN statement or in an ALWAYS statement.

Table 17. Automation Table Actions

<table>
<thead>
<tr>
<th>Action item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTOMATED</td>
<td>Significant action indicator</td>
</tr>
<tr>
<td>BEEP</td>
<td>Sound an audible alarm</td>
</tr>
<tr>
<td>CNM493I</td>
<td>Write message CNM493I to the network log for this statement</td>
</tr>
<tr>
<td>COLOR</td>
<td>Set foreground color</td>
</tr>
<tr>
<td>CONTINUE</td>
<td>Continue scanning the table even after a match is found.</td>
</tr>
</tbody>
</table>
Table 17. Automation Table Actions (continued)

<table>
<thead>
<tr>
<th>Action item</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISPLAY</td>
<td>Display the message</td>
</tr>
<tr>
<td>DOMACTION</td>
<td>Request that the removal of the message (by DOM signal) should cause an automation action (second). See also ACTIONMG and ACTIONDL.</td>
</tr>
<tr>
<td>EDIT</td>
<td>Edit AIFR data</td>
</tr>
<tr>
<td>EXEC</td>
<td>Issue a command or route a message</td>
</tr>
<tr>
<td>HCYLOG</td>
<td>Log the message in the hardcopy log if the hardcopy task is active</td>
</tr>
<tr>
<td>HIGHINT</td>
<td>Set high-intensity 3270 mode</td>
</tr>
<tr>
<td>HOLD</td>
<td>Hold the message on the screen</td>
</tr>
<tr>
<td>NETLOG</td>
<td>Log the message in the network log and activate a status monitor message indicator for specified operators or group of operators</td>
</tr>
<tr>
<td>SRF</td>
<td>Set recording filter attributes for the MSU to control the recording of data in the hardware monitor database</td>
</tr>
<tr>
<td>SYSLOG</td>
<td>Log the message in the system log</td>
</tr>
<tr>
<td>TRACE</td>
<td>Sets tracing on</td>
</tr>
<tr>
<td>XHILITE</td>
<td>Set foreground highlighting</td>
</tr>
<tr>
<td>XLO</td>
<td>Specify external logging only</td>
</tr>
</tbody>
</table>

Complete the following steps to add a new automation table statement:

1. Using your system editor, such as ISPF on MVS/ESA, edit the source file that contains the portion of the automation table that you want to modify.

2. If you have your table divided using BEGIN/END sections, locate the section of the automation table to modify. For example, if you were adding a statement to automate IST400I, you should add the new statement in the BEGIN/END section that contains statements for messages that start with IST. For example:

   ```
   IF MSGID = 'IST' . THEN
   BEGIN;
   ::
   (add your statement here)
   ::
   END;
   ```

3. Add the statement to the automation table, considering the consequences of the placement:

   - Put the new statement within an appropriate member and BEGIN/END section, according to pre-existing organization.
   - Do not to duplicate other statements. If identical or overlapping comparisons exist, combine them.
   - If you cannot group duplicate comparisons within one IF-THEN statement, specify CONTINUE(YES), although this has performance disadvantages. Because CONTINUE(YES) continues comparisons after finding a matching condition statement, it increases processing time.

   Also, consider the performance implications of the new statement. For example, if you anticipate your statement will be matched infrequently, place it near the
bottom of the automation table. Placing an infrequently automated statement at
the top of the table will use unnecessary processing time. See “Analyzing
Automation Table Usage” on page 233 for information on the correct placement
of statements in the automation table.

To allow your message or MSU to be available for automation processing,
ensure that it has not been suppressed. For messages, check the MVS
Message Processing Facility (MPF) or the NetView installation exit DSIEX02A.
To ensure MSUs are not suppressed, check NetView installation exit XITCI.

If you need to take actions not supported in the automation table, such as
calculations or referencing information stored in a member, you might need to
create a command list to complete the automation of the condition that caused
the message or MSU.

4. Test the syntax of the automation table by using the TEST keyword of the
NetView AUTOTBL command.

5. Optionally, after correcting any syntax errors, you can temporarily place your
new statement in the automation table with no actions to verify that the
statement is correctly matching on the messages or MSUs that it is supposed
to. To temporarily test a statement:
   a. Comment out the actions specified on the statement. For example:
      * ABC123 indicates an abnormal termination
      IF MSGID = 'ABC123I' THEN
      * Comment these actions out during test period
      * EXEC(CMD('ABCSTART'))
      * ROUTE(ONE AUTO1 ABCOPER *)
      * DISPLAY(N)
      CONTINUE(Y)
      ;
   b. Verify with a detailed automation usage report that the statement is being
      processed and is matching when expected.
   c. Remove CONTINUE(Y) and verify that the statement does not interfere with
      later statements.
   d. When the statement processes correctly, it is ready for production use.
      Uncomment the sections to enable the automation actions.

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. An example automation statement with a TRACE action
   follows:
   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 will include
   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 would 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:

   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 command to end the test:

   autotest off
   autotest source=off

6. Browse the report as follows:

   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

   Following is an example of a syntax error as 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 DW0044 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 you assume that a block of automation table statements in member DSITBL01 are identified by LABEL=VTAM and ENDLABEL=VTAM, you can enter the following:

```plaintext
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:

```plaintext
autotbl member=dsitbl01 disable block=vtam
```

If instead you wanted to enable the single automation table statement identified by LABEL=VTAM (and not the entire block of statements), enter the following:

```plaintext
autotbl member=dsitbl01 enable label=vtam
```

You can also enable or disable automation table statements with the AUTOMAN command. Refer to the Tivoli NetView for OS/390 Automated Operation 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 should 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 match messages or MSUs, but should not
- To recognize statements that do not match, but should
- 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:

```plaintext
autocnt stats=detail report=both file=report
```

You will also receive a summary 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 will 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 121 on page 235 and Figure 122 on page 235.
Storing Summary Usage Reports
You should store summary data for comparison purposes so that you can see the impact of automation when changes are made to the environment, such as:

- 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 AUTOCN T 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 executed 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 executed 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. You should 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 should be performed. For example, the following statement indicates that automation processing should stop for any message with a message identifier that begins with XYZ:

\[
\text{IF MSGID = 'XYZ'. THEN;}
\]

And, the next example indicates that automation processing should stop for all Problem Determination statistics major vectors (key X'0025'):

\[
\text{IF MSUSEG(0025) \neq ' THEN;}
\]

**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*

<table>
<thead>
<tr>
<th>Indicators</th>
<th>Possible Error Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMPARE COUNT = MATCH COUNT</td>
<td>The automation table statement might have a logic error causing it to always match a message or MSU when it is compared</td>
</tr>
<tr>
<td>MATCH COUNT &gt; 0</td>
<td></td>
</tr>
<tr>
<td>A I (Always Indicator) = blank</td>
<td></td>
</tr>
<tr>
<td>COMPARE COUNT = 0</td>
<td>There might be a prior statement that is preventing this statement from being compared when it should be compared</td>
</tr>
<tr>
<td>MINUTES ELAPSED = substantial</td>
<td></td>
</tr>
<tr>
<td>MATCH COUNT = 0</td>
<td>This statement might no longer be needed because the message or MSU the statement is trying to match is no longer generated or there might be a coding error on the condition items preventing the message or MSU from matching.</td>
</tr>
<tr>
<td>MINUTES ELAPSED = substantial</td>
<td></td>
</tr>
</tbody>
</table>
Where possible (without changing the automation logic), order the automation table as follows:

- 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 should 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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTOTBL and AUTOCNT commands</td>
<td>NetView online help</td>
</tr>
<tr>
<td>Automation table language, automation table listings, and automation table usage reports</td>
<td><a href="#">Tivoli NetView for OS/390 Automation Guide</a></td>
</tr>
<tr>
<td>Planning for automation</td>
<td><a href="#">Tivoli NetView for OS/390 Automation Guide</a></td>
</tr>
<tr>
<td>MSUs in NetView</td>
<td><a href="#">Tivoli NetView for OS/390 Automation Guide</a></td>
</tr>
<tr>
<td>MSUs in SNA</td>
<td>SNA Management Services Reference and SNA Formats</td>
</tr>
</tbody>
</table>
The Resource Object Data Manager (RODM) is an in-storage data cache that is used by the NetView program to maintain status information for operational objects and their relationship to one another. This information is used by GMFHS to present graphical views for monitoring and controlling network resources.

RODM can invoke automation routines when information is accessed or changed. These automation routines are called *methods* and run under the control of the RODM program. The NetView program provides a set of methods for some commonly used functions. You can create methods to perform specialized functions.

The automation capabilities of RODM can be integrated with existing automation capabilities provided by the NetView automation table. For example, a RODM method can issue a command to be run under a NetView autotask. Also, the NetView program can access or change data in RODM as well as cause a RODM method to run. This can be done from a command list or from the NetView automation table.

**Writing a RODM Method**

There are two classes of RODM methods:

- **Object-independent methods**
- **Object-specific methods**

**Object-independent methods** are invoked to perform a series of actions against multiple objects in RODM. They can be invoked from either another method in RODM or from outside of RODM. A special case of an object-independent method is the initialization method. This method is invoked during RODM initialization to establish initial conditions within the RODM data cache.

**Object-specific methods** are invoked to perform a function against a single object in RODM. There are several types of object-specific methods:

- **Change methods**
  Invoked by RODM when a transaction attempts to change the value of an object’s field. The change method can accept or override the value specified by the transaction.

- **Query methods**
  Invoked by RODM when a transaction requests the value of an object’s field. The query method can override the value returned to the transaction.

- **Notify methods**
  Invoked by RODM after a transaction changes the value of an object’s field. The notify method can send the new value of the field to subscribed users.

- **Delete methods**
  Invoked by RODM when a transaction deletes an object. The delete method can notify subscribed users that an object has been deleted.

- **Named methods**
  Invoked by name to perform multiple coordinated actions against an object. The named method can be invoked from either another method in RODM or from outside of RODM.
Although the NetView program provides a set of methods for commonly used functions, you might want to provide your own methods for specialized functions. For example, you might want to restrict the value of a particular attribute to a predefined set of values. To do this, you could write a change method to examine the value being set and override this value with a valid one if necessary.

Other Uses for RODM Methods

The EKGSPPI method uses the program-to-program interface (PPI) to send commands to the NetView task, DSIQTSK. The DSIQTSK task is dedicated to communicating with the RODM address space and to managing RODM. This task is a NetView task of type OPT; it is defined in DSIDMN and is started with the START TASK command.

You can use the EKGSPPI method to issue commands from your RODM methods. These commands can include any command that can be processed from a NetView autotask. For example, if a resource fails, you might want to trigger a method to attempt activation of that resource automatically using the VTAM VARY command. The VARY command cannot be processed from the RODM address space, so the command is sent to the NetView address space.

The commands from the EKGSPPI method are sent to the NetView address space and dispatched by DSIQTSK to NetView autotasks for processing.

When defining RODM, a task such as DSIQTSK must be defined as a dedicated receiver of the PPI queue. If a task is not defined, RODM cannot send commands to the NetView address space.

Although RODM offers a wide variety of functions, RODM programming is beyond the scope of this book, and is not recommended for simple automation tasks.

Invoking a RODM Method from the NetView Program

You can use the NetView ORCONV command or EKGVMETM command to invoke methods in RODM from:

- The NetView automation table
- Command lists
- The command facility

For example, from the automation table, you can issue the ORCONV command with data from a message to trigger a RODM method.
In message IEF450I, the second token is JOB1:

IEF450I JOB1 - ABEND=S222 U0000 REASON=00000000

The following automation table statement traps the message and triggers an object-independent method (VERIFY):

```
IF MSGID='IEF450I' & TOKEN(2)=JOBNAME THEN
  EXEC(CMD('ORCONV TYPE=OBJIND,OBJINDEP=VERIFY,PARM=\'' JOBNAME \'',
           PARMTYPE=CHARVAR')
       ROUTE(ONE AUTO4));
```

The same ORCONV command can be issued from a command list or from the command facility.

Before using EKGV commands to work with RODM, you must be connected to RODM (using the EKVACTM command).

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORCONV or EKGV commands</td>
<td>NetView online help</td>
</tr>
</tbody>
</table>

### Changing a RODM Object Attribute Value Directly from the NetView Program

You can use the NetView ORCONV command or EKVCHGM command to update a field in RODM. For example, to update the STATE field of a JOB object when a job abnormally terminates, include the following statement in your NetView automation table:

```
IF MSGID='IEF450I' & TOKEN(2)=JOBNAME THEN
  EXEC(CMD('ORCONV CLASS='JOB',OBJECT=''' JOBNAME''',
           FIELD='STATE',
           DATA='256',ERROR=ERRROUT,ID='JOBABEND')
       ROUTE(ONE AUTO4));
```

When ORCONV changes the STATE field in RODM, any change methods associated with the field are invoked. To prevent change methods from being invoked, you can change the VALUE subfield instead of the entire field. In this case, the automation table statement is:

```
IF MSGID='IEF450I' & TOKEN(2)=JOBNAME THEN
  EXEC(CMD('ORCONV CLASS='JOB',OBJECT=''' JOBNAME''',
           FIELD='STATE',SUBFIELD=VALUE,
           DATA='256',ERROR=ERRROUT,ID='JOBABEND')
       ROUTE(ONE AUTO4));
```

**Note:** Before using EKGV commands to work with RODM, you must be connected to RODM (using the EKVACTM command).

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORCONV or EKVCHGM commands</td>
<td>NetView online help</td>
</tr>
</tbody>
</table>
Using RODMView EKGV Commands

You can use the NetView EKGV commands to trigger a RODM method, and to add, change, and delete the values of RODM classes, objects, and fields. These commands perform the same function as the RODMView panels, but can be issued from automation.

Example: Setting a Field Value

To set the DisplayStatus field of object NAP.RES1 in the GMFHS_Managed_Real_Objects_Class to 129, enter:

```
NETVASIS EKGVCHGM EKGXRODM OPER1 Y GMFHS_Managed_Real_Objects_Class
0 NAP.RES1 0 DisplayStatus 0 INTEGER 129
```

If you were using a NetView REXX command list, you could use a variable to substitute values, such as the operator ID. Refer to the NetView online help for more information about the EKGV commands: EKGVACTM, EKGVCHGM, EKGVCREM, EKGVCREM, EKGVLNKM, EKGVLOCM, EKGVMETM, EKGVQUEM, and EKGVSUBM.
Chapter 15. Using Automation Solutions

There are various solutions that extend the base automation capabilities of the NetView program. Specifically, they offer:

- Improved systems and network availability. This includes faster reaction to planned and unplanned situations and improved recovery processes.
- Increased operator productivity through more intuitive interfaces and the automation of repetitive tasks.
- Improved enterprise-wide management, that involves the integration of all your systems under a central point of control.

Figure 123 shows you the various applications that let you use the NetView program as a platform for automating your network and system needs.

Using the Target System Control Facility (TSCF)

You can use TSCF to extend the NetView program’s operations and automation support to local or remote target systems. TSCF allows a focal-point System/370™ or System/390 processor to manage a variety of target systems, including:

- IBM Enterprise System/390 Microprocessor complexes (9672 and 9674)
- 9021 and 9121 processors
- S/3090
- ES/9000® and ES/3090™ in Logical Partition Mode
- 308X and 4381 systems that run MVS, VM, VSE
- Transaction Processing Facility (TPF) operating system
You can use TSCF to accomplish the following automation tasks:
- Initial microprogram load (IML) or initial program load (IPL)
- Time-of-day clock setting
- Hardware reconfiguration
- System initialization
- Wait-state detection

TSCF can improve productivity by increasing the span of control available to you or to automation applications at the focal-point host. TSCF presents processed target-systems status information and consolidates messages from multiple targets. As a result, you can monitor many systems, select the desired level of detail, and focus on a single target when needed. Automated routines and the use of color to indicate system status lets you manage more systems and allows you to become more productive.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using the Target System Control Facility</td>
<td>Target System Control Facility Operations and Commands</td>
</tr>
</tbody>
</table>

**Using System Operations for OS/390**

You can use the System Operation (previously known as AOC) component to automate system operator tasks normally handled by a console operator. These tasks include the startup, monitoring, recovery, and shutdown of MVS subsystems, components, and applications including VTAM, RMF™, JES2, JES3, and TSO. In addition, you can use System Operations to automate operator console messages, initiate timer-based actions, and prevent critical MVS resource shortages.

You can use the SETAUTO and TIMEAUTO commands to control automation for specific resources. The SETAUTO command turns automation on or off for a specific resource or group of resources. The TIMEAUTO command switches automation on or off for a specific resource or group of resources for a specific time period and then switches it back.

**CICS Automation Option (CICS)**

You can use CICS Automation Option to significantly improve CICS console operation productivity, reduce complexity, and improve end-user application availability across a CICS complex. Specifically, CICS Automation Option provides the following functions:

- Operator single point of control for CICS:
  - Ability to control multiple CICS regions, within a single central electronic complex (CEC) or across multiple CECs, from one NetView terminal
  - Ability to start/stop any CICS in any CEC
  - Ability to view status of the CICS complex at a glance
  - Operator friendly interface for most master terminal transaction (CEMT) functions
- Starting/stopping CICS regions:
  - Handle VTAM ACB open/close programs
  - Tracking startup/shutdown processing to ensure timely processing
  - Ability to override startup parameters from operator interface
  - Interface with timer facilities to provide timed startup/shutdown
  - Provide interface so startup/shutdown triggers can come from batch or job scheduling packages
- Recovery of CICS regions:
- Handle CICS ABEND situations
- Monitor and resolve problems with Inter-system Communication (ISC) and Inter-region Communication (IRC) links
- Reconnect ISC sessions after selected VTAM failures
- Threshold and notification capabilities for application failures
- Provide problem determination assistance and recovery processing for recursive storage violation problems
- Notifications issued for critical recovery situations where action cannot be taken

- Miscellaneous functions
  - Basic health monitoring of the CICS regions

**IMS Automation Option (IMS)**

You can use the IMS Automation Option {4} to manage your IMS systems, both XRF and non-XRF, across your entire enterprise from a single NetView terminal. The IMS Automation Option runs as an application under System Automation for OS/390 using the NetView automation products. Specifically, the IMS Automation Option provides the following functions:

- Operator single point of control for IMS:
  - Ability to control multiple IMS systems, within a single central electronic complex (CEC) or across multiple CECs, from one NetView terminal
  - Ability to start/stop any IMS in any CEC
  - Ability to view status of the IMS complex at a glance
  - Operator-friendly interface for most master terminal operator (MTO) functions

- Starting/stopping IMS systems:
  - Handle VTAM ACB open/close problems
  - Track startup/shutdown processing to ensure timely processing
  - Override startup parameters from operator interface
  - Interfaces with timer facilities to provide timed startup/shutdown

- Recovery of IMS systems:
  - Handle IMS abnormal end (abend) situations
  - IMS Log (OLDS) archive errors notification
  - Threshold and notification capabilities for application failures
  - Notifications issued for critical recovery situations where action cannot be taken
  - Program and transaction recovery actions
  - Multiple Systems Coupling (MSC) link recovery

- Additional IMS/XRF functions:
  - Force termination of inoperative old Active IMS
  - Automatic UNLOCK response to Availability Manager messages
  - Cancel DBRC on old Active IMS
  - Start a new alternate IMS after takeover
  - Dependent message region synchronization between the active and the alternate IMS systems

**OPC/ESA Automation Option (OPC)**

You can use the OPC Automation Option {5} to allow the scheduling and control capabilities of OPC/ESA to work together with NetView automation applications. Systems automation requires many preplanned actions that take place at different times on different days. For example, business days can have a significantly different schedule from weekend and holidays. In addition, business cycles might vary each month and especially at year end. OPC/ESA production management systems automatically schedule and control the flow of large production workloads in a data center taking into consideration these different business cycles. NetView
automation applications (System Automation for OS/390) manage the interactive or online tasks of the data center such as responding to messages, initializing subsystems, or shutting down and restarting various applications. When OPC/ESA and the NetView program work in collaboration through the high-performance OPC interface, comprehensive checking, monitoring, and multi-tiered processes can work together to improve system utilization and effectiveness.

The OPC Automation Option runs as an application of System Automation for OS/390 and uses the automation products of the NetView program. For additional information, refer to System Automation for OS/390 Library.

Using Automated Operations Network

Automated Operations Network (AON) is an integrated automation solution for NetView and provides a sophisticated level of automation that includes:

- **Thresholding** — AON {11} keeps track of how often a resource encounters problems. You can set thresholds for infrequent problems (for example, occurring at the rate of about 4 problems in 8 hours), frequent problems (for example, occurring at the rate of about 4 problems in 4 hours), or critical problems (for example, occurring at the rate of about 8 problems in 2 hours). Based on these thresholds, AON can then take actions to reactivate the resource, log a record of the problems, notify you, and so on, before a failure occurs.

- **Recovery** — AON can recover (reactivate) failed resources based on your automation policy. Automated Operations Network also looks at how often recovery has been attempted for each resource. After a specified number of recovery attempts, Automated Operations Network stops recovery attempts for that resource to avoid wasting CPU cycles, logs the data, and notifies the appropriate operators.

- **Logging and generating automation reports.**

- **Proactive and passive monitoring** — Automated Operations Network can check critical resources at chosen intervals (proactive monitoring) or only when it receives events about the resource (passive monitoring).

- **Problem determination** — The automated help desk facility displays a color-coded diagram of a resource and how it is connected to the network. Specific colors are associated with resource states, such as active, inactive, and so on. You can use the automated help desk to resolve problems associated with that resource. The help desk isolates and attempts to fix the problem.

- **Dynamic Display Facility (DDF)** — DDF lets you see the status of the network.

- **Single point of control** — You can monitor and automate many NetView programs from a single NetView workstation.

- **Automation Notification** — Using the Automation Notification policy you can customize when, how, and who AON notifies of network events, and also the action that is taken by automation. You can choose to have messages, alerts, Tivoli Enterprise Console updates, beeper requests, or Email requests generated based on a specific resource name, resource type, or for a particular region within your network.

AON/LAN Automation

You can use the AON/LAN {6} component operating under the NetView program to extend the AON automation capabilities to token ring LANs. AON/LAN shows you the status of the LANs, notifies you when changes occur in the LAN environment, and tells you if any intervention is required. AON/LAN also provides automatic and
managed routine recovery of the bridges connecting LANs, also automation for recovery of your LAN Network Manager Service Points.

AON/LAN also provides an automated mechanism for capturing LAN performance data through its Remote Traffic Analysis Program Agent (RTAP). You can capture performance data when Bridge or Adapter congestion is detected and then take action; such as removing the workstation causing the problem.

**AON/SNA Automation**

You can use the AON/SNA component (7) to extend the automation capabilities for SNA networks and systems. Specifically, AON/SNA provides the following functions:

- **Automatic switched network backup (SNBU).** This automatically switches modems to a lower speed when a communication line experiences temporary errors, such as noise or poor line quality, or switch from a leased line to a dialed line when a communication line experiences permanent errors.
- **Support for X.25 support interface between data terminal equipment and packet switching networks.** This enhances problem determination for packet switching networks by providing an exit to trap hardware alerts from X.25 resources and translate them into meaningful alerts. You can use these alerts to gain a clear interpretation of the error, including the meaning of the error bytes, and more specific recommended action.
- **Support for the APPN environment.**
  In an APPN environment, AON provides menu-driven commands to simplify VTAM topology and directory database management. This environment accepts operator commands for common APPN VTAM functions and allows active monitoring of control points and control point sessions.
- **Support for your traditional VTAM subarea resources:** lines, PUs, NCPs, CDRMs, etc. Based on your automation policy AON/SNA will attempt to recover these resources for you. AON/SNA also provides you a helpdesk facility for problem determination.

**AON/TCP Automation**

AON/TCP (8) is a component that assists you with management of your TCP/IP resources by proactively monitoring critical resources and by responding to network events.

AON/TCP provides support for Tivoli NetView for AIX as a service point and TCP/IP for OS/390.

The Tivoli NetView for AIX support can detect performance problems involving disk space, CPU utilization, and security authorization failures.

With the TCP/IP for OS/390 support, you can issue any IP or UNIX command (Ping, Tracerte, Netstat) from NetView, display connections such as TN3270, FTP, and SMTP and then perform problem diagnosis for those connections. You can also manage your IP resources and the NetView TSO and UNIX servers. The Proactive Monitoring Capabilities enable you to use SNMP functions for MIB Polling (for example, identifying a failed interface) or MIB Thresholding (for example, checking customer defined performance MIBs for a key router).
Using the NetView AutoBridge

The NetView AutoBridge/MVS \{9\} enables communication of automation data between the NetView program and Information/Management. You can:
- Create, update, and search the Information/Management database
- Monitor for specific alerts, messages, and application data
- Manage multiple, local, or remote sites
- Complete records with post processing

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using the NetView AutoBridge/MVS</td>
<td>NetView AutoBridge/MVS General Information and the NetView AutoBridge/MVS Installation and User’s Guide</td>
</tr>
</tbody>
</table>

Using AIX NetView Service Point

You can use the Any Service Point \{12\} program to monitor a non-SNA network, report network-management data to the NetView program, and pass commands from the NetView program to devices in the non-SNA network. This allows you to use service point application programs to expand the scope of NetView automation. The AIX NetView Service Point program, which runs under the AIX operating system, serves as an interface for communications between Tivoli NetView (for AIX) and Tivoli NetView for OS/390.

The Tivoli NetView (for AIX) program helps you manage your network by providing a graphical interface that lets you perform configuration, fault, and performance management functions for your network resources. It supports networks that use protocols other than IP through use of SNMP agents.

| Topic:      | Reference:                                                      |
|-------------|                                                                |
| AIX Service Point | AIX NetView Service Point Installation, Operation, and Programming Guide |
Chapter 16. 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 will take effect once 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 will fail.

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: Assigning Operators to Groups | 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 17. Setting Up an Autotask to Handle Automation

Creating and using NetView automated operator station tasks (autotasks) allows work to be performed automatically. Autotasks can do work normally performed by operators, thus allowing operators more time to perform less repetitive tasks. Autotasks can:

- 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.

Defining Autotasks

To define an autotask, do the following:

1. Define the name for the autotask. If the autotask is to be started with the AUTOTASK command, the name should convey the work that the autotask is to perform.

   If you start tasks remotely using the RMTCMD command, it is best to use the same name for RMTCMD autotasks on all systems to simplify tracking and administration. For example, if operator task OPER1 logs on to the NetView program at domain CNM01, but needs to access domains CNM02 and CNM99 using RMTCMD, the operator name OPER1 should be reserved for this purpose on CNM02 and CNM99.

2. Determine whether the autotask will be an MVS interface task used by the MVS console to enter NetView commands. This only applies to autotasks started with the AUTOTASK command. If so, you must specify to which MVS console it is connected when the autotask is started. For example, to connect autotask AUTO1 to MVS console CONS05, enter the following when AUTO1 is started:

   ```
   autotask opid=auto1,console=cons05
   ```

   Because everything from the autotask is echoed to the MVS console to which the autotask is connected, limit the MVS interface autotask usage to the processing of NetView commands from the MVS operator.

   NetView routes commands received from the MVS master console to either the autotask associated with the console name of the master console or to the autotask associated with the console "MASTER". Assigning an autotask to a console ID "MASTER" is recommended so that your master console operator can always enter NetView commands. The autotask continues to receive commands from the new master when the master console is switched to a new device.

3. Define the autotask to the NetView program. All operator station tasks (OSTs), including autotasks, must be defined in the NetView member DSIOPF, in the SAF product, or in both, depending on the OPERSEC setting. When defined in DSIOPF, an operator profile should be assigned to the autotask. The operator profile includes an optional initial command that should be processed when the task is started. You can examine the sample operator profile (DSIPROFC) and initial command list (CNME1032) provided for the AUTO1 autotask to get an idea of the kinds of things that can be done.
Part of the operator definition is determining what commands the task is allowed to run, if you use command security. For an overview of autotask definitions, refer to "Security Considerations for Automation" in the *Tivoli NetView for OS/390 Administration Reference*. For a description of command security, refer to "Controlling Access to Commands" in the *Tivoli NetView for OS/390 Security Reference*.

4. Use sample CNMSTYLE to automatically start your autotasks during NetView initialization. Autotask AUTO1 is started during NetView initialization by CNMSTYLE. Autotask AUTO2 is an MVS interface task which is also started during NetView initialization by CNMSTYLE.

When you have defined and started the autotask, enter a list status=tasks command to determine whether the task is active.

**Attention:** If NetView is started before VTAM, any autotasks started while VTAM is inactive will be assigned a specific VTAM application identifier (APPLID) using the hexadecimal numbering scheme. Because NetView does not know whether the assigned APPLID will be available when VTAM is started, it must assume that the APPLID will be available for use. Therefore, you must define consecutively numbered VTAM APPL statements for each of these autotasks. Numbering uses the hexadecimal scheme. Refer to sample CNMS0013.

### Starting Autotasks

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**

<table>
<thead>
<tr>
<th>Autotasks started with the AUTOTASK command:</th>
<th>Autotasks started with the RMTCMD command:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Are used to perform tasks normally reserved for NetView operators.</td>
<td>• Are used to provide cross domain communication using LU 6.2.</td>
</tr>
<tr>
<td>• 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.</td>
<td>• 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.</td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
</tr>
</tbody>
</table>

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: AUTOTASK and RMTCMD commands

<table>
<thead>
<tr>
<th>Reference:</th>
<th>NetView online help</th>
</tr>
</thead>
</table>

252 User's Guide
Defining operators using a security application

Chapter 18. 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.

If SA/390 2.1 (or higher) is available, you can display and manage timers on remote systems. If it is not available, fields will be grayed out on panels where they appear.

Like other NetView commands, timed commands can be issued from:
- An operator’s console
- An autotask
- Within a command list or command processor
- Any active task

NetView timer commands include: AT, AFTER, CHRON, and EVERY.

They are designed to:
- Let you issue commands whenever you choose
- Make it convenient to issue commands repeatedly

**Note:** The timed command is subject to any restrictions of the task under which it runs.

Timer commands can automatically perform tasks that human operators traditionally perform, such as:
- 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 two ways:
- Using NetView commands at the command line
- Using NetView Timer Management Panels

### Preparing to Issue NetView Timer Commands

Before you issue a NetView timer command, 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 will be using 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 two ways:
     - by checking the authorization of the originating task
     - by protecting the PPT operand for the timer commands
If you are using CMDAUTH=TABLE or CMDAUTH=SAF, you can specify AUTHCHK=SOURCEID on the OPTIONS statement in DSIDMN or on the REFRESH command to cause command security to 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 the "Controlling Access to Commands" in Tivoli NetView for OS/390 Security Reference for a description of how to protect timer command 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 Tivoli NetView for OS/390 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 will attempt to process on the task that issued the timer. This can present the following problems:

- The operator might not be logged on at the specified time the timed command is scheduled to run, in which case the command is not processed.
- The operator is in the middle of an important task when the command starts processing, in which case 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 fewer commands are restricted from processing on autotasks than on the PPT and 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:

```
AT 09/24 09:00:00,ID=statrep,statrep
```

Issuing Commands at Regular Intervals

To issue timed 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:
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:
after 1:00:00, id=statvtam, chkvtam

Displaying Timers That Are Waiting to Process
The LIST TIMER command will list:
- The type of timer command
- When the timed command is due to process
- What timed command will 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:
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,
enter:
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:
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 which 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:
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:

\texttt{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, type:

\texttt{restore timer}

To erase all saved timer records from the database, add the DELETE option.

\texttt{restore timer delete}

<table>
<thead>
<tr>
<th>Topic: AT, AFTER, CHRON, EVERY, LIST, PURGE, and RESTORE commands</th>
<th>Reference: NetView online help</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timed commands</td>
<td>Tivoli NetView for OS/390 Automation Guide</td>
</tr>
<tr>
<td>Using AOC to set timers</td>
<td>SystemView Automated Operations Control/MVS Operations</td>
</tr>
</tbody>
</table>

### 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 as follows:

- From a command list
- At the command line
- The Timer Management panel

**Note:** If SA/390 2.1 (or higher) is present, the Target and Target Network ID fields on the Timer Management panel are active and you can enter data. If it is not present, the fields are grayed out and do not permit data entry.

To display the Timer Management panel, type \texttt{TIMER} on any command line; or, if using AON, type \texttt{AON 1.6} at the command line.

The Timer Management panel displays, as shown in Figure 124 on page 259.

**Note:** Although \texttt{D} for Delete does not appear as an option on the Timer Management panel, the system does support it.
The Timer Management panel displays the following columns of data:

**Target** Specifies the ID of the remote system whose timers you want to display (if you do not specify the Target Network ID).

If you do specify the Target Network ID, NetView interprets the Target ID as a domain name.

**Target Network ID**

Specifies the ID of the remote domain whose timers you want to display.

**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 will be issued.

**Type**

Specifies the type of timer.

The Types are:

- EVERY
- AT
- AFTER
- CHRON

**Interval**

Specifies how often timers repeat.

**Task**

Specifies which task is to issue the command.

If task=PPT, the command does not require a specific task in order to be issued.

**Save**

Indicates to NetView whether this timer event is saved to the NetView SAVE/RESTORE database.

Figure 124. Timer Management Panel

The Timer Management panel displays the following columns of data:

<table>
<thead>
<tr>
<th>TIMER ID</th>
<th>SCHEDULED</th>
<th>TYPE</th>
<th>INTERVAL</th>
<th>TASK</th>
<th>SAVE</th>
<th>Catchup</th>
</tr>
</thead>
<tbody>
<tr>
<td>LONGEVERY</td>
<td>10/16/00 10:54:28</td>
<td>CHRON</td>
<td>00:10:20</td>
<td>OPER1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disconid</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LONGAT</td>
<td>10/16/00 14:40:49</td>
<td>AT</td>
<td>KENNIE</td>
<td>OPER1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>who</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LONGREM2</td>
<td>10/16/00 23:20:56</td>
<td>CHRON</td>
<td>00:10:20</td>
<td>OPER1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disconid</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LONGLONG</td>
<td>10/16/00 23:21:22</td>
<td>CHRON</td>
<td>DAY</td>
<td>OPER1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disconid</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EVERY</td>
<td>10/17/00 00:00:01</td>
<td>EVERY TUESDAY</td>
<td>KENNIE</td>
<td>msg all Today is Tuesday!!!</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AFTER9</td>
<td>10/25/00 10:43:21</td>
<td>AFTER</td>
<td>KENNIE</td>
<td>msg all This timer was set 9 days ago.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Command ===>

F1=Help  F2=End  F3=Return  F5=Refresh  F6=Roll
F7=Backward F8=Forward F9=Purged Timers  F12=Cancel
If SAVE=YES, the timer is stored in the NetView SAVE/RESTORE database. If SAVE=NO, or is left blank, the timer is not saved. The YES option allows this timer to be restored after a NetView outage. If CATCHUP=YES is specified in the AON control files, SAVE=YES is required.

**Catchup**

Allows a timer that has been saved 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, as shown on the Timer Management panel in Figure 124 on page 259:

- Target Network ID
- Target System

---

**Figure 125. Timer Management Panel for Local System**

Type ? in the Target field and press Enter.
NetView displays the Remote Target Selection Panel.

**Figure 126. Timer Management Panel with ? to Display Target Selection Panel**

NetView displays the Remote Target Selection Panel.

**Figure 127. Remote Target Selection Panel**

The Remote Target Selection panel displays the following columns of data:

**Filter** Enables you to specify a DOMAIN, SYSTEM, SYSPLEX, or COMM method to display.

**DOMAIN** Specifies the IDs of 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 data is transferred between remote domains.

Type any character to select a target system, as shown in Figure 127 on page 261 and press Enter.

NetView displays the active timers for the Target that you selected.

```
EZLK6000 TIMER MANAGEMENT IPUFD KEEN 10/16/00 19:28:58
1 To 5 Of 22
Target: AOCA Target Network ID: Total Selected Timers: 22
Total Purged Timers: 0
Filter criteria:
Type one action code. Then press ENTER.
1=Add 2=Change 3=Purge 4=Add CHRON timer
TMER ID SCHEDULED TYPE INTERVAL TASK SAVE Catchup
AOFIO069 10/16/00 19:29:53 AFTER PPT
AOFRASCD AOFWRK10 AOFRSMD STARTUP,FLGFDDINO00,,NORM,NO,,**,YES
AOFI0085 10/16/00 19:30:08 AFTER PPT
AOFRASCD AOFWRK08 AOFRSMD STARTUP,FLGFDDAIO00,,NORM,NO,,**,YES
AOFI000C 10/16/00 19:30:49 EVERY 00:10:00 PPT
AOFRASCD AOFWRK16 AOFRSMN2 HUGGORAPPL
RGTAMCPU 10/16/00 19:31:17 EVERY 00:05:00 AUTRGT)
RGTAMCPU
RGTMONIT 10/16/00 19:31:27 EVERY 00:05:00 AUTRGTM
RGTMONIT
AOFMON 10/16/00 19:33:13 EVERY 00:59:00 PPT
AOFRASCD MONOPER MONITOR $SYSTEM
```

Figure 128. 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 258.

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 129 on page 263 in which an EVERY timer was selected:
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 four types of timers are:

**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 [Tivoli NetView for OS/390 Command Reference](#) 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 258.

2. Display the Timer Set panel.
   
   To display the Timer Set panel, see [Setting Timers for a Specific Date and Time](#) on page 262.

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 13.0, is displayed with the EVERY pop-up window.

4. Define whether you want messages generated if the requested timer fails. Specify TIMEOUT as follows:
   • 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
   
   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:
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 as follows:
   • 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 258.
2. Display the Timer Set panel.
   To display the Timer Set panel, see [Setting Timers for a Specific Date and Time] on page 262.
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 131 on page 266.
Note: To set the timer for a different domain or system, see Selecting Remote Targets on page 260.

4. Define whether or not you want messages generated if the requested timer fails.
Specify TIMEFMSG as follows:
- Type 1 if you do not want messages generated.
- Type 2 if you want messages generated.

5. Type the time of day when you want the timer to display the setting in the Time field of the pop-up window.
The time is shown in an hh:mm:ss format. For example, to specify 2:43:58 p.m., type:
14 : 43 : 58

6. Type the date when you want the timer to display the date setting in the Date field of the pop-up window.
The date follows the mm/dd/yy format. For example, to specify August 3, 2001, type:
08/03/01

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.

---

Figure 131. Timer Set Panel with Timer Type of AT

---
To display the Timer Management panel, see "Using NetView Timer Management Panels" on page 258.

2. Display the Timer Set panel.
   To display the Timer Set panel, see "Setting Timers for a Specific Date and Time" on page 262.

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 132, is displayed.

   ![Timer Set Panel with Timer Type of AFTER](image)

Figure 132. 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 260.

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:
   \[\text{Intvl} \ 14 \ : \ 00 \ : \ 00\]
   \[\text{Days} \ 000\]
   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 as follows:
   • 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 258.

2. Display the Timer Set panel.
   To display the Timer Set panel, see "Setting Timers for a Specific Date and Time" on page 262.

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 EVERY pop-up window, shown in Figure 133 on page 269, is displayed.
Note: To set the timer for a different domain or system, see "Selecting Remote Targets" on page 260.

- You can specify how often you want your command to be issued by selecting one of the following three options from the intervals popup:
  - Type 1 to specify how often the command will be issued in your local time format.
  - Type 2 to specify how often the command will be issued in programmer format, which specifies intervals greater than 24 hours.
  - Type 3 to specify that the command will be issued every 24 hours.

Note: The popups 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 Timerid in the Timerid field (Optional).
- Type the operator ID which will 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 or type 2 to automatically have the task started to issue the command or 3 to purge the timer if the task is not active.
- Type 1 for Yes, in the Refresh field 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 for Yes, in the Debug field 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.
• Type the command that you want to be issued in the Command field.

The following is a description of the function keys for CHRON TIMER panels:

F1  Brief help for the panel that is being displayed.
F2  Displays the results of the CHRON command that was issued when F9 was pressed.
F3  Returns you to the previous panel. No data is saved.
F4  Displays the options panel.
F5  This function key is only available for a CHRON EVERY timer; it enables you 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 will be issued when you press F9.
F12 Displays the previous panel. No data is saved.

When you press F10 in the timer set panels, the panel shown in Figure 134 is displayed.

Figure 134. Timer Notify Panel

- Type one or more operator IDs in the IGNORE field to specify which operators will be notified 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 will be notified when the command does not run because it was purged.
• Type one or more operator IDs in the REMOVE field to specify which operators will be notified when the command does not run because it was removed.

• Type one or more operator IDs in the RUN field to specify which operators will be notified when the command runs.

When you press F4 in the timer set panels, the panel shown in Figure 135 is displayed.

![Figure 135. Timer Options Panel to Create a New Timer or Copy a Timer]

- To Create a new timer, do this:
  a. Press F9 to create a timer.
  b. Type 1.
- To copy this timer, type 2.
  You can copy a timer only if it was set previously.

If you press F5 in the timer set panels, the panel shown in Figure 136 on page 272 is displayed:
**Start timer AT** displays a panel where you can specify the time when the EVERY will start.

**Start timer AFTER** displays a panel where you can specify a delay interval after which the EVERY will 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.

To see the options that are set in the CHRON command, press **F11**.

The following two panels (Figure 137 on page 273 and Figure 138 on page 273) are examples of the CHRON EVERY Timer panel showing the preview keyword.
Press F9 to set the timer. Then press F2 to display the results of the CHRON command shown in (Figure 139 on page 274, Figure 140 on page 274, and in Figure 141 on page 275).
COMMAND ISSUED:
CHRON AT=(10/16/00 23:20:56),EVERY=(INTERVAL=(00:10:20 MXREPEAT=25),REMOVE=(10/27/00 00:20:56),DAYS=(1 5 7 9 22 24 26 LAST LAST-3 LAST-15 LAST-30),CALENDAR=(NOT Kennes_Birthday again Sandy_Birthday again Independence_day Judys_birthday Sandy's_Birthda y again Amandas_birthday Moms_Birthday again Denises_Birth da y again Quigleys_Birth Kochs_Birth Memorial_day Christmas_day Ke nnies IBM_anniversary Sandy's_Birthday again Independence_day Judys_birthday Sandy's_Birthda y again Amandas_birthday Moms_Birthday again Denises_Birth da y again Quigleys_Birth Kochs_Birth Memorial_day Christmas_day Ke

COMMAND RESPONSE:
BNH53I CHRON DEBUG OUTPUT
DSI201I TIMER REQUEST SCHEDULED FOR EXECUTION 'ID=LONGREM2'

DSICHRON: LocalDiff=-000-04.00.00.000000
DSICHRON: AtTimerSTCK=2000-10-16-23.20.56.000000
DSICHRON: EverySTCK= 000-00.10.20.000000
DSICHRON: OFFSTCK= 000-04.18.20.000000
DSICHRON: REMOVESTCK=2000-10-27-00.20.56.000000
DSICHRON: STCKx=2042-09-17-19.53.47.370496
DSICHRON: SaveAtIdx=1 KeyWord=AT
DSICHRON: SaveOptIdx=2 KeyWord=NOTIFY
DSICHRON: GMTOptIdx=4 KeyWord=LOCAL
DSICHRON: RouteName=OPER1
DSICHRON: TimerIDname=LONGREM2
DSICHRON: TimerFlags=0x00000000
DSICHRON: REM='THIS IS A test of a VERY long remark. The intent is to see ho w we deal with it',COMMAND='Disconid'

1=HLP 2=END 3=RET 4=KYS 5=LOG 6=ROL 7=BCK 8=FWD 9=TOP 10=WIN 11=ENT 12=RTV
CMD=>

Figure 139. CHRON EVERY Timer Display Results Window (Part 1 of 4)
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 does not appear as an option on the Timer Management panel, the system does support it.
Figure 143 shows a timer being purged.

![Figure 143: Example of Purging a Timer](image)

After you press Enter to purge a specific timer, the panel shown in Figure 144 is displayed. In the following example, the Total Purged Timers is now set to 1, and **F9=Purged Timers** is displayed.

![Figure 144: Active Timer Panel After a Purge](image)

To display purged (or deleted) timers, press **F9** on the Active Timer panel.
Reinstating Timers

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 outlined above for changing timers and make any necessary changes before setting the timer.

Figure 145 shows an example of a Purged Timer panel.

![Figure 145: 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 Total Purged (or Deleted) Timers is incremented by 1.
- The Total Purged (or Deleted) Timers is decremented by 1.

Press F9 to display your active timers.

Figure 146 on page 278 shows an example of changes on the panel.
TYPE ONE ACTION CODE. THEN PRESS ENTER.

1|R=Reinstall

<table>
<thead>
<tr>
<th>TIMER ID</th>
<th>SCHEDULED</th>
<th>TYPE</th>
<th>INTERVAL</th>
<th>TASK</th>
<th>SAVE</th>
<th>Catchup</th>
</tr>
</thead>
</table>

Command ===>
F1=Help    F2=End    F3=Return    F6=Roll
F7=Backward F8=Forward F9=Active Timers F12=Cancel

Figure 146. Purged (or Deleted) Timer Panel After Reinstalling
Chapter 19. Writing a NetView Command

If you find that you enter the same series of commands often or perform particular tasks routinely, consider writing a command list or command processor to simplify your process.

The REstructured eXecutor eXtended language, or REXX language, is a versatile, easy to use structured programming language. It offers a simple format, powerful functions, extensive mathematical capabilities, and the ability to issue commands to multiple environments.

Writing a NetView REXX command list is the easiest way to automate your processing. If you have specialized needs, also consider writing a command processor.

Command lists can be invoked in the same way that you can invoke any of the NetView commands, and can be protected by command security as described in "Controlling Access to Commands" in the Tivoli NetView for OS/390 Security Reference.

Requirements for Writing Command Lists

Before you write a command list, ensure that you have:

- Access to a valid TSO user ID and an editor, such as the ISPF editor.
- Access to a data set where the NetView command lists are stored. These data sets are specified by the DSICLD DD statement. Access to data sets can be controlled by a system authorization facility (SAF) security product, such as Resource Access Control Facility (RACF). Refer to "Controlling Access to Data Sets and Members" in the Tivoli NetView for OS/390 Administration Reference for more information.
- Access to the DSIPARM data set containing the DSICMD member. The DSICMD member contains the CMDMDL statements used to assign synonyms and opclass values for command lists. Note that this is an optional step; if you do not plan on assigning synonyms or using scope of command authorization for command security on your command lists, it is not necessary to update the data set containing the DSICMD member.
- A NetView operator ID for testing the command list.
- A command list naming convention, so that naming conflicts are avoided. This will simplify cataloging and maintenance of new and existing command lists.

Defining a Data Set

Define at least one data set to store your command lists. Ensure that your command lists follow your site naming conventions. The data sets are defined in the NetView startup procedure, CNMPROC (CNMSJ009), using the DSICLD statement. Add the names of any data sets that you have defined for your command lists before those of the NetView sample command lists, as shown in the following example:

```
//DSICLD DD DSN=DATASET1,DISP=SHR
// DD DSN=&SQ1..CNMCLST,DISP=SHR
```

In this example, the data set DATASET1 is used in the DD statement. It defines the names of your NetView command lists. The data set &SQ1..CNMCLST is defined for the NetView-supplied command lists.
Creating a Command List

To create a command list, choose a command list name, edit the data set using an editor, and understand the capabilities of command lists.

For REXX command lists, character strings are enclosed in quotes. If you use a variable, ensure that it is outside the quotes.

The following example shows a REXX command list, demonstrating input capabilities:

```
0001 /* An introduction to REXX */
0002 say "Hello! I am REXX."
0003 say "Enter your name, in the format 'GO name'."
0004 parse pull who
0005 if who = "" then
0006   say "Hello stranger"
0007 else
0008   say "Hello" who
0009 exit
```

Figure 147. A sample REXX command list

Where:

<table>
<thead>
<tr>
<th>Line number</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001</td>
<td>This is a comment that explains what the program does. A comment starts with a /* and ends with a */. All REXX command lists must start with a comment.</td>
</tr>
<tr>
<td>0002, 0003</td>
<td>The SAY instruction puts the text between the quotes onto the screen. In this example, the text asks for the user's name. NetView requires that you use the GO before input.</td>
</tr>
<tr>
<td>0004</td>
<td>The PULL instruction reads what is entered on the keyboard and assigns it to a variable, WHO.</td>
</tr>
<tr>
<td>0005</td>
<td>The IF instruction tests a condition. In this case, the condition compares the keyboard entry with an empty character string. If the keyboard entry is pressing Enter with no characters or only blank spaces, the WHO variable will be empty.</td>
</tr>
<tr>
<td>0005, 0006</td>
<td>The THEN statement will process if the comparison is true. In this case, if the value of the variable who is null, the screen displays Hello stranger.</td>
</tr>
<tr>
<td>0007, 0008</td>
<td>The ELSE statement will process if the comparison is false. In this case, if the value of the variable who is not null, the screen displays Hello followed by the name entered.</td>
</tr>
<tr>
<td>0009</td>
<td>The EXIT instruction cause the program to stop at this point.</td>
</tr>
</tbody>
</table>

In general, a REXX command list can consist of statements that allow you to:

- Process NetView and REXX functions
- Handle command message responses
- Display panels
- Issue messages
- Obtain input
- Automate responses to messages and MSUs
- Issue commands
• Store information in global variables
• Access data set members
• Parse input

Using REXX Functions

The REXX language has built-in functions that greatly simplify character manipulation and conversion, as well as many other functions for which you might otherwise have to write your own command list.

REXX enables you to use function calls anywhere in an expression. Function calls will perform the requested computations and return results. In an expression, REXX substitutes the value of the result of a function call as each function call is evaluated.

Table 20 summarizes some of the more commonly used REXX built-in functions:

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARG()</td>
<td>Returns an argument string, or information about the argument string to a program or internal routine</td>
<td>ARG(3) returns 'b' following &quot;Call name 'a', 'b'&quot;</td>
</tr>
<tr>
<td>C2D()</td>
<td>Returns the decimal value of the binary representation of a string</td>
<td>C2D('09'X) returns 9</td>
</tr>
<tr>
<td>C2X()</td>
<td>Returns a string, in character format, that represents a string converted to hexadecimal</td>
<td>C2X('72s') returns 'F7F2A2'</td>
</tr>
<tr>
<td>DATE()</td>
<td>Returns the local date</td>
<td>DATE() might return '01 Oct 93'</td>
</tr>
<tr>
<td>D2C()</td>
<td>Returns a string, in character format, that represents a decimal number converted to binary</td>
<td>D2C(129) returns 'a'</td>
</tr>
<tr>
<td>D2X()</td>
<td>Returns a string, in character format, that represents a decimal number converted to hexadecimal</td>
<td>D2X(129) returns '81'</td>
</tr>
<tr>
<td>LENGTH()</td>
<td>Returns the length of a string</td>
<td>LENGTH(abc def') returns 7</td>
</tr>
<tr>
<td>POS()</td>
<td>Gives the starting position of a string in another string</td>
<td>POS('day', 'Saturday') returns 6</td>
</tr>
<tr>
<td>QUEUED()</td>
<td>Returns the number of lines remaining in the external data queue</td>
<td>QUEUED() might return 5</td>
</tr>
<tr>
<td>SUBSTR()</td>
<td>Returns the substring of a string (starting at a specified character and of a specified character length)</td>
<td>SUBSTR('abc', 2, 4) returns 'bc'</td>
</tr>
<tr>
<td>TIME()</td>
<td>Returns the time in 24-hour format</td>
<td>TIME() might return '16:54:22'</td>
</tr>
<tr>
<td>WORD()</td>
<td>Returns the text of a specified word in a phrase</td>
<td>WORD('Now is the time', 3) returns 'the'</td>
</tr>
<tr>
<td>WORDINDEX()</td>
<td>Returns the position of a specified word in a phrase</td>
<td>WORDINDEX('Now is the time', 3) returns 8</td>
</tr>
</tbody>
</table>
Table 20. REXX Built-in Functions (continued)

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORDLENGTH()</td>
<td>Returns the length of a specified word in a phrase</td>
<td>WORDLENGTH('Now is the time', 2) returns 2</td>
</tr>
<tr>
<td>WORDPOS()</td>
<td>Returns the position of a word within a phrase</td>
<td>WORDPOS('the', 'now is the time') returns 3</td>
</tr>
<tr>
<td>WORDS()</td>
<td>Returns the number of blank-delimited words in a string</td>
<td>WORDS(&quot;Now is the time&quot;) returns 4</td>
</tr>
<tr>
<td>X2C()</td>
<td>Returns a string, in character format, of a string of hexadecimal characters</td>
<td>X2C(F7F2 A2') returns '72s'</td>
</tr>
<tr>
<td>X2D()</td>
<td>Returns the decimal value of a string of hexadecimal characters</td>
<td>X2D(0E) returns 14</td>
</tr>
</tbody>
</table>

Using NetView Functions

NetView has built-in functions that allow you to access operator and message information.

Table 21 lists some of the more commonly used functions written in REXX for use by the NetView program. These functions can only be used with NetView.

Table 21. Functions Used with the NetView Program

<table>
<thead>
<tr>
<th>Function</th>
<th>Returns</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAIN()</td>
<td>The 1- to 5-character name of the current NetView domain.</td>
<td>IF DOMAIN() = 'CNM01' THEN ...</td>
</tr>
<tr>
<td>MSGID()</td>
<td>Message identifier of the message that drove this command list or that satisfied a WAIT instruction</td>
<td>IF MSGID() = 'IST075I' THEN ...</td>
</tr>
<tr>
<td>OPID()</td>
<td>Operator ID or task ID that issued the command list</td>
<td>IF OPID() = 'OPER1' THEN ...</td>
</tr>
<tr>
<td>TASK()</td>
<td>The 3-character string indicating the type of task under which the command list is running.</td>
<td>IF TASK() = 'PPT' THEN...</td>
</tr>
</tbody>
</table>

Handling Command Message Responses

Use the NetView PIPE command and the CORRWAIT pipe stage command to manage command responses. The following example shows how to use the PIPE command to send the LIST OPER6 command to a remote NetView and the CORRWAIT pipe stage command to manage the incoming responses. The output is displayed as a multiple line message.

```
PIPE NETVIEW RMTCMD LU=CNM01,OPERID=OPER6,LIST OPER6
| CORRWAIT 10 |
| TOSTRING /END OF STATUS DISPLAY/ |
| COLLECT   |
| CONSOLE   |
```
Table 22 describes the processing steps involved with each Pipe stage.

<table>
<thead>
<tr>
<th>Pipe stage</th>
<th>Processing involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIPE NETVIEW RMTCMD LU=CNM01, OPERID=OPER6, LIST OPER6</td>
<td>The RMTCMD command runs on the local NetView and sends the LIST OPER6 command to the remote NetView with a domain ID of CNM01. The LIST OPER6 commands runs on the remote NetView under the RMTCMD autotask and produces single line output. Each output message is processed and sent separately to the operator on the local NetView.</td>
</tr>
<tr>
<td>CORRWAIT 10</td>
<td>The CORRWAIT 10 stage in the local NetView waits to receive output from the RMTCMD command. For each message received, the CORRWAIT 10 stage has a timeout reset, allowing up to 10 seconds between messages.</td>
</tr>
<tr>
<td>TOSTRING /END OF STATUS DISPLAY/</td>
<td>The TOSTRING stage examines the message buffers for END OF STATUS DISPLAY. When this message is received (which is the last output message of the LIST OPER6 command), the TOSTRING stage causes the CORRWAIT 10 stage to complete as there are no more messages that this pipeline is interested in waiting for.</td>
</tr>
<tr>
<td>COLLECT</td>
<td>The COLLECT stage builds all of its input messages into a single multiple-line message.</td>
</tr>
<tr>
<td>CONSOLE</td>
<td>The CONSOLE stage displays the multiple line message on the operator console.</td>
</tr>
</tbody>
</table>

The output to the local NetView console is similar to Figure 148.

```
NCCF    Tivoli Netview   CNM02 OPER1   04/12/99 14:20:22
* CNM02    PIPE NETVIEW RMTCMD LU=CNM01, OPERID=OPER6, LIST OPER6 | CORRWAIT 10 | TOSTRING /END OF STATUS DISPLAY/ | COLLECT | CONSOLE
- CNM01
STATION: OPER6
HCOPY: NOT ACTIVE PROFILE: DSIPROFA
STATUS: ACTIVE
DOMAIN LIST: CNM01 (I) CNM02 (I) CNM99 (I) B01NV (I)
ACTIVE SPAN LIST: NONE
END OF STATUS DISPLAY
-----------------------------------------------------------------

???
```

Figure 148. Output from Sending a Command to a Remote NetView
Displaying Panels

Use the NetView VIEW command processor to display full-screen panels from your command lists. The VIEW command lets you design your own panels and control the color and highlighting of the panel text. The panels provide interaction between your command lists and the operator. For additional information on using the VIEW command, refer to "Using the VIEW Command" in the Tivoli NetView for OS/390 Customization Guide.

Issuing Messages

Issue messages using the REXX SAY instruction or the NetView MSG, WTO, and WTOR commands. The REXX SAY instruction is used in a command list to issue messages to the operator running the command list. The MSG command sends a message to one or all other operators or to the network log. The WTO command sends a message to the MVS operator console. The WTOR command sends a message to the MVS operator and waits for a reply.

Using the REXX SAY Instruction

You can use the REXX SAY instruction in a REXX command list to issue a character string to the operator, where the character string is any length up to a maximum of 32728 characters. When you issue this instruction in a REXX command list for the NetView program, a 12-character header precedes the data displayed on the operator's screen. The header contains the one-character NetView message type followed by three blanks and the identifier of the domain under which the command list is running. For example, to have the command list process a YES or NO answer from the operator, you can code the following SAY and PARSE PULL instructions:

```rexx
say 'Enter "GO YES" or "GO NO" to continue'
parse pull answer
```

Using MSG

Use the MSG command to send a message to one or all operators or to the network log. For example, to notify all active NetView operators that the system is shutting down in 15 minutes, enter:

```
msg all, system shutdown in 15 minutes
```

To send a message about the status of resource L21E78B to the network log, you can enter the following:

```
msg log, l21e78b was in session with tappl2 at time of failure
```

Using WTO

Use this command for instances that require operator intervention, such as adding paper to a printer or choosing among several processing alternatives. You can send a character string or use a variable name to set the contents of the message you want to send. For example, if printer PRT1 is out of paper, you can send the following message to the MVS system operator console:

```
wto PRINTER PRT1 OUT OF PAPER
```
Using WTOR
Use this command with care because command list processing is suspended while waiting for a reply. If the command list is written in REXX, the operator reply is stored in the WTOREPLY variable, and the ID of the system console that replied is stored in the SYSCONID variable. You can send a character string or use a variable name set to the value of the message you want to send.

For example, you can determine where to send output by sending the following message to the MVS system operator console:

'wtor specify printer to send output to'

Obtaining Input from the Operator
Use the REXX PARSE PULL instruction with the NETVASIS command prefix to receive input from the keyboard without converting the input to uppercase. The input is stored into memory just as it was entered.

For example, in response to the following statements:

say "Hello! What's your name?"
say "Enter 'GO' before your input"
parse pull name

If you enter netvasis go JohNnIe, the value JohNnIe is assigned to the variable name. If you did not use NETVASIS for your input, or if you used the PULL or PARSE UPPER PULL instruction, the value JOHNNIE is assigned to name.

Issuing Commands
Use NetView, VTAM, and MVS commands from within command lists. These commands are limited by the operator’s authority to issue them.

If you include NetView commands, use the appropriate prefix:
• NLDM for session monitor commands
• NPDA for hardware monitor commands
• STATMON for status monitor commands

To include MVS commands, use the NetView MVS command:
'MVS  S  jobname'

For REXXX command lists, commands and character strings are enclosed in quotes. If you use a variable, ensure that it is outside the quotes.

Storing Information in Global Variables
Use the GLOBALV command to allow several command lists to share a common set of values and retain them either temporarily or permanently, for subsequent use.

For example, we have two command lists called FIRST and SECOND. A variable is established as a common global variable in the FIRST command list as follows:

/* Command list FIRST */
count = 99 /* set COUNT to 99 */
'globalv putc count' /* define count as global variable */
The SECOND command list can retrieve the global variable as follows:

/* Command list SECOND */
'globalv getc count' /* retrieve value of COUNT */
say count /* display the value */

For more information on setting and retrieving values of global variables, see "Chapter 20. Storing Information in NetView Global Variables" on page 293.

Accessing Data Set Members

Use the NetView PIPE command to read lines from a sequential file or partitioned data set member to variables.

You can use the TSO/E EXECIO command to:

- Read lines from a sequential file or partitioned data set member to the program stack or variables.
- Write lines from the program stack or variables to a sequential file or a partitioned data set member.

First, use the NetView ALLOCATE command to allocate a data set to the NetView program and to associate it with a name. In this case, the new data set is associated with the name MYFILE.

allocate data set(user.init) file(myfile)

To use PIPE to read all of the lines of MYFILE to a stem variable named MYVAR, specify:

pipe < myfile | stem myvar.'

To use EXECIO to read the first two lines of MYFILE and to assign the variables X.1 and X.2 one line each, specify:

'execio 2 diskr myfile (stem x. finis'

Parsing Input

When arguments are passed to a command list or subroutine, you can use the REXX PARSE ARG instruction to store each of the arguments as variables. For example, the CALL instruction is used to send the data to a command list:

CALL passdata "a string of words",5

The PARSE ARG statement brings the data into the PASSDATA command list, and the PARSE ARG statement assigns the data to separate variables:

/* Command list PASSDATA */
PARSE ARG chardata numdata
PARSE VAR chardata first second third fourth rest
EXIT

The resulting values are stored in the command list variables:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>first</td>
<td>a</td>
</tr>
<tr>
<td>second</td>
<td>string</td>
</tr>
<tr>
<td>third</td>
<td>of</td>
</tr>
<tr>
<td>fourth</td>
<td>words</td>
</tr>
<tr>
<td>numdata</td>
<td>5</td>
</tr>
</tbody>
</table>
Testing a Command List

After you write a command list, test it, if possible, on a test system. REXX provides a useful and powerful TRACE instruction to debug your command lists. If your command list does not behave correctly, you can use this instruction to debug the command list. Some useful forms of the TRACE instruction are:

TRACE I
As each expression is evaluated, the result of each operation (intermediate result) is displayed.

TRACE R
When each expression has been evaluated, the final result is displayed.

TRACE N
Only commands that are rejected by the environment are displayed.

For example, to trace intermediate results for an expression, you can write:

```
TRACE I
... expression
TRACE N
```

For this example:

```
/* Example to show how an expression is evaluated */
x = 9
y = 2
trace I
if x + 1 > 5 * y then
   say "x is big enough"
trace N
```

The following output is displayed:

```
6 *-* if x + 1 > 5 * y
>\*> "9"
>\*> "1"
>\*> "10"
>\*> "5"
>\*> "2"
>\*> "10"
>\*> "0"
8 *-* trace N
```

Where:

** The instruction being traced
>\*> Value of a variable
>\*> Value of a literal
>\*> Result of an operation

You can see that the final result is 0 (false). Because the IF expression is false, the THEN clause is not processed.

Adding a CMDMDL Statement

Use the CMDMDL statement to define both command security *opclasses* and synonyms for command lists. If you choose not to define either for a command list, adding a CMDMDL statement is not required. CMDMDL statements are located in the DSICMD sample. Changes made to DSICMD do not take effect until the NetView program is recycled.
For example, to define a command list called USER001 to the NetView program, add the following statement to DSICMD:

```plaintext
USER001 CMDMDL MOD=DSICCP
```

You can assign the command list a more meaningful name by using the CMDSYN statement. For example, to be able to process the USER001 command list as USERCALC, add the following statement:

```plaintext
USER001 CMDMDL MOD=DSICCP
   CMDSYN USERCALC
```

You can specify command security for the command list using:

- Scope of command authorization
- The NetView command authorization table
- A SAF product such as RACF.

For example, if your system uses scope of command authorization, you can assign CMDCLASS 1 to the USER001 command list. Then, after you recycle NetView so these changes take effect, only operators with scope class 1 or without any scope class values can issue the command list.

```plaintext
USER001 CMDMDL MOD=DSICCP
   CMDSYN USERCALC
   CMDCLASS 1
```

Using the NetView command authorization table or a SAF product, a CMDMDL is not required to protect a command list, command security can be dynamically updated.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
</table>
| Writing REXX command lists | • SAA® Common Programming Interface REXX Level 2 Reference  
|                  | • IBM Compiler and Library for REXX/370 User’s Guide and Reference  
| CMDMDL statements | [NetView Definition Statement Reference](#) in the Tivoli NetView for OS/390 Administration Reference |
| Command security | [Controlling Access to Commands](#) in the Tivoli NetView for OS/390 Security Reference |

---

**Improving the Performance of Command Lists**

Following is a list of things that you can do to improve the performance of your command lists:

- If you have the REXX Compiler product (Compiler and Library for SAA REXX/370), you should compile your REXX command lists once you have verified that they process correctly. Programs run more quickly when compiled, and compiling also provides security, because the actual contents of the compiled command list will be unavailable for viewing.

- If the command list is used frequently you can use the NetView LOADCL or MEMSTOR command to load it into main storage. These provide a faster response time when you run the command list.

For example, to load the command list WTOR2 into main storage, enter:

```plaintext
loadcl wtor2
```
Note: If you issue the LOADCL command for a command list, then update that command list, the changes are not effective until the command list is reloaded.

- Use the REXXENV, REXXSLMT, and REXXSTOR operands in the NetView DEFAULTS and OVERRIDE commands to tune REXX environment values:
  - The REXXENV operand specifies the number of inactive, but initialized, REXX environments to be retained. The default is to retain up to 10 environments per NetView task.
  - The REXXSLMT operand specifies the amount of storage that a REXX environment is allowed to accumulate before being terminated after its current use is completed. The default is unlimited storage.
  - The REXXSTOR operand specifies the amount of initial storage acquired by REXX environment initialization processing. The default is determined by TSO/E.

If a system has storage constraints, setting REXXENV to zero will release all REXX environment storage after processing completes. If a system has processing constraints but available storage, large REXXENV, REXXSLMT, and REXXSTOR values are appropriate.

- If you use command security, especially using a SAF product, specifying SEC=BY on the CMDMDL statement will bypass all security checking and can improve system performance. Do not bypass command security unless you have protected the command list from being modified, and unless you want to allow all operators to be able to use the command list.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tuning automation performance</td>
<td><a href="#">Chapter 21. Optimizing Your Automation</a> on page 297 and</td>
</tr>
<tr>
<td></td>
<td>the <a href="#">Tivoli NetView for OS/390 Tuning Guide</a></td>
</tr>
<tr>
<td>Bypassing command security checking</td>
<td><a href="#">Overview of NetView Security</a> in the <a href="#">Tivoli NetView for OS/390 Administration Reference</a></td>
</tr>
</tbody>
</table>

## Writing an HLL Command Processor

A high-level language (HLL) command processor performs a particular service or function, such as manipulating NetView global variables, processing automated messages, or presenting information to the operator. You can write a HLL command processor using PL/I or C. Under the NetView program, an HLL command processor can:

- Invoke a NetView command, including command lists, REXX command procedures, assembler command procedures, NetView applications such as the session monitor, and other HLL command processors.
- Schedule a NetView command to be processed asynchronously under any NetView task.
- Send requests and wait for replies, even over NetView-NetView cross-domain operator sessions.
- Accept line mode input from the operator.
- Send line mode output to a NetView operator, the operating system console, another task, the authorized receiver, or a group of operators defined by the NetView ASSIGN command.
- Invoke the NetView VIEW command to provide full-screen interaction with the operator.
- Provide for:
- Message trapping
- Message automation
- MSU automation
- Command list variable access
- Access to NetView information such as domain ID or message attributes
- Access to VSAM files

- Send and receive data over the communication network management interface (CNMI)
- Access the NetView partitioned data sets
- Copy storage from one address to another
- Allocate and free an area of virtual storage and associate a name with it so that other HLL command processors running under the same task can access this area of storage
- Obtain, release, and test the control of a named block
- Parse character strings
- Retrieve information on the current NetView environment and obtain attributes of messages
- Update command authorization
- Send message output to the network log, and external log, and a sequential log

When you have written a command processor, you can debug it using the following methods:

- All HLL API service routine calls can be trapped and displayed using a remote interactive debugger (RID).
- ABENDs can be identified from 8-entry continuously wrapping trace entries, which are recorded at entry to and exit from HLL service routines and at other key points inside the HLL routines using the first failure data capture trace (FFDCT).

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Writing an HLL Command Processor</td>
<td>Tivoli NetView for OS/390 Customization: Using PL/I and C</td>
</tr>
</tbody>
</table>

## Writing an Assembler-Language Command Processor

Assembler command processors perform a particular service or function, such as extracting relevant data from a control block and presenting the data to an operator. Although writing in assembler requires a greater coding effort than writing command lists, assembler provides you with the following advantages:

- You can take advantage of special display features of your workstation, such as wide screens or cursor-dependent functions. You can also gain direct access to the 3270 data streams.
- You can handle special data, such as reentrant updates to a global data structure or complex functions at operator logoff or when re-instating after abnormal termination.
- You can access system macros and control blocks.
- You can examine the status of, or wait on, asynchronous events other than the standard set that the VIEW command provides.
- Faster performance of certain kinds of data manipulation.
- Certain NetView exits can only be written in assembler.
<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Writing an assembler-language command processor</td>
<td>Tivoli NetView for OS/390 Customization Using Assembler</td>
</tr>
</tbody>
</table>
You can use NetView global variables to store information about the system or network. The global variables are kept in private storage above 16M. Once a global variable is assigned a value, the value can be retrieved from a command list, command processor, and the automation table. Each NetView operator task, NetView-to-NetView task, and the PPT has its own task global variables that can be used within command lists, command processors, and the automation table only under that task. Common global variables can be shared among all NetView tasks.

Here is a list of the different ways to set and retrieve values of NetView global variables:

<table>
<thead>
<tr>
<th>Environments</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATF('DSICGLOB')</td>
<td>Automation Table</td>
</tr>
<tr>
<td></td>
<td>Retrieving values of common global variables</td>
</tr>
<tr>
<td>ATF('DSITGLOB')</td>
<td>Automation Table</td>
</tr>
<tr>
<td></td>
<td>Retrieving values task global variables</td>
</tr>
<tr>
<td>CGED</td>
<td>Operator console</td>
</tr>
<tr>
<td></td>
<td>Displaying and setting values of common global variables. A panel interface that also supports wildcards of variable names.</td>
</tr>
<tr>
<td>&amp;CGLOBAL</td>
<td>NetView command list language</td>
</tr>
<tr>
<td></td>
<td>Setting and retrieving values of common global variables</td>
</tr>
<tr>
<td>CNMVARS</td>
<td>HLL</td>
</tr>
<tr>
<td></td>
<td>Setting and retrieving values of task and common global variables</td>
</tr>
<tr>
<td>DSIVARS</td>
<td>Assembler</td>
</tr>
<tr>
<td></td>
<td>Setting and retrieving values of task and common global variables</td>
</tr>
<tr>
<td>GLOBALV</td>
<td>REXX, HLL, and NetView command list language</td>
</tr>
<tr>
<td></td>
<td>Setting, retrieving, saving, restoring, and purging task and common global variables</td>
</tr>
<tr>
<td>PIPE</td>
<td>NetView Pipelines</td>
</tr>
<tr>
<td></td>
<td>Setting and retrieving values of common or task global variables</td>
</tr>
<tr>
<td>PIPE VARLOAD</td>
<td>NetView Pipelines</td>
</tr>
<tr>
<td></td>
<td>Setting and retrieving values of common or task global variables</td>
</tr>
<tr>
<td>QRYGLOBL</td>
<td>Operator and NetView command lists</td>
</tr>
<tr>
<td></td>
<td>Displaying NetView global variables</td>
</tr>
<tr>
<td>SETCGLOB</td>
<td>Operator console and NetView command lists</td>
</tr>
<tr>
<td></td>
<td>Setting values of common global variables</td>
</tr>
<tr>
<td>&amp;TGLOBAL</td>
<td>NetView command list language</td>
</tr>
<tr>
<td></td>
<td>Setting and retrieving values of task global variables</td>
</tr>
</tbody>
</table>

Global variable values reside in storage and are not automatically saved when the NetView program ends. Global variables and their values can be explicitly saved to VSAM and restored when the NetView program is restarted.

Designing Global Variables

Use the following steps to design your global variables:

1. Decide on a naming convention for your variables. You can reserve the first several letters of the variable name to indicate grouping and usage of the variables. This makes it simpler to save and restore the values of groups of
variables, and makes the intended usage of a variable clear to anyone reading or modifying your procedures that use the variables. For example, you could name all common global variables that are related to JES such that the variable names begin with JES.

2. Decide whether task global or common global variables are best suited for what you need. You only need to use common global variables to store information that is needed in more than one task.

3. Decide when and where to set the variables. You need to set the value of the variables before the point where the information contained is needed by another process or task. You use the GLOBALV PUTC and the GLOBALV PUTT commands to set the variables.

4. Decide which variables to save in case the NetView program or task is restarted. You can use the GLOBALV SAVEC command to save the contents of any common global variables that you need to access if the NetView program is restarted. You can use GLOBALV SAVET to save the contents of any task global variables that you need to access if the task is restarted. Common global variables and task global variables are saved in the DSISVRT VSAM file.

To keep the global variables with their saved copy in the VSAM database, save the value of the variable immediately after setting it. For example, to set the value of common global variable JESPRT1 to ACTIVE and checkpoint its value, use:

```
JESPRT1=`ACTIVE`
'GLOBALV PUTC JESPRT1'
'GLOBALV SAVEC JESPRT1'
```

You can also save groups of variables with a single command if you have chosen their names carefully. For example, you can save all common global variables relating to JES with the command

```
'GLOBALV SAVEC JES*'
```

5. Decide when and where to retrieve the variable. You need to restore the values of saved common global variables during NetView initialization. Use the GLOBALV RESTC command to restore common global variables to their last saved value before the NetView program ended. One method to accomplish this is to use the NetView automation table to trap message DSI530I for the DSISVRT task and issue the GLOBALV RESTC command.

You can automatically retrieve the values of saved task global variables by adding the GLOBALV RESTT command to the task’s initial command list.

6. If you have thousands of variables, use the QRYGLOBL command to obtain the count of task global and common global variables, and place this number in the NetView constants module (DSICTMOD). With over one thousand variables, this will improve performance when variables are set or retrieved.

7. In general, do not use variable names beginning with EZL, FKV, FKW, FKX or other NetView prefixes.

---

### Displaying the Current Value of a Global Variable

You can display the current value of a global variable by using the QRYGLOBL command. For example, suppose you had set the value of a variable named VTAMSTATUS to DOWN in a REXX command list:

```rexx
/* REXX Command List to set VTAMSTATUS to DOWN */
VTAMSTATUS = 'DOWN'
'GLOBALV PUTC VTAMSTATUS'
EXIT
```

You can display the current value of VTAMSTATUS by using the QRYGLOBL command.

```rexx
QRYGLOBL VTAMSTATUS
```

This command will display the current value of VTAMSTATUS.
You can then display the current value of a common global variable by using the QRYGLOBL command:

```plaintext
qryglobl common vars=vtamstatus
```

The value will be displayed as shown in the following example:

```
BNH031I NETVIEW GLOBAL VARIABLE INFORMATION
BNH103I COMMAND ISSUED AT: 02/09/96 14:22:38
BNH061I
BNH032I COMMON GLOBAL VARIABLES
BNH036I GLOBAL VARIABLE NAME: GLOBAL VARIABLE VALUE:
BNH061I --------------------- ----------------------
BNH039I VTAMSTATUS        DOWN
BNH035I NUMBER OF VARIABLES FOUND: 1
BNH061I
BNH037I NETVIEW GLOBAL VARIABLE INFORMATION COMPLETE
```

In the previous example, notice the value of VTAMSTATUS is DOWN as set by the preceding command list. The expected number of variables is the value found in the NetView constants module (DSICTMOD). The actual number of variables is the number of common global variables which currently have been defined.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>&amp;TGLOBAL, &amp;CGLOBAL, and GLOBALV</td>
<td>Tivoli NetView for OS/390 Customization: Using REXX and the NetView Command List Language</td>
</tr>
<tr>
<td>CNM_VARS</td>
<td>Tivoli NetView for OS/390 Customization: Using PL/I and C</td>
</tr>
<tr>
<td>DSIVARS</td>
<td>Tivoli NetView for OS/390 Customization: Using Assembler</td>
</tr>
<tr>
<td>QRYGLOBL, SETCGLOB, and other commands</td>
<td>NetView online help</td>
</tr>
<tr>
<td>ATF('DSICGLOB') and ATF('DSITGLOB')</td>
<td>Tivoli NetView for OS/390 Automation Guide</td>
</tr>
<tr>
<td>Specifying the expected number of tasks and common global variables</td>
<td>Tivoli NetView for OS/390 Automated Operations Network User’s Guide</td>
</tr>
<tr>
<td>(performance enhancement)</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 21. Optimizing Your Automation

You can use NetView and the operating system to filter and suppress incoming information. This can:
• Decrease system traffic, resulting in improved system performance
• Decrease the number of messages sent the operator console.

Deciding Which Alerts to Filter

For Graphical Enterprise feature and Procedural feature users: To decide what alerts to filter, use the information from the Alerts-Dynamic panel or from the Most Recent Events panel.

Use the following steps to decide what to filter:
1. Disable all filter settings: the default filter settings and the filters that you set. Alerts for all events will then be created and displayed.
2. From this information, decide what is important and what is not using these criteria:
   • Exclude alerts that you do not need
   • Add alerts that are critical

See “Overview of Filter Types” on page 194 for additional information on constructing filters.

Deciding Where to Filter Each Alert

The NetView program provides a set of default filters that you can override. Use the PDFILTER command list to set your recording filters. It is invoked by the automation table when the NetView program is initialized.

Implementing Filtering Decisions

Using the XITCI exit can optimize performance. An XITCI exit written in assembler can be the quickest way to filter MSUs within NetView.

The XITCI exit is called by the BNJDSERV task after receiving an MSU. You can modify, replace, or delete MSUs before they go to the automation table or to the hardware monitor database. The XITCI exit lets you implement functions that the NetView program does not normally provide. An advantage of using BNJDSERV’s XITCI exit instead of DSICRTR’s is that BNJDSERV processes MSUs from ALERT-NETOP, in addition to MSUs from DSICRTR. For MVS, XITCI can be written in assembler, PL/I, or C, but assembler is recommended for performance reasons.

In unusual conditions, you might want to bypass normal filtering. You can write an XITCI installation exit routine that gives a return code of 252 to specify external logging only for a record. In this case, NetView sets all filters to BLOCK for the record. You can also give an XITCI return code of 253, in which case NetView sets the ESREC filter to PASS but all other filters to BLOCK.

Using the RATE Statement

The number of events that are recorded before the newest one replaces the oldest one is specified by the WRAP value of the hardware monitor initialization member with supplied name BNJMBDST. The rate at which new events can replace old ones is controlled by the RATE statement. If the time between the newest event
being recorded and the oldest event being overwritten is less than the value in RATE, a filter is set up to block recording for that event. This provides a way to avoid a situation where a major outage can cause the Alerts-Dynamic panel to be flooded by the same event, such as when a T1 line goes down and the peripheral resource events conceivably fill the screen.

The filter created as a result of the RATE statement remains in effect until NetView is restarted or until the operator initiates a delete. It is recommended that you check filter settings after a major outage and then delete any filters added by the RATE statement, either explicitly or using automation.

The steps to automate this procedure are as follows:
1. Create an automation table statement for the message that was generated when the RATE statement request was processed.
2. Create an event using GENALERT to notify the operator that the RATE statement has been processed.
3. Invoke a timer using the AFTER command to run a command list after a specified interval to clear the filter.

Using the Hardware Monitor SRFILTER Command
One way to implement filters using the hardware monitor SRFILTER command is to make a broad filtering decision. For example, you can filter all the MSUs associated with a particular product. You can then fine tune the filtering by using the automation table SRF action for specific overrides.

Using the Automation Table SRF Function
The SRF function in an IF/THEN statement of the automation table allows you to filter individual alerts or MSUs. Any filtering done in the automation table will override previously set SRFILTER statements for that specific alert or MSU.

Using the DSIEX16B Exit
The NetView program calls DSIEX16B after an MSU has been processed by the automation table and before any commands issued from the automation table are processed. You can examine or modify an MSU and its attributes, change the results of automation processing, or monitor the effectiveness of your MSU automation.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examining and altering MSUs</td>
<td><a href="#">Writing Installation Exit Routines</a> in <a href="#">Tivoli NetView for OS/390 Customization: Using Assembler</a> and <a href="#">Tivoli NetView for OS/390 Customization: Using PL/I and C</a></td>
</tr>
</tbody>
</table>

Suppressing a System Message
One of the first steps in automating operations is to suppress unnecessary messages. Your operating system has facilities for suppressing unnecessary system messages before they get to NetView. Those facilities are the message processing facility (MPF) for MVS, programmable operator (PROP) for VM, and Operator Communication Control Facility (OCCF) for VSE. Some system messages, such as MVS messages which must be identified by both message ID and job name, cannot be suppressed by the operating system. In this case, you can trap the message using the NetView automation table.
Using MVS Message Processing Facility (MPF)

On MVS systems, use MPF to suppress unnecessary system messages. System messages are messages from systems, subsystems, and applications; they include WTOs and WTORs. To suppress system messages, enter statements in an MPFLSTxx member in SYS1.PARMLIB. NetView provides two sample MPFLSTxx members in CNMSAMP, CNMS6201, and CNMS6202. You can combine these samples to form an MPFLSTxx, or code an MPFLSTxx of your own.

In the following example, logon and logoff messages are not to be retained and are to be suppressed from display:

```
.DEFAULT,RETAIN(NO),SUP(YES)
IEF125I /*LOGGED ON*/
IEF126I /*LOGGED OFF*/
```

This example will be used to show how to code an MPF statement to suppress a system message.

The steps are as follows:

1. Use the .DEFAULT statement to apply a common set of options to a list of messages. The system applies the options to each statement listed below that statement, until a new .DEFAULT statement is encountered.

```
.DEFAULT,RETAIN(NO),SUP(YES)
IEF125I /*LOGGED ON*/
IEF126I /*LOGGED OFF*/
```

2. Specify RETAIN(YES) in the .DEFAULT statement to retain a message in the action message retention facility. Otherwise, add RETAIN(NO): This option applies only to action messages or WTORs.

```
.DEFAULT,RETAIN(NO),SUP(YES)
IEF125I /*LOGGED ON*/
IEF126I /*LOGGED OFF*/
```

3. Specify SUP(NO) in the .DEFAULT statement to enable the messages to be displayed on the MCS console; otherwise, specify SUP(YES):

```
.DEFAULT,RETAIN(NO),SUP(YES)
IEF125I /*LOGGED ON*/
IEF126I /*LOGGED OFF*/
```

4. Add the messages that are to be suppressed:

```
.DEFAULT,RETAIN(NO),SUP(YES)
IEF125I /*LOGGED ON*/
IEF126I /*LOGGED OFF*/
```

Forwarding a Message to NetView:

To allow a message to be eligible for NetView automation, use the AUTO(YES) option in the .DEFAULT statement. For example, to inhibit IMS messages having a prefix of DFS from displaying on the system console but mark them eligible for automation by the NetView program, enter:

```
.DEFAULT,AUTO(YES),RETAIN(NO),SUP(YES)
DFS* /*messages beginning with DFS (IMS messages)*/
```

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Using MPF installation exits</td>
<td>MVS/ESA System Programming Library: Installation Exits</td>
</tr>
</tbody>
</table>
Suppressing VTAM Messages

Use values on the SUPP= keyword of the MODIFY VTAM command to suppress VTAM messages at their source. For instance, specifying SUPP=INFO will suppress information messages, SUPP=WARN suppresses both warning and information messages, and SUPP=NORM suppresses normal, warning, and information messages.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>MODIFY VTAM command</td>
<td>Refer to the VTAM Library.</td>
</tr>
</tbody>
</table>
Chapter 22. Monitoring NetView Automation

Although automation can solve many problems and relieve network and system operators from repetitive tasks, there are times when it does not work as expected.

It is important to monitor automation to detect automation problems early, and notify operators when automated recovery has stopped.

Using Operations Planning and Control/ESA

The following topics describe how you can use operations planning and control/ESA functions to manage operations and workstations.

OLTP Shutdown Triggered by OPC/ESA Deadline WTOs

When you define your online transaction processing (OLTP) regions to OPC/ESA you can specify that a write-to-operator (WTO) be issued when the operation reaches its deadline time. The resulting WTO can be used to issue the appropriate commands to shutdown the region and report back to OPC/ESA that the process is complete thereby enabling the batch workload to commence. The OPC/ESA sample library member EQQNETW1 provides you a NetView command list to trap the deadline WTO message generated by OPC/ESA and issue the commands to shutdown the online system.

Setting Special Resource Availability

Sometimes, the availability of a special resource cannot be determined directly by OPC/ESA, that is, the fact that a task is started does not necessarily imply it is ready for subsequent processing. This is especially true in the case of OLTPs, where programs and databases can be stopped and started individually. In such cases you can use the OPC/ESA sample library member EQQNETW3 to build a special resource availability event when the condition is detected.

Invoking the OPC/ESA Program Interface (PIF) or the API

OPC/ESA provides a program interface (PIF) which can be used to perform any of the functions available in the dialog. Additionally, you can use the OPC/ESA API from any SAA compliant platform to get information about the operations and workstations in the current plan. The OPC/ESA sample library contains many PIF and AOI programs that can be used for many purposes from many operating environments.

Scheduling NetView Activities from OPC/ESA

OPC/ESA has powerful scheduling capabilities which can be customized for your business processing cycles, work days, and holidays. You can schedule a WTO operation to trigger a NetView process on the day you want and at the time you want, once business dependencies have been satisfied. Schedules are customized by modifying sample EQQNETW2.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using OPC/ESA</td>
<td>Operations Planning and Control Messages and Diagnosis Guide</td>
</tr>
</tbody>
</table>
Chapter 23. Debugging Automation

In the course of automating your enterprise using the NetView program, there might be times when the unexpected will happen: 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) should 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 should 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 CNMSSIR task is active. Issue the NetView command, LIST STATUS=OPT, to find out if the CNMSSIR 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 CNMSSIR active

Optionally, you can have another task receive AUTO(YES) messages.

Checking Other Areas

Following are additional steps you can follow 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 due to 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 as well as 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 there are multiple statements in the automation table that 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 23 on page 305](#) shows how to interpret some of the data from the detail report.
Table 23. Determining Why a Message Was Not Automated Using the Detail Report

<table>
<thead>
<tr>
<th>Indicators</th>
<th>Possible explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMPARE COUNT &gt; 0</td>
<td>The automation table statement might be coded incorrectly,</td>
</tr>
<tr>
<td>MATCH COUNT = 0</td>
<td>in which case the automation statement never matches the message</td>
</tr>
<tr>
<td>MATCH COUNT = 0</td>
<td>It is possible that a prior statement in the automation table</td>
</tr>
<tr>
<td>COMPARE COUNT = 0</td>
<td>matches the message and prevents the statement from being processed</td>
</tr>
</tbody>
</table>

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 will 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. Examples of situations that will cause a command list to not finish running, thus possibly preventing other command lists from running, are:
  - Using an &WAIT (NetView command list) or a TRAP or WAIT (REXX) without a timeout value. The command list will wait 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, will cause the command list to wait forever because there is no console to provide input.
  - Using a WTOR to the system console that never gets a reply.
  - Processing in an infinite loop, which will never complete.

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 will 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 CMDMDL statement.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The AUTOTBL, AUTOCNT,</td>
<td>NetView online help</td>
</tr>
<tr>
<td>and TASKUTIL commands</td>
<td></td>
</tr>
</tbody>
</table>
### 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('MSGNETOP1 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) = 'xxxxxxxx' 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 due to 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 there are multiple statements in the automation table that 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 24 shows how to interpret some of the data from the detail report.

Table 24. Determining Why an Alert Was not Automated Using the Detail Report

<table>
<thead>
<tr>
<th>Indicators</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMPARE COUNT &gt; 0 MATCH COUNT = 0</td>
<td>The automation table statement might be coded incorrectly, in which case the automation statement never matches the alert</td>
</tr>
<tr>
<td>MATCH COUNT = 0 COMPARE COUNT = 0</td>
<td>It is possible that a prior statement in the automation table matches the alert and prevents the statement from being processed</td>
</tr>
</tbody>
</table>

8. Determine whether the conditions and actions are coded correctly on the automation statement.

9. Determine whether there is a typographical error in an automation table MSUSEG function.

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 will 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. Examples of situations that cause a command list to not finish running, thus possibly preventing other command lists from running, are:

   - Using an &WAIT (NetView command list) or a TRAP or WAIT (REXX) without a timeout value. The command list will wait 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 there is no console to provide input, the command list will wait forever. This applies only to command lists running under an autotask.
– Using a WTO to the system console that never gets a reply.
– Processing in an infinite loop, which will never complete.

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 will not indicate commands scheduled with timer commands, started using EXCMD from other tasks, and other non-operator commands.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>RATE, AUTORATE</td>
<td>statements [NetView Definition Statement Reference] in the Tivoli NetView for OS/390 Administration Reference</td>
</tr>
<tr>
<td>SRFILTER, AUTOTBL, AUTOCNT, TASKUTIL commands</td>
<td>NetView online help</td>
</tr>
<tr>
<td>Using the TASKUTIL command</td>
<td>“Additional Tuning Considerations” in the Tivoli NetView for OS/390 Tuning Guide</td>
</tr>
<tr>
<td>MSUSEG condition item</td>
<td>[Automating Messages and MSUs] in Tivoli NetView for OS/390 Automation Guide</td>
</tr>
<tr>
<td>DSIEX16B installation exit</td>
<td>[Writing Installation Exit Routines] in Tivoli NetView for OS/390 Customization: Using Assembler</td>
</tr>
</tbody>
</table>

**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 [Tivoli NetView for OS/390 Command Reference] for information on how to code the TECROUTE filter. The TECROUTE filter may 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 Tivoli NetView for OS/390 V1R4 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 would result in a NetView error message, and the event would not be 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 Tivoli NetView for OS/390 V1R4. Check the following:
   - 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 may 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 may 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
Determining Why a Command List Does Not Complete

There are times when 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:
   - Scope of command authorization
   - The NetView command authorization table
   - A SAF product, such as RACF

   If command security prevented the command list from running, message DSI213I in the netlog will indicate that the command list is being protected.

   Look in the DSICMD members for a CMDMDL statement. If you use a synonym for the command list, the command identifier in the CMDMDL statement should match the command security in effect. Without a CMDMDL statement, the command list cannot be protected by scope of command authorization.

   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 CMDMDL statement.

   If your security administrator has set up command security to protect your command list, refer to "Checklist for Debugging Security Problems" and to "Controlling Access to Commands" in the Tivoli NetView for OS/390 Administration Reference to get your security matching your expectations.

2. Verify that the command list was called correctly, as follows:

<table>
<thead>
<tr>
<th>If called from...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automation table</td>
<td>Verify that it ran under an active task. Unless you specify otherwise, there should be a CNM493I message in the network log for each command list called from the automation table.</td>
</tr>
<tr>
<td>A TIMER command</td>
<td>Verify that the timed command was scheduled to run, and that the task that was to run the command was active.</td>
</tr>
<tr>
<td>Another command list</td>
<td>Check to see that the logic path to call the command list was taken in the prior command list.</td>
</tr>
</tbody>
</table>

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 there is no console 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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRACE, PULL instruction</td>
<td>TSO/E REXX/MVS Reference</td>
</tr>
<tr>
<td>WAIT instruction</td>
<td>REXX Instructions Provided by NetView in Tivoli NetView for OS/390 Customization: Using REXX and the NetView Command List Language</td>
</tr>
<tr>
<td>CMD, DEFAULTS, OVERRIDE, RESET, TASKUTIL commands</td>
<td>NetView online help</td>
</tr>
<tr>
<td>Using the TASKUTIL command</td>
<td>“Additional Tuning Considerations” in the Tivoli NetView for OS/390 Tuning Guide</td>
</tr>
</tbody>
</table>

**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 could be protecting using scope of command authorization, NetView command authorization table, or a SAF product such as RACF.

In addition, depending which task is checked for command authorization, there could be the wrong level of authorization at the source of the timer command, or the ability of timer commands to route a command to be processed under another task (for instance, using the RUNCMD command). Refer to [Checklist for Debugging Security Problems] and to [Controlling Access to Commands] in the Tivoli NetView for OS/390 Administration Reference to get your timer command security matching your expectations.
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 will run 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 due to 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, the command should be scheduled to run under an autotask or other operator task.

6. Determine whether the timer command was issued successfully. For example, it should have been issued from a command list but the command list never completed due to a syntax error in the command. The NetView log should contain 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. Examples of situations that will cause a command list to continue running, thus possibly preventing other command lists from running, are:
   • Using an &WAIT (NetView command list) or a TRAP or WAIT (REXX) without a timeout value. The command list will wait 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 there is no console to provide input, the command list will 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 will never complete.

See "Determining Why a Command List Does Not Complete" on page 310 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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFTER, AT, EVERY command</td>
<td>NetView online help</td>
</tr>
</tbody>
</table>
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 CPU, 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 (CPU 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 will result in processing savings.
- 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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>TASKUTIL, AUTOCNT commands</td>
<td>NetView online help</td>
</tr>
<tr>
<td>Using the TASKUTIL command</td>
<td>“Additional Tuning Considerations” in the Tivoli NetView for OS/390 Tuning Guide</td>
</tr>
<tr>
<td>Using the AUTOCNT command</td>
<td>“Tuning for Automated Operations” in the Tivoli NetView for OS/390 Tuning Guide</td>
</tr>
<tr>
<td>Using the XITCI exit</td>
<td>[Writing Installation Exit Routines] in Tivoli NetView for OS/390 Customization: Using Assembler</td>
</tr>
<tr>
<td>TASKMON</td>
<td>NetView Online Help</td>
</tr>
</tbody>
</table>

Determining Why a Message Is Routed to the Wrong Operator

Following are some things that you can check 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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASSIGN, LIST commands</td>
<td>NetView online help</td>
</tr>
<tr>
<td>EXEC(ROUTE) action</td>
<td>[Automating Messages and MSUs](Tivoli NetView for OS/390 Automation Guide)</td>
</tr>
<tr>
<td>MSGROUTE command</td>
<td>[Automation Resource Management](Tivoli NetView for OS/390 Customization: Using REXX and the NetView Command List Language)</td>
</tr>
<tr>
<td>Solicited and unsolicited messages</td>
<td>[How Messages Flow](Tivoli NetView for OS/390 Customization: Using Assembler)</td>
</tr>
<tr>
<td>Exits DSIEX16 and DSIEX17</td>
<td>[Control Blocks](Tivoli NetView for OS/390 Customization: Using Assembler)</td>
</tr>
<tr>
<td>Exit DSIEX02A</td>
<td>[Control Blocks](Tivoli NetView for OS/390 Customization: Using Assembler) or [HLL Installation Exit Routines](Tivoli NetView for OS/390 Customization: Using PL/I and C)</td>
</tr>
</tbody>
</table>

**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 [Tivoli NetView for OS/390 Customization: Using Pipes](Tivoli NetView for OS/390 Customization: Using Pipes).
Part 5. Problem Diagnostics

Chapter 24. Proactive Investigating .............................................. 319
Preventing Problems ................................................................. 319
Analyzing System Performance Using TASKUTIL (Command Facility) .... 320
Initiating Error Recovery (Status Monitor) .................................. 322
Displaying Resource Status (Status Monitor) ............................... 322
Identifying Intermittent Problems (Hardware Monitor) .................... 324
Determining Controller Status (Hardware Monitor) ......................... 325
Checking Session Monitor and Hardware Monitor Database Status (Command Facility) ............................................. 329

Chapter 25. Reactive Investigating ................................................. 331
Hung Session (Session Monitor) .................................................. 331
Broken Session (Session Monitor) ................................................ 334
Line Failure (Hardware Monitor) .................................................. 338
Blocked Virtual Route (VTAM) ...................................................... 344
Modem Problems (Status Monitor, Hardware Monitor, Session Monitor) ... 344
Hung or Looping NetView Tasks (Command Facility) ....................... 351
NetView Abends (First Failure Support Technology) ....................... 351
  FASTService Option ................................................................. 352
  Resolving an Abend ............................................................... 352
Measuring Response Time with Control Units Using RTM (Session Monitor) 353
Sluggish Network Performance (NPM) .......................................... 355
Using the NetView Help Desk ...................................................... 365

Chapter 26. Managing Problems .................................................... 367
Using the Hardware Monitor ...................................................... 367
  Creating a Problem Report ...................................................... 368
Using NetView AutoBridge/MVS .................................................. 369
  Implementing NetView AutoBridge ............................................. 370
Chapter 24. 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 24. 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 AON/LAN Automation, the NetView Graphic Monitor Facility, command facility, status monitor, and hardware monitor. For more information on user scenarios you can use the Tivoli OS/390 Tutorial.

Chapter 25. Reactive Investigating on page 331 provides problem scenarios that illustrate how to solve problems that have already occurred. The tools used to solve these problems are the NetView Graphic Monitor Facility, session monitor, hardware monitor, VTAM commands, NPM, AON (including AON/LAN), command facility, and First Failure Support Technology (FFST).

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 25 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 25. Proactive Scenarios Cross Reference

<table>
<thead>
<tr>
<th>Problem Scenario</th>
<th>Component Used to Resolve Problem</th>
<th>Resources Involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyzing system performance using TASKUTIL</td>
<td>Command facility</td>
<td>Subarea</td>
</tr>
<tr>
<td>Initiating error recovery</td>
<td>Status monitor</td>
<td>Subarea</td>
</tr>
<tr>
<td>Displaying the status of a resource</td>
<td>Status monitor</td>
<td>Subarea</td>
</tr>
<tr>
<td>Identifying intermittent problems</td>
<td>Hardware monitor</td>
<td>Subarea</td>
</tr>
<tr>
<td>Determining controller status</td>
<td>Hardware monitor</td>
<td>Subarea</td>
</tr>
<tr>
<td>Checking the status of the session monitor and hardware monitor databases</td>
<td>Command facility</td>
<td>Subarea</td>
</tr>
<tr>
<td>Generating LAN traffic reports</td>
<td>AON/LAN Automation</td>
<td>non-SNA</td>
</tr>
<tr>
<td>Anticipate excessive use of task resources</td>
<td>Command facility</td>
<td>task-specific CPU, storage, I/O, task-to-task messages</td>
</tr>
<tr>
<td></td>
<td>Automate messages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BNH162I and BNH163I</td>
<td></td>
</tr>
<tr>
<td>Anticipate depletion of NetView's address space storage</td>
<td>Command facility</td>
<td>Netview storage</td>
</tr>
<tr>
<td></td>
<td>Automate messages</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BNH162I and BNH163I</td>
<td></td>
</tr>
</tbody>
</table>
Analyzing System Performance Using TASKUTIL (Command Facility)

This topic applies to Unattended, Procedural, and Graphical Enterprise features users.

You can use the TASKUTIL or the newer TASKMON command to display performance information, including central processing unit (CPU) utilization, queue lengths, storage use, and active command lists. Consider setting an EVERY timer under an autotask to invoke TASKUTIL or TASKMON at least once a day (or even once every hour). The output from TASKUTIL can be compared to the previous day’s output and used to diagnose performance or storage problems.

For example, if you enter:

```bash
taskutil type=dst
```

A response similar to **Figure 149** is received (by default, command responses are also sent to the network log).

For each task, the task name (TASKNAME), task type (TYPE), dispatching priority (DPR), and CPU usage (CPU-TIME) is displayed. In addition, the following information (shown in **Figure 149**) is displayed to enable you to diagnose performance or storage problems.

```
<table>
<thead>
<tr>
<th>TASKNAME</th>
<th>TYPE</th>
<th>DPR</th>
<th>CPU-TIME</th>
<th>N-CPU%</th>
<th>S-CPU%</th>
<th>MESSAGEQ</th>
<th>STORAGE-K</th>
<th>CMDLIST</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAUTSKLP</td>
<td>DST</td>
<td>249</td>
<td>22019.13</td>
<td>49.02</td>
<td>9.37</td>
<td>0</td>
<td>87521</td>
<td>N/A</td>
</tr>
<tr>
<td>BNJDSERV</td>
<td>DST</td>
<td>250</td>
<td>4466.25</td>
<td>7.35</td>
<td>1.41</td>
<td>0</td>
<td>357</td>
<td>N/A</td>
</tr>
<tr>
<td>DSIELTSK</td>
<td>DST</td>
<td>253</td>
<td>4731.99</td>
<td>7.24</td>
<td>1.38</td>
<td>0</td>
<td>31</td>
<td>N/A</td>
</tr>
<tr>
<td>DSICRTR</td>
<td>DST</td>
<td>251</td>
<td>1362.16</td>
<td>1.97</td>
<td>0.38</td>
<td>0</td>
<td>32</td>
<td>N/A</td>
</tr>
<tr>
<td>DSILog</td>
<td>DST</td>
<td>254</td>
<td>624.64</td>
<td>1.40</td>
<td>0.27</td>
<td>0</td>
<td>23</td>
<td>N/A</td>
</tr>
<tr>
<td>DSIAMLUT</td>
<td>DST</td>
<td>248</td>
<td>1145.74</td>
<td>1.34</td>
<td>0.26</td>
<td>0</td>
<td>26</td>
<td>N/A</td>
</tr>
<tr>
<td>AAUTCNMI</td>
<td>DST</td>
<td>249</td>
<td>94.44</td>
<td>0.33</td>
<td>0.06</td>
<td>0</td>
<td>463</td>
<td>N/A</td>
</tr>
<tr>
<td>BNJDSE36</td>
<td>DST</td>
<td>249</td>
<td>0.04</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>25</td>
<td>N/A</td>
</tr>
<tr>
<td>CNMTAMEL</td>
<td>DST</td>
<td>249</td>
<td>0.36</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>49</td>
<td>N/A</td>
</tr>
<tr>
<td>CNM01LUC</td>
<td>DST</td>
<td>251</td>
<td>306.54</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>43</td>
<td>N/A</td>
</tr>
<tr>
<td>DSI0GDS</td>
<td>DST</td>
<td>254</td>
<td>1.89</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>46</td>
<td>N/A</td>
</tr>
<tr>
<td>DSIP0DST</td>
<td>DST</td>
<td>252</td>
<td>2.15</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>39</td>
<td>N/A</td>
</tr>
<tr>
<td>DSIKREM</td>
<td>DST</td>
<td>250</td>
<td>2.15</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>549</td>
<td>N/A</td>
</tr>
<tr>
<td>DSIROVS</td>
<td>DST</td>
<td>251</td>
<td>0.03</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>13</td>
<td>N/A</td>
</tr>
<tr>
<td>DSISOVST</td>
<td>DST</td>
<td>253</td>
<td>0.93</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>105</td>
<td>N/A</td>
</tr>
<tr>
<td>DSIUODST</td>
<td>DST</td>
<td>250</td>
<td>2.59</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>14</td>
<td>N/A</td>
</tr>
<tr>
<td>DSIDO8ST 251</td>
<td>DST</td>
<td>28.98</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>41</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>NETVIEW OTHR</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>0.00</td>
<td>0.00</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>NETVIEW SRB</td>
<td>N/A</td>
<td>4026.90</td>
<td>5.93</td>
<td>1.13</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>NETVIEW TOTAL</td>
<td>157</td>
<td>54766.96</td>
<td>100.00</td>
<td>19.11</td>
<td>253</td>
<td>157477</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>SYSTEM TOTAL</td>
<td>N/A</td>
<td>N/A</td>
<td>63.70</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
```

*Figure 149. TASKUTIL Command Output*

and CPU usage (CPU-TIME) is displayed. In addition, the following information (shown in **Figure 149**) is displayed to enable you to diagnose performance or storage problems.
### Table 26. TASKUTIL Output Description

<table>
<thead>
<tr>
<th>Field Name/Description</th>
<th>How to Use</th>
</tr>
</thead>
</table>
| **N-CPU% (NetView program CPU utilization)** Task’s relative contribution to the NetView program’s CPU utilization, based on a maximum of 100%. | - If this value is continuously high for an operator task, autotask, distributed task, or NNT, this could 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 build-up for an operator task, autotask, distributed task, or NNT, this could indicate that the command list is stuck in a WAIT. |
| **S-CPU% (system CPU utilization)** Task’s contribution to the total system CPU utilization, based on a maximum of 100%. | - If this value is continuously high for an operator task, autotask, distributed task, or NNT, this could 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 build-up for an operator task, autotask, distributed task, or NNT, this could indicate that the command list is stuck in a WAIT. |
| **MESSAGEQ** Number of messages currently backed up on the task’s 3 public message queues (HIGH, NORMAL, and LOW). | - If this value is high, with the same command list active and low CPU usage for an operator task, autotask, distributed autotask, or NNT, this could 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 the NetView program’s workload activity should be fairly uniform, and if the total system CPU utilization is near 100%, this could 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 CPU-intensive applications to relieve the system CPU 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 could 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 build-up and low CPU usage for an operator task, autotask, distributed autotask, or NNT, this could indicate that the command list is stuck in a WAIT. |

### Topic: Reference:

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tuning your system using TASKUTIL</td>
<td>Additional Tuning Considerations in the Tivoli NetView for OS/390 Tuning Guide</td>
</tr>
<tr>
<td>TASKUTIL command</td>
<td>NetView online help</td>
</tr>
</tbody>
</table>
Initiating Error Recovery (Status Monitor)

**Graphical Enterprise feature or Procedural feature users** 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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>MONIT, MONON, MONOFF commands</td>
<td>NetView online help</td>
</tr>
</tbody>
</table>

Displaying Resource Status (Status Monitor)

This topic applies to **Graphical Enterprise or Procedural feature users only**.

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 150 on page 323 is displayed.
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 100.

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 151 on page 324 is displayed.

---

<table>
<thead>
<tr>
<th>STATMON.DSS</th>
<th>DOMAIN STATUS SUMMARY</th>
<th>15:24</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOST: HOST01</td>
<td><em>1</em></td>
<td><em>2</em></td>
</tr>
<tr>
<td>....3 NCP/CA/LAN/PK</td>
<td>ACTIVE</td>
<td>PENDING</td>
</tr>
<tr>
<td>....17 LINES</td>
<td>....2</td>
<td>......</td>
</tr>
<tr>
<td>....47 PUS/CLUSTERS</td>
<td>....1</td>
<td>......</td>
</tr>
<tr>
<td>....1 SWITCHED/XCA</td>
<td>......</td>
<td>......</td>
</tr>
<tr>
<td>....1 PU/XCA LINE</td>
<td>......</td>
<td>......</td>
</tr>
<tr>
<td>....1 LU/XCA PU</td>
<td>......</td>
<td>......</td>
</tr>
<tr>
<td>....2 LOCAL MAJ NDS</td>
<td>......</td>
<td>......</td>
</tr>
<tr>
<td>....1 PUS</td>
<td>......</td>
<td>......</td>
</tr>
<tr>
<td>....13 LUS/TERMS</td>
<td>......</td>
<td>......</td>
</tr>
<tr>
<td>....3 APPL MAJ NDS</td>
<td>......</td>
<td>......</td>
</tr>
<tr>
<td>....87 APPLICATIONS</td>
<td>......</td>
<td>......</td>
</tr>
<tr>
<td>....1 CDRM MAJ NDS</td>
<td>......</td>
<td>......</td>
</tr>
<tr>
<td>....5 CDRMS</td>
<td>......</td>
<td>......</td>
</tr>
<tr>
<td>....1 CDRSC MAJ NDS</td>
<td>......</td>
<td>......</td>
</tr>
<tr>
<td>....2 CDRSCS</td>
<td>......</td>
<td>......</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>....185 TOTAL NODES</td>
<td>......</td>
<td>......</td>
</tr>
</tbody>
</table>

Figure 150. Domain Status Summary 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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring and controlling resources using the status monitor</td>
<td>[Using the Status Monitor (SNA Subarea)” on page 99]</td>
</tr>
</tbody>
</table>

Figure 151. 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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring and controlling resources using the status monitor</td>
<td>[Using the Status Monitor (SNA Subarea)” on page 99]</td>
</tr>
</tbody>
</table>

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.
Interruption problems are often related to performance problems. For example, if a resource oscillates between active and inactive, try to see if there is a correlation between the problem and the time it occurs. If the problem occurs during a period of high system usage, this could indicate a performance problem. You might then have to tune your system's performance (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 136. You might want to keep in mind the following failure-cause code points used to identify intermittent problems:

<table>
<thead>
<tr>
<th>Hex value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0411</td>
<td>INTERMITTENT STORAGE CONTROLLER ERROR</td>
</tr>
<tr>
<td>0412</td>
<td>INTERMITTENT WORKSTATION CONTROLLER ERROR</td>
</tr>
<tr>
<td>0413</td>
<td>INTERMITTENT COMMUNICATIONS SUBSYSTEM CONTROLLER ERROR</td>
</tr>
</tbody>
</table>

### Determining Controller Status (Hardware Monitor)

This topic applies to Graphical Enterprise and Procedural feature users only.

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 152 on page 326 is displayed.
2. Select option 5 to display the Controller Information Display panel. A panel similar to Figure 153 is displayed.

Figure 152. Hardware Monitor Main Menu

3. Enter the name of the controller for which to display information in the command line. A panel similar to Figure 153 on page 327 is displayed.

Figure 153. Hardware Monitor Controller Information Display Panel
4. Select option 1 to display link data for the controller. A panel similar to Figure 155 is displayed.

**Figure 154. Hardware Monitor Controller Selection Menu Panel**

**Figure 155. 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 156 is displayed.

![Figure 156. Hardware Monitor Release Level Panel](image)

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 157 on
page 329 is displayed.
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 158 on page 330 shows the response to the LISTCAT command.
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 should 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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintaining hardware monitor databases (including switching to a secondary database using the DBAUTO command)</td>
<td><a href="#">“Maintaining the Hardware Monitor Database” on page 21</a></td>
</tr>
<tr>
<td>Maintaining session monitor databases (including switching to a secondary database using the DBAUTO command)</td>
<td><a href="#">“Using and Maintaining the Session Monitor Database” on page 214</a></td>
</tr>
<tr>
<td>DBAUTO command</td>
<td>NetView online help</td>
</tr>
</tbody>
</table>

---

**Figure 158. 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 should 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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintaining hardware monitor databases (including switching to a secondary database using the DBAUTO command)</td>
<td><a href="#">“Maintaining the Hardware Monitor Database” on page 21</a></td>
</tr>
<tr>
<td>Maintaining session monitor databases (including switching to a secondary database using the DBAUTO command)</td>
<td><a href="#">“Using and Maintaining the Session Monitor Database” on page 214</a></td>
</tr>
<tr>
<td>DBAUTO command</td>
<td>NetView online help</td>
</tr>
</tbody>
</table>
Chapter 25. 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 27 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 may not be applicable, depending on which option of NetView is installed.

Table 27. Reactive Investigating Cross Reference

<table>
<thead>
<tr>
<th>Problem Scenario</th>
<th>Product Used to Resolve the Problem</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finding and repairing the cause of a hung session</td>
<td>Session monitor</td>
<td>331</td>
</tr>
<tr>
<td>Finding and repairing the cause of a broken session</td>
<td>Session monitor</td>
<td>332</td>
</tr>
<tr>
<td>Handling a line failure</td>
<td>Hardware monitor</td>
<td>338</td>
</tr>
<tr>
<td>Determining if a virtual route is blocked</td>
<td>VTAM commands</td>
<td>344</td>
</tr>
<tr>
<td>Identifying modem problems</td>
<td>Status monitor, session monitor, hardware monitor</td>
<td>344</td>
</tr>
<tr>
<td>Identifying and terminating looping or hung NetView tasks</td>
<td>Command facility</td>
<td>351</td>
</tr>
<tr>
<td>Handling NetView abends</td>
<td>First Failure Support Technology</td>
<td>351</td>
</tr>
<tr>
<td>Measuring response time with control units using the RTM feature</td>
<td>Session monitor</td>
<td>353</td>
</tr>
<tr>
<td>Resolving Sluggish Network Performance</td>
<td>NPM</td>
<td>355</td>
</tr>
</tbody>
</table>

Hung Session (Session Monitor)

Graphical Enterprise feature and Procedural feature users

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 list t11 from the session monitor command line to display the session list for resource T11. A panel similar to Figure 159 on page 332 is displayed:
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 there is a contradiction, you will 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 160 is displayed.

Figure 159. 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 there is a contradiction, you will 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 160 is displayed.

Figure 160. 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 161 is displayed.

```
NLDM.PIUT SPECIFIC SESSION TRACE DATA
---------- PRIMARY ----------------+---------- SECONDARY --------------+- DOM -
NAME BADAPPL SA 0000000B EL 0008 | NAME T11 SA 00000004 EL 00DC | CNM01
-----------------------------------+-----------------------------------+-------
<table>
<thead>
<tr>
<th>SEL# GMT SEQ# DIR TYPE</th>
<th>********** REQ/RESP HEADER</th>
<th>RULEN SENS T</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 1) 11:28:56 0018 P-S BIND</td>
<td>.....OC.DR.........................</td>
<td>37</td>
</tr>
<tr>
<td>( 2) 11:28:58 0016 S-P (+)RSP</td>
<td>.....OC.DR.........................</td>
<td>1</td>
</tr>
<tr>
<td>( 3) 11:29:03 0019 P-P SDT</td>
<td>.....OC.DR.........................</td>
<td>1</td>
</tr>
<tr>
<td>( 4) 11:29:04 0017 S-P (+)RSP</td>
<td>.....OC.DR.........................</td>
<td>1</td>
</tr>
<tr>
<td>( 5) 11:29:10 0020 P-S DATA</td>
<td>.....OC.ER.......BB...............</td>
<td>9</td>
</tr>
<tr>
<td>( 6) 11:29:10 0021 P-S DATA</td>
<td>.....OC.ER........EB...............</td>
<td>9</td>
</tr>
<tr>
<td>( 7) 11:30:03 0018 S-P DATA</td>
<td>.....OC.ER........EB...............</td>
<td>32</td>
</tr>
<tr>
<td>( 8) 11:30:12 0022 P-S DATA</td>
<td>.....OC.ER........BB...............</td>
<td>9</td>
</tr>
<tr>
<td>(10) 11:36:12 0024 P-S DATA</td>
<td>.....OC.ER........BB...............</td>
<td>49</td>
</tr>
</tbody>
</table>
```

**END OF DATA**
ENTER SEL# or COMMAND
CMD=>

Figure 161. Specific Session Trace Data Panel

Figure 161 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 so that the operator could respond with more data.

Further resolution of this problem will be up to the BADAPPL programmer.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using the session monitor panels</td>
<td>[Session Monitor Scenarios” on page 80]</td>
</tr>
</tbody>
</table>
Broken Session (Session Monitor)

Graphical Enterprise feature and Procedural feature users

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 162 is displayed.

```
NLDM.SESS                PAGE 1
NAME: A04T0011            SESSION LIST
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)
```

Figure 162. Session List Panel

The active SSCP-LU session (option 1) indicates that the user's 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 163 on page 335 is displayed:
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 appears 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 164 on page 336 is displayed.

Figure 163. Session Configuration Data 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. This will help the system programmer 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 165 on page 337 is displayed.
7. Enter 1 to look at the active session configuration and to determine the route. A panel similar to Figure 166 is displayed. Note that a different explicit route (ER 03) is used for this session.

![Figure 165. Session List Panel](image)

8. Enter er to view the explicit route. A panel similar to Figure 167 on page 338 is displayed.

![Figure 166. Session Configuration Data Panel](image)
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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using the session monitor panels</td>
<td><em>Session Monitor Scenarios</em> on page 80</td>
</tr>
</tbody>
</table>

**Line Failure (Hardware Monitor)**

**Graphical Enterprise feature and Procedural feature users**

The following scenario illustrates how to handle a link error caused by a faulty line:

1. Enter `ald` from the command line to access the Alerts-Dynamic panel. A panel similar to Figure 168 on page 333 is displayed.
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 169 is displayed.

**Figure 168. 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 169 is displayed.

**Figure 169. 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 130 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 170 is displayed.

![Figure 170. Recommended Action Panel](image)

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 171 on page 341 is displayed.
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 172 is displayed.

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.

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 173 is displayed.

```
Tivoli NetView SESSION DOMAIN: CNM99 OPER6 04/12/99 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.. (8/18/96) EV.. (8/18/96) ST.. (8/18/96) GMFA. (8/18/96)

ENTER SEL#
BNJ911I SESSION DOMAIN NOW CNM99 , WAS CNM01
???
CMD==>
```

Figure 173. 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 174 is displayed.

```
Tivoli NetView SESSION DOMAIN: CNM99 OPER6 04/12/99 11:06:20
NPDA-020 * 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 174. 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 175 is displayed.

```
Figure 175. LPDA-2 Command Menu Panel
```

9. Select option 3 to perform the line analysis test. A panel similar to Figure 176 is displayed.

```
Figure 176. 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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using the hardware monitor panels</td>
<td><a href="#">Monitoring the Network Using the Hardware Monitor Panels</a> on page 130</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTAM DISPLAY ROUTE command</td>
<td>Refer to the VTAM Library.</td>
</tr>
<tr>
<td>Using the NetView Performance Monitor to determine if a virtual route is blocked</td>
<td>NetView Performance Monitor User’s Guide</td>
</tr>
<tr>
<td>Using the session monitor to determine if a virtual route is blocked</td>
<td><a href="#">Typical LU-LU Session for an SNA Subarea Network</a> on page 80</td>
</tr>
</tbody>
</table>

### Modem Problems (Status Monitor, Hardware Monitor, Session Monitor)

Graphical Enterprise feature and Procedural feature users
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 177 is displayed.

```
STATMON.DSD(DESC)       DOMAIN 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
? CORSCS
? ACT
? EVERY
? INACT
? PENDING
? BFRUSE
? VARY INACT
? I  ? F
? VARY ACT
? ONLY  ? ALL
CMD==>
TO SEE YOUR KEY SETTINGS, ENTER 'DISPFK'
```

Figure 177. Status Monitor Domain 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 will be 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 178 on page 346 is displayed.
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. You can return to the first menu panel by entering the NetView SVTAM command or pressing PF10, if you use the NetView supplied default status monitor PF keys.

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.
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 SMCLIST command to access the Node Status Detail (Description) panel. The NetView supplied default PF key value for SCLIST is PF11.

![Figure 179. Displaying the Status for line A04L05](image)

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.

Figure 179. Displaying the Status for line A04L05

![Figure 180. Status for Line A04L05 and Available VTAM Commands](image)

Figure 180. 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.

```plaintext
+ CNM01  V NET,ACT,ID=A04L05,SCOPE=ALL
CNM01  IST097I  VARY ACCEPTED
CNM01  IST380I  ERROR FOR ID = A04L05 - REQUEST: ACTLINK , SENSE: 08220000
CNM01  IST105I  A04L05 NODE NOW INACTIVE
```

**Figure 181. 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.

```plaintext
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.
```

**Figure 182. 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.

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 there is a problem with the modem. Type 1 and press Enter to display the recommended corrective actions for this problem. A panel similar to Figure 184 on page 350 is displayed.

![Figure 183. Alerts-History Panel Containing the Alert Associated with the Failure of Line A04L05](image-url)
9. Continue your investigation by following the recommended actions in sequence. Notice that USER CAUSED tells you that the problem could 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.


<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACT command</td>
<td>NetView online help</td>
</tr>
<tr>
<td>Explanations of alert flags</td>
<td>NetView online help:</td>
</tr>
<tr>
<td></td>
<td>HELP NPDA 'DOMAIN'</td>
</tr>
<tr>
<td></td>
<td>For domain alert flags</td>
</tr>
<tr>
<td></td>
<td>HELP NPDA 'RESNAME'</td>
</tr>
<tr>
<td></td>
<td>For resource alert flags</td>
</tr>
<tr>
<td></td>
<td>HELP NPDA 'PROBABLE CAUSE'</td>
</tr>
<tr>
<td></td>
<td>For probable cause alert flags</td>
</tr>
</tbody>
</table>
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 04/12/99 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 there is work queued to the task.

2. Cancel the looping command list by using the EXCMD command as follows:

   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

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXCMD, STOP, TASKMON, LOGTSTAT, and TASKURPT command</td>
<td>NetView online help</td>
</tr>
</tbody>
</table>

NetView Abends (First Failure Support Technology)

FFST™ also provides a panel-driven interface to the Interactive Problem Control System (IPCS) allowing you to format the hexadecimal dump to a readable format.

To use FFST, install FFST under MVS Version 2 Release 2 or later. FFST does not forward probes for user-written code abends or for NetView abends that do not dump the NetView address space.
If you receive a system or user abend when FFST is active, FFST builds a keyword string. FFST then forwards a probe primary symptom string and a probe secondary symptom string to the MVS system console. The probe primary symptom string is also forwarded to the NetView hardware monitor. For the NetView hardware monitor, you can view the probe primary symptom string on the hardware monitor Recommended Action panel.

**Figure 185** shows an example of the alert information, including probe primary and secondary symptom strings (the lines are numbered so they can be referenced in the descriptions that follow).

1. **FFST STC00015 EPW0401I FFSTPROC: EVENT DETECTION INVOKED BY NETVIEW**
2. **EPW0406I DUMP DATASET IS: USER1.FFST.NETVIEW.DMP00079**
3. **EPW0407I FOUND ON VOLUME: CPDLB2**
4. **EPW0402I PRIMARY SYMPTOM STRING FOR PROBEID DSIABN01 FOLLOWS:**
5. **EPW0404I PIDS/5655007 LVLS/240 PCSS/DSIABN01 AB/S0C6 RIDS/DSIINP**
6. **EPW0404I FLDS/OFFSET VALU/H00000059**
7. **EPW0402I SECONDARY SYMPTOM STRING FOR PROBEID DSIABN01 FOLLOWS:**
8. **EPW0404I FLDS/DOMAIN VALU/CCNM01 FLDS/COMPDATE VALU/C93.030**
9. **EPW0404I FLDS/PTFLEVEL VALU/CNV31MVSE FLDS/TRACEFLAG VALU/OFF**

**Figure 185. Messages Sent by FFST for a NetView Abend**

The symptom strings provide pertinent information about NetView system and user abends, including:

- **The FFST header**, including:
  - A notification that an event occurred (line 1)
  - The name of the dataset in which the FFST dump of the abend is stored (line 2)
  - The volume where the dataset is located (line 3)
- **Product identification string** (5655007 in line 5)
- **NetView version and release** (240 in line 5)
- **The abend code** (S0C6 in line 5)
- **The name of the module where the abend occurred** (DSIINP in line 5)
- **The hexadecimal offset indicating the location in the module where the probe was triggered** (hexadecimal value of 00000059 in line 6)
- **The domain name** (CNM01 in line 8)
- **The module’s compile date** (93.030 in line 8)
- **The module’s program temporary fix (PTF) level** (NV31MVSE in line 9)
- **A TRACEFLAG field indicating whether the NetView trace was active at the time of the abend** (OFF in line 8)

**FASTService Option**

For NetView system and user abends, if you have the FASTService option installed, FFST builds a keyword string and searches the RETAIN® database for known problems. If FASTService locates information pertaining to your abend in the RETAIN database, you receive an authorized program analysis report (APAR) abstract. If there is no information pertaining to your abend in the RETAIN database, a problem record is put on the appropriate IBM Service queue.

**Resolving an Abend**

If you receive an FFST probe, refer to “Diagnostic Tools for the NetView Program” in *Tivoli NetView for OS/390 Diagnosis Guide* for information on how to use FFST.
to resolve a NetView abend.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using FFST to resolve a NetView abend</td>
<td>“Diagnostic Tools for the NetView Program” in <em>Tivoli NetView for OS/390 Diagnosis Guide</em></td>
</tr>
<tr>
<td>Viewing the hardware monitor Recommended Action panel</td>
<td>“Monitoring the Network Using the Hardware Monitor Panels” on page 130</td>
</tr>
</tbody>
</table>

### Measuring Response Time with Control Units Using RTM (Session Monitor)

This topic applies to **Graphical Enterprise feature and Procedural feature users only**.

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 as:
- 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:

1. Determine the user’s terminal ID (LU name). In this case, the user’s 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 186 on page 354 is displayed:
You notice that the user’s 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’s response times does 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 187 on page 355 is displayed:

![Figure 186. Response Time Summary Panel](image)
You notice that the user’s 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 APPN)" on page 76 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: AUTOCOLL, COLLECT, RTREND, RTSUM, QUERY RANGE, SET RANGE command | Reference: NetView online help |

**Sluggish Network Performance (NPM)**

The screens shown in the following section are taken from Graphical Enterprise feature and Procedural feature systems. If you are using the Unattended feature, the session monitor panels are not available.

The following scenario shows how to use the NetView program in conjunction with NPM 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:

You notice that the user’s 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 APPN)" on page 76 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: AUTOCOLL, COLLECT, RTREND, RTSUM, QUERY RANGE, SET RANGE command | Reference: NetView online help |

**Sluggish Network Performance (NPM)**

The screens shown in the following section are taken from Graphical Enterprise feature and Procedural feature systems. If you are using the Unattended feature, the session monitor panels are not available.

The following scenario shows how to use the NetView program in conjunction with NPM 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’s terminal is in session with CICSA running on HostA.

2. Enter `list usr01` from the session monitor command line to list the sessions for resource USR01. A panel similar to Figure 188 is displayed.

```
NLDM.SESS SESSION LIST PAGE 1
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 ***
```

Figure 188. Session List Panel

From this panel, you can see that:

- The CICSA-USR01 session is active.
- There are no other USR01 sessions 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 189 on page 357 is displayed.
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 logon to NPM. A panel similar
to Figure 190 is displayed.

Figure 189. 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).

5. Select 2 to display the session management panel. The panel shown in
Figure 191 on page 358 is displayed.

Figure 190. NPM Primary Options Panel

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
6. Select 1 to start collecting data for the user’s LU (USR01). A panel similar to Figure 192 is displayed.

Figure 191. NPM Session Management Panel

Figure 192. NPM 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. NPM lets you split the total transit time between:

- 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 user’s LU name in the Resource Name field and press Enter. A panel similar to Figure 193 is displayed.

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 194 on page 360 is displayed.
Select 4 to display the transit time summary. A panel similar to Figure 195 is displayed.

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 196 is displayed.

*Figure 196. NPM 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 197 on page 362 is displayed.
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 198 is displayed.

**Figure 197. NPM 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 198 is displayed.

**Figure 198. NPM NCP Management Network Review Panel**
16. **Type Detail** in the **Data Type** field and press Enter. A panel similar to Figure 199 is displayed.

<table>
<thead>
<tr>
<th>Command ====&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host Name</strong> = LOCAL <strong>Resource Name</strong> = LINE1 <strong>Data Type</strong> = LINE DETAIL</td>
</tr>
<tr>
<td><strong>Date/Time:</strong> from 01/25/96 11:45:00 to 01/25/96 15:00:00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>End Interval</th>
<th>Queue</th>
<th>Msgs</th>
<th>Bytes</th>
<th>Line-Ut</th>
<th>Polls/Min</th>
<th>Retransmit</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:45:00</td>
<td>00:15:00</td>
<td>0</td>
<td>21</td>
<td>108</td>
<td>19</td>
<td>0</td>
</tr>
<tr>
<td>12:00:00</td>
<td>00:15:00</td>
<td>0</td>
<td>76</td>
<td>244</td>
<td>41</td>
<td>0</td>
</tr>
</tbody>
</table>

PF 1=HELP 2= 3=END 4= 5= 6= 7= 8= 9=SUMMARY 10= 11= 12=RETURN

**Figure 199. NPM 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, there are three 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 361 through 16 (specifying the NCP name, NCP01, in the **Resource Name** field of the NCP Management Network Start panel). A panel similar to Figure 200 on page 364 is displayed.
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 361 through 16 on page 363 (specifying the TIC name, TIC1, in the Resource Name field of the NCP Management Network Start panel). See the note in 12 on page 361 to determine how to obtain the TIC name.

A panel similar to Figure 201 on page 365 is displayed.

---

**Figure 200. NPM 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 361] through [16 on page 363] (specifying the TIC name, TIC1, in the Resource Name field of the NCP Management Network Start panel). See the note in [12 on page 361] to determine how to obtain the TIC name.

A panel similar to [Figure 201 on page 365] is displayed.
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 there is too much data flowing through the TIC, the system programmer can then redistribute the attached resources by using another TIC.

<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using NPM</td>
<td>NetView Performance Monitor User's Guide</td>
</tr>
<tr>
<td>Using the session monitor panels</td>
<td>[Session Monitor Scenarios” on page 80]</td>
</tr>
</tbody>
</table>

**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 26. 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

This topic applies to Procedural feature users only.

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 28.

Table 28. Hardware Monitor to Information/Management Data Transfer

<table>
<thead>
<tr>
<th>NPDA Field Name</th>
<th>Length (Bytes)</th>
<th>V2 Info/Mgmt Field Name</th>
<th>Length (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Name (see note)</td>
<td>8–40</td>
<td>Resource Names</td>
<td>8–40</td>
</tr>
<tr>
<td>EV/AL DESC:PROB CAUSE</td>
<td>48</td>
<td>Description Abstract</td>
<td>45 (might be truncated)</td>
</tr>
<tr>
<td>Date</td>
<td>8</td>
<td>Date Occurred</td>
<td>8</td>
</tr>
<tr>
<td>Time</td>
<td>5</td>
<td>Time Occurred</td>
<td>5</td>
</tr>
<tr>
<td>Operator ID</td>
<td>8</td>
<td>Reported By</td>
<td>8</td>
</tr>
<tr>
<td>Constant (NPDA)</td>
<td>4</td>
<td>Reporter Dept</td>
<td>4</td>
</tr>
<tr>
<td>Domain Name</td>
<td>5</td>
<td>System Name</td>
<td>5</td>
</tr>
<tr>
<td>Action Panel ID</td>
<td>8</td>
<td>Action Panel ID</td>
<td>8</td>
</tr>
<tr>
<td>Detail Event Description</td>
<td>1040</td>
<td>Free Form Description</td>
<td>1040</td>
</tr>
<tr>
<td>Recommended Action</td>
<td>1120</td>
<td>Free Form Status</td>
<td>1120</td>
</tr>
<tr>
<td>Resource Type</td>
<td>4–20</td>
<td>Resource Types</td>
<td>4–20</td>
</tr>
</tbody>
</table>

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 202 appears. This single-page panel continuously shows the system being monitored. As failures occur, each alert appears at the top of the panel, and the alert at the bottom of the panel is removed.

```
Tivoli NetView SESSION DOMAIN: CNM01 OPER9 04/12/99 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 202. 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 203 is displayed.

```
Tivoli NetView SESSION DOMAIN: CNM01 OPER9 04/12/99 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 203. 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 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.

| Topic: Configuring Information/Management to work with the NetView program | Reference: Information/Management Planning, Installing, and Maintenance Guide |

---

**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 NMC 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 204 on page 370.

```
EZL501W 08:31 : RECOVERY FOR PU TA1P42A HALTED - 4 ERRORS SINCE 15:30 ON 08/11/93 - CRITICAL ERROR THRESHOLD EXCEEDED
```

Chapter 26. Managing Problems 369
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:

---

**Figure 204. Sample Information/Management Problem Reporter Panel**

The previous message can also produce the following Information Integration Facility record:

---

**Figure 205. Sample IIF Problem Reporter Panel**

---
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 should drive the NetView AutoBridge. Identify alerts and error messages which should 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 would be 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 as follows:

<table>
<thead>
<tr>
<th>NetView Customization</th>
<th>NetView AutoBridge Customization</th>
<th>Information/Management Customization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Customize the automation table to trigger the NetView AutoBridge for the selected MSUs and messages.</td>
<td>1. Code the process table. This defines actions to take, such as adding or parsing data and creating or updating a record.</td>
<td>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).</td>
</tr>
<tr>
<td>2. Add the necessary autotasks and profiles and command model statements.</td>
<td>2. Code the mapping table. This specifies the data from the incoming MSU or message to put into the Information/Management record.</td>
<td>2. Create a new session member for postprocessing the record.</td>
</tr>
<tr>
<td>3. Add the NetView AutoBridge data sets to the NetView startup procedure.</td>
<td>3. Code the initialization table. This defines the database target address, table names, retry counts and intervals, dispatchers, and adapters.</td>
<td>3. Create a mapping reference record to define how a record is postprocessed.</td>
</tr>
<tr>
<td>4. Create a VSAM file for checkpointed problem records and define the associated DSTs.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 29. Customizing the NetView Program, Information/Management, and AutoBridge

Topic: Reference:

Using the NetView AutoBridge

NetView AutoBridge/MVS R 1.0 Installation and User’s Guide
<table>
<thead>
<tr>
<th>Topic:</th>
<th>Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collecting problem data using the NetView Bridge</td>
<td><a href="#">Tivoli NetView for OS/390 Bridge Implementation</a></td>
</tr>
<tr>
<td>Using the Information Integration Facility</td>
<td><a href="#">Information/Management Integration Facility Guide</a></td>
</tr>
</tbody>
</table>
Part 6. Appendixes
Appendix A. Message Format

Most messages have the following format:

\[ \text{type domid code msgno text} \]

Where:

- **type** Message type. For more information on message type symbols refer to HDRMTYPE’s in macro DSITIB.
- **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 Tivoli NetView for OS/390 Messages and Codes
- **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"
- "Using the Hardware Monitor Panels" on page 376
- "Using the 4700 Support Facility Panels" on page 383
- "Using the Session Monitor Panels" on page 385
- "Using the Status Monitor Panels" on page 389
- "Using the RODMView Panels" on page 391

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) will take you to the "Help Overview" for the current component.

Entering help netview or pressing PF1 from the NetView MAINMENU panel will show you the NetView Help Facility Main Menu, similar to the screen shown in Figure 206.

Navigating the Help Panel Hierarchy

Figure 207 on page 376 shows the general relationship of the NetView help panels.
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

Graphical Enterprise feature and Procedural feature users
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 208 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 208, to go directly to the desired information.

The panels in Figure 208 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 363 for additional information. A C in column 80 indicates that there are correlated records 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 there are correlated records 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 there are correlated records 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 should know how the different components in your system or network are connected to each other and to the host controller. You should also understand how the hardware monitor sees your configuration, because the probable cause terminology used by the hardware monitor might be unfamiliar to you.
Figure 209 gives you more information on how the hardware monitor’s physical components and levels are related to each other in one typical configuration.

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 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 CPU by the channel

**LDEV**
A device attached to a channel-attached cluster controller

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>CPU (SSSSS)</td>
<td>For CPU devices (such as 3090)</td>
</tr>
<tr>
<td>CPU</td>
<td>$LOCAL</td>
<td>For the 43X1 loop adapter and the 3274 MDL 1A</td>
</tr>
<tr>
<td>CHAN</td>
<td>CH (XX)</td>
<td>For channels (such as 2860) running in an MVS environment</td>
</tr>
<tr>
<td>LCTL</td>
<td>LCTL (XXYZ)</td>
<td>For local SNA display controllers (such as 3274 MDL 1A)</td>
</tr>
<tr>
<td>LCTL</td>
<td>LCTL (XXY)</td>
<td>For local non-SNA display controllers (such as 3272)</td>
</tr>
<tr>
<td>LCTL</td>
<td>LCTL (User-defined)</td>
<td>For local display controllers (such as 3274)</td>
</tr>
<tr>
<td>TCU</td>
<td>TAPE (XXY)</td>
<td>For tape controllers (such as 3803)</td>
</tr>
<tr>
<td>SCU</td>
<td>DASD (XXY)</td>
<td>For DASD storage controllers (such as 3830)</td>
</tr>
<tr>
<td>IOCU</td>
<td>ICOU (XXY)</td>
<td>For printer controllers</td>
</tr>
<tr>
<td>LDEV</td>
<td>LDEV (XXYZ)</td>
<td>For local non-SNA display devices (such as 3277)</td>
</tr>
</tbody>
</table>
Table 30. Symbolic Names for Locally Attached Devices  (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(NNNN)</td>
<td>TDEV (XXYZ)</td>
<td>For tape devices (such as 3420)</td>
</tr>
<tr>
<td>(NNNN)</td>
<td>DDEV (XXYZ)</td>
<td>For DASD devices (such as 3350)</td>
</tr>
<tr>
<td>(NNNN)</td>
<td>IODV (XXYZ)</td>
<td>For printer devices</td>
</tr>
</tbody>
</table>

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 4700 Support Facility Panels

Graphical Enterprise feature and Procedural feature users

The 4700 Support Facility includes support for the 3600 and 4700 Finance Communications System.

Navigating the 4700 Support Facility Panel Hierarchy

Figure 210 on page 384 shows the general relationship of the 4700 support facility 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 4700 support facility command, as shown in the left column in Figure 210, to go directly to the desired information.
The panels in Figure 210 are described in the following list:

**Menu Panel**
Provides entry into the panel sequence by direct selection.

**Display Control Commands Panel**
Gives a brief description of all the 3600 and 4700 panel commands.

**Command Selection Panel**
Gives a brief description of the commands not described in the HELP panel.

**All Controllers Panel**
Provides a list of all 3600 and 4700 controllers.

**Controller Summary Panel**
Provides information about a specific controller and its attached loops and workstations.

**Loop Most Recent Status Panel**
Provides a list of the most recent status changes for the selected controller and loop.

**Loop Most Recent Error Panel**
Provides the most recent loop error data for the selected controller and loop.
Workstation Most Recent Response Time Panel
Provides the most recent response time measurements for the selected controller and workstation.

For an explanation of the fields shown on the panels, enter:
\texttt{help tara 'term'}

Where \text{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 4700 support facility, 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 Session Monitor Panels

Graphical Enterprise feature and Procedural feature users

The session monitor collects and correlates data about Systems Network Architecture (SNA) sessions (subarea and APPN). 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 APPN), 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 appear to 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. 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 APPN sessions, a session monitor must be available at the interchange node.

Navigating the Session Monitor Panel Hierarchy

\textbf{Figure 211 on page 386} 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 \textbf{Figure 211}, to go directly to the desired information.
The panels in Figure 211 are described in the following list:

**Menu Panel**
Allows you to select the type of resource list, 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, APPN 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
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 SSCP s 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 and/or secondary stage data for a TG ending in either an NCP or VTAM.

**APPN Session Route Configuration Panel**
Displays the route configuration through the SNA APPN network(s). 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**

*Graphical Enterprise feature and Procedural feature users*

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 212 on page 390](#) 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 212](#) to go directly to the desired information.
The panels in Figure 212 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:

* This panel is also accessible from any of the other status monitor panels

Figure 212. Status Monitor Panel Hierarchy
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, all the status monitor panels will only display information 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 netlogx 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 213 on page 392 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. Each Help panel enables you to access the Keys Help panel, which explains 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 213 on page 392.
For a description of the panels in Figure 213, refer to "RODM Tools" in Tivoli NetView for OS/390 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 (APPN), or mixed networks. This section provides scenarios that show:

- Typical SNA subarea and SNA advanced peer-to-peer networking (APPN) 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 APPN session configurations, refer to “Centralizing Operations” in the Tivoli NetView for OS/390 Installation: Configuring Additional Components.

Sessions-Data Availability Scenarios

In the SNA APPN environment, a VTAM interchange node and the NCP it owns are viewed logically as a single SNA APPN node (referred to as a composite network node), allowing them to interact with other SNA APPN nodes. At the same time, they continue to provide subarea support. Session PD support enables the user to view both SNA APPN 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 APPN 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 APPN 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 214 on page 394 is composed of an LU-LU session in a pure SNA subarea network. There is an SSCP-SSCP session between SSCP1 and SSCP2.
Interpreting Session Data

![Diagram of SNA Session](image)

Where: \(\ldots\ldots\) = session path

**Figure 214. SNA Session**

<table>
<thead>
<tr>
<th>Node</th>
<th>Available data</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSCP1</td>
<td>• Session awareness (SAW) data</td>
</tr>
<tr>
<td></td>
<td>• Subarea route data (explicit route and virtual route)</td>
</tr>
<tr>
<td>SSCP2</td>
<td>• SAW data</td>
</tr>
<tr>
<td></td>
<td>• Subarea route data (explicit route and virtual route)</td>
</tr>
</tbody>
</table>

### SNA APPN Session through a Composite Node

The configuration shown in [Figure 215](#) is composed of an LU-LU session going through a composite node. This configuration contains two NCP subarea nodes. There are CP-CP sessions between CP1-CP2 and CP2-CP3.

![Diagram of SNA APPN Sessions through Composite Nodes](image)

Where: \(\ldots\ldots\) = session path

\(\text{RSCV} = (\text{TG1,CP2,TG2,CP3})\)

**Figure 215. SNA APPN Sessions through Composite Nodes**
SNA APPN Session through Non-Adjacent Composite Nodes

The configuration shown in Figure 216 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.

![Diagram of SNA APPN Session through Nonadjacent Composite Nodes]

Where: = session path
RSCV = (TG1,CP2,TG2,CP3,TG3,CP4,TG4,CP5)

Figure 216. SNA APPN Session through Nonadjacent Composite Nodes
### Interpreting Session Data

<table>
<thead>
<tr>
<th>Node</th>
<th>Available data</th>
</tr>
</thead>
</table>
| CP2  | - SAW data, including Virtual Route (VR) information for VR1  
  - Complete APPN 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 session’s Route Selection Control Vector (RSCV)  
  - Complete APPN 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 APPN 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 session’s RSCV  
  - Complete APPN 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 APPN Session through Adjacent Composite Nodes

The configurations shown in Figure 217 on page 397 and Figure 218 on page 398 consist of a single network with adjacent composite nodes. These nodes can be connected in two ways. Figure 217 on page 397 shows them connected with a Casual Connection (FID2). Figure 218 on page 398 shows them connected with a VR.
Table 31 displays the data available with a Casual connection.

**Table 31. Data Available for SNA APPN Session through Adjacent Composite Nodes with Casual Connection**

<table>
<thead>
<tr>
<th>Node</th>
<th>Available data</th>
</tr>
</thead>
</table>
| CP1  | • Session awareness (SAW) data, including the session’s Route Selection Control Vector (RSCV)  
      • Complete APPN 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 APPN 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 APPN 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 session's RSCV  
      • Complete APPN 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) |

Where: ---- = session path  
RSCV = (TG1,CP2,TG2,CP3,TG3,CP4)

Figure 217. SNA APPN Session through Adjacent Composite Nodes with FID2 Connection

Appendix C. Interpreting Session Data
Interpreting Session Data

Table 32 displays the data available with a VR connection.

Table 32. Data Available with SNA APPN Session through Adjacent Composite Nodes with a VR Connection

<table>
<thead>
<tr>
<th>Node</th>
<th>Available data</th>
</tr>
</thead>
</table>
| CP1  | • Session awareness (SAW) data, including the node’s local Route Selection Control Vector (RSCV), RSCV1  
       • APPN 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 APPN 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 node’s local RSCV (RSCV1) and Virtual Route (VR) information for VR1  
       • APPN 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 APPN Session Route Configuration panel  
       • Origin flow control data (data for TG1 in the primary direction) by soliciting NCP1 |
| CP3  | • SAW data, including the node’s local RSCV (RSCV2) and Virtual Route (VR) information for VR1  
       • Complete APPN 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 APPN Session Route Configuration panel  
       • Destination flow control data (data for TG3 in the secondary direction) by soliciting NCP3 |

Where: ------ = session path  
RSCV1 = (TG1,CP2,IN-TG,CP4)  
RSCV2 = (IN-TG,CP3,TG3,CP4)
Table 32. Data Available with SNA APPN Session through Adjacent Composite Nodes with a VR Connection (continued)

<table>
<thead>
<tr>
<th>Node</th>
<th>Available data</th>
</tr>
</thead>
</table>
| CP4  | • SAW data, including the node's local RSCV (RSCV2)  
      |   • Complete APPN 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 APPN 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 APPN Session through a SNI Gateway**

The configuration shown in Figure 219 consists of two composite nodes connected through a gateway NCP. This configuration always results in multiple RSCVs.

![SNA APPN Session through SNI Gateway](image)

Where:  
RSCV1 = (TG1,CP2,IN-TG,CP4)
RSCV2 = (IN-TG,CP3,TG3,CP4)

**Figure 219. SNA APPN Session through SNI Gateway**

<table>
<thead>
<tr>
<th>Node</th>
<th>Available data</th>
</tr>
</thead>
</table>
| CP1  | • Session awareness (SAW) data, including the session's 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 APPN Session Route Configuration panel  
      |   • Flow control data for TG1 in the secondary direction |
### Interpreting Session Data

<table>
<thead>
<tr>
<th>Node</th>
<th>Available data</th>
</tr>
</thead>
</table>
| 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 APPN 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 APPN 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 APPN Session Route Configuration panel  
- Flow control data for TG3 in the primary direction |

### Session between 2 SNA APPN Subnetworks with a LEN Connection

The configuration shown in Figure 220 consists of 2 SNA APPN subnetworks joined with a LEN connection. This type of connection results in multiple RSCVs for the session.

![Figure 220. Session between 2 SNA APPN Subnetworks through a LEN Connection](image)

Where:

- **RSCV1** = session path
- **RSCV1** = ((TG1,CP2))
- **RSCV2** = ((TG2,NN4,TG3,NN5)|(LEN,NN3))
SNA Session through an APPN Network

The configuration shown in Figure 221 illustrates a session using a DLUS-DLUR pipe to cross an APPN network.

The APPN 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.

There are SSCP-LU (1) and SSCP-PU (2) sessions 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 221. SNA Session through an APPN Network](image)

<table>
<thead>
<tr>
<th>Node</th>
<th>Available data</th>
</tr>
</thead>
</table>
| CP1  | • Session awareness (SAW) data, including the session’s Route Selection Control Vector (RSCV1) for the first subnetwork  
      • APPN 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 APPN 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 APPN Session Route Configuration (built from RSCV1 and RSCV2)  
      • Flow control data for TG1 in the primary direction |
SSCP Takeover/Giveback Scenarios

There are four scenarios of SSCP Takeover/Giveback that will be 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 may 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 222 on page 403 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.
Table 33 shows the data available before and after CP3 takes over the connection to ALS2.

### Table 33. Data Comparisons for Takeover/Giveback Scenario 1

<table>
<thead>
<tr>
<th>Node</th>
<th>Initial State</th>
<th>After Giveback</th>
<th>After Takeover</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP1</td>
<td>Session monitor receives SAW data for the session.</td>
<td>No change.</td>
<td>No change. Session monitor still thinks CP2 owns the connection to ALS2.</td>
</tr>
</tbody>
</table>
| CP2  | Session monitor receives SAW data for the session.                           | • If the line between the NCPs is PUTFIELD=4, the session is displayed on the session monitor's 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 PUTFIELD=2, the session is displayed on the session monitor's session list as ACTIVE and with a GIVEBACK indicator.  
  • The resource names are displayed with a GBK (giveback) indicator. | No change.                                                                                         |
| CP3  | Session monitor is not aware of the session.                                 | Session monitor does not have any awareness of the session. It will become aware of the session after the session is taken over. | • The session is displayed on the session monitor's session list as ACTIVE and with a TAKEOVER indicator.  
  • The resource names are displayed with a TOV (takeover) indicator.  
  • Due to 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 223 on page 404](#), 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 APPN 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.

Table 34 shows the data available before and after CP2 takes over the connection to ALS1 and ALS2.

Table 34. Data Comparison for Takeover/Giveback Scenario 2

<table>
<thead>
<tr>
<th>Node</th>
<th>Initial State</th>
<th>After Giveback of both links</th>
<th>After Takeover of both links</th>
</tr>
</thead>
</table>
| CP1  | Session monitor receives SAW data for the session. | • The session is displayed on the session monitor's session list with an end time and with a GIVEBACK indicator.  
• The resource names are displayed with a GBK (giveback) indicator. | No change. |
| CP2  | Session monitor is not aware of the session. | Session monitor is not aware of the session. It will become aware of the session after the session is taken over. | • The session is displayed on the session monitor's session list as ACTIVE and with a TAKEOVER indicator.  
• The resource names are displayed with a TOV (takeover) indicator.  
• Due to 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 224 on page 405, 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.
Table 35 shows the data available before and after CP2 takes over the connection to ALS1.

<table>
<thead>
<tr>
<th>Node</th>
<th>Initial State</th>
<th>After Giveback</th>
<th>After Takeover</th>
</tr>
</thead>
</table>
| CP1   | Session monitor receives SAW data for the session. | • The session is displayed on the session monitor’s session list as ACTIVE and with a GIVEBACK indicator  
       |                                                   | • The resource names are displayed with a GBK (giveback) indicator.             | No change.                                                                     |
| CP2   | Session monitor is not aware of the session.        | Session monitor is not aware of the session. It will become aware of the session after the session is taken over. | • The session is displayed on the session monitor’s session list as ACTIVE and with a TAKEOVER indicator.  
       |                                                   |                                                                               | • The resource names are displayed with a TOV (takeover) indicator.            |
|       |                                                   |                                                                               | • Due to 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 225 on page 406, 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.
Table 36 shows the data available before and after CP2 takes over the connection to ALS1.

Table 36. Data Comparison for Takeover/Giveback Scenario 4

<table>
<thead>
<tr>
<th>Node</th>
<th>Initial State</th>
<th>After Giveback</th>
<th>After Takeover</th>
</tr>
</thead>
</table>
| CP1  | Session monitor receives SAW data for the session. | • The session is displayed on the session monitor’s session list with an end time and with a GIVEBACK indicator.  
• The resource names are displayed with a GBK (giveback) indicator. | No change. |
| 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’s session list as ACTIVE and with a TAKEOVER indicator.  
• The resource names are displayed with a TOV (takeover) indicator.  
• Due to 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 publications for general users and publications specifically for Graphical Enterprise feature users. The following NetView publications are grouped by task.

**Note:** Most of the publications are also available on the web at [http://www.tivoli.com/nv390](http://www.tivoli.com/nv390).

Table 37. The Tivoli NetView for OS/390 Library

<table>
<thead>
<tr>
<th>Task</th>
<th>Publications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automation</td>
<td>Tivoli NetView for OS/390 Automation Guide</td>
</tr>
<tr>
<td>Customization</td>
<td>Tivoli NetView for OS/390 Automated Operations Network Customization Guide</td>
</tr>
<tr>
<td></td>
<td>Tivoli NetView for OS/390 Customization Guide</td>
</tr>
<tr>
<td></td>
<td>Tivoli NetView for OS/390 Customization: Using Assembler</td>
</tr>
<tr>
<td></td>
<td>Tivoli NetView for OS/390 Customization: Using Pipes</td>
</tr>
<tr>
<td></td>
<td>Tivoli NetView for OS/390 Customization: Using PL/I and C</td>
</tr>
<tr>
<td></td>
<td>Tivoli NetView for OS/390 Customization: Using REXX and the NetView Command List Language</td>
</tr>
<tr>
<td>Diagnosis</td>
<td>NetView for OS/390 Diagnosis Guide</td>
</tr>
<tr>
<td>Training</td>
<td>Introducing Tivoli NetView for OS/390</td>
</tr>
<tr>
<td>Installation and Administration</td>
<td>Tivoli NetView for OS/390 Administration Reference</td>
</tr>
<tr>
<td></td>
<td>Tivoli NetView for OS/390 Installation: Getting Started</td>
</tr>
<tr>
<td></td>
<td>Tivoli NetView for OS/390 Installation: Migration Guide</td>
</tr>
<tr>
<td></td>
<td>Tivoli NetView for OS/390 Installation: Configuring Additional Components</td>
</tr>
<tr>
<td></td>
<td>Tivoli NetView for OS/390 Installation: Configuring Graphical Components</td>
</tr>
<tr>
<td></td>
<td>Tivoli NetView for OS/390 Tuning Guide*</td>
</tr>
<tr>
<td>Operation</td>
<td>Tivoli NetView for OS/390 APPN Topology and Accounting Agent Guide*</td>
</tr>
<tr>
<td></td>
<td>Tivoli NetView for OS/390 Bridge Implementation</td>
</tr>
<tr>
<td></td>
<td>Tivoli NetView for OS/390 NetView Management Console User’s Guide</td>
</tr>
<tr>
<td></td>
<td>Tivoli NetView for OS/390 SNA Topology Manager and APPN Accounting Manager Implementation Guide</td>
</tr>
<tr>
<td></td>
<td>Tivoli NetView for OS/390 User’s Guide</td>
</tr>
<tr>
<td>Programming</td>
<td>Tivoli NetView for OS/390 Application Programmer’s Guide</td>
</tr>
<tr>
<td></td>
<td>Tivoli NetView for OS/390 Resource Object Data Manager and GMFHS Programmer’s Guide</td>
</tr>
</tbody>
</table>
Using the NetView Library

Table 37. The Tivoli NetView for OS/390 Library (continued)

<table>
<thead>
<tr>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli NetView for OS/390 Command Reference</td>
</tr>
<tr>
<td>Tivoli NetView for OS/390 Data Model Reference</td>
</tr>
<tr>
<td>Tivoli NetView for OS/390 Messages and Codes</td>
</tr>
<tr>
<td>Tivoli NetView for OS/390 Security Reference</td>
</tr>
</tbody>
</table>

Note: An asterisk (*) beside the book title indicates that the book applies only to the Graphical Enterprise feature.

Finding the Right Information

See Table 38 for information about the contents of each book. Table 38 lists NetView tasks and the publication where you will find the information about that task:

Table 38. Finding the Information That Can Help with Your Task

<table>
<thead>
<tr>
<th>If your task is...</th>
<th>Use this book...</th>
</tr>
</thead>
<tbody>
<tr>
<td>To change or add resource definitions.</td>
<td>Tivoli NetView for OS/390 Administration Reference</td>
</tr>
<tr>
<td>To write applications that send network management vector transports, formatted alerts to NetView, send buffers to other applications, or develop applications for the program-to-program interface</td>
<td>Tivoli NetView for OS/390 Application Programmer's Guide</td>
</tr>
<tr>
<td>To use the Communications Manager/2 APPN Topology and Accounting Agents and Common Management Information Protocol (CMIP) services</td>
<td>Tivoli NetView for OS/390 APPN Topology and Accounting Agent Guide</td>
</tr>
<tr>
<td>To automate your system operations and networks</td>
<td>• Tivoli NetView for OS/390 Automation Guide</td>
</tr>
<tr>
<td></td>
<td>• Tivoli NetView for OS/390 Automated Operations Network User's Guide</td>
</tr>
<tr>
<td>To send transactions between NetView and a database that is in another address space</td>
<td>Tivoli NetView for OS/390 Bridge Implementation</td>
</tr>
<tr>
<td>To see information about NetView commands, their syntax diagrams, and attributes</td>
<td>Tivoli NetView for OS/390 Command Reference</td>
</tr>
<tr>
<td>To customize NetView</td>
<td>Tivoli NetView for OS/390 Customization Guide</td>
</tr>
<tr>
<td>To tailor NetView for unique requirements or design, write, and install programs in assembler</td>
<td>Tivoli NetView for OS/390 Customization: Using Assembled</td>
</tr>
<tr>
<td>To write installation exit routines, command lists, command processors, and subtasks using PIPEs in a REXX, PL/I, or C environment</td>
<td>Tivoli NetView for OS/390 Customization: Using Pipes</td>
</tr>
<tr>
<td>To write installation exit routines, command processors, and subtasks using PL/I, and C</td>
<td>Tivoli NetView for OS/390 Customization: Using PL/I and C</td>
</tr>
<tr>
<td>To write simple and advanced command lists that simplify network operator tasks</td>
<td>Tivoli NetView for OS/390 Customization: Using REXX and the NetView Command List Language</td>
</tr>
<tr>
<td>To get information about data models for topology manager, RODM, and MultiSystem Manager</td>
<td>Tivoli NetView for OS/390 Data Model Reference</td>
</tr>
</tbody>
</table>
### Table 38. Finding the Information That Can Help with Your Task (continued)

<table>
<thead>
<tr>
<th>If your task is...</th>
<th>Use this book...</th>
</tr>
</thead>
<tbody>
<tr>
<td>To identify, classify, and report problems to Tivoli Customer Support</td>
<td>Tivoli NetView for OS/390 Diagnosis Guide</td>
</tr>
<tr>
<td>To install and prepare NetView for operation</td>
<td>Tivoli NetView for OS/390 Installation: Getting Started</td>
</tr>
<tr>
<td>To use, customize, and operate MultiSystem Manager</td>
<td>Tivoli NetView for OS/390 MultiSystem Manager User’s Guide</td>
</tr>
<tr>
<td>To use the NetView Management Console to monitor and control networks</td>
<td>Tivoli NetView for OS/390 NetView Management Console User’s Guide</td>
</tr>
<tr>
<td>To read about the new function added to NetView in this release</td>
<td>Tivoli NetView for OS/390 Installation: Migration Guide</td>
</tr>
<tr>
<td>To streamline NetView installation by performing tasks prior to installation and to estimate resources for a NetView installation</td>
<td>Tivoli NetView for OS/390 Installation: Configuring Additional Components</td>
</tr>
<tr>
<td>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</td>
<td>Tivoli NetView for OS/390 Resource Object Data Manager and GMFHS Programmer’s Guide</td>
</tr>
<tr>
<td>Set up NetView security</td>
<td>Tivoli NetView for OS/390 Security Reference</td>
</tr>
<tr>
<td>To use SNA Topology Manager, APPN Accounting Manager, and CMIP</td>
<td>Tivoli NetView for OS/390 SNA Topology Manager and APPN Accounting Manager Implementation Guide</td>
</tr>
<tr>
<td>To control and improve NetView performance using tuning values</td>
<td>Tivoli NetView for OS/390 Tuning Guide</td>
</tr>
<tr>
<td>To train novice users</td>
<td>Introducing Tivoli NetView for OS/390 User’s Guide</td>
</tr>
<tr>
<td>To monitor and control, investigate and solve problems, and automate networks and systems</td>
<td>Tivoli NetView for OS/390 User’s Guide</td>
</tr>
</tbody>
</table>

Because the formerly separate Automated Operations Network/MVS and MultiSystem Manager MVS/ESA products have been merged with Tivoli NetView for OS/390, 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 39. Information Map for MultiSystem Manager and Automated Operations Network Components

<table>
<thead>
<tr>
<th>Information Type</th>
<th>AON</th>
<th>MSM</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control file entries, focal-point services, reporting, message processing, and file control manager interface</td>
<td>X</td>
<td></td>
<td>Tivoli NetView for OS/390 Administration Reference</td>
</tr>
<tr>
<td>Getting started, using and implementing SNA, LAN, and TCP/IP automation</td>
<td>X</td>
<td></td>
<td>Tivoli NetView for OS/390 Automation Guide</td>
</tr>
</tbody>
</table>
### Table 39. Information Map for MultiSystem Manager and Automated Operations Network Components (continued)

<table>
<thead>
<tr>
<th>Information Type</th>
<th>AON</th>
<th>MSM</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>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</td>
<td>X</td>
<td></td>
<td><a href="#">Tivoli NetView for OS/390 Automated Operations Network Customization Guide</a></td>
</tr>
<tr>
<td>Getting started (SNA, LAN, 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 NetView, 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</td>
<td></td>
<td>X</td>
<td><a href="#">Tivoli NetView for OS/390 Automated Operations Network User's Guide</a></td>
</tr>
<tr>
<td>AON/SNA, AON/LAN, AON/TCP, and MultiSystem Manager commands</td>
<td>X</td>
<td>X</td>
<td><a href="#">Tivoli NetView for OS/390 Command Reference</a></td>
</tr>
<tr>
<td>Initialization and recovery</td>
<td></td>
<td>X</td>
<td><a href="#">NetView for OS/390 Diagnosis Guide</a></td>
</tr>
<tr>
<td>Planning and requirements, tailoring NetView, gateways, and focal points, defining AON, testing installations, verifying installation and components, and implementing SNA and LAN components</td>
<td>X</td>
<td>X</td>
<td><a href="#">Tivoli NetView for OS/390 Installation Getting Started</a>, <a href="#">Tivoli NetView for OS/390 Installation Migration Guide</a>, <a href="#">Tivoli NetView for OS/390 Installation Configuring Graphical Components</a>, <a href="#">Tivoli NetView for OS/390 Installation Configuring Additional Components</a></td>
</tr>
<tr>
<td>All messages</td>
<td>X</td>
<td>X</td>
<td><a href="#">Tivoli NetView for OS/390 Messages and Codes</a></td>
</tr>
<tr>
<td>Getting started, using and customizing, operation of agents and MultiSystem Manager, managing alerts, using global variables, using agents, solving problems, and samples</td>
<td></td>
<td>X</td>
<td><a href="#">Tivoli NetView for OS/390 MultiSystem Manager User's Guide</a></td>
</tr>
</tbody>
</table>
Table 39. Information Map for MultiSystem Manager and Automated Operations Network Components (continued)

<table>
<thead>
<tr>
<th>Information Type</th>
<th>AON</th>
<th>MSM</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workstation interface overview; installing, using, tailoring, and programming workstation interface; enabling automation in progress (AIP)</td>
<td></td>
<td>X</td>
<td>Tivoli NetView for OS/390 NetView Management Console User’s Guide</td>
</tr>
<tr>
<td>Protecting commands</td>
<td></td>
<td>X</td>
<td>Tivoli NetView for OS/390 Security Reference</td>
</tr>
<tr>
<td>Tuning for performance and compiling REXX functions</td>
<td></td>
<td>X</td>
<td>NetView for OS/390 Tuning Guide</td>
</tr>
</tbody>
</table>

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 40 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 40. Types of Help Information

<table>
<thead>
<tr>
<th>To obtain help for...</th>
<th>Enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetView commands</td>
<td>HELP commands</td>
</tr>
<tr>
<td>NetView components</td>
<td>HELP component</td>
</tr>
<tr>
<td>NetView commands by component</td>
<td>HELP component command</td>
</tr>
<tr>
<td>NetView messages</td>
<td>HELP msgid</td>
</tr>
<tr>
<td>NetView product</td>
<td>HELP NetView</td>
</tr>
<tr>
<td>VTAM return codes and feedback codes</td>
<td>RCFB code, feedback_code</td>
</tr>
<tr>
<td>SNA sense codes</td>
<td>SENSE sense_code</td>
</tr>
<tr>
<td>VTAM status codes</td>
<td>STATUS code</td>
</tr>
<tr>
<td>Explicit and virtual route status codes</td>
<td>ERST code and VRST code</td>
</tr>
<tr>
<td>Recommended actions for hardware monitor panels</td>
<td>ACTION number</td>
</tr>
<tr>
<td>Field descriptions</td>
<td>HELP component 'field'</td>
</tr>
<tr>
<td>The Help Desk</td>
<td>HELPDESK</td>
</tr>
<tr>
<td>Help index</td>
<td>INDEX letter</td>
</tr>
</tbody>
</table>
Extensive, context-sensitive, workstation help information is provided for the NetView Management Console (NMC). The information provides help for all functions, windows, fields, and buttons. Workstation help offers the following functions:
- A comprehensive hypertext system that enables you to link to more detailed or related information
- A detailed index
- Color graphics
- Search capability
- Print capability

NMC help information is available only with the Graphical Enterprise feature.

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 Tivoli NetView for OS/390 Web site. Point your browser to http://www.tivoli.com/nv390.
Index

Special Characters
??? indicator, NetView panel 39
@D command 171
%INCLUDE automation table statement 226
(AON/SNA) automation operations network/SNA 7
&CGLOBAL global variable 293
&D 171
*I S 171
&TGLOCAL global variable 293
=X= indicator, NetView panel 39

Numerics
3270 session, logging on 32
4700 Support Facility
database 213
removing data 213
reorganizing 213
switching 213
using and maintaining 213
panel hierarchy 383

A
accounting
APPC session and conversation 57
definition 26
ACTIVE status monitor state 100
adding
AFTER timers 266
AT timers 265
CHRON timers 268
EVERY timers
from Timer Management panels 263
adding timers
EVERY, AT or AFTER
from Timer Management panels 262
address spaces
host environment 29
stopping 30
AFTER command
issuing at the command line 257
AFTER timer
adding 262
from Timer Management panels 266
alert adapter component 13
alerts
blocking 197
data types 224
debugging 306, 308, 309
defining receiver 193
definition 24, 127
deleting 194
error thresholds 206
filtering
determining 297
using automation table SRF 298
using DSIEX16B exit 298
alerts (continued)
filtering (continued)
using RATE statement 297
using SRFILTER command 298
using XITCI exit 297
flows 24
forwarding
overview 149
generating 205
using GENALERT 205
using PPI 205
information available through hardware monitor 132
LU 6.2 receiver support 193
receiver 194
SMF log 212
alerts-dynamic panel
creating problem reports 368
line failures, handling 338
network management vector transport alerts 136
non-network management vector transport alerts 131
alerts-history panel 349
alerts-static panel
alert forwarding 149
creating problem reports 369
line failures, handling 339
network management vector transport alerts 137
non-network management vector transport alerts 132
ALWAYS automation table statement 226
AON 246
AON, finding information 408
AON 1.6
typing at the command line 258
AON/LAN Automation 246
AON/SNA 247
application detail window 61
application management interface 8
application trend window 61
APPLSPEN command 66
APPN
accounting agent, overview 6
accounting manager, overview 6
network configurations 393
session between subnetworks using LEN connection 400
Session Route Configuration panel 90
typical SNA APPN CP-CP session 90
typical SNA APPN LU-LU session 94, 95
session through adjacent composite nodes 396
session through composite node 394
session through non-adjacent composite nodes 395
session through SNI gateway 399
topology agent, overview 6
ARG function 281
assembler-language command processor 290
ASSIGN command 249
assigning operators to groups 249

413
AT command
issuing at the command line 256
AT timer
adding
from Timer Management panels 262, 265
ATF('DSICGLOB') global variable 293
ATF('DSITGLOB') global variable 293
AUTOCNT command 233
automated operations network (AON/TCP), overview 247
automated operations network, overview 6, 246
Automated Operations Network, overview 246
Automated Operations Network/SNA, overview 247
automatic reactivation 109
automating, definition 26
automation
issuing commands after a time period at the command line 257
issuing commands at regular intervals at the command line 256
issuing timed commands at the command line 256
operator consoles 244
overview 243
scheduling commands 255
using
AIX NetView Service Point 248
AON/TCP 247
automation table 223
CICS Automation Feature 244
IMS Automation Feature 245
NetView AutoBridge/MVS 248
OPC Automation Feature/MVS 245
OPC/ESA 301
RODM 239
status monitor 322
System Operations 244
TSCF 243
writing commands 279
automation table
listing 184
SRF automation table condition item 298
autotask
defining 251
functions 251
RMTCMD, listing 69
starting using AUTOTASK 252
starting using RMTCMD 252
AUTOTBL command 225, 232
AUTOTEST command 231
AUTOWRAP command 192
autowrap indicator, NetView panel 37
autowrap warning 39
B
BEGIN-END automation table statement 226
BLOCK filter option 197
BLOG, printing inactive network log 206
BLOG command 207
boundary function NCP data 78
browse
automation tables 225
browse (continued)
data set 184
network log message format 375
network log panel 109
browse, NetView log 207
BROWSE command 184, 206
built-in NetView functions 282
C
C2D function 281
C2X function 281
CGED 293
change method (RODM) 239
choosing, monitoring process 63
CHRON EVERY panel
Timer Management panels 272
CHRON EVERY Timer Display Results panel 1
Timer Management panels 274
CHRON EVERY Timer Display Results panel 2
Timer Management panels 274
CHRON EVERY Timer Display Results panel 3
Timer Management panels 275
CHRON EVERY Timer Display Results panel 4
Timer Management panels 275
CHRON EVERY Timer Preview panel
Timer Management panels 273
CHRON Notify panel
Timer Management panels 270
CHRON Options panel
Timer Management panels 271
CHRON timer
adding
from Timer Management panels 268
CICS Automation Feature
obtaining subsystem status information 116
overview 20, 244
panels 116
main menu, obtaining detailed subsystem status 116
subsystem information 117
CLEAR filter option 198
CMDMDL statement, adding 179, 287
CNM560I message 169
CNM564I message 170
CNM566I message 170
CNM567I message 170
CNM568I message 170
CNMPSSI subsystem 32
CNMS0003 sample 188
CNMS4501 sample exit 211
CNMSAMP sample 299
CNMSCNFT sample 37
CNMVARS global variable 293
cold starting RODM 29
command entry area
length 40
NetView panel 39
command facility 44
creating trace data 210
displaying trace data 210
DSIPRT program 210
Index 415

command facility 44 (continued)
hung task, identifying 351
hung task, terminating 351
looping task, identifying 351
looping task, terminating 351
measuring response time using TASKUTIL 320
overview 5
panels 69
JES3 command response 171
LAN ADP command response 72
LAN QNETWORK command response 72
LISTCAT, active VSAM data base for BNJDSEVR 329
RMTSESS command response 69
TASKUTIL command response 351
trace 210
command flows 23
command list
accessing data set members 286
assigning synonym in NetView 288
browsing 184
command security 288
creating 280
debugging 310
defining data sets 279
defining to NetView 288
displaying panels 284
getting input 285
global variables 285
improving performance 288
issuing commands 285
issuing messages 284
LAN 71
parsing input 286
requirements 279
specifying scope checking in NetView 288
storing global variables 285
testing 287
writing 279
command prefix labels
EXCMD-type 70
RMTCMD-type 70
usage 70
command processor
writing, assembler 290
writing, HLL 289
command response display panel, JES2
commands 173
command response display panel (MVS) 172, 173
commands
@D 171
*I S 171
AFTER 257
APPLSPEN 66
ASSIGN 249
AT 256
AUTOCNT 233
AUTOTBL 225
AUTOTEST 231
AUTOWRAP 192
BLOG 207
command response display panel (MVS) 172, 173
commands (continued)
BROWSE 184, 206
DBAUTO 211, 215
defining in NetView 179
DISCONID 170
DISG 66
DISPLAY ID 64
DISPLAY ROUTE 344
entering mixed case 191
EVERY 256
EXECIO 286
FIND 206
FOCALPT ACQUIRE 203, 204
FOCALPT CHANGE 203
FOCALPT DELETE 204
FOCALPT DISPLOC 204
FOCALPT QUERY 204
FOCALPT REFRESH 205
GENALERT 205
GETCONDID 170
ISQCCMD 165
ISQXDST 159
ISQXIII 165
JES2, issuing 170
JES3, issuing 171
LIST 209
LIST LU 81
LIST TIMER
displaying timers that are waiting to process 257
LISTCAT 211, 329
MODIFY 300
MONIT START 322
MONIT STOP 322
MONOFF 322
MONON 322
MSG 284
MSGROUTE 249
MVS 170
MVS $DU,PRT15 171
MVS $IPRT15 171
MVS $PPRT15 171
MVS D A,L 169
ORCONV 241
PIPE 282, 286
PURGE 257
QRYGLOB 295
RECORD 214
REFRESH 188
RELCONDID 170
repeating 190
REPLY 30
REPORTS 212
RESTORE
issuing at the command line 258
RETRIEVE 190
RMTCMD 68, 69
RMTSESS 69
RUNCMD 110
scheduling 255
SESS 90
SESSMDIS 99
commands (continued)
  SET 189
  SRATIO 206
  SRFILTER 150, 195, 298
  suppressing from log 191
  SVFILTER 150, 195
  SWITCH 209
  SWRAP 212
  TASKUTIL 320, 351
  TIMER 255, 258
    setup 255
    timers 258
  TRACE 210
  VPALL 155
  VPDCMD 155
  WTO 284
  WTOR 285
common monitor tasks 10
common task components 10
Communications Manager/2
  configuring, LU 6.2 commands 112
  Remote Operations Service point 115
console 43
console, defining and releasing 170
controller (CTRL) selection menu panel 326
controller information display panel 326
controlling 26
  APPN resources 55
  definition 26
  operating system resources 169
  operation 187
  remote processors 159
  screen 189
  SNA subarea resources 55
tasks 65
  activating NCP 65
  activating NCP, remote NetView 68
  assigning operators to groups 249
  collecting vital product data 155
  controlling remote resources 68
  controlling TCP/IP resources 115
  draining printer 171
  inactivating a resources using VTAM 65
  inactivating NCP 65
  initializing target system 165
  interrupting printer job 171
  issuing commands, service point applications 110
  loading NCP 65
  loading target system 165
  managing command responses using PIPE 282
  performing IPL, target system 165
  reactivating resources using VTAM 65
  routing messages 249
  running modem and link tests 143
  sending solicited messages 250
  sending unsolicited messages 249
  shutting target system 166
  writing, REXX command list 279
  writing vital product data to external log 155
  using NetView commands 66
controlling 26 (continued)
  using VTAM commands 64
  correlating command responses 69
  CP-CP session, SNA APPN network, scenario 87
  CP-MSU 223
  current filter status panel 195
D
D219 run DCE test panel 340
D219 run line analysis test panel 341
D2C function 281
D2X function 281
data
  checkpointing RODM 217
  hardware monitor 211
  NetView trace 210
  problem management 204, 205
  session monitor trace 210
  SMF 212
data availability scenarios 393, 401
data collection using the hardware monitor 125
data flow 22
data set
  browsing 184
database
  4700 Support Facility 213
    removing data 213
    reorganizing 213
    switching 213
  hardware monitor 211
    clearing 212
    controlling amount of data 212
    removing data 212
    reorganizing 212
    switching 211
  save/restore 215
    clearing 215
    removing data 215
    reorganizing 215
    switching 215
  session monitor 214
    clearing 214
    collecting in SMF 214
    removing data 214
    reorganizing 214
    switching 214
date and time, after
  setting timers from Timer Management panels 266
date and time, specific
  setting timers from Timer Management panels 265
DATE function 281
DBAUTO command 211, 215
debugging
  alert automation 306
  alert forwarding to Tivoli Enterprise Console 308
  automation, debugging 303
  command list automation 310
  CPU usage 313
  message automation, automation table 303
debugging (continued)
  message routing 314
  processing time 313
  timer command automation 311
  Tivoli Enterprise Console event forwarding to
  NetView 309
defining consoles 170
defining operators, receive alerts 194
DELETE command
  issuing at the command line 257
DELETE filter option 197
delete method (RODM) 239
deleting held messages 39
deleting timers
  from Timer Management panels 275
destination flow control 92
detail panels, status monitor 102
DFILTER command 199
diagnosing problems
  abends 351
  broken session, repairing 334
  controller status, determining 325
diagnosing performance problems using
  TASKUTIL 320
diagnosing storage problems using TASKUTIL 320
  filter not working 199
  hung session 331
  hung session, repairing 331
  hung task, identifying 351
  hung task, terminating 351
  initiating error recovery using status monitor 322
  intermittent problems, identifying 324
  line failures 338
  looping task, identifying 351
  looping task, terminating 351
  measuring response time using TASKUTIL 320
  modern problems, identifying 344
  NetView trace data 210
  resource status, displaying 322
  response time, measuring using RTM 353
  session monitor database, checking status 329
  sluggish network performance, resolving using
  NPM 355
  virtual route blocked, determining 344
directing commands, NetView 40
DISCONID command 170
DISG command 66
DISPLAY ID command 64
DISPLAY ID VTAM command response panel 64
DISPLAY ROUTE command 344
displaying
  automation timer set panel 262
  Timer Management Panel 258
distributed database retrieval 150
distributed hosts 148
DOMAIN() function 282
domain status
  detail panel 107
  detail panel, activity/analysis option 105, 106
  detail panel, command lists 104
  detail panel, display/detail menu 345, 346
environment, NetView 179 (continued)
  PPI trace data 211
  session monitor trace data 210
defining 179
  alert receivers 193
  NetView command 179
  network resources 180
  new operators 188
  PF and PA keys 189
deleting 188
  alert receivers 194
  new operators 188
displaying 184
  command facility trace data 210
  focal point sphere of control 204
  NetView data sets 184
  NetView trace data 210
  network log 206
  PPI trace data 211
  primary backup focal point 204
  session monitor trace data 210
entering mixed case commands 191
formatting RODM log 216
maintaining 180
  MVS system log (SYSLOG) 215
  network log 206
  RODM objects 180
  RODM relationships 180
  refreshing focal point sphere of control 205
removing 204
  data from hardware monitor database 212
  entry point, sphere of control 204
  save/restore database data 215
  session monitor log data 214
reorganizing 213
  4700 support facility database 213
  save/restore database 215
repeating commands 190
setting alert error thresholds 206
starting or stopping NetView task 187
suppressing commands, NetView log 191
switching 211
  4700 support facility database 213
  hardware monitor databases 211
  RODM log 216
  save/restore database 215
  session monitor logs 214
  using GENALERT to generate alerts 205
  using network log 206
  using PPI to generate alerts 205
EQQNETW2 sample 301
error recovery (continued)
  hung task, identifying 351
  hung task, terminating 351
  initiating error recovery using status monitor 322
  intermittent problems, identifying 324
  line failures 338
  looping task, identifying 351
  looping task, terminating 351
  measuring response time using TASKUTIL 320
  modem problems, identifying 344
  NetView trace data 210
  resource status, displaying 322
  response time, measuring using RTM 353
  session monitor database, checking status 329
  sluggish network performance, resolving using NPM 355
  virtual route blocked, determining 344
error-to-traffic ratio 206
ESCON Manager 21
Event/Automation Service 15
event detail
  menu panel 139
  NSC/SS station panel 134
  panel 138
event detail panel 138
  event flow subsystem 11
  event flows 24
  event receiver component 14
  event services, GEM 31
  event services component 12
  events 24, 127
  Events 31
  EVERY command
    issuing at the command line 256
  EVERY timer
    adding
      from Timer Management panels 262, 263
  EXCMD correlated response 69
  EXECIO command 286
  exit
    DSIEX16B 298
    XITCI 297

F

failure-cause code points, intermittent problems 325
FASTService option 352
filter
  automating 224
  definition 194
  determining problem 199
  displaying 199
  option
    BLOCK 197
    CLEAR 198
    DELETE 197
    PASS 197
  recording 195
  resetting 198
  setting recording 197
  setting viewing 197
global variables (continued)
  saving 215
  SETCGLOB 293
  setting and retrieving 293
  storing 293
GLOVALB global variable 293
GMFALEnTS 127
GMFHS
  starting 30
  stopping 31
GMFHS component 10
GTF 210

H
hardware monitor
  abbreviations 382
  alert 194
  checking database status 329
  collecting solicited data 125
  collecting unsolicited data 125
  controller status, determining 325
  creating problem reports 368
  database 194
  deleting alert 194
  maintaining 211
  removing data 212
  displaying total events 140
  displaying total statistical data 141
  distributed database retrieval 150
  distributed hosts 148
  filter 194
  focal point domain 148
  forwarding alerts 149
  Information/Management link 367
  intermittent problems, identifying 324
  investigating NMVT alerts 135
  investigating non-NMVT alerts 131
  line failures 338
  Link Problem Determination Aid (LPDA) 143
  logical databases 211
  managing multiple domains 148
  modem problems, identifying 344
  overview 5
  owning domains 149
panel 131
  alerts-dynamic, creating a problem report 368
  alerts-dynamic, handling line failures 338
  alerts-dynamic, investigating NMVT alerts 136
  alerts-dynamic, investigating non-NMVT alerts 131
  alerts-history 349
  alerts-static, alert forwarding 149
  alerts-static, creating a problem report 369
  alerts-static, handling line failures 339
  alerts-static, investigating NMVT alerts 137
  alerts-static, investigating non-NMVT alerts 132
  controller (CTRL) selection menu 326
  controller information display 326
  current filter status 195
  D219 run DCE test 340
  D219 run line analysis test 341

G
  gateway NCP data 78
  GEM event services 31
  GENALERT command 205
  generic automation receiver function 125
  GETCONID command 170
  getting help 411
  global variables
    &CGLOBAL 293
    &TGLOBAL 293
    ATF('DSICGLOB') 293
    ATF('DSITGLOB') 293
    CNMVARS 293
    designing 293
    displaying current value 294
    DSIVARS 293
    GLOBALV 293
    QRYGLOBL 293
    restoring 215

filter (continued)
  strategy, implementing 195
  viewing 195
FIND command 206
finding information, AON/MSM 408
First Failure Support Technology (FFST)
  abends 351
  FASTService option 352
  flow control data panel 92, 93
  focal point
    changing 203, 204
    definition 203
    description 3
    displaying 204
    refreshing sphere of control 205
    relationship, entry point and service point 3
    removing entry point, sphere of control 204
  sphere of control 148, 204
  focal point domain 148
  FOCALPT ACQUIRE command 203, 204
  FOCALPT CHANGE command 203
  FOCALPT DELETE command 204
  FOCALPT DISPSOC command 204
  FOCALPT QUERY command 204
  FOCALPT REFRESH command 205
  format, time 264
  forwarding alerts
    methods 127
    overview 149
  full-screen session panel 44
  function keys, directing commands 41
  functions 40
    DOMAIN() 282
    MSGID() 282
    NMC 53
    OPID() 282
    REXX 281, 282
    ROLL 40
    SRF 298
    TASK() 282
hardware monitor (continued)
event detail 138
event detail, BSC/SS station 134
event detail menu 139
line analysis-link segment level 1 147, 343
link data, SNA controller 327
LPDA-2 command menu 144, 343
main menu, determining controller status 325
main menu, handling line failures 342
main menu, investigating NMVT alerts 136
main menu, investigating non-NMVT alerts 131
modem and line status (first) 145
modem and line status (second) 145
modem and line status (third) 146
most recent events 328
recommended action, selected event, handling line failures 340
recommended action for selected event, identifying modem problems 349
recommended action for selected event, investigating NMVT alerts 137
recommended action for selected event, investigating non-NMVT alerts 134
release level, SNA controller 328
test information display 143, 342
total events (first level) 140
total events (second level) 140
total statistical data (first level) 141
total statistical data (second level) 142
total statistical data (third level) 143
transmit receive test-link segment lvl 1 147
panel hierarchy 379
record type 127
alerts 127
events 127
GMFALERTs 127
resolutions 127
statistics 127
running modem and link tests 143
scenarios 131
displaying total events 140
displaying total statistical data 141
investigating network management vector transport alerts 135
investigating non-network management vector transport alert 131
running modem and link tests 143
secondary recording of event records 130
session domains 149
terminology in panels 381
using panels to monitor network 130
hardware monitor main menu panel
controller status, determining 325
investigating NMVT alerts 136
investigating non-NMVT alerts 131
line failures, handling 342
held messages 38
held-screen indicator, NetView panel 37
help 377
help, host 411
help, workstation 412
help panels, browsing 184
higher node 100
HPR 95
HPRC 95
I
I/O Operations 21
IBM LAN NetView Tie program
description 114
starting 114
stopping 114
IF-THEN automation table statement 226
IGCMGC10 200
IIF problem data panel 370
IMS Automation Feature
obtaining subsystem status information 118
overview 20, 245
panels 118
inquire subsystem components 118
main menu, obtaining detailed status 118
subsystem information 118
INACT status monitor state 100
Information/Management
overview 17
problem reporter entry panel 369
instrumentation 8
interested operator list panel 164
intermittent problems, failure-cause code points 325
interpreting session data 393
intervals, regular
setting CHRON timers
from Timer Management panels 268
investigating
proactive 319
reactive 331
investigating, definition 27
ISQCCMD command 165
ISQXDST command 159
ISQXIII command 165
issuing commands
determining problems 169
from command list 285
JES2 commands 170
JES3 commands, NetView 171
MVS system 169
NetView commands, MVS 31
setup 169
specific destinations 40
J
JES common global variables, saving 294
JES2, issuing commands 170
JES2 DU,ALL command 173
JES3 171
command response panel 171
issuing commands from NetView 171
K
KEEPDISC initialization statement 78
label, command prefix 69
LAN ADP command response panel 72
LAN command list, using 71
LAN Network Manager
  overview 18
  service point, communicating 71
LAN QNETWORK command response panel 72
LENGTH function 281
line, displaying status 66
line analysis-link segment level 1 panel 147, 343
link data, SNA controller panel 327
Link Problem Determination Aid (LPDA) 143
LIST command 209
LIST LU command 81
LIST TIMER
  timers that are waiting to process
    issuing at the command line 257
LISTCAT, active VSAM database 329
LISTCAT command 211, 329
listing PF and PA key settings 41
listing sessions 66
log
  BLOG 206
  MVS system 215
  network 206
  printing 206
  RODM 216
    formatting 216
    switching 216
    using and maintaining 216
  session monitor 214
    removing data 214
    switching 214
    suppressing commands 191
logging on, NetView 32, 43
logon panel, NetView 32
lower node 100
LPDA (Link Problem Determination Aid) 143
LPDA-2 command menu panel 144, 343
LU
  activating, using status monitor 324
  status, displaying 66
LU 6.2
  alert receiver support 193
  commands, configuring for Communications Manager 112
LU-LU session
  SNA APPN network scenarios 90
  subarea network scenarios 80

message (continued)
  held, deleting 39
  rearranging on screen 38
  replying 30
  routing
    controlling 249
    debugging 314
    using ASSIGN 249
    solicited 250
    unsolicited 249
    using windows 39
message adapter component 13
message area, NetView panel 37
messages
  codes 375
  filtering 22
  flows 24
  format 375
  wrapping 192
methods 239
methods, forwarding alerts 127
minor node 180
modem and line status panel
  first 145
  second 145
  third 146
modem problems, identifying 344
MODIFY command 300
MONIT 109
MONIT START command 322
MONIT status monitor state 100
MONIT STOP command 322
monitoring 26
  application program details and trends 61
  APPN resources 55, 63
  choosing process 63
  definition 26
  MVS resources using System Operations 57
  network status, Operations Planning and Control/ESA 121
  non-SNA resources 64
  SNA subarea resources 55
  subarea resources 63
  system workflow 59
  tasks 64
    active sessions, listing 66
    collecting NCP resource data 122
    collecting performance data 122
    communicating with LAN Network Manager service point 71
    displaying adapters on LAN segment 72
    displaying LAN configuration 71
    displaying LAN workstation characteristics 72
    displaying logical view of network 121
    displaying printer status 171
    displaying session and storage information 99
    listing LAN segments managed by service point 71
    listing RMTCMD autotasks 69

Index 421
monitoring 26 (continued)

obtaining CICS subsystem status information 116
obtaining IMS subsystem information 118
resource status, checking 64
resource status, listing 66
using NetView commands 66
using VTAM commands 64
monitoring network resources 63
MONOFF command 322
MONON command 322
most recent events panel 328
MPF (Message Processing Facility)
forwarding message to NetView 299
suppressing a system message 299
MSG command 284
MSGID() function 282
MSROUTE command 249
MSM, finding information 408
MSM agent component 13
MSU
automation 225
description 223
multidomain services LU 6.2 transport 111
multiple domains, managing 148
MultiSystem Manager
maintaining RODM 181
overview 6, 15
MVS (Multiple Virtual Storage) 31
@D 171
$DU,PRT15 command 171
$IPRT15 command 171
$PPRT15 command 171
command 170
D A,L command 169
error messages 169
issuing JES2 commands 170
issuing NetView commands 31
issuing system commands 169
issuing system console commands 169
Message Processing Facility (MPF)
command response display 172, 173
command response display for JES2 commands 173
system log, using 215
MVS command automation 169

N
named method (RODM) 239
NCP 363 (continued)
management network review panel (NPM) 362
management network start panel (NPM) 361
status, displaying 66
NetSP/SLC product 33
NetView
breaking link between RMTCMD and autotask 68
built-in functions 282
changing a RODM object attribute value 241
changing screen settings 42
command prefix 31
commands, issuing from MVS 31
default command designator 31
directing commands using function keys 41
environment 179
changing backup focal point from current focal point 203
changing backup focal point from entry point 204
changing primary focal point from entry point 203
changing primary focal point from new focal point 203
changing screen layout 192
checkpointing RODM 217
collecting hardware monitor data in SMF data set 212
collection session monitor data in SMF data set 214
defining NetView command 179
defining network resources 180
defining new operators 188
defining PF and PA keys 189
deleting alerts 194
deleting new operators 188
directing commands using function keys 41
entering mixed case commands 191
entering screen layout 202
formatting RODM log 216
maintaining MVS system log (SYSLOG) 215
maintaining network log 206
maintaining RODM objects 180
maintaining RODM relationships 180
prefixing commands with NETVASIS 191
refreshing focal point sphere of control 204
removing data from hardware monitor database 212
removing entry point, sphere of control 204
removing save/restore database data 215
NetView (continued)
removing session monitor log data 214
reorganizing 4700 support facility database 213
reorganizing save/restore database 215
repeating commands 190
setting alert error thresholds 206
starting or stopping NetView task 187
suppressing commands, NetView log 191
switching 4700 support facility database 213
switching hardware monitor databases 211
switching RODM log 216
switching save/restore database 215
switching session monitor logs 214
using GENALERT to generate alerts 205
using network log 206
using PPI to generate alerts 205
using the OVERRIDE command with NETVASIS 191
examining a RODM object attribute 182, 242
function 282
DOMAIN() 282
MSGID() 282
OPID() 282
TASK() 282
generic automation receiver function 125
host and workstation components 4
host environment MVS address spaces 29
how data arrives 22
invoking RODM method 240
issuing commands 40
from command list 285
MVS system 169
specific destinations 40
listing PF and PA key settings 41
logging on 32
logging on NetView 3270 management console 43
logon panel 32
main menu panel 35
message forwarding from MPF 299
modifying resource ceilings 175
news panel 34
operating system filters 22
operating system resources, controlling 169
operation, controlling 187
operation tasks 25
panel indicators 37
panels 34
alerts-dynamic, creating a problem report 368
alerts-dynamic, handling line failures 338
alerts-dynamic, investigating NMVT alerts 136
alerts-dynamic, investigating non-NMVT alerts 131
alerts-history 349
alerts-static, alert forwarding 149
alerts-static, creating a problem report 369
alerts-static, handling line failures 339
alerts-static, investigating NMVT alerts 137
alerts-static, investigating non-NMVT alerts 132
APPN session route configuration, typical SNA
APPN CP-CP session 90

NetView (continued)
panels 34 (continued)
APPN session route configuration, typical SNA
  APPN LU-LU session 94, 95
  browse network log 109
  command response display 172, 173
  command response display for JES2 commands 173
  controller (CTRL) selection menu 326
  controller information display 326
  current filter status 195
  D219 run DCE test 340
  D219 run line analysis test 341
domain status detail 107
domain status detail, activity/analysis option 105, 106
domain status detail, command lists 104
domain status detail, display/detail menu 345, 346
domain status detail, VTAM commands, displaying status of resource 323
domain status detail, VTAM commands, identifying modem problems 345, 347
domain status detail, VTAM commands, moving through panels 104
domain status summary 102
event detail 138
event detail, BSC/SS station 134
event detail menu 139
flow control data 92, 93
hardware monitor main menu, determining controller status 325
hardware monitor main menu, handling line failures 342
hardware monitor main menu, investigating NMVT alerts 136
hardware monitor main menu, investigating non-NMVT alerts 131
JES3 command response 171
LAN ADP command response 72
LAN QNETWORK command response 72
line analysis-link segment level 1 147, 343
link data, SNA controller 327
LISTCAT, active VSAM data base for BNJDSERV 329
LPDA-2 command menu 144, 343
modem and line status (first) 145
modem and line status (second) 145
modem and line status (third) 146
most recent events 328
password 34
recommended action, selected event, handling line failures 340
recommended action for selected event, identifying modem problems 349
recommended action for selected event, investigating NMVT alerts 137
recommended action for selected event, investigating non-NMVT alerts 134
release level, SNA controller 328
resource name list 81, 88

Index 423
NetView (continued)
response time summary 353
response time trend panel 354
RMTSESS command response 69
sense code description 348
session configuration data, repairing broken
session 334, 337
session configuration data, repairing hung
session 332
session configuration data, resolving sluggish
performance 356
session configuration data, typical SNA APPN
CP-CP session 89
session configuration data, typical SNA APPN
LU-LU session 91
session configuration data, typical SNA LU-LU
session 82
session list, repairing broken session 334, 336
session list, repairing hung session 331
session list, resolving sluggish performance 356
session list, typical SNA APPN LU-LU
session 90
session list, typical SNA LU-LU session 82
session list, typical takeover/giveback session 97
session monitor main menu 80, 87
session parameters 84
session trace data 83
SESSMDIS session monitor session and storage
information 99
specific ER configuration, repairing broken
session 335, 337
specific ER Configuration, typical SNA LU-LU
session 85
specific session trace data 333
status summary 322
TASKUTIL command response 351
test information display 143, 342
total events (first level) 140
total events (second level) 140
total statistical data (first level) 141
total statistical data (second level) 142
total statistical data (third level) 143
transmit receive test-link segment lvl 1 147
virtual route status 85, 86, 92
VTAM display : NCP 67
password panel 34
products that work with NetView 16
program, starting 29
rrearranging messages on screen 38
start procedure 32
starting 29
stopping program 30
stopping subsystem 31
structure, managing open networks 3
subsystem, starting 29
system resources, managing 169
task 187
tasks 25
vital product data, setting up 156
NetView 3270 management console 43
command facility 44
NetView 3270 management console (continued)
full-screen session 44
logging off 45
logging on 43
required environments 43
NetView AutoBridge/MVS
implementing 370
overview 18, 248, 369
NetView for AIX service point 114
NetView Graphic Monitor Facility host subsystem
starting 30
stopping 31
NetView instrumentation 9
NetView library, using 407
NetView Pipelines 293
NetView Web server 45
network accounting and availability measurement
data 79
Network Asset Management
overview 155
network inventory, managing 155
network log
displaying 206
maintaining 206
message format 375
printing 209
switching 209
network management vector transport alerts,
investigating 135
Network Security program 33
network status
monitoring 121
using NetView Performance Monitor 122
using NTune 122
using Operations Planning and Control/ESA 121
using Performance Reporter 121
using Systems Automation for OS/390 57
NEVACT status monitor state 100
NMC (NetView management console)
functional overview 53
how information is collected 53
working with Systems Automation for OS/390 57
NMVT automation 223
node
definition 180
status, displaying 66
non-network management vector transport alerts,
investigating 131
non-VTAM devices, collecting data 110
notify method (RODM) 239
Novell NetWare, overview 19
NPM (NetView Performance Monitor)
overview 18
panel 357
NCP management network review 362
NCP management network review data 363
NCP management network review data for NTRI
resources 364
NCP management network start 361
primary options 357
session management 357
problem determination (continued)
resource status, displaying 322
response time, measuring using RTM 353
session monitor database, checking status 329
sluggish network performance, resolving using NPM 355
virtual route blocked, determining 344
problem management data, controlling processing 205
problem reporter entry panel 369
problem reports, creating using hardware monitor 368
using NetView Autobridge 369
Processor Operations
AOC/MVS interface 60
controlling remote processors 159
initializing target system 165
ISQCCMD command 165
ISQXDST command 159
ISQXIII command 165
loading target system 165
overview 20, 243
panel 159
interested operator list 164
PS/2 detail 163
PS/2 port detail 163
target hardware summary 162
target resource 161
target system LPAR resource 161
target system summary 160
TSCF status summary 159
performing IPL, target system 165
sending commands, target system 60
shutting target system 166
using status panels 159
PS/2 detail panel 163
PS/2 port detail panel 163
pseudosession trace buffer 78
PU, displaying status 66
PURGE command
issuing at the command line 257
purging timers
from Timer Management panels 275

Q
QRYGLOBL command 295
QRYGLOBL global variable 293
query method (RODM) 239
QUEUED function 281

R
RATE statement 297
reactive investigating 331
rerearranging messages, NetView screen 38
RECFMS automation 223
RECMS automation 223
recommended action, selected event panel
investigating NMVT alerts 137
investigating non-NMVT alerts 134
line failures, handling 340
modern problems, identifying 349
RECORD command 214
record types
alerts 127
events 127
GMFALETs 127
resolutions 127
statistics 127
recording filter
definition 195
setting 223
REFRESH command 188
reinstalling timers
from Timer Management panels 277
RELCONID command 170
release level, SNA controller panel 328
releasing consoles 170
remote processors, controlling 159
Remote Target Selection panel 261
REPLY command 30
reply messages 38
replying, WTOR message 30
REPORTS command 212
resolutions 127
resource
attached through service points, controlling with automation table 116
ceilings, modifying using OPC/ESA 175
collecting NCP data using NTune 122
defining in network 180
displaying status, status monitor 322
inactivating using VTAM 65
lines, displaying status 66
LU, displaying status 66
monitoring
APPN 63
non-SNA 64
subarea 63
using service points 64
NCP 65
activating, remote NetView 68
activating and loading 65
inactivating 65
status, displaying 66
nodes, displaying status 66
PU, displaying status 66
reactivating using VTAM 65
remote, controlling 68
status, checking using VTAM 65
status, listing 66
types, OPC/ESA 174
utilization, controlling using OPC/ESA 174
resource name list panel 81, 88
response area, NetView panel 39
response flows 23
response time monitor (RTM) 77, 353
response time summary panel 353
response time trend panel 354
RESTORE command
issuing at the command line 258
RETRIEVE command 190
REXX
command lists, writing 279
functions 281
overview 281
reference 281, 282
SAY instruction 284
RMTSESS command 69
RMTSESS command response panel 69
RODM (Resource Object Data Manager)
checkpointing 217
cold start 29
definition 180
DSIQTSK task 240
EKGSPPPI method 240
examining an object attribute from NetView 182, 242
invoking method from NetView 240
log, formatting 216
log, using and maintaining 216
maintaining 180
objects 180
relationships 180
using load utility 181
using MultiSystem Manager 181
using RODMView 182
methods 239
object-independent method types 239
object-specific method types 239
overview 15, 239
panel 182
RODMView access and control panel 182
RODMView main menu 182
RODMView method actions 183
panel hierarchy 391
RODMView command 182
starting 29
stopping 31
triggering a method using RODMView 182
updating an object attribute 241
warm start 30
RODM component 10
RODM load utility 181
RODMGR component 11
RODMView
access and control panel 182
examining RODM object attribute value 182, 242
main menu panel 182
maintaining RODM 182
method actions panel 183
overview 15
triggering a RODM method 182
ROLL function 40
route data 79
routing messages
controlling 249
using ASSIGN 249
RUNCMD command 110

S
SAF (System Authorization Facility)
automation table 224

sample 37
CNMS0003 188
CNMSAMP 299
CNMSCNFT 37
DSICMD 287
DSICNM 102
EQQNETW2 301
save/restore database, maintaining 215
saving
TIMER
issuing at the command line 257
saving JES common global variables 294
SAW data 79, 210
SAY instruction 284
scenario
hardware monitor 131
displaying total events 140
displaying total statistical data 141
investigating network management vector
transport alerts 135
investigating non-network management vector
transport alert 131
running modem and link tests 143
session monitor, configuration 393
session between SNA APPN subnetworks using LEN connection 400
SNA APPN session through adjacent composite nodes 396
SNA APPN session through composite node 394
SNA APPN session through non-adjacent composite nodes 395
SNA APPN session through SNI gateway 399
SNA session 393
session monitor, using panels 80
CP-CP session, SNA APPN network 87
LU-LU session, SNA APPN network 90
LU-LU session, subarea network 80
takeover/giveback session 97
session monitor SSCP takeover/giveback, NCP BF connection 402, 406
scheduling
commands 255
scheduling command
debugging 311
using timer commands 255
screen
controlling contents 189
controlling format 189
customizing format 192
listing format 193
message wrapping 192
secondary recording of event records 130
security
automation table 224
selecting a target system
from Timer Management panels 262
selecting remote targets 260
sending
command to remote NetView (example) 283
sending instrumentation data 9
sense code description panel 348

Index 427
service point application, receiving command from REXX command list 115

service points 111
applications 110
description 3, 110
overview 17
relationship, entry point and focal point 3
transport type 111
multidomain services LU 6.2 transport 111
SSCP-PU transport 111
using automation table to control resources 116

SESS command 90
session activation parameters 78
session awareness data 79
session configuration data panel
broken session, repairing 334, 337
hung session, repairing 332
sluggish performance, resolving 356
typical SNA APPN CP-CP session 89
typical SNA APPN LU-LU session 91
typical SNA LU-LU session 82
session domains 149
session identification line, NetView panel 37
session list panel
broken session, repairing 334, 336
repairing hung session 331
sluggish performance, resolving 356
typical SNA APPN CP-CP session 89
typical SNA APPN LU-LU session 90
typical SNA LU-LU session 82
typical takeover/giveback session 97
session management LU detail analysis panel (NPM) 359
session management panel (NPM) 357
session management session analysis summary - logical unit panel (NPM) 360
session management session monitor selection panel (NPM) 359
session management start session panel (NPM) 358

session monitor 77 (continued)
interpreting session data 393
KEEPDISC initialization statement 78
log, removing data 214
main menu panel 80
NCP 78
boundary function trace data 78
gateway trace data 78
network accounting and availability measurement data 79
origin flow control 92
overview 5
pacing data 94
panel 80
APPN session route configuration, typical SNA APPN CP-CP session 90
APPN session route configuration, typical SNA APPN LU-LU session 94, 95
flow control data 92, 93
main menu 80
resource name list 81, 88
response time summary 353
response time trend panel 354
sense code description 348
session configuration data, repairing broken session 334, 337
session configuration data, repairing hung session 332
session configuration data, resolving sluggish performance 356
session configuration data, typical SNA APPN CP-CP session 89
session configuration data, typical SNA APPN LU-LU session 91
session configuration data, typical SNA LU-LU session 82
session list, repairing broken session 334, 336
session list, repairing hung session 331
session list, resolving sluggish performance 356
session list, SNA APPN CP-CP session 89
session list, typical SNA APPN LU-LU session 90
session list, typical SNA LU-LU session 82
session list, typical takeover/giveback session 97
session monitor main menu 87
session parameters 84
session trace data 83
SESSMDIS session monitor session and storage information 99
specific ER configuration, repairing broken session 335, 337
specific ER configuration, typical SNA LU-LU session 85
specific session trace data 333
virtual route status 85, 86, 92
panel hierarchy 385
PIU data 78
components 78
recording 210
primary session trace data, displaying 83
pseudosession trace buffer 78
session monitor 77 (continued)
response time, measuring using RTM 353
route data 79
SAW data, recording 210
scenarios 80
    CP-CP session, SNA APPN network 87
    LU-LU session, SNA APPN network 90
    LU-LU session, subarea network 80
    takeover/giveback session 97
secondary session trace data, displaying 83
session activation parameters 78
session awareness data 79
session awareness data, types 79
session response time data 77
session trace data 78
setting session awareness data filters, VTAM 199
setting session awareness filters 200
setup 80
switching logs 214
    takeover/giveback notifications 98
    takeover/giveback scenarios 402
trace processing of discarded PIUs 78
transmission groups 79
virtual route 86
session parameters panel 84
session response time data 77
session trace data 78
session trace data panel 83
sessions
    activation status 80
    listing 66
    partner types 79
SESSMDIS
    command 99
    session monitor session and storage information panel 99
SET command 189
SETCGLQBL global variable 293
setting CHRON timers
    from Timer Management panels 268
setting timers for a specific date and time
    from Timer Management panels 262, 263, 265
setting timers for after a specific date and time
    from Timer Management panels 266
settings
timers
    at Timer Management panels 258
setup
    TIMER commands 255
SMF data set 214
SNA Manager/6000
    comparison with NMC 54
    overview 19
SNA topology manager
    maintaining RODM 181
    overview 56
SNATM component 11
solicited data 125
solicited message flows 24
solving, definition 27
special resources, OPC/ESA 175
specific ER configuration panel
    broken session, repairing 335, 337
    typical SNA LU-LU session 85
specific session trace data panel 333
sphere of control 148, 203
SRATIO command 206
SRFILTER command 150, 195, 298
SSCP-PU transport 111
START command 187
starting
    automatic node reactivation, session monitor 41
    GMFHS 30
NetView 29
    NetView program 29
    NetView subsystem 29
    NetView task 187
    RODM 29
starting event services 31
statistic flows 24
statistics 127
status
    converting to message for automation 223
status monitor
    activating a resource 324
    description 99
    directing commands 41
    higher node 100
    initiating error recovery 322
    lower node 100
    modem problems, identifying 344
    overview 5
panel 102
    browse network log 109
    domain status detail 107
    domain status detail, activity/analysis option 105, 106
    domain status detail, command lists 104
    domain status detail, display/detail menu 345, 346
    domain status detail, VTAM commands, displaying status of resource 323
    domain status detail, VTAM commands, identifying modem problems 345, 347
    domain status detail, VTAM commands, moving through panels 104
    domain status summary 102
    status summary 322
panel hierarchy 389
panel types 102
resource hierarchy 100
resource states 100
    corresponding VTAM states 101
    types 100
    resource status, displaying 322
    setup 101
    using the panels 102
STOP command 187
stopping
    GMFHS 31
NetView address spaces 30

Index 429
stopping (continued)
  NetView program 30
  NetView subsystem 31
  NetView task 187
  RODM 31
stopping event services 31
SUBSTR function 281
summary panels, status monitor 102
SUPPCHAR keyword 192
suppressing system messages 298
suppression character 191
SVFILTER command 150, 195
SWITCH command 209
SWRAP command 212
SYN automation table statement 226
system console commands, issuing 169
system messages, suppressing
  using Message Processing Facility (MPF) 299
  using MODIFY VTAM command 300
system trend window 60
Systems Automation for OS/390 57
T
  takeover/giveback notifications 98
takeover/giveback session, scenario 97
target hardware summary panel 162
target resource panel 161
target system LPAR resource panel 161
target system summary panel 160
  TASK() function 282
task scheduling
  debugging 311
  using timer commands 255
tasks
  NetView supplied 187
  priority 187
  starting and stopping 187
  TASKUTIL command 320, 351
  TASKUTIL command response panel 351
TCP/IP
  overview 17
test information display panel 143, 342
time, specifying intervals 264
  TIME function 281
timed commands 255
timed events 215
  TIMER 255
timer command
  debugging 311
deleting
    issuing at the command line 257
displaying 257
    restoring
      issuing at the command line 258
      setup 255
typing at the command line 258
  TIMER command
  saving
    issuing at the command line 257
  Timer Management panels
    active timer panel after a purge 276
    CHRON EVERY panel 272
    CHRON EVERY Timer Display Results panel 1 274
    CHRON EVERY Timer Display Results panel 2 274
    CHRON EVERY Timer Display Results panel 3 275
    CHRON EVERY Timer Display Results panel 4 275
    CHRON EVERY Timer Preview panel 273
    CHRON Notify panel 270
    CHRON Options panel 271
deleting timers 275
example of a purged (or deleted) timer panel 277
example of purging a timer 276
purging timers 275
reinstating 277
Remote Target Selection panel 261
selecting a target system 262
selecting remote targets 260
setting CHRON timers 268
setting timers for a specific date and time 262, 263, 265
setting timers for after a specific date and time 266
  Timer Interval panel 272
using to issue TIMER commands 258
timers
  AFTER 266
  AT 265
  CHRON 268
using to issue TIMER commands 258
  management panel 258
  setting 258
Timers
  deleting 275
  purging 275
  reinstating 277
Tivoli Enterprise Console (TEC) 9
Tivoli NetView for OS/390 3
TME 10 NetView
  automating with NetView Service Point 248
  overview 22
token ring devices, collecting data 110
topology display subsystem 9
total events (first level) panel 140
total events (second level) panel 140
total statistical data (first level) panel 141
total statistical data (second level) panel 142
total statistical data (third level) panel 143
trace
  command facility 210
  PPI 211
  session monitor 210
TRACE command 210
trace data, creating and displaying 210
TRACE REXX instruction 287
transfer TSCF window 60
transmission groups 79
transmit receive test-link segment level 1 panel 147
triggering 175
TSCF status summary panel 159
TSO
  overview 17

UNIX
  overview 17
unsolicited data 125
unsolicited message 24
unsolicited message flows 24
usage report data set 184
using, NetView library 407
using System Operations for OS/390, overview 244

VIEW command processor 284
viewing filter 195
virtual route
  blocked, determining 344
  definition 86
virtual route status panel 85, 86, 92
vital product data 155
  collecting 155
  setting up 156
  VPDALL command 155
  VPDCMD command 155
  writing to external log 155
Vital Product Data
  overview 155
  VPDALL command 155
  VPDCMD command 155
VTAM (Virtual Telecommunications Access Method)
  activating, loading NCP 65
  command 64
    DISPLAY ID 64
    DISPLAY ROUTE 344
  filter table 199
  inactivating NCP 65
  inactivating resources 65
  overview 22
  panel 64
    DISPLAY ID command response 64
    VTAM display : NCP 67
PIU data 78
reactivating resources 65
resource status, checking 64
setting session awareness data filters 199
status, corresponding status monitor states 101
using commands, control network configuration 64
virtual route blocked, determining 344
VTAM display : NCP panel 67
VTAM display : physical unit panel 66
VTAMLST 180

wait indicator, NetView panel 37
warm starting RODM 30
warning, autowrap 39
Web server 45

INDEX

WINDOW command 39
WORD function 281
WORDINDEX function 281
WORDLENGTH function 281
WORDPOS function 281
WORDS function 281
workstation information, help 412
workstation resources, OPC/ESA 175
writing REXX command list 279
WTO command 284
WTOR command 285
WTOR message
  replying 30
  valid command replies 30

X2C function 281
X2D function 281
XITCI exit 297